ГЛОБАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОСТИ: ПОИСКИ И ПУТИ РЕШЕНИЯ

Материалы общественного онлайн-обсуждения
«Threats to international peace and security caused by terrorist acts (Угрозы международной безопасности, вызванные терроризмом)», 27 октября 2022 г. и круглого стола со всероссийским участием «The Right to Privacy in the Digital Age (Право на неприкосновенность частной жизни в век цифровизации)», 29 ноября 2022 г.

Комсомольск-на-Амуре
2022

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

ГЛОБАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОСТИ: ПОИСКИ И ПУТИ РЕШЕНИЯ

Материалы общественного онлайн-обсуждения
«Threats to international peace and security caused by terrorist acts (Угрозы международной безопасности, вызванные терроризмом)», 27 октября 2022 г. и круглого стола со всероссийским участием «The Right to Privacy in the Digital Age (Право на неприкосновенность частной жизни в век цифровизации)», 29 ноября 2022 г.

Комсомольск-на-Амуре
2022

УДК 3:001.12
ББК 95.4
Г547

Глобальные проблемы современности: поиски и пути решения :
Г547 материалы общественного онлайн-обсуждения и круглого стола, Комсомольск-на-Амуре, 27 октября-29 ноября 2022 г. / редкол. : Г. А. Шушарина (отв. ред.), О. И. Лопатина. – Комсомольск-на-Амуре : ФГБОУ ВО «КнАГУ», 2022. – 272 с.

ISBN 978-5-7765-1532-3

Материалы сборника посвящены изучению угроз международной безопасности, вызванных терроризмом, кибербезопасности, соблюдению прав людей на частную жизнь, краже личной информации и ее предотвращению, а также влиянию цифровизации на современное общество.

Приводимые материалы могут быть полезны преподавателям вузов, руководителям предприятий, а также студентам и аспирантам.

Конференция проведена в рамках гранта в форме субсидий из федерального бюджета образовательным организациям высшего образования на реализацию мероприятий, направленных на поддержку студенческих научных сообществ.

УДК 3:001.12
ББК 95.4

ISBN 978-5-7765-1532-3

РАЗДЕЛ 1
THREAT TO INTERNATIONAL PEACE AND SECURITY CAUSED BY TERRORIST ACTS
УГРОЗЫ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ, ВЫЗВАННЫЕ ТЕРРОРИЗМОМ

УДК 323

Актанко Максим Александрович, студент, Комсомольский-на-Амуре государственный университет
Aktanko Maxim Alexandrovich, student of Komsomolsk-na-Amure State University
Мусалитина Евгения Александровна, кандидат культурологии, доцент кафедры «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Musalitina Evgenia Aleksandrovna, PhD in Culture Studies, Assistant Professor, «Linguistics and Cross-Culture Communication Department», Komsomolsk-na-Amure State University

РЕЛИГИОЗНЫЕ АСПЕКТЫ ТЕРРОРИЗМА

RELIGIOUS ASPECTS OF TERRORISM

Аннотация. Начиная со второй половины XX в. все чаще можно встретить упоминание в мировых СМИ о «религиозном терроризме» и «исламском терроризме». В силу этого возникает необходимость выявления причин религиозных предпосылок возникновения терроризма. В статье рассматриваются виды религиозного терроризма, а также причины его возникновения.
Abstract. Starting from the second half of the XX century references to "religious terrorism" and "Islamic terrorism" in the world media can be found more often. Because of this, it becomes necessary to identify the causes of religious preconditions for the emergence of terrorism. The article discusses the types of religious terrorism, as well as the causes of its occurrence.
Ключевые слова: ислам, религия, религиозный терроризм, идеология.
Key words: Islam, religion, religious terrorism, ideology.

Начиная со второй половины XX в. все чаще можно встретить упоминание в мировых СМИ о «религиозном терроризме» и «исламском терроризме». В силу этого возникает необходимость выявления причин религиозных предпосылок возникновения терроризма. Обращаясь к истории, можно отметить, что между этими двумя понятиями нет прямой связи. Однако, в современном обществе ислам нередко ассоциируется с преступлениями, направленными против человечества.

Обратимся к рассмотрению видов международного терроризма, имеющего религиозную окраску. Исследователи выделяют три категории:

1) терроризм в сочетании с национальным сепаратизмом;
2) религиозный экстремизм;
3) культовый терроризм.

Все эти три вида объединены первопричиной, а, именно, конфликтом политических и экономических интересов [3].

В настоящее время существует множество организаций и направлений современного терроризма, осуществляемого на основе религии или диктуемого фанатичным религиозным подтекстом. Эти причины объясняют появление таких понятий как «религиозный терроризм» и «исламский терроризм».

Из-за более активной террористической деятельности в исламском мире, а также из-за того, что Запад рассматривает исламскую цивилизацию как угрозу, в обществе формируется негативное понимание ислама, которое приобретает массовый характер.

Американский исследователь Д. Эспозито указывал, что из-за длительного существования этой тенденции «в результате ислам и исламское возрождение были сведены к архетипам антизападного ислама, войны ислама против современности или мусульманского гнева, экстремизма, фанатизма и терроризма» [1]. Исследователь отмечает, необходимо анализировать взаимосвязь религии и политики, религии и нации, деятельность сектантов и религию в соответствии с природой религии и ее социальной функцией.

Исторически терроризм не имеет связи с религией. В древности и средневековье религия находилась в положении возвращения к культу, от образования к закону, от земледельцев и пастухов к ученым и чиновникам. Наряду с этим, вся жизнь средневекового общества, действия и мышление людей хотя и бессознательно, но были основаны на религии. Поэтому политическая, военная и экономическая деятельность такого общества в той или иной степени будет религиозной.

На протяжении всей истории общество сталкивалось с религиозными войнами и преследованиями. Но, навряд ли эти явления можно назвать терроризмом. Однако, в истории зафиксировано несколько фактов агрессии, которые могут быть отнесены к террористическим действиям. Среди них деятельность группировки наджитов, исламской секты, совершившей массовые убийства [5].

Анализ мотивов преступлений этой секты позволяет сделать вывод о том, что террористическая деятельность религиозных сект проявляется в ожесточенных межэтнических и региональных конфликтах; в политической борьбе; управляется фанатичными лидерами, придерживающимися радикальных взглядов.

Религия представляет собой сложное социальное, историческое и культурное явление. Ее социальные функции также разнообразны, но важнейшая из них заключается в создании групп через распространение общих убеждений, религиозных чувств и формирование самосознания. Это так называемая функция социальной интеграции и контроля.

Для закрепления своей власти правящие классы сменявших друг друга династий опирались, с одной стороны, на диктатуру государственной власти, а с другой стороны, прибегали к духовной власти. Религия, как особая духовная сила, обладает характеристиками, общими с политикой и правом, и может служить инструментом эффективного управления массами. Всеобъемлющее влияние религии позволяет ей проникать в разные сферы, интегрировать разные слои, прикрывать светские цели сакральным ореолом. Правители, осознающие социальную функцию религии, стараются сделать ее духовной опорой для укрепления правящего порядка

Необходимо отметить, что практически все основные мировые религии были возведены в ранг институциональных или государственных религий, что доказывает идею о поддержании религией господствующего порядка. Поэтому, в целом, функцию религии можно определить как трансляцию культурных традиций, урегулирование социальных конфликтов, поддержание существующего общественного порядка.

Возникновение терроризма в настоящее время имеет не только социальную причину, но и для его роста, но и подходящую для его развития соответствующие внешние условия. Среди них можно выделить этнические и региональные конфликты, которые привели к эскалации насильственных действий и активизации терроризма. Так, существует множество этнических и региональных конфликтов, которые являются следствием колониализма и империализма. Кроме того, вмешательство крупных держав по-

творствует одной стороне, нападая на другую сторону, что обостряет противоречия и провоцирует широкомасштабные вооруженные конфликты, вызывает усиление конфронтации.

Вышерассмотренные проблемы тесно взаимосвязаны и являются предпосылками для формирования терроризма. Ситуация усугубляется борьбой за политическую власть и материальные интересы. Когда противоречие обостряется, существовавшие ранее этнические и религиозные антагонизмы могут сделать конфликт весьма серьезным. Наряду с этим, религиозный экстремизм и этнический сепаратизм могут направить людей на путь терроризма.

Современный международный терроризм очень сложен и имеет свои проявления от крайне левых до крайне правых. Для удобства анализа террористическую деятельность, связанную с религиозными конфликтами или религиозным экстремизмом, условно можно разделить на три категории: первая – терроризм в сочетании с этническим сепаратизмом, вторая – терроризм на основе религиозного экстремизма, третья – терроризм религиозных культов.

Среди террористической деятельности, сочетающейся с национальным сепаратизмом, наиболее древней и типичной является террористическая деятельность в Северной Ирландии, где исторической предпосылкой стали национальные противоречия между британскими иммигрантами и ирландцами. В наше время здесь действует крупная экстремистская организация «Временная фракция ИРА», выступающая за «использование оружия и бомб» для достижения своих целей [1].

Другим примером террористического движения, основанного на религиозных убеждениях, может послужить этнический конфликт в Шри-Ланке. Обострение политических конфликтов между сингальцами, исповедующими буддизм, и тамильцами, исповедующими индуизм, привело к возникновению тамильской национальной экстремистской организации «Тигры освобождения Тамил-Илама», которая с 1975 года осуществляет террористическую деятельность, стремясь к установлению независимости.

Чеченская война также является примером этнического сепаратистского конфликта. Здесь ошибки в этнической и религиозной политике, исторические вопросы, несбалансированное экономическое и культурное развитие, социальное неравенство, политическая нестабильность стали источником этноконфессионального конфликта.

В настоящее время страны бывшего Советского Союза, Центральная и Восточная Европа, Ближний Восток, Южно-Азиатский субконтинент, Юго-Восточная Азия и Африканский континент являются очагами этнических и религиозных конфликтов, обусловленных вышеуказанными внутренними и внешними причинами.

Второй тип религиозного терроризма – это террористическая деятельность, в которой преобладает религиозный экстремизм. Согласно распространенному в последнее время мнению, исламский экстремизм стал синонимом терроризма. Однако терроризм не является продуктом самого ислама. Вопреки распространенному мнению, рост терроризма затронул не только ислам, но и развился внутри иудаизма и христианства [4].

Исламское возрождение и фундаментализм стали социальной мыслью и движением, охватившим исламский мир, как ответ на исторические проблемы. Исламское возрождение – это трансформация исламского учения в современных условиях и переосмысление его политических и социальных положений. Когда оно используется для организации масс возникает тенденция к религиозной политизации. Исламский экстремизм является деформированным продуктом этой социальной атмосферы. Исламские экстремисты, занимающиеся террористической деятельностью, представляют собой радикальные группировки, отличные от политической оппозиции. Их практика имеет

ярко выраженный религиозный оттенок, но они далеки от самого ислама, что ведет к неправильному толкованию ислама.

Необходимо отметить, что основные учения и принципы ислама требуют от мусульман вести себя с добротой, противостоять насилию и запрещать причинение вреда невинным гражданам. Те, кто занимается террористической деятельностью во имя Ислама, не могут найти основания в Коране [2]. Терроризм во имя религии крайне обманчив и, на самом деле, он идет вразрез с официальным курсом государства и подрывает интересы народа.

В случае разрешения острых социально-политических противоречий и экономических интересов масс террористическая деятельность экстремистов потеряет поддержку населения, как это произошло, например, в Алжире. Следует также отметить, что экстремисты совершают различные преступления во имя религии. Однако, на самом деле, их цель – политика, а не религия. Можно сказать, что, используя религию и искажая ее, они уничтожают религию. Хотя экстремизм и терроризм во имя ислама тесно связаны, необходимо отличать ислам и религиозные круги как религию от учений и террористических организаций, неверно истолковываемых экстремизмом.

В заключении необходимо отметить, что движение исламского возрождения не тождественно исламу, а исламский экстремизм не тождествен исламскому возрождению, поскольку небольшой процент людей стремится заниматься террористической деятельностью. Террористическая деятельность, спланированная исламскими экстремистами, является радикальной политической акцией, не имеющей ничего общего с религией. Однако форма ее реализации дает основание полагать, что она имеет мощный религиозный подтекст. Несмотря на усиление международной борьбы с религиозным терроризмом, проблема имеет серьезную идеологическую основу и не может быть решена в ближайшем будущем. Ее решение требует масштабной работы в области религиозного просвещения не только в исламском мире, но и в западном обществе.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Исаев А. В. Международный религиозный экстремизм и терроризм в условиях конфликтогенности мировой политики / А. В. Исаев, В. А. Матвиенко // Вестник ОрелГИЭТ. 2020. № 4(54). С. 142-147. – DOI 10.36683/2076-5347-2020-4-54-142-147.

2. Мухаммад А. Политический терроризм как результат религиозно-этнического экстремизма / А. Мухаммад // Евразийский юридический журнал. 2021. № 7(158). С. 444-447.

3. Расулова М. А. Терроризм - явление социальное, а не религиозное / М. А. Расулова // European Science. 2019. № 1(43). С. 35-38.

4. Rakhmetulina B. S. Terrorism and religious extremism in modern Kazakhstan / B. S. Rakhmetulina, Zh. A. Alimbetova // Региональное и муниципальное управление: вопросы политики, экономики и права. – 2021. – Vol. 8. – No 4(26). – P. 207-212. – DOI 10.35775/PSI.2021.26.4.004.

5. Юсупова Г. И. Религиозный терроризм: новые глобальные и региональные вызовы / Г. И. Юсупова, К. М. Магомедалиева // Власть. 2021. Т. 29. № 6. – С. 65-70. – DOI 10.31171/vlast.v29i6.8684.

УДК 1234.56

Беляева Ксения Александровна, студентка, Комсомольский-на-Амуре государственный университет
Belyaeva Kseniya Aleksandrovna, student of Komsomolsk-na-Amure State University
Орлова Элеонора Валерьевна, студентка, Комсомольский-на-Амуре государственный университет
Orlova Eleonora Valerevna, student of Komsomolsk-na-Amure State University
Когай Сергей Геннадьевич, старший преподаватель, Комсомольский-на-Амуре государственный университет
Kogai Sergei Gennadevich, senior lecturer, Komsomolsk-na-Amure State University

ШАНХАЙСКАЯ ОРГАНИЗАЦИЯ СОТРУДНИЧЕСТВА И БЕЗОПАСНОСТЬ КИТАЯ

SHANGHAI COOPERATION ORGANIZATION AND CHINA SECURITY

Аннотация. В данной статье рассматривается работа Шанхайской Организации Сотрудничества (ШОС). Одна из основных направленностей ШОС- обеспечение безопасности стран, входящих в данную организацию. Цель статьи – показать вклад данной организации в борьбу с международным терроризмом. В работе описаны основные меры, которые были приняты ШОС для безопасности Китая и мира в целом.
Abstract. This article discusses the work of the Shanghai Cooperation Organization (SCO). One of the main directions of the SCO is to ensure the security of the countries that are members of the organization. The purpose of the article is to show the contribution of this organization to the fight against international terrorism. The paper describes the main measures that were taken by the SCO for the security of China and the world as a whole.
Ключевые слова: шанхайская организация сотрудничества, борьба с терроризмом, мировая угроза.
Key words: shanghai cooperation organization, fight against terrorism, global threat.

Наш мир стремительно развивается, и этот процесс идет рука об руку с увеличением угроз, представляющих опасность для всего человечества. В последние десять лет наиболее болезненной и актуальной стала проблема терроризма. С развитием информационных технологий подготовка и организация террористического акта стали намного проще, а их опасность возросла в несколько раз. Перед государствами больше не стоял вопрос объединения для качественной борьбы с данным явлением, это стало необходимостью. Были созданы международные и региональные структуры для ликвидации терроризма.

Благоприятные условия развитию экстремизма и сепаратизма были сложены во время обострения ситуации в регионах Азиатско-Тихоокеанском и Средней Азии, в условиях правового нигилизма и острых межнациональных противоречий. Это и стало предлогом создания Шанхайской организации сотрудничества (ШОС).

В настоящее время Шанхайская организация сотрудничества является действующей. Она одна из самых крупных и стремительно развивающихся международных объединений.

Создание организации на протяжении нескольких лет обсуждалось лидерами Китая, России, Таджикистана, Киргизии, Казахстана и Узбекистана. В 14 июля 2001 году было подписано соглашение об основании Шанхайской организации сотрудничества (ШОС). Их первоначальной задачей была стабилизация обстановки в Центральной Азии, а также укрепление дружественных отношений между участниками объедине-

ния, развитие сотрудничества во всех сферах жизни стран. Основной целью ШОС является борьба с террористическими организациями, сепаратизмом и деяниями экстремистов в государствах.

Состоялось принятие Шанхайской конвенции в 2001 г., она определила обязательные элементы терроризма, сепаратизма и экстремизма. Среди них выявили насильственные действия, преследуемые в соответствии с принятым законодательством стран, организацию и планирование такого действия, пособничество и подстрекательство его совершению.

Помимо этого, произошло принятие РАТС (соглашения о региональной антитеррористической структуре). РАТС было подписано со многими целями. Во-первых, выполнение плана и собрание совета для коллективной деятельности по противостоянию терроризму, а также исполнение плана и обсуждение скорого развития совместной деятельности стран в этой борьбе, поддержка и взаимопомощь сторон в борьбе с терроризмом. Во-вторых, подготовка информации от стран, являющихся участниками объединения, по вопросам искоренения терроризма и формирование массива данных о действующих террористических организациях, её анализ, проведение учений, направленных на быстрое реагирование в случае террористического акта, и, также стимулирование сборов для реализации мероприятий по антитеррористической борьбе.

РАТС ШОС активно пополняет актуальной информацией свои базы данных. Такие документы как «Списки лиц, объявленных спецслужбами и правоохранительными органами членов ШОС в международный розыск за совершение или по подозрению в совершении преступлений террористического, сепаратистского и экстремистского характера» и «Единый розыскной реестр органов безопасности и специальных служб членов ШОС» помогают идентифицировать и выяснить местоположения людей, участвующих в подготовке или организации актов терроризма на территориях стран-членов ШОС. Предотвращение огромного количества трагедий и задержание преступников во многом заслуга РАТС.

В последние несколько лет одной из самых серьезных и широко обсуждаемых тем стало использование террористическими объединениями IT- технологий в своей деятельности. Впоследствии, в 2009 году государствами-участниками было принято решение о подписании межнационального соглашения о содействии в области информационной безопасности, в котором борьба с кибертерроризмом рассматривается в качестве приоритета.

Большое внимание также уделяется подготовке сотрудников военных служб и правоохранительных органов стран-участниц Шанхайской организации сотрудничества.

При проведении учений Китай показал высочайший уровень квалификационной подготовки руководящих структур и персонала спецслужб немедленного реагирования, правоохранительных органов стран при проведении широкомасштабных спецопераций для соответствия обстановке крупномасштабных беспорядков и связанных с ними террористических актов.

В интересах противостояния трансграничной преступности, которая является обязательно присутствующей частью терроризма и экстремизма, усовершенствован механизм взаимодействия министерств внутренних дел и правоохранительных органов участников ШОС по поддержанию общественной безопасности. Сформулирован и подписан договор о взаимопомощи в противостоянии преступности, создана центральная база данных, в которой анализируются сведения о незаконной международной торговой деятельности граждан и юридических лиц в странах, входящих в состав Шанхайской организации сотрудничества.

Несмотря на все приложенные усилия в сопротивлении расширяющейся угрозе терроризма, Организация на данный момент не может с однозначным успехом противодействовать вызовам со стороны экстремистских группировок. На сей день главные проблемы ШОС нельзя назвать решенными. К сожалению, ШОС не показала ожидаемую от принятых мер эффективность. К этому добавляется крайне низкая способность

к согласованным действиям, отсутствие возможности к мгновенному реагированию, небезупречное исполнение соглашений о всестороннем экономическом сотрудничестве. На данный момент правительство Китая старается повысить качество слабых сторон и увеличить эффективность данной Организации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ШОС: история создания и особенности организации / Новости – наше все | РЕН ТВ. URL: https://ren.tv/longread/987748-shos-istoriia-sozdaniia-i-osobennosti-deiatelnosti-organizatsii (дата обращения 6.10.2022). – Режим доступа: свободный.

2. 15 лет ШОС: история и развитие Шанхайской организации сотрудничества / Новости в мире и России – ТАСС. URL: https://tass.ru/mezhdunarodnayapanorama/3355240?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&um_referrer=yandex.ru (дата обращения 6.10.2022). – Режим доступа: свободный.

3. Концепция сотрудничества государств – членов Шанхайской организации сотрудничества в борьбе с терроризмом, сепаратизмом и экстремизмом / Президент России. URL: http://www.kremlin.ru/supplement/3667 (дата обращения 13.10.2022). – Режим доступа: свободный.

4. Антитеррористические учения Шанхайской организации сотрудничества / Журнал международная жизнь. URL: https://interaffairs.ru/jauthor/material/2085 (дата обращения 15.10.2022). – Режим доступа: свободный.

5. В ШОС выступили за усиление борьбы с терроризмом при центральной роли ООН / РИА Новости – события в Москве, России и мире. URL: https://ria.ru/20220303/terrorizm-1776181251.html (дата обращения 15.10.2022). – Режим доступа: свободный.

6. Петрунина Ж.В. Стратегия «Один пояс - Один путь» как катализатор изучения иностранных языков в Китае // В сборнике: Россия и Китай: история и перспективы сотрудничества. Материалы XI международной научно-практической конференции. Отв. редактор А.В. Друзяка. Благовещенск, 2021. С. 513-516.

УДК 621.9:519.8

Богатырев Денис Львович, студент, Комсомольский-на-Амуре государственный университет;
Bogatyrev Denis Lvovich, student of Komsomolsk-na-Amure State University
Ющук Екатерина Сергеевна, студентка, Комсомольский-на-Амуре государственный университет;
Yushuk Ekaterina Sergeevna, student of Komsomolsk-na-Amure State University
Когай Сергей Геннадьевич, старший преподаватель, Комсомольский-на-Амуре государственный университет
Kogai Sergei Gennadevich, senior lecturer, Komsomolsk-na-Amure State University

ОСОБЕННОСТИ ПОЛИТИКИ КИБЕРБЕЗОПАСНОСТИ В КИТАЙСКОЙ НАРОДНОЙ РЕСПУБЛИКЕ

THE SPECIFICS OF PEOPLE'S REPUBLIC OF CHINA’S CYBERSECURITY POLICY

Аннотация. Данная работа посвящена исследованию политики кибербезопасности, предпосылок возникновения и развития мер по ее обеспечению в Китайской Народной Республике, а также анализу применения средств информационного контроля в различных сферах деятельности на основании экспертных оценок, опубликованных в средствах массовой информации.

Abstract. This work is devoted to the study of cybersecurity policy of the People's Republic of China, preconditions and development of its enforcement measures, as well as analysis of information control tools implementations in various fields of activity based on expert assessments published in mass media.
Ключевые слова: цензура, социальные сети, Китай, кибербезопасность.
Key words: censorship, social networks, China, cybersecurity.

В XXI веке глобализация и изменения в геополитической ситуации сделали противодействие террористической угрозе одним из важнейших ориентиров международной политики стран. Китай не является исключением, деятельность на его территории таких террористических групп, как «Исламское движение Восточного Туркестана», «Информационный центр Восточного Туркестана» и др., требует от китайского правительства действий по обеспечению мировой и региональной безопасности.

Значительное внимание уделяется кибербезопасности. Начиная с 2003 года, по всему Китаю действует так называемый «Золотой Щит» - система фильтрации содержимого интернета. Эта система ограничивает доступ не только к сайтам, находящимся в черном списке, но и к сайтам, содержимое которых включает «запрещенные» ключевые слова. Запросы через крупные поисковые системы также фильтруются.

В связи с наличием системы «Золотой Щит», а также официальным запретом на использование виртуальных частных сетей (VPN), в Китае сформировался собственный набор сервисов и приложений, независимых от зарубежных компаний. Эти сервисы в значительной степени интегрированы в повседневную жизнь населения КНР. Например, приложение WeChat, аналог WhatsApp, выполняет не только функции мессенджера, но и платежной системы (статистика по использованию). У WeChat более чем 1.17 миллиарда пользователей, а платежными функциями приложения пользуются более 900 миллионов человек. Также под пристальным вниманием китайского руководства находятся социальные сети. Douyin, прямой аналог TikTok в Китае, пользуется огромным спросом у китайской аудитории (600 млн. пользователей). TikTok и Douyin являются интеллектуальной собственностью частной многонациональной компании ByteDance Ltd. Наличие двух разных платформ обусловлено строгостью цензуры в Китае. Столь мощные инструменты воздействия на китайских граждан не остались без контроля. Мониторингу подвергаются как зарубежные, так и зарегистрированные в Китае учетные записи, однако цензура распространяется только на последние. Полученные данные используются для тренировки алгоритмов распознавания запрещенного контента.

Китай также является лидером в технологиях, связанных с распознаванием лиц. Такое развитие обосновано, среди прочих факторов, значительно меньшей заботой о защите персональных данных. Распознавание лиц в Китае имеет широчайший спектр применения: оплата, кредитование, поиск преступников и пропавших без вести, даже обеспечение соблюдения масочного режима. При регистрации мобильного номера обязательным условием является наличие сканов лица пользователя. Таким образом, база данных для системы распознавания лиц растет с каждым днем.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Цензура (контроль) в интернете. Опыт Китая / TAdviser — портал выбора технологий и поставщиков. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A6%D0%B5%D0%BD%D0%B7%D1%83%D1%80%D0%B0_(%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C)_%D0%B2_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5._%D0%9E%D0%BF%D1%8B%D1%82_%D0%9A%D0%B8%D1%82%D0%B0%D1%8F (дата обращения 10.10.2022). – Режим доступа: свободный.

2. TikTok Revenue and Usage Statistics (2022) / Business of Apps – the latest app industry news, analysis and insights. URL: https://www.businessofapps.com/data/tik-tok-statistics/ (дата обращения 10.10.2022). – Режим доступа: свободный.

3. История создания приложения Tik-Tok / EPICSTARS – база блогеров. URL: https://ru.epicstars.com/istoriya-sozdaniya-prilozheniya-tik-tok/ (дата обращения 10.10.2022). – Режим доступа: свободный.

4. What is Alipay? WeChat Pay? How to pay Like a Local in China / Professional Dragon Social – Social Media Marketing in China. URL: https://www.dragonsocial.net/blog/what-is-alipay-wechat-pay-payments/ (дата обращения 10.10.2022). – Режим доступа: свободный.

5. WeChat Surveillance Explained / The Citizen Lab - University of Toronto. URL: https://citizenlab.ca/2020/05/wechat-surveillance-explained/ (дата обращения 10.10.2022). – Режим доступа: свободный.

6. I helped build ByteDance's censorship machine / Protocol — The people, power and politics of tech. URL: https://www.protocol.com/china/i-built-bytedance-censorship-machine (дата обращения 10.10.2022). – Режим доступа: свободный.

7. Почему Китай лидирует в технологии распознавания лиц / «Ведомости» – ведущее деловое издание России. URL: https://www.vedomosti.ru/economics/articles/2019/06/16/804290-kitai-lidiruet (дата обращения 10.10.2022). – Режим доступа: свободный.

8. В Китае ввели обязательное распознавание лиц при регистрации новых телефонных номеров / Bird In Flight – интернет-журнал о фотографии и визуальной культуре. URL: https://birdinflight.com/ru/novosti/20191202-china-face-recognition-phones.html (дата обращения 10.10.2022). – Режим доступа: свободный.

УДК 323.2

Богданов Клим Алексеевич, студент, Комсомольский-на-Амуре государственный университет
Bogdanov Klim Alekseevich, student, Komsomolsk-on-Amur State University
Подкич Светлана Александровна, старший преподаватель, кафедра «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Podkich Svetlana Alexandrovna, Senior Lecturer, Department of Linguistics and Intercultural Communication, Komsomolsk-on-Amur State University

ОСНОВНЫЕ МЕТОДЫ ПРОФИЛАКТИКИ И ПРЕДОТВРАЩЕНИЯ ТЕРРОРИСТИЧЕСКОЙ УГРОЗЫ, ПРИМЕНЯЕМЫЕ В МЕЖДУНАРОДНОЙ ПРАКТИКЕ

MAIN METHODS OF TERRORISM THREATS PREVENTION USED IN INTERNATIONAL PRACTICE

Аннотация. В данной статье рассматривается методы профилактики и предотвращения террористических угроз. Особое внимание уделяется причинам возникновения, проявления и методам профилактики террористической угрозы, понять, как государства бороться с этим злом, разобраться какие цели мотивы они преследуют. Все террористические действия приводят к многочисленным жертвам со стороны мирного населения и правоохранительных органов.

Abstract. This article discusses methods of prevention and prevention of terrorist threats. Special attention is paid to the causes, manifestations and methods of prevention of the terrorist

threat, to understand how states fight this evil, to understand what goals and motives they pursue. All terrorist actions lead to numerous victims on the part of the civilian population and law enforcement agencies.

Ключевые слова: терроризм, экстремизм, противодействие, методы, профилактика.
Key words: terrorism, extremism, counteraction, methods, prevention.

Ведение

В XXI веке проблема терроризма и экстремизма стала самой серьезной проблемой для всех стран и мирового общества.

Термин «терроризм» ведет свое происхождение от латинского «terror» – страх, ужас. В словаре русского языка С.И. Ожегова сказано, что «террор - это устрашение политических оппонентов, выражающееся в физическом насилии, вплоть до их физического уничтожения».

Терроризм и борьба с ним приобрели глобальный характер – такова тенденция, наблюдаемая повсеместно в последние годы. Само явление терроризма угрожает не только безопасности и личным интересам граждан, но и таким аспектам функционирования общества и государства как социальная безопасность, национальная стабильность, международные и государственные отношения.

Борьба с террористическими актами сейчас являются основной задачей прогрессивного мира. Не только государственным аппаратам, но и рядовым гражданам необходимо быть осведомленными о происходящем, чтобы быть готовыми защитить себя. С каждым годом проявления терроризма становятся все более организованными и безжалостными, используя самые прогрессивные технологии, вооружения и средства коммуникации. Оттого борьба с терроризмом является одной из главных общегосударственных задач.

Основная часть.

В современной России также существует проблема террористических проявлений, которые становятся все заметнее. Как правило, угроза терроризма возникает на фоне усиления распространения политического, народного и духовного экстремизма, который представляет серьезную угрозу обществу и государству.

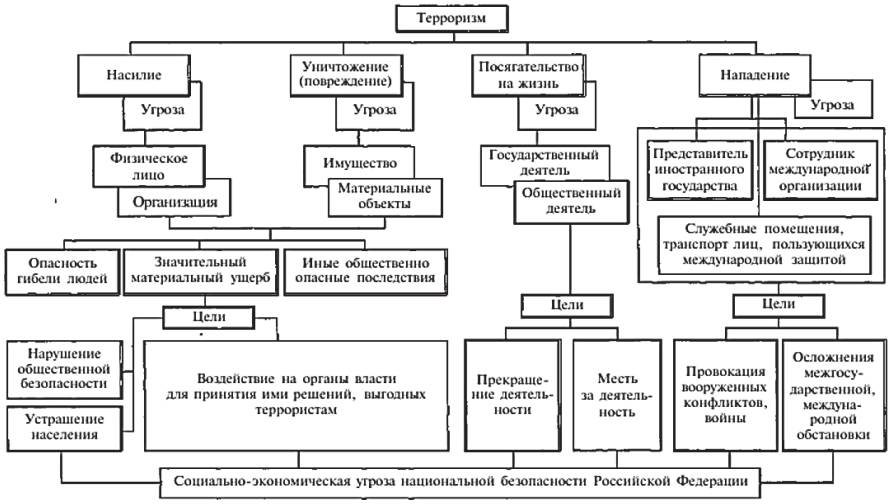

Рисунок 1 – Схема понятия «терроризма и террористических актов»

Среди методов профилактики террористических проявлений можно выделить следующие:

- выявление, разыскивание и устранение первопричин и условий, которые способствуют совершению террористических актов, возникновению и распространению терроризма как явления и ведению террористической деятельности;

- создание условий, препятствующих совершению террористических актов, а также сведение к минимуму их последствий;

- выявление тех, кто может быть вовлечен или причастен к террористической деятельности.

Борьба с идеологией терроризма охватывает в себе комплекс организационных, общественно политических, справочно пропагандистских мер, указанных для предупреждения распространения убеждений, пропаганды, настроений, мотивов и установок в обществе, сориентированных на конкретное изменение существующих общественных и политических институтов государства. Все физические и юридические лица, многочисленные поселения людей, недвижимость, жизненно важная инфраструктура, транспорт, средства к существованию могут рассматриваться как потенциальные мишени террористических устремлений. В этой связи особая роль принадлежит эффективному внедрению административно правовой системы, предустановленной законодательством Российской Федерации.

У этой проблемы не может быть простого пути решения. Терроризм, каким он стал в XXI веке - это сложная, многоуровневая система. Он формируется из комплекса взаимодополняющих процессов: идеологического, уголовного, военного, экономического, политического, религиозного и националистического. Каждое проявление терроризма имеет свои истоки, причины и последствия, и эти причины могут быть как глобальными, политическими и историческими, так и индивидуальными, психологическими особенностями конкретного исполнителя. Между тем, определенные общие тенденции все же присутствуют. Некоторыми исследователями терроризм сейчас рассматривается как ответ на значительные опоздания в решении насущных политических, народных и социальных проблем, поскольку именно они, накопившись в общественном сознании наряду с рядом иных причин, которые будут освещены ниже, могут послужить причиной террористических проявлений.

В международной и национальной судебно-правовой практике нет четкого и общепринятого понятия явления терроризма. Многие способы определения понятия «терроризм» объясняются региональными, государственными и историческими традициями, степенью демократичности общества и государства, стабильностью политической ситуации в той или иной стране, особенностями юридической научной традиции. Роль также играют и культурные, и даже языковые традиции. Тем не менее, мы можем провести анализ нескольких определений понятия «терроризм» и на основании выявленных общих черт сформировать некое общее определение, включающее в себя в достаточной мере справедливое и объективное понимание общественно-политического феномена терроризма.

В целом, можно определить терроризм следующим образом: это явление, представляющее собой организованные группы, объединенные некой идеей, которые в первую очередь пытаются достичь своей заявленной миссии путем регулярного применения насилия.

Выявление причин этого явления также может стать темой для обширного исследования. Каждый случай проявления терроризма становится совокупностью множества факторов, как социальных, так и индивидуально-психологических, культурных, исторических, и каждый может быть рассмотрен отдельно. Тем не менее, можно выделить ряд общих причин.

Одной из основных, базовых для многих исследователей, становится усиление противоречий в политической, экономической, общественной, духовной, государственно-правовой сферах. Любые противоречия ведут к обострению настроений в обществе, и потенциально могут привести к эскалации радикальных проявлений.

Кроме того, в ряду причин возникновения терроризма стоит отметить нежелание влиятельных лиц, групп и организаций следовать порядку социальной жизни, обще-

принятому большинством общества, и их желание извлечь выгоду из насилия. Подобные явления встречаются и в виде исторических фактов, и как современные локальные явления.

Применение террористических методов отдельными лицами, организациями и государствами для достижения, финансовых, социальных и других целей – также одна из основных и базовых причин, которые ведут к возникновению террористических проявлений.

Кроме того, существует ряд специфических факторов, которые стоит рассмотреть отдельно. Мощной базой для взращивания террористических настроений может стать национальный и/или духовный материал, связанный с традициями и обычаями данной группы. Как правило, на почве борьбы за свои национальные ценности проявления терроризма случаются нередко, поскольку конфликты на почве национального самосознания затрагивают самоощущение, самооценку, экзистенциальный смысл той или иной группы.

Близко к этому стоит и такое явление, как религиозный фанатизм. Нередко на базе религии создаются организации, либо выдвигаются отдельные личности, наделяющие себя магическими и мессианскими способностями. Они пропагандируют учения, которые преподносятся как единственно верные, несущие общее благо, справедливость и спасение. При этом зачастую отношение к представителям иных воззрений формируется среди последователей подобных радикальных учений в весьма нетерпимом ключе, и способствовать образованию еще более радикально настроенных ячеек. Подобные настроения также могут послужить основой для формирования террористических проявлений.

Следует также отметить, что накопившиеся в обществе экономические и социальные проблемы, которые не были решены и не предполагаются к решению долгое время, взяточничество, потеря доверия к органам власти и иные внутригосударственные проблемы также могут повлиять на распространение экстремистских настроений, что в свою очередь приводит к проявлениям терроризма.

В контексте обсуждения проблемы терроризма нельзя не упомянуть о таком явлении, как экстремизм. В общественном сознании эти понятия зачастую являются взаимозаменяемыми, но определенная разница все же есть. Экстремизм (от латинского extremus – "крайний, чрезмерный") — верность крайним и радикальным взглядам, методам действий и воздействий.

Такие меры включают провокации массовых беспорядков, террористические акты и партизанские методы.

Немаловажным фактором появления экстремизма обычно является финансовый и социальный кризис, который несет с собой резкое падение уровня жизни большинства населения, сформировавшаяся в государстве тоталитарная политическая система с подавлением оппозиции властями, преследованием инакомыслия, и в этих условиях крайние меры могут стать решающим фактором. Зачастую терроризм в таких ситуациях представляется для определённой категории людей и организаций единственным способом эффективно повлиять на ситуацию, и они прибегают к террористическим актам.

Террористический акт - это совершение подрыва, минирование школ и других зданий, несущих значимость в обществе, поджога или других действий, которые запугивают жителей и создают опасность гибели людей, причинения значительного материального ущерба и других серьезных последствий, с целью подрывание организованной деятельности органов власти.

Террористические акты наказываются лишением свободы на срок от восьми до пятнадцати лет (статья 205 Уголовного кодекса Российской Федерации).

Принципы противодействия экстремистских действий основаны на следующих принципах:

• Соблюдение, знание основных правовых норм гражданами;

• Связи с общественностью органами власти;

• Особый приоритет обеспечения безопасности Российской Федерации и ее граждан;

• Принятие жестких мер по предотвращению экстремистской деятельности;

• Сотрудничество страны с общественными, духовными организациями и другими организациями, гражданскими в противодействии экстремистской деятельности;

• Неминуемое наказание за осуществление любой деятельности, относящейся к экстремизму с лишением свободы или иных наказаний.

Заключение

Увеличение опасности терактов различного масштаба сегодня происходит на фоне обострения политического, народного и религиозного экстремизма. Это представляет серьезную опасность для государства, поскольку несет угрозу безопасности государства и его граждан, территориальной целостности и международных отношений. Глобальный характер, который приобретают проявления терроризма, также становится угрозой политической стабильности в различных государствах и регионах мира.

Противодействие угрозе терроризма в инфраструктуре страны означает снижение роста возможного ущерба функционированию промышленных, энергетических, научных и других комплексов, гарантируя не только национальную безопасность страны, но и жизни людей, а также формирование политических и финансовых последствий. Неблагоприятные социальные процессы, которые могут быть вызваны диверсиями или террористическими актами в определенных местах.

Каждый год наше государство предпримет ряд эффективных шагов по обузданию терроризма и созданию лучшего государства.

Государственная система способна противодействовать этому. Однако нынешний терроризм отличается необычайной живучестью. Он быстро приспосабливается к изменениям, укрепляется, становится умнее и бьет все больнее и с большим количеством жертв.

Терроризм распространяется, и борьба с ним становится делом каждого человека. Необходимо не только пассивное наблюдение, но и активные действия: соблюдение мер безопасности, принимаемых правоохранительными органами, получение знаний, необходимых для предотвращения террористических актов. Обязанностью каждого гражданина становится получить знания и навыки в области борьбы с терроризмом, чтобы гарантировать как свою личную, так и общественную безопасность.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Беляшев К.А., Борьба с международным терроризмом: сб. документов // К.А.Бекяшев, М.Р.Авясов. // М.'Проспект, 2005 – 671 с.

2. Вишняков Я.Д. Основы противодействия терроризму: учеб. пособие для студ. высш. учеб. заведений // Я. Д. Вишняков, Г. А. Бондаренко, С.Г.Васин, Е.В.Грацианский. М.: Издательский центр «Академия», 2006 – 240 с.

3. Аникина Т.А., Крылова А.В., Гиззатуллин А.Р., Зверев А.А., Зефиров Т.Л. «Предотвращение террористических угроз среди населения» // Т.А. Аникина, А.В. Крылова, А.Р. Гиззатуллин, А.А. Зверев, Т.Л. Зефиров // Казань: 2016 – 101 с.

4. Ольшанский Д. В. Психология террора / Д. В. Ольшанский. // М.: Академический проект, 2002 – 205 с.

УДК 343.301

Боровик Екатерина, студент; Комсомольский-на-Амуре государственный университет
Borovik Ekaterina, student of Komsomolsk-na-Amure State University
Малышева Наталья Васильевна, кандидат филологических наук, доцент; Комсомольский-на-Амуре государственный университет
Malysheva Natalia Vasilievna, PhD in Philology, Associate Professor, Komsomolsk-na-Amure State University

ЛЕКСИКО-СЕМАНТИЧЕСКОЕ ПОЛЕ «ПРОТИВОДЕЙСТВИЕ ТЕРРОРИЗМУ» (НА ОСНОВЕ ДОКУМЕНТОВ СОВЕТА БЕЗОПАСНОСТИ ООН)

LEXICO-SEMANTIC FIELD "COUNTERING TERRORISM": A STUDY OF UN SECURITY COUNCIL DOCUMENTS

Аннотация: В статье рассматривается структура лексико-семантического поля «противодействие терроризму», выявленная в документах Совета Безопасности ООН. Анализируемые документы содержат относительно высокую степень специализированности, что отражается, прежде всего, в политической терминологии.
Abstract: The article deals with the structure of the lexico-semantic field "countering terrorism", identified in the documents of the UN Security Council. The analyzed documents contain a relatively high degree of specialization, which is reflected in political terminology.
Ключевые слова: лексико-семантическое поле, концентрация терминов, ядро, периферия поля.
Key words: lexico-semantic field, concentration of terms, field core, field periphery.

В последнее несколько лет весь мир все чаще слышит это ужасное слово «теракт». Где бы ты не был, в какой угодно стране, части света, где, казалось бы, безопасно, терроризм может застать тебя врасплох, он не будет предупреждать или давать шансы, он не оставляет шансов вообще, никому. Самое печальное, что данную угрозу практически невозможно распознать – она появляется неожиданно, без предупреждения, принося слезы, боль и утраты. Но есть ли способ навсегда искоренить это зло из нашего мира?

Данный вопрос набирает обороты, а вместе с ним и понятие «противодействие терроризму». Так в ресурсе Wordstat.yandex.ru за последний месяц количество запросов, связанных так или иначе с данным понятием, составила около 78 тысяч показов. Частота употребления слов контртерроризм и антитерроризм также постоянно растет.

Якоб Гримм считал, что язык – это самое живое свидетельство о народах [1]. Слова, которые в определенный отрезок времени используются с большей частотой, наиболее хорошо фиксируют состояние эпохи на этот момент. Такие слова являются ключевыми.

Само понятие «противодействие терроризму» является теперь часто употребляемым и социально-значимым, так как охватывает большую часть мирового сообщества. Для современной лингвистики важно изучать актуальные и значимые слова, чтобы следить за динамикой развития семантики слов.

Противодействие терроризму – это комплекс мер государственной власти, органов местного самоуправления, физических и юридических лиц по выявлению, предупреждению, пресечению, раскрытию и расследованию данного террористического акта [2].

Основная цель настоящей статьи – выделить лексико-семантическое поле в документации ООН по борьбе с терроризмом и изучить его структуру.

Исходя и этой цели, были поставлены следующие задачи:

1 рассчитать количество терминов и лексем общеупотребительного языка;

2 выявить наибольшее скопление терминов в разных частях и фрагментах текста;

3 выявить различия в терминологической частотности в отдельных частях текста.

В данной статье мы рассмотрим лексико-семантическое поле «противодействие терроризму». Вера Арсеньевна Белошапкова относила семантическое поле к наиболее общим терминам. По ее мнению, он является гиперонимом по отношению к таким понятиям, как лексико-семантическое поле, функционально-семантическое поле, метафорическое поле, ассоциативное поле и т. д. Тогда соответственно, вышеперечисленные термины являются по отношению друг к другу со-, когипонимами. Лексико-семантическая группа, в свою очередь, является подвидом внутри лексико-семантического поля. Семантическое поле – это иерархическая структура множества лексических единиц, объединенных общим (инвариантным) значением [3].

Лексико-семантический анализ будет осуществлен нами на основе документов ООН объемом 9 тысяч печатных знаков [4].

Основой анализируемого текста является общеязыковая лексика. Доля терминов достаточно высока, однако термины распределены неравномерно. Было выявлено, что полная страница, содержащая только текст, без учета графиков и таблиц, состоит из 800 – 1000 слов, значительную часть которой составляет специальная политическая лексика.

Для правильного понимания значения изучаемой лексемы предварительно ознакомимся с семантикой понятия «противодействие терроризму». Обратимся к толковым словарям английского языка Oxford English Dictionary и Cambridge Dictionary.

Counterterrorism - action taken to prevent the activities of political groups who use violence to try to achieve their aims. Борьба с терроризмом - действия, принимаемые для предотвращения деятельности политических групп, которые используют насилие для достижения своих целей [5].

Anti-terrorism - activities intended to prevent or reduce terrorism (= violent acts for political purposes). Борьба с терроризмом - деятельность, направленная на предотвращение или сокращение масштабов терроризма (= насильственные действия в политических целях).

Теперь перейдем к рассмотрению указанного лексико-семантического поля, которое подразделяется на ядерную лексему и периферию [6].

Ядро лексико-семантического поля «Counterterrorism» (противодействие терроризму) представлено следующими терминами: anti-terrorism (антитерроризм), fighting terrorism (борьба с терроризмом), to prevent terrorism (предотвращать терроризм), to combat terrorism (бороться с терроризмом), fight against terrorism (борьба против терроризма), counter terrorist threats (противодействие террористическим угрозам).

Периферией является «Counter Terrorism Strategy» (противотеррористическая стратегия): counter-terrorism operation (оперfция по борьбе с терроризмом), UN Counter-Terrorism Committee (Контртеррористический Комитет ООН), counter-terrorism priorities (приоритеты в области борьбы с терроризмом), counter-terrorism efforts (усилия по борьбе с терроризмом), anti-terrorist operations (антитеррористические операции), counter-terrorism measures (контртеррористические меры).

Полученные данные отразим в таблице (см. Таблица 1).

Таблица 1 - Корреляция частотности употребления терминов в документах ООН

Лексико-семантическое поле	Структура лексико-семантического поля	Частотность употребления (количество единиц)
Counterterrorism	anti-terrorism	2
	fighting terrorism	3
	to prevent terrorism	1
	to combat terrorism	4
	fight against terrorism	1
	counter terrorist threats	3
	counter-terrorism operation	2
	UN Counter-Terrorism Committee	8
	counter-terrorism priorities	4
	counter-terrorism efforts	6
	anti-terrorist operations	2
	counter-terrorism measures	3

Исследования показали, некоторые из лексических единиц данного поля имеют ярко выраженный семантический компонент «counterterrorism». Другие обладают им в меньшей степени, но по семантике и ассоциативно тесно связаны понятием «противодействие терроризму». Что касается принадлежности терминов к частям речи, то в большей степени термины представлены глаголами и существительными.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Grimm. Geschichte der deutschen Sprache. Leipzig, 1880. S .4.

2 РФ. Федеральный закон «О противодействии терроризму» от 06.03.2006 N 35-ФЗ (ред. от 31.12.2014) [Электронный ресурс]. – URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=173583 (дата обращения: 18.10.2022)

3 Белошапкова В. А. Современный русский язык. – М.: Азбуковник, 1999. – 800 с.

4 The UN Global Counter-terrorism Strategy (2006). Resolution adopted by the General Assembly, A/RES/60/288, 20.9

5 Оксфордский словарь // Oxford Learner's Dictionaries : словарь. URL: https://www.oxfordlearnersdictionaries.com/ (дата обращения: 18.10.2022).

6 Кэмбриджский словарь // Cambridge Dictionary : словарь. URL: https://dictionary.cambridge.org/ (дата обращения: 18.10.2022).

УДК 94

Букреев Никита Андреевич, студент, Дальневосточный Государственный Университет Путей Сообщения
Bukreev Nikita Andreevich, student, Far Eastern State Transport University

ИЗ ИСТОРИИ ПРОЕКТИРОВАНИЯ И СТРОИТЕЛЬСТВА БАЙКАЛО-АМУРСКОЙ ЖЕЛЕЗНОДОРОЖНОЙ МАГИСТРАЛИ (1920-е – НАЧАЛО 1940-х гг.)

FROM THE HISTORY OF DESIGN AND CONSTRUCTION OF THE BAIKAL-AMUR RAILWAY IN THE (1920 s – EARLY 1940 s)

Аннотация. Целью статьи является изучение исторического опыта проектирования и строительства Байкало-Амурской железнодорожной магистрали в 1920-х – начале 1940-х годов. Автор затрагивает один из сложных ключевых этапов железнодорожного строительства на территории советского Дальнего Востока, в ходе которого учёными,

изыскателями, инженерами был накоплен богатейший опыт в деле сооружения железной дороги и последовательного освоения дальневосточных рубежей России. В резюме отмечается важность рассматриваемого предмета исследования – Байкало-Амурской железнодорожной магистрали, которой в общегосударственном контексте мероприятий в указанных хронологических границах принадлежала ведущая позиция по развитию транспортной инфраструктуры дальневосточной территории.
Abstract. The purpose of the article is to study the historical experience of the design and construction of the Baikal-Amur railway in the 1920s - early 1940s. The author touches upon one of the complex key stages of railway construction in the territory of the Soviet Far East, during which scientists, prospectors, engineers accumulated a wealth of experience in the construction of the railway and the consistent development of the Far Eastern borders of Russia. The summary notes the importance of the subject of the study under consideration – the Baikal-Amur Railway, which in the national context of activities within the specified chronological boundaries held the leading position on the development of the transport infrastructure of the Far Eastern territory.
Ключевые слова: Байкало-Амурская магистраль, советский Дальний Восток, железнодорожная магистраль, проектирование, строительство.
Key words: Baikal-Amur mainline, soviet Far East, railway line, design, construction.

Байкало-Амурская магистраль является не только мега-проектом позднесоветского периода, но и ведущей железнодорожной трассой на территории Восточной Сибири и российского Дальнего Востока, а наряду с Транссибом, – вторым выходом Российской Федерации к Тихоокеанскому побережью. Общая протяжённость железнодорожной магистрали от Тайшета до Советской Гавани составляет 4,3 тыс. км.

Целью строительства Байкало-Амурской железнодорожной магистрали в 1920-х – начале 1940-х годов являлось наращивание промышленно-транспортной мощности дальневосточного региона в условия индустриальной модернизации и нараставшей внешнеполитической нестабильности на восточных рубежах государственной границы (на случай военного времени советское высшее партийное руководство предусматривало для неё функционал рокадной дороги), укрепление геополитического положения Дальнего Востока СССР в целом.

Начальный этап проектирования и последовавшего затем строительства Байкало-Амурской магистрали неразрывно связан с разноплановой исследовательской деятельностью Владимира Клавдиевича Арсеньева. Ещё 1900 г. он в качестве офицера царской армии проходил военную службу на дальневосточной окраине Российской империи. Это время совпало с сооружением Амурской железной дороги (1908 – 1910), которая представляла собой завершающий этап строительства Транссибирской магистрали. Особую заинтересованность проявляли предприниматели, в частности, золотопромышленники, неоднократно поднимавшие перед местным руководством Приамурья вопросы о важности и необходимости строительства Николаевской, Де-Кастринской и Сихотэ-Алиньской железнодорожных дорог. Актуальность проблемы не обошла стороной В.К. Арсеньева, который в дальнейшем стал вплотную заниматься изысканиями, проектированием и железнодорожным строительством. Окончание Гражданской войны и военной интервенции на Дальнем Востоке позволили ему детально изучить проблему. По результатам ряда экспедиций В.К. Арсеньев предложил два проектных варианта трассы: по первому – железная дорога пролегала по долинам рр. Удоми и Хунгари (ныне р. Гур) и далее уходила к р. Амур, а затем – вдоль берега на Хабаровск; по второму – она поднималась вверх по долине р. Коппи, пересекала хребет Сихотэ-Алинь и по р. Немпту подходила к Хабаровску. Одновременно В.К. Арсеньев подготовил предложения и по железнодорожной линии, соединявшей Хабаровск и Де-Кастри. Выдающийся изыскатель железных дорог, высококвалифицированный специалист

В.К. Арсеньев понимал и глубоко осознавал стратегическую необходимость железнодорожного строительства в Приамурском крае, поэтому в 1922 г. вместе с ведущими инженерами-железнодорожниками он приступил к разработке магистральных мероприятий по восстановлению и реконструкции железнодорожного транспорта советского Дальнего Востока.

Весной 1930 г. В.К. Арсеньев разработал и направил в Правление Уссурийской железной дороги, Далькрайисполком, Далькрайплан и Совет Народных Комиссаров (СНК) докладную записку, в которой обоснованно излагал свои предложения по проектированию и строительству второго железнодорожного выхода к Тихому океану. Именно тогда впервые будущая железная дорога была официально названа Байкало-Амурской магистралью. Одновременно по инициативе дальневосточного учёного-исследователя при поддержке председателя СНК СССР А.И. Рыкова и Академии наук СССР была организована Дальневосточная комплексная экспедиция для изучения районов будущей железнодорожной трассы. Возглавил её В.К. Арсеньев. Однако экспедиция так и не состоялась, так как 19 июля 1930 г. учёный выехал в низовья Амура для инспектирования изыскательских отрядов, где простудился и заболел. В.К. Арсеньев вернулся во Владивосток 26 августа 1930 г., а 4 сентября 1930 г. умер от тяжёлого воспаления легких. Собранный богатейший научно-исследовательский материал В.К. Арсеньева стал мощным подспорьем для различных организаций по технико-экономическим изысканиям и проектированию новых железнодорожных магистралей на Дальнем Востоке России.

В сложных условиях глобальных изменений на внешнеполитической арене, росте военной напряжённости, усиления режима власти внутри страны, нового витка политических репрессий, расширения полномочий карательных органов, расцвета плановой системы хозяйствования и формированной индустриализации строительство БАМа продолжилось в 1930-е гг. О государственной важности развития железнодорожной инфраструктуры дальневосточной территории свидетельствует докладная записка Далькрайкома ВКП (б), адресованная в ЦК ВКП (б) и СНК СССР. В ней излагались идеи о важности активизации деятельности экспедиции Дальжелдорстроя по рекогносцировочным транспортным изысканиям трассы Хабаровск – Советская Гавань, проектированию и строительству второй транссибирской железнодорожной магистрали с выходом к Тихому океану

Изучая историю БАМа в целом, невозможно не отметить героизм советских людей (инженеров, рабочих, заключённых и др.), их стремление трудиться самоотверженно, с полной отдачей, нередко даже ценой собственной жизни. Многие верили в силу ВКП (б), в авторитет И.В. Сталина, как главы Советского государства, полагая, что никаких непреодолимых препятствий для строительства нет, есть лишь некоторые сложности, которые возможно преодолеть.

В июне 1938 г. на основании Постановления СНК СССР о строительстве БАМа, дорогу необходимо было сдать в постоянную эксплуатацию в 1945 г., однако дальнейшие события, связанные с началом Второй мировой и Великой Отечественной войн внесли в эти планы кардинальные изменения.

Одной из важных страниц в истории проектирования и строительства Байкало-Амурской железнодорожной магистрали является сооружение трассы Волочаевка – Комсомольск-на-Амуре или ВОЛК, которое связано с постановлением Совета Труда и Обороны СССР «О строительстве железной дороги от станции Уруша Уссурийской железной дороги до села Пермское-на-Амуре», принятым в январе 1932 г. Это был ещё один шаг высшего партийного советского руководства, направленный на военно-стратегическое и промышленное укрепление дальневосточного форпоста. В то же время началось строительство в районе с. Пермское-на-Амуре судостроительного, авиационного и машиностроительного заводов, о чём 23 февраля 1932 г. правительственная

комиссия подписала государственный акт. Традиционно для рассматриваемого хронологического периода дальневосточная индустриальная новостройка была объявлена Всесоюзной ударной комсомольской. С присущим советской молодёжи энтузиазмом тысячи юношей и девушек с комсомольской путёвкой по организационному набору или самостоятельно ехали работать на Дальний Восток СССР. Первые 800 строителей-комсомольцев прибыли в Пермском 10 мая 1932 г.

В тяжелейших условиях шла работа на трассе ВОЛК. Зима 1932 – 1933 г. была неимоверно суровой, температуры крайне низкие. Экспедиция, которую возглавляли заключённые И.Н. Пилин и М.А. Павлов, несмотря на трудности зимнего периода, проложила трассу для дороги к Комсомольску-на-Амуре.

Главная задача по сооружению автогужевой дороги, которая проходила параллельно железнодорожному полотну, была 7 ноября 1934 г., а 11 декабря 1934 г. по маршруту Хабаровск – Комсомольск-на-Амуре открылось автобусное движение с продолжительностью рейса 23 часа.

Заканчивать сооружение линии ВОЛК советское правительство поручило железнодорожному строительному управлению ГУЛАГа НКВД на Дальнем Востоке. С этой целью был сформирован Юго-Восточный лагерь, но летом 1938 г. на многих руководителей его подразделения обрушились репрессии. В ходе расследования так называемого «Большого дела БАМа» было полностью арестовано руководство лагеря, многие ведущие специалисты и выполнить государственные производственные задания и намеченные планы не удалось. Пришлось перенести сроки ввода в эксплуатацию железнодорожной линии с 1938 на 1939 год. На основании приказа НКВД СССР от 4 января 1940 г. Юго-Восточный, Восточный, Нижнетамбовский и Нижне-Амурский лагеря объединялись в Нижне-Амурский лагерь. Теперь перед ним ставилась важная задача – завершить сооружение железной дороги Волочаевка – Комсомольск-на-Амуре и закончить строительство мостового перехода через р. Тунгуску. В результате 6 августа 1940 г. правительственная комиссия приняла в постоянную эксплуатацию железнодорожную линию ВОЛК, подписала государственный акт передачи этой железной дороги из системы НКВД в постоянную эксплуатацию Дальневосточной железной дороги (ДВЖД). Её сооружение являлось исторической необходимостью и сопровождалось многочисленными трудовыми подвигами инженеров и строителей железных дорог на Дальнем Востоке СССР.

В системе общегосударственных мероприятий по развитию железнодорожного транспорта в 1920-х – начале 1940-х гг. строительство Байкало-Амурской магистрали на Дальнем Востоке СССР занимает особое место.

В ходе экономической модернизации главный акцент был сделан именно на восстановлении и строительстве новых железных дорог на дальневосточной территории, которая остро нуждалась в собственной промышленности, финансах, трудовых ресурсах и т.д. Особую окраску этому процессу придавало пограничное положение региона, формируя острую потребность ускоренного создания на востоке мощного военно-стратегического форпоста. Ежегодно увеличивались и объёмы транспортных грузоперевозок. Во многом расширение сети путей сообщения стало ответом на внешнеполитические и экономические вызовы со стороны как европейских, так и азиатских государств накануне двух больших войн.

Несомненным фактом является самоотверженный труд тысяч строителей, инженеров, проектировщиков, заключённых, которые, несмотря на трудности, слабость материально-технической базы, нехватку продовольствия, одежды, инструментов, оборудования, практически полуголодные, раздетые с киркой и лопатой в руках строили железные дороги Дальнего Востока, как правило, рекордными темпами.

В современных условиях эпохи глобализации и трансформации БАМ сохраняет свою значимость для роста экономического потенциала Российской Федерации в це-

лом, а также Восточной Сибири и российского Дальнего Востока в частности. Сегодня главным вектором его экономической модернизации должно стать активное участие в динамично развивающемся процессе взаимодействия нашей страны со странами Азиатско-Тихоокеанского региона. Поэтому его научно-технический уровень развития не может уступать Трансазиатской железнодорожной магистрали, которая способна взять на себя большую часть транзитного грузопотока.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Бабий, В.И. Дальневосточное ожерелье / В.И. Бабий, С.А. Шатохин, В.Ф. Зуев. – Комсомольск-на-Амуре, 1997. – 141 с.

2 Дальневосточная магистраль России (1897 – 1997): К 100-летию Дальневосточной железной дороги / сост. В.Ф. Буркова, В.Ф. Зуев. – Хабаровск: Кн. изд-во, 1997. – 352 с.

3 Дальний Восток СССР: 1941 – 1945 гг. / под общ. ред. чл. корр. РАН Н.. Крадина; отв. ред. Г.А. Ткачева. (История Дальнего Востока России. Т. 3. Кн. 3). – Владивосток: Дальнаука, 2020. – 944 с.

4 Еланцева, О.П. Обречённая дорога: БАМ: 1932 – 1941 / О.П. Еланцева. – Владивосток: Изд-во Дальневост. Ун-та, – 188 с.

5 Еланцева, О.П. Строительство Байкало-Амурской железнодорожной магистрали (30-е – начало 50-х годов). Исторический опыт: Автореф. дис. д-ра. истор. наук / О.П. Еланцева. – Владивосток: Изд-во ДВТУ, 1996. – 44 с.

6 Зуев, В.Ф. Первооткрыватель будущих трасс / В.Ф. Зуев // Дальневосточная магистраль, 1997. – № 47. С. 35 – 46.

7. Платонова, Н.М. Дальний Восток и Байкало-Амурская магистраль. Причины, цели и проблемы строительства (на примере Восточного участка) – ретроспективный обзор за 1974 – 1984 гг. / Н.М. Платонова // Проблемы Дальнего Востока. 2009. № 4. С. 81 – 90.

УДК 327

Воронин Александр Алексеевич, студент, Комсомольский-на-Амуре государственный университет
Voronin Alexander Alekseevich, student, Komsomolsk-na-Amure State University
Лопатина Ольга Ивановна, старший преподаватель, Комсомольский-на-Амуре государственный университет
Lopatina Olga Ivanovna, senior lecturer, Komsomolsk-on-Amur State University

ИРЛАНДСКАЯ РЕСПУБЛИКАНСКАЯ АРМИЯ ИЛИ НАЦИОНАЛИСТИЧЕСКОЕ ЛИЦО ТЕРРОРИЗМА

THE IRISH REPUBLICAN ARMY OR THE NATIONALISTIC FACE OF TERRORISM

Аннотация. В данном докладе рассмотрены этапы становления Ирландской республиканской армии. Название Ирландская республиканская армия (ИРА) впервые появилось в новостях 30 августа 1919 года. Именно тогда это название было присвоено вооруженным группам, сражавшимся в войне за независимость Ирландии 1919-1921 годов сначала с британской полицией, а затем с регулярной армией. Организация ИРА того времени может быть описана, с точки зрения опыта 20-го века, как вооруженная партизанская структура, ориентированная на аспект национальной независимости, практически первая подобная организация в Европе 20-го века. Однако значительное

число британских, но также и ирландских ученых, журналистов и особенно политиков считали ИРА террористической организацией.
Abstract. This paper examines the stages of the formation of the Irish Republican Army. The name Irish Republican Army (IRA) first appeared in the news on August 30, 1919. That was when the name was given to the armed groups that fought in the Irish War of Independence of 1919-1921, first against the British police and then against the regular army. The organization of the IRA at that time can be described, in terms of 20th-century experience, as an armed guerrilla structure oriented toward the aspect of national independence, practically the first such organization in 20th-century Europe. However, a significant number of British but also Irish scholars, journalists, and especially politicians viewed the IRA as a terrorist organization.
Ключевые слова: Ирландская республиканская армия, независимость Ирландии, национальная независимость, терроризм.
Key words: Irish Republican Army, Irish independence, national independence, terrorism.

Название Ирландская республиканская армия (ИРА) впервые появилось в новостях 30 августа 1919 года. Именно тогда это название было присвоено вооруженным группам, сражавшимся в Ирландской войне за независимость 1919-1921 годов сначала с британской полицией, а затем с регулярной армией. Организацию ИРА того времени можно охарактеризовать, с точки зрения опыта 20 века, как вооруженную партизанскую структуру, практически первую в Европе 20 века.

В связи с приведенным выше первоначальным мнением ряд британских, а также ирландских ученых, журналистов и особенно политиков считали ИРА террористической организацией. Это утверждение, однако, практически прекращает любую дискуссию. Это означает игнорирование индивидуальных мотивов вооруженных республиканцев, но, особенно, игнорирование политико-правового контекста актов насилия. Действительно, очень трудно отличить террор, основанный на идеологических и политических критериях, от борьбы за национальное освобождение par excellence. Это различие не имеет шансов получить полностью объективную интерпретацию, особенно со стороны политиков, хотя, как отметил Кшиштоф Карольчак, "(...) терроризм - это сугубо политическое явление. Это не идеология, а вид политической активности или средство для достижения намеченной политической цели".

В Ирландии национализм - более широкое понятие, чем республиканизм. Сегодня дебаты о национализме носят скорее идеологический, чем академический характер, в основном из-за множества драматических событий, произошедших в 20 веке в глобальном масштабе.

Что касается эволюции ирландского национального вопроса, особенно до раздела острова в 1921 году, то целью ирландского национализма было завоевание одной из трех форм политической независимости для неразделенной Ирландии: территориальной автономии, равноправия в общем государстве Великобритании или статуса независимой республики. Правовые методы достижения первых двух форм составляют суть так называемого конституционного национализма, для которого республиканская форма государства была менее важна.

Хронологически истоки ирландского республиканизма следует искать в периоде непосредственно перед Французской революцией, когда впервые появился просвещенный национализм. Социальное восприятие республиканизма изменилось в 19-м и начале 20-го века. Его антиномией, принимающей форму синусоиды, стал вышеупомянутый конституционный национализм, в то время гораздо более сильный, чем республиканизм.

В прошлом веке ИРА приобрела имидж организации, являющейся эманацией этнически эксклюзивного национализма в сочетании с непререкаемой догмой о создании независимой республики на неразделенном острове Ирландия. Таким образом, деятельность ИРА была преднамеренной и практически осуществленной формой насилия,

вытекающей из аксиологии республиканского национализма. Следует помнить, что точка зрения, согласно которой ИРА, согласно ее происхождению и ее сторонникам, является одной из военизированных организаций, борющихся за национальное освобождение, критикуется большинством наблюдателей.

Также трудно интерпретировать случаи людей, которых сначала считали террористами, но которые через некоторое время смогли изменить свой имидж и стать политиками, хотя их прошлое часто использовалось против них, например, партия Ирландских республиканцев, Герри Адамс, или бывший заместитель первого министра автономного правительства Северной Ирландии и начальник штаба ИРА в 1978-1982 годах, Мартин МакГиннесс.

Точками отсчета для насилия, применяемого организациями, которые заявляли, что борются за национальное освобождение, включая ИРА, являются такие понятия, как нация, этническая группа или национальное меньшинство.

В последние сто лет такое культурное понимание нации преобладало среди исследователей, анализирующих случай ирландской нации, что, в свою очередь, стало частью сугубо политических дебатов.

Однако все еще существующие взаимные предрассудки позволяют нам лишь сказать, что в результате этого Договора возникла разделенная этнополитическая нация. Это следует воспринимать как отправную точку для развития в будущем еще одного, окончательного варианта ирландской нации, т.е. единой политической нации. Этот процесс может быть успешным, если обязательства, вытекающие из Договора, будут соблюдаться обеими сторонами. Продвижение к такой цели было небезопасным, однако оно продолжалось, и, что важно, с 2006 года практически не было актов террора, связанных с конкретными военизированными структурами. Ход этого процесса стал неопределенным после объявления Brexit, то есть после британского референдума 23 июня 2016 года. Возникающие опасности, связанные с ожидаемыми ограничениями пограничного движения, могут породить язык ненависти, который может привести к актам ненависти. Подтверждением этой угрозы является, например, событие 10 сентября 2019 года во втором по величине городе Северной Ирландии, где полиция предотвратила взрыв. Это остановит процесс формирования социально-экономических связей между жителями независимой Республики и Северной Ирландии, и особенно двух общин, католической и протестантской, внутри последней.

Существует множество причин, по которым группа людей, определяемая как малая или зависимая нация, оказывает военное сопротивление, пять из них являются ключевыми. Первая - когда оккупационное государство намеренно и постоянно применяет репрессии, отказывая целевой группе в праве на этнонациональное различие и, как следствие, на любую форму политического представительства.

Угнетающее, оно же оккупационное государство, игнорирует волю к отделению, демократически выраженную зависимым населением. Ярким примером являются военные, или партизанские, действия, предпринятые ИРА против британских войск в 1919-1921 годах (Townshend 1975). Практически каждый случай военных действий, проводимых военными организациями, представляющими вышеперечисленные группы, требует глубокого сравнительного анализа.

Нападение на культурные и образовательные учреждения или гражданское население, не вовлеченное непосредственно в конфликт, означает, что идея реальной борьбы за национальное освобождение подменяется вырожденной версией насилия, т.е. политически мотивированным терроризмом. Такой политический терроризм, имеющий лишь криминальные результаты, политически контрпродуктивен для населения, борющегося за изменение своего статус-кво. Что касается имиджа, то последний упомянутый тип терроризма неоднократно наблюдался в военных действиях ИРА, включая ее многочисленные расколотые организации, однако, не исключительно.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ
1Абдулмуталинова, Т.А. Современные тенденции развития международного терроризма // Актуальные проблемы гуманитарных и социально-экономических наук. 2019. Т. 13. № 4. С. 12-14.
2 Скопылатова, В. И . Борьба кабинета Маргарет Тэтчер с Ирландской Республиканской Армией (1981 г.) // Журнал исторических, политологических и международных исследований. 2016. № 2 (58). С. 68-73.

УДК 343.301

Галдобин Данил Романович, студент; Комсомольский-на-Амуре государственный университет
Galdobin Danil Romanovich, student of Komsomolsk-na-Amure State University
Малышева Наталья Васильевна, кандидат филологических наук, доцент; Комсомольский-на-Амуре государственный университет
Malysheva Natalia Vasilievna, PhD in Philology, Associate Professor, Komsomolsk-na-Amure State University

ВЛИЯНИЕ COVID-19 НА УСИЛЕНИЕ НАПРЯЖЕНИЯ В ЗОНАХ ВОЗМОЖНЫХ ТЕРРОРИСТИЧЕСКИХ АТАК

IMPACT OF COVID-19 ON INCREASED TENSION IN ZONES OF POSSIBLE TERRORIST ATTACKS

Аннотация. В статье рассматриваются социальные и экономические последствия пандемии и ее влияние на терроризм, текущие тенденции, касающиеся экстремистской и террористической деятельности, а также то, как экстремистские или террористические группы использовали пандемию и связанные с ней ответные меры правительства.
Abstract. The paper investigates social and economic fallout of the pandemic and its effects on terrorism, the current trends concerning extremist and terrorist activities and how the extremist or the terrorist groups have been exploiting the pandemic and its consequent government responses.
Ключевые слова: коронавирус, терроризм, COVID-19, полиция, ИГИЛ, безопасность, пандемия.
Key words: coronavirus, terrorism, COVID-19, police, ISIS, security, pandemic.

Прошло более двух лет, как COVID-19 был объявлен мировым сообществом и Всемирной Организацией Здравоохранения (ВОЗ) глобальной пандемией. Тем не менее он продолжает оказывать значительное влияние на геополитический ландшафт в большинстве областей внутренней и внешней политики. Хотя некоторые государства добились прогресса в нейтрализации негативных последствий пандемии, чему способствовали программы вакцинации и другие меры сдерживания, COVID-19 по-прежнему представляет проблему во многих частях мира [0].

Борьба с COVID-19 отвлекает государственные ресурсы от борьбы с боевиками и преступными организациями, создавая возможности для террористических групп и международных торговцев наркотиками, которые процветают в условиях отсутствия безопасности. Несомненно, COVID-19 будет препятствовать внутренней безопасности и международным усилиям по противодействию террористическим и экстремистским движениям, позволяя группировкам беспрепятственно готовить террористические атаки и усиливать повстанческую войну в различных регионах [0].

Итак, цель данной статьи мы видим в исследовании динамики террористической активности на фоне COVID-19 в зонах возможных террористических атак.

Исходя из поставленной цели, определим круг задач:

1) собрать материал в интернет-источниках;

2) описать статистику террористической активности за последние годы;

3) охарактеризовать влияние COVID-19 на деятельность террористических и экстремистских организаций в странах различных регионов.

Статья основана на таких материалах сети интернет как:

1) онлайн СМИ;
2) международные академические исследования;
3) нормативно-правовые документы.

Анализ новостных интернет-источников показал активизацию деятельности наиболее крупных террористических организаций. Например, ИГИЛ призвало своих членов усилить борьбу с прозападными правительствами, особенно в Ираке. Террористическая организация "Боко Харам" активизировалась в Западной Африке. Иран, несмотря на тяжелую вспышку COVID-19, поддерживает своих шиитских доверенных лиц в Ираке в их атаках на американские базы.

США выражает свою обеспокоенность по поводу запасов Ирана: «вспышка коронавируса делает Тегеран более опасным» [0]. Силы западной коалиции, включая Великобританию, Францию и Испанию, вывели войска из Ирака из-за пандемии. COVID-19, ослабление коалиции и напряженность в отношениях между государствами приводят к снижению влияния на контролируемых территориях и, как следствие, к затруднениям и подчас невозможности сдерживать повстанцев ИГИЛ.

Гэри Акерман и Хейли Питерсон (Колледж готовности к чрезвычайным ситуациям, внутренней безопасности и кибербезопасности), специализирующиеся на террористической идеологии, опубликовали в журнале Perspectives on Terrorism отчет о том, какие проблемы и возможности представляет COVID-19 для террористических организаций. «Во времена кризиса мы часто видим, как террористы эксплуатируют ситуацию и используют ее для пропаганды», - пишет Аккерман. «Это особенно актуально среди антиправительственных группировок как крайне правых, так и крайне левых. Они пользуются широко распространенной тревогой и недоверием к правительству для усиления радикализации и насилия» [5].

Авторы отмечают опасность COVID-19, во-первых, как биологического оружия, применяемого террористами и экстремистами, во-вторых, как триггера, провоцирующего длительный период экономической стагнации и социальной нестабильности, что также используется сторонниками террористического движения [0].

Полицейские службы играют ведущую роль в борьбе с внутренним терроризмом, но это не является их текущим приоритетом. В дополнение к обычным полицейским обязанностям полиции приходится сталкиваться со значительными дополнительными обязанностями, возникшими как последствие коронавируса. Так, западные правительства приняли жесткие меры - чрезвычайное законодательство, позволяющее полиции обеспечивать карантин и социальную изоляцию. Например, в период локдауна в Италии и Франции люди должны были иметь при себе письменное заявление с указанием причин ухода из дома и быть готовыми по требованию предъявить его полиции. Испания запретила все прогулки на свежем воздухе, за исключением выгула собак. Для обеспечения соблюдения этих карантинов были задействованы десятки тысяч дополнительных сотрудников полиции и жандармерии. Все более ужесточающие ограничения начали вызывать локальные беспорядки в Италии, особенно в бедных районах Юга. Даже в Великобритании, с ее традицией более лояльного отношения к полицейской деятельности, карантинные меры вызвали жалобы на жестокое правоприменение [0].

Теперь обратим внимание на статистику. Общее число погибших в результате террористических атак в 2019 году составило 13826 человек. В 2021 году это число составило 7142, что является сокращением примерно на 49% [6, 7].

Основной причиной этого сокращения в 2021 году стало снижение интенсивности конфликта на Ближнем Востоке и последующее ослабление "Исламского государства" в Ираке и Сирии. Увеличение числа смертей было зарегистрировано в трех из девяти регионов - Азиатско-Тихоокеанском регионе, Северной Америке и Южной Азии. При этом Северная Америка оказалась на очень низком уровне, зафиксировав три смерти от терроризма в 2020 году и пять в 2021 году [0].

Глобальный индекс терроризма (GTI) показал, что в среднем ситуация остаётся неизменной. В 2021 году в 25 странах было зафиксировано сокращение числа смертей от терроризма, в то время как в 21 стране было зафиксировано увеличение, а в 117 странах число смертей не изменилось. В ста пяти странах не было зарегистрировано ни одного случая терроризма [0].

Итак, несмотря на первоначальные прогнозы о том, что COVID-19 усугубит последствия терроризма в определенных регионах, на основании проанализированных источников мы можем отметить, что пандемия оказала незначительное влияние на распространение террористического движения в 2020 и 2021 годах. Спад терроризма на Западе совпал с пандемией COVID-19. Ограничения на свободу передвижения, общественные собрания, поездки и непосредственная угроза личному здоровью могут помочь объяснить этот спад. Однако экстремисты стремятся извлечь выгоду из многих вторичных последствий, вызванных пандемией, таких как изоляция, возросшая онлайн активность и недовольство по поводу вакцин и карантина. Экстремисты обращаются к тем, у кого есть реальные или возможные обиды, с сообщениями, в которых они объединяют жалобы на систему здравоохранения с идеологической пропагандой с целью усиления гнева и разочарования [0].

Как только чрезвычайные меры будут отменены и общество начнёт жить с COVID-19, существует вероятность активизации террористической деятельности. Чтобы предотвратить это, общество должно принимать системные, многоэтапные и скоординированные меры реагирования, направленные на решение таких проблем, как психическое здоровье, потеря веры в политическую систему и отсутствие экономических возможностей.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Update on the impact of the COVID-19 pandemic on terrorism, counter-terrorism and countering violent extremism // URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jun/cted_covid_paper_15june2021_1.pdf (дата обращения: 08.10.2022).

2 Covid-19 and its impact on Terrorism // URL: https://www.researchgate.net/publication/351812982_Covid-19_and_its_impact_on_Terrorism (дата обращения: 08.10.2022).

3The COVID-19 Pandemic: A Preliminary Assessment of the Impact on Terrorism in Western States / James K. Wither // URL: https://www.marshallcenter.org/en/publications/occasional-papers/covid-19-pandemic-preliminary-assessment-impact-terrorism-western-states (дата обращения: 10.10.2022).

4 What is the impact of COVID-19 on terrorism and 27rganized crime? / INTERNATIONALINSIDER / URL: https://internationalinsider.org/what-is-the-impact-of-covid-19-on-terrorism-and-organised-crime/ (дата обращения: 08.10.2022).

5 Researchers investigate the impact of COVID-19 on terrorism // URL: https://phys.org/news/2020-08-impact-covid-terrorism.html (дата обращения: 10.10.2022).

6 GLOBAL TERRORISM INDEX 2020 // URL: https://nonews.co/wp-content/uploads/2021/01/GTI2020.pdf (дата обращения 15.10.2022).

7 GLOBAL TERRORISM INDEX 2022 // URL: https://www.economicsandpeace.org/wp-content/uploads/2022/03/GTI-2022-web.pdf (дата обращения 15.10.2022).

УДК 364.01

Геращенко Руслан Игоревич, студент, Комсомольский-на-Амуре государственный университет
Gerashchenko Ruslan Igorevich, student, Komsomolsk-on-Amur State University
Шинкорук Марина Владимировна, кандидат педагогических наук, доцент, Комсомольский-на-Амуре государственный университет
Shinkaruk Marina, Candidate of Pedagogical Sciences, Associate Professor, Komsomolsk-on-Amur State University

ИССЛЕДОВАНИЕ СОДЕРЖАНИЯ ПОНЯТИЯ «БЕЗОПАСНОСТЬ» В СУБЪЕКТИВНЫХ ПРЕДСТАВЛЕНИЯХ ЛИЧНОСТИ

THE STUDY OF THE CONTENT OF THE CONCEPT OF "SECURITY" IN THE SUBJECTIVE REPRESENTATIONS OF THE INDIVIDUAL

Аннотация. В статье осуществлен анализ современных исследований безопасности; описаны результаты исследования, направленного на выявление субъективных смыслов категории «безопасность» у 110 респондентов; приведен анализ полученных данных и сделаны выводы относительно содержания категории «безопасность» в представлениях респондентов.
Abstract. The article analyzes modern security studies; describes the results of a study aimed at identifying the subjective meanings of the category "security" in 116 respondents; analyzes the data obtained and draws conclusions about the content of the category "security" in the respondents' views.
Ключевые слова: психологическая безопасность, социальная безопасность, общество, индивид, состояние, условия, процессы.
Key words: psychological security, social security, society, individual, condition, conditions, processes.

Происходящие в последнее время в мире события, оказывают существенное влияние на самосознание человека, его эмоциональное, интеллектуальное, личное и социальное благополучие, с которыми связана такая личностная категория как «безопасность». В существующих социально-психологических условиях деструктивные события в мире приводят к разрушению пространства различных психологических процессов, границы социальных категорий становятся размыты. В полной мере это касается и такой широкой категории, как безопасность. Радикальные изменения в обществе все чаще становятся частью жизни, при этом понятие границ и безопасных форм жизни постоянно меняется, а оценки их значимости иногда противоположны тем, которые были на начальном этапе изменений.

В современной науке и практике проблемам личностной безопасности уделяется достаточно внимания. Так, например, авторов интересуют направления развития культуры здоровьесбережения в системе личностной безопасности (Ахмалиева М.Г., Коняева М.А.) [1], гендерные проблемы личностной безопасности (Виноградов, С.М. Рущин Д.А.) [3], роль личностно-психологической безопасности в адаптивности личности (Сошина, О.Н.) [6], личностная безопасность в контексте рецепции информации (Горбунов, А.С) [4], личностные аспекты проблемы выживания как условие обеспечение

безопасности в современном мире (Крылова, Ю.А, Тимошина И.Н., Богатова С.В.) [5], психологическая безопасность в условиях межэтнических взаимодействий (Белова, С.И., Каяшева О.И., Николаева Н.В.) [2] и множество других аспектов этой сложной, многокомпонентной проблемы.

Мы в свою очередь, тоже не смогли остаться равнодушными к этой важной для современного мира проблеме и предприняли попытки исследования феномена безопасности в субъективных представлениях жителей Хабаровского края.

В нашем исследовании приняли участие 116 человек, 42 человека – студенты ФГБОУ ВО «КнАГУ» и 74 – жители Хабаровского края, представители различных профессиональных сообществ.

Инструментом проводимого исследования была разработанная нами анкета, включающая 9 вопросов. Вопросы были направлены на выявление общих представлений о безопасности, ценностное отношение к данному феномену, локус контроля в отношении безопасности и связанные с безопасностью ассоциации. Так, мы интересовались у респондентов: какое место занимает безопасность в индивидуальной системе ценностей; что означает слово «безопасность»; где и с кем чаще всего ощущается безопасность; чем обеспечивается безопасность (внутренним состоянием или окружающей обстановкой); есть ли возможность влиять на собственную безопасность.

Далее мы представим некоторые из полученных результатов, представляющие интерес в контексте заявленной темы.

В результате проведенного опроса нам не удалось зафиксировать отношение к безопасности как к личностной ценности. Так, безопасность как высшую ценность выделяют лишь 14,6 % опрошенных, из них 9,5 % - студенты, т.е. для студентов личностная значимость безопасности ниже, чем для взрослых респондентов. Для 4,3 % опрошенных безопасность в системе личностных приоритетов стоит на последнем месте.

Формулируя собственное понимание слова «безопасность», большинство опрошенных нами связывают его с категорией чувств – «чувство безопасности, защищенности, комфорта». Некоторые из опрошенных раскрывают эту категорию через возможности: возможность действовать, реализовывать свои цели, что-то делать. Часть респондентов описывали безопасность из внешнего локуса, видя в собственной безопасности результат действий других людей, общества, государства. В этой же связи интересны были ответы на вопрос о возможности самому заботиться о своей безопасности, контролировать её. На этот вопрос положительно ответили 50,8 % респондентов, из них 28,5 % студенты.

Развивают контекст обращения с собственной безопасностью ответы респондентов на вопрос о том, приходилось ли им жертвовать своей безопасностью ради личных целей. Здесь мы получили 67,2 % положительных ответов, 21,4 % ответов – студенческих.

Среди наиболее безопасных мест респонденты выделяют: дом (75 %), компанию друзей (25 %), работу (11 %).

Таким образом, проведенное нами исследование показало, что безопасность является сложным личностным конструктом, представляемым в категориях чувств, ощущений, представлений, а так же места, объектов и отношений, то есть во внутренних и внешних феноменах. Большинство опрошенных отмечают, что их чувство безопасности во многом определяется той обстановкой и теми людьми, в которой и с которыми они находятся. При этом респонденты видят возможность самостоятельно заботиться о собственной безопасности и предпринимать усилия по её поддержки.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Ахмалиева М.Г., Коняева М.А. Направления развития культуры здоровьесбережения у студентов в системе личностной безопасности // Евразийский союз ученых. 2020. № 4-8. С. 4-8.

2 Белова С.И., Каяшева О.И., Николаева Н.В. Психологическая безопасность как социокультурный феномен и личностная характеристика в условиях межэтнических взаимодействий // Санкт-Петербург, 2015. С. 46-55.

3 Виноградова С.М., Рущин Д.А., Гендерные проблемы социальной и личностной безопасности // Вестник Ленинградского государственного университета им. А. С. Пушкина, 2015. Том 2. № 3. С. 170-180.

4 Горбунов А.С. Личностная безопасность и рецепция информации в информационном массовом обществе // В сборнике Международной научной конференции. 2019. № 3. С. 99-108.

5 Крылова Ю.А., Тимошина И.Н., Богатова С.В. Глобально-личностный аспект проблем выживания и обеспечения безопасности в современном мире // ФГБОУ «УГПУ им. И.Н. Ульянова». 2013. № 3. С. 133-139.

6 Сошина О.Н. Личностно-психологическая безопасность человека в профессиональной среде и безопасность организации как условие адаптивности // Проблемы управления рисками в техносфере. 2012. № 3. С. 100-104.

УДК 343.301

Грачева Ярослава, студент; Комсомольский-на-Амуре государственный университет
Gracheva Yaroslava, student of Komsomolsk-na-Amure State University
Малышева Наталья Васильевна, кандидат филологических наук, доцент; Комсомольский-на-Амуре государственный университет
Malysheva Natalia Vasilievna, PhD in Philology, Associate Professor, Komsomolsk-na-Amure State University

ТЕРРОРИСТИЧЕСКИЕ ДВИЖЕНИЯ В РОССИИ В КОНЦЕ XIX ВЕКА

TERRORIST MOVEMENTS IN RUSSIA AT THE END OF THE XIX CENTURY

Аннотация. В данной статье рассматривается развитие терроризма в России. Оно имеет длинную историю, особенно сильно выделяется период конца XIX века. Из-за многочисленности террористических происшествий можно выделить отдельные террористические движения того периода и последствия, к которым привела их деятельность, а так же влияние, оказанное на историческое развитие страны.
Abstract. This article examines the development of terrorism in Russia. It has a long history, the period at the end of the nineteenth century in particular stands out. Because of the multitude of terrorist incidents, it is possible to identify the individual terrorist movements of that period and the consequences their activities led to, as well as the impact they had on the historical development of the country.
Ключевые слова: терроризм, история терроризма в России, террористические движения, конец XIX века.
Key words: terrorism, history of terrorism in Russia, terrorist movements, late XIX century.

В настоящее время теме терроризма уделяется большое внимание как со стороны правительства, так и со стороны граждан Российской Федерации. Но не стоит забывать, что данная проблема была актуальна и в прошлом. Так, именно терроризм стал неизменной составляющей частью российского революционного движения. В российской истории особенно ярко прослеживается всплеск террористической борьбы в период с 1878-1882 годов.

Основной целью данной статьи является обзор террористических движений в России конца XIX века.

Исходя из цели, были поставлены следующие задачи:

1) изучить причины роста террористических настроений;

2) провести обзор ряда террористических движений, действующих в России в конце XIX века;

3) определить последствия деятельности данных террористических движений.

Хронологический рубеж появления терроризма в России неслучайно является концом XIX века. Он напрямую связан с началом реформ императора Александра II, которые должны были радикально изменить строй страны, проведя переход к конституционному устройству с соответствующими свободами и правами личности [1]. Но уже на этапе подготовки реформ механизм их проведения показал отсутствие диалога между государством и обществом, что в свою очередь вызвало критику реформ. К причинам, обусловившим переход революционных движений к террору, историки также причисляют:

1) месть правительству за репрессии, в том числе к радикалам;

2) способ реорганизовать правительство и подтолкнуть его к полноценным реформам;

3) отстраненность большей части общества от революционного движения;

4) возможность побудить народ к восстанию, тем самым ускорив ход истории.

Одними из ключевых движений того времени можно назвать народников и организацию «Земля и воля». Стоит отметить, что у каждого движения был главный фактор перехода к террору. Так, для движения народников, продвигавших социалистические идеи, триггерными стали: провал «хождения в народ», а также массовые аресты. Последовавшие за этими событиями жестокие расправы над участниками данного движения [2] также способствовали увеличению количества сторонников движения. Что привело к ключевому моменту в российской истории – выстрелу В. И. Засулич, - которым 24 января 1878 года был тяжело ранен петербургский градоначальник Ф. Ф. Трепов. Однако революционерка была оправдана судом присяжных и отпущена домой. Вынесенный оправдательный приговор дал народником надежду на возможное сочувствие со стороны общества.

В тоже время для «Земли и воли» понятие террора изначально рассматривалось как орудие самозащиты и мести, но в реальной жизни террор играл более важную роль. Именно из-за таких убеждений в 1878 году последовал целый ряд террористических актов. Начиная с убийства агента сыскной полиции А. Г. Никонова, заканчивая покушением на прокурора Киева М. М. Котляревского.

Но самой важной целью обоих движений выступило покушение на Александра II, что повлекло за собой ряд попыток покушений на императора. Первой такой попыткой стал выстрел А. К. Соловьева (участника движения «Земля и воля») в царя на Дворцовой площади. Террорист не смог попасть в Александра II, был схвачен и в скором времени повешен.

Данное событие сильно повлияло на движение, приведя к нарастанию внутренних разногласий и, в итоге, разделению общества на «Народную волю» (сторонников метода террора) и «Черный передел», в который вошли противники данного метода. В общем на российского императора было совершенно 10 покушений, последнее из которых привело к его смерти.

В последствии большинство непосредственных участников цареубийства были арестованы и приговорены к смертной казни.

Однако, смерть Александра II привела к прямо противоположенным результатам, чем те, на которые рассчитывали народовольцы. Еще недавно восхищавшееся террористами общество полностью сменило свое отношение к ним.

Многие подвижки в сторону либерализма, проводимые Александром II, были сведены на нет контрреформами Александр III. Сама «Народная воля» к 1883 году была разгромлена, последующие попытки ее восстановления успеха не имели.

Тем не менее, следует отметить, что опыт борьбы данного движения оказал колоссальное влияние на последующих ход революционного движения в России. Терроризм стал расцениваться как весьма действенное средство противостояния властям, что, в свою очередь, привело к последующим попыткам совершения террористических актов в отношении Александра III [3].

Подводя итог к вышесказанному, можно сделать вывод, что данные объединения сильно повлияли как на развитие истории, так и на подход самого государства к борьбе с терроризмом.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Колотков М. Б. Идеология терроризма в России в конце XIX - начале XX века: историко-правовой аспект / М. Б. Колотков // 2018. С.14-31. URL: https://elibrary.ru/item.asp?id=35173423 (дата обращения: 16.10.2022). – Режим доступа: свободный.

2 Луценко В. С. Терроризм в России: понятие, исторические этапы развития / В. С. Луценко // 2019. С.4-9. URL: https://elibrary.ru/item.asp?id=39323864 (дата обращения: 15.10.2022). – Режим доступа: свободный.

3 Руденок К. В. Терроризм в России: ХМСП исследование / К. В. Руденок // 2018. С.160-173. URL: https://elibrary.ru/item.asp?id=36941851 (дата обращения: 15.10.2022). – Режим доступа: свободный.

УДК 621.9:519.8

Грачева Ярослава, студент; Комсомольский-на-Амуре государственный университет
Gracheva Yaroslava, student of Komsomolsk-na-Amure State University
Когай Сергей Геннадьевич, старший преподаватель; Комсомольский-на-Амуре государственный университет
Kogai Sergei Gennadevich, senior lecturer, Komsomolsk-na-Amure State University

ПРОФИЛАКТИКА ТЕРРОРИЗМА И ЭКСТРЕМИЗМА В МОЛОДЕЖНОЙ СРЕДЕ КИТАЙСКОЙ НАРОДНОЙ РЕСПУБЛИКИ

PREVENTION OF TERRORISM AND EXTREMISM AMONG YOUNG PEOPLE OF CHINA

Аннотация. В последнее время политика Китая уделяет все большее внимание проблеме подросткового экстремизма и терроризма, активно поддерживает антитеррористические движения и программы как на международном, так и на государственном уровне. В данной статье исследуется методы, используемые в Китайской Народной Республике по противодействию терроризму и экстремизму среди молодежи.
Abstract. Recently, Chinese policy has paid increasing attention to the problem of adolescent extremism and terrorism, actively supporting counter-terrorism movements and programmes both internationally and at the state level. This article examines the methods used in the People's Republic of China to counter terrorism and extremism among young people.
Ключевые слова: Китай, подростки, терроризм, экстремизм, профилактика терроризма и экстремизма.
Key words: China, Adolescents, Terrorism, Extremism, Prevention of Terrorism and Extremism.

Современный мир претерпевает глобальные изменения, вступая в новую эру стремительного развития и больших перемен. Глобализация принесла человечеству не только позитивные, но и негативные явления. Одним из которых является развитие подросткового терроризма и экстремизма. Целью данной статьи является исследование возможных мер профилактики терроризма и экстремизма среди подростков Китая. Исходя из цели, были поставлены следующие задачи:

1) исследовать историю подросткового терроризма и экстремизма в Китайской Народной Республике (КНР);

2) изучить причины подросткового терроризма и экстремизма в КНР;

3) выявить профилактические меры, используемые в Китае для предотвращения подросткового экстремизма и терроризма.

Китай - страна с многовековой историей, включающей в себя и акты терроризма. Но особенно сильно по количеству терактов и экстремистских настроений выделяется Синьцзян-Уйгурский автономный округ, который вошел в состав КНР 1 октября 1955 года. И оставался довольно мирным регионом до 1990-ых годов, когда произошел резкий скачок террористических угроз, что было объяснено использованием религиозных чувств населения с целью разжигания экстремистских настроений, что было особо актуально среди молодежи [4]. Особенно потрясли весь мир террористические акты 5 июля 2009 года, которые унесли огромное число человеческих жизней [2]. Также, впоследствии рассматривая данный террористический акт исследователи придут к выводу, что есть ряд причин, из-за которых он стал возможен. Из них основными стали:

1) Относительная закрытость округа;

2) Недостаток современных научных знаний об окружающем мире;

3) Неэффективность скотоводства и сельского хозяйства, соединяющих традиционный общественный уклад.

В последние годы Китай активно поддерживает антитеррористические движения и программы как на международном, так и на государственном уровне. Так, в 2019 году была опубликована новая “Белая книга”, в которой описывается возможный план по противодействию экстремистским настроениям среди молодежи [1].

Одним из самых распространенных средств по борьбе с экстремизмом среди молодежи стало создание специальных школ, в которых происходит перевоспитание подростков [3]. Так, в Синьцзяне в данных школах проходит образовательная и профессиональная подготовка, включающая в себя разностороннее развитие. В программу исправительных школ обязательно входят повышение уровня культуры и знаний, помощь в освоении профессиональных навыков и помощь в трудоустройстве.

Кроме того к часто используемым профилактическим мерам по борьбе с подростковым экстремизмом и терроризмом в Китае относят: проведение бесед в учебных заведениях на тему терроризма и экстремизма, доступ молодых людей к телефону горячей линии поддержки, а также дни памяти проводимые на общегосударственном уровне в дни террористических актов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Белая книга Китая // Официальная англоязычная платформа электронных коммуникаций Государственного совета Китайской Народной Республики. URL: http://english.www. gov.cn/archive/whitepaper/201908/17/content_ WS5d57573cc6d0c6695ff 7ed6c.html (дата обращения: 08.10.2022). – Режим доступа: свободный.

2 Борьба с терроризмом в Синьцзяне Китая // Генеральное Консульство Китайской Народной Республики в городе Владивостоке. URL: http://vladivostok.chinaconsulate.gov.cn/rus/zlgdt_2/202001/t20200103_3785551.htm (дата обращения: 08.10.2022). – Режим доступа: свободный.

3 Васильев Л.Е. О некоторых аспектах борьбы Китая с силами “трех зол”/ Л.Е. Васильев // – 2018. – С.92-106. – URL: https://elibrary.ru/item.asp?id=35729314 (дата обращения: 08.10.2022). – Режим доступа: свободный.

4 Сизов Г.А. Китай рассказал о опыте противодействия экстремизму. URL: https://riss.ru/analitycs/61808/ (дата обращения: 08.10.2022). – Режим доступа: свободный.

5 Петрунина Ж.В. Стратегия «Один пояс - Один путь» как катализатор изучения иностранных языков в Китае // В сборнике: Россия и Китай: история и перспективы сотрудничества. Материалы XI международной научно-практической конференции. Отв. редактор А.В. Друзяка. Благовещенск, 2021. С. 513-516.

УДК 327

Гукало Екатерина Константиновна, студентка, Комсомольский-на-Амуре государственный университет
Gukalo Ekaterina Konstantinovna, student, Komsomolsk-na-Amure State University
Лопатина Ольга Ивановна, старший преподаватель, Комсомольский-на-Амуре государственный университет
Lopatina Olga Ivanovna, senior lecturer, Komsomolsk-on-Amur State University

ПРОТИВОДЕЙСТВИЕ ТЕРРОРИЗМУ: МЕЖДУНАРОДНЫЕ И РОССИЙСКИЕ ОРГАНИЗАЦИИ

COUNTERING TERRORISM: INTERNATIONAL AND RUSSIAN ORGANIZATIONS

Аннотация. В данной статье рассматриваются ранние антитеррористические переговоры в рамках международных организаций (МО) и их результаты. В ней оценивается, как возникло международное сотрудничество в специализированных, региональных и глобальных МО, а также дается долгосрочный обзор. Опираясь на первоисточники и научную литературу, статья выявляет закономерности, тенденции и ключевые характеристики успешно принятых мер. Рассмотренные здесь антитеррористические усилия в основном носили превентивный характер и были направлены на предотвращение будущих террористических актов путем обеспечения того, чтобы безопасные убежища были закрыты, а виновные предстали перед судом.

Abstract. This article examines early counterterrorism negotiations within international organizations (IOs) and their outcomes. It assesses how international cooperation emerged in specialized, regional and global IOs and provides a long-term overview. Drawing on primary sources and academic literature, the article identifies patterns, trends and key characteristics of successful interventions. The counterterrorism efforts reviewed here were largely preventive in nature and aimed at preventing future terrorist attacks by ensuring that safe havens were closed and perpetrators brought to justice.

Ключевые слова: противодействие терроризму, международные организации, антитерроризм, ООН.

Key words: counter-terrorism, international organizations, anti-terrorism, UN.

Вопрос о том, выигрывают или проигрывают Соединенные Штаты и их союзники войну с терроризмом, вызывает ожесточенные споры среди авторов и в средствах массовой информации. Одни указывают на успехи, такие как аресты лидеров, убийства террористов или количество денег террористов, замороженных после 11 сентября (далее 9/11). Другие отмечают неудачи в виде продолжающихся терактов на Бали, в Мадриде и Лондоне, а также растущую усталость союзников США. Независимо от того,

является ли "война" правильным термином для этого конфликта, и можно ли выиграть такую войну или нет, эти дебаты поднимают некоторые очень важные вопросы: как мы можем знать, действительно ли политика, направленная на борьбу с терроризмом, приносит хоть какую-то пользу? Контр-терроризм так же стар, как и сам терроризм, поскольку правительства всегда пытались бороться с "террористическими" группами, которые им противостоят. Контртерроризм относится ко всем видам политики, операций и программ, которые правительства осуществляют для борьбы с терроризмом.

Терроризм уже давно является предметом повышенного внимания международного сообщества. Разработка международных антитеррористических мер часто представляет собой громоздкий и длительный процесс, который иногда не приводит к каким-либо ощутимым результатам. Организация Объединенных Наций (ООН), например, пытается разработать всеобъемлющую конвенцию против терроризма с начала 1970-х годов, но даже в 2021 году эта цель остается труднодостижимой. Сегодня, как и в 1970-е годы, согласованные международные действия по борьбе с терроризмом остаются сложной задачей, однако некоторые результаты уже достигнуты.

Кампания "Лучший мир" работает над укреплением отношений между Соединенными Штатами и Организацией Объединенных Наций посредством информационно-просветительской деятельности, коммуникаций и адвокации. Мы призываем руководство США повысить способность ООН выполнять свою бесценную международную работу во имя мира, прогресса, свободы и справедливости. В этих усилиях мы привлекаем политиков, СМИ и американскую общественность к повышению осведомленности и поддержки ООН.

Центр глобального антитеррористического сотрудничества - это непартийная исследовательская и политическая организация, которая работает над улучшением международно-координированных ответов на постоянно меняющуюся угрозу терроризма, предоставляя правительствам и международным организациям своевременные, актуальные для политики исследования и анализ. Основываясь на многолетних исследованиях региональных и международных инициатив по борьбе с терроризмом, Центр продолжает выявлять пути укрепления невоенных усилий по борьбе с терроризмом.

В целом, антитеррористические инструменты принимались примерно в три этапа. Начиная с законодательства, касающегося безопасности авиации и судоходства, ранние документы разрабатывались с 1960-х до начала 1990-х годов и касались конкретных видов террористических преступлений. Примечательно, что акты, совершенные во время "освободительных конфликтов", были прямо отнесены к исключениям из террористических преступлений. Самый последний этап отражает расширение, после категоризации террористических групп и "причин", включение таких групп, как Талибан, Аль-Каида и ИГИЛ, и таким образом, отражая современную террористическую угрозу для международного сообщества. В рамках этого последнего этапа были разработаны антитеррористические инструменты, которые касаются новых преступлений, связанных с террористическими взрывами, финансированием терроризма и ядерным терроризмом.

После исследования Ландеса появился исследовательский интерес к измерению эффективности конкретной контртеррористической политики. Даже если технологические барьеры могут препятствовать определенному типу террористических инцидентов, такие барьеры могут иметь непреднамеренные последствия, поскольку они вызывают перенос атак.

Например, металлодетекторы сделали более дорогостоящим захват самолетов, в то время как другие виды захвата заложников стали относительно менее дорогостоящими. Как следствие, количество захватов с помощью металлоискателей снизилось, в то время как похищения стали более частыми.

Действия по обеспечению безопасности, скажем, американцев на территории США посредством обеспечения внутренней безопасности привели к увеличению числа нападений на американцев на иностранной территории. До и после 11 сентября около 40% транснациональных террористических атак были направлены против интересов США, хотя после 11 сентября очень мало таких атак произошло на территории США. Очевидно, террористы взвешивали меняющиеся риски, как и предсказывает рациональное действие, когда они выбирали, где и как атаковать.

Поэтому после угона самолета авиакомпании El Al в 1968 году генеральный секретарь ООН У Тан призвал государства принять решительные меры против "предосудительного акта" угона. Совет Европы (СЕ), Международная ассоциация воздушного транспорта и Международная федерация ассоциаций пилотов авиакомпаний поддержали его. Все эти институты рассматривали ИКАО как организацию, несущую главную ответственность за принятие мер. ИКАО прислушалась к призывам разработать дополнительные инструменты против угонов: Гаагская конвенция (1970) и Монреальская конвенция (1971) устранили некоторые недостатки Токийской конвенции 1963 года. Таким образом, ИКАО является местом рождения современных (то есть после Второй мировой войны) глобальных антитеррористических усилий.

Разрозненный подход к международным антитеррористическим усилиям продолжал набирать обороты и в других МО. Захват круизного судна "Ахилле Лауро" в 1985 году заставил Международную морскую организацию (ИМО) действовать.

Протокол о стационарных платформах был направлен на борьбу с опасностью для морских платформ, особенно нефтебуровых, с целью обеспечения безопасности мировых поставок нефти. Этот протокол (наряду с конвенцией Международного агентства по атомной энергии (МАГАТЭ), о которой речь пойдет ниже) был единственным в стороне от международных усилий по борьбе с терроризмом в 1980-х годах.

Мысль о том, что ядерный терроризм может стать возможным сценарием будущего, была понятна в свете того, что террористы очень хорошо умеют использовать новые технологии (например, самолеты). Поэтому в октябре 1977 года члены МАГАТЭ приступили к разработке Конвенции о физической защите ядерного материала, которая была принята в 1980 году.

Другая группа МО также занималась вопросами терроризма: региональные организации. По мере того как угоны самолетов становились все более частыми, участились случаи похищения или убийства дипломатов. Организация американских государств (ОАГ) включила этот вопрос в свою повестку дня. Межамериканскому юридическому комитету было поручено разработать конвенцию, текст которой в январе 1971 года был направлен на рассмотрение Генеральной Ассамблеи. Она была принята в феврале 1971 года.

Вопросами терроризма занимались две организации: СЕ и Европейские сообщества (ЕС).

Конференция по безопасности и сотрудничеству в Европе (СБСЕ) была еще одной структурой, занимавшейся вопросами терроризма, но она занималась терроризмом только на периферии. Ее главной целью было поддержание внутригосударственного мира и укрепление сотрудничества за "железным занавесом".

Международные организации, в частности ООН, играют важнейшую роль в создании и мониторинге реализации международных правовых рамок, которые обеспечивают важнейшую основу для сотрудничества между государствами в борьбе с терроризмом и привлечении террористов к ответственности.

Мириады различных международных функциональных органов, таких как органы, занимающиеся борьбой с финансированием терроризма, авиационной и морской безопасностью, способствуют установлению стандартов и повседневному техническому сотрудничеству, необходимому для борьбы с терроризмом. ООН играет уникальную

и неоценимую роль в качестве важного посредника и поставщика этих усилий среди функциональных, региональных и субрегиональных организаций. Соединенные Штаты не могут просто определять и финансировать свои собственные приоритеты. Безопасность американцев в борьбе с терроризмом переплетается с безопасностью других стран. США должны работать с этими странами, чтобы определить и финансировать приоритеты борьбы с терроризмом во всех уголках мира. Эффективная ООН может помочь использовать имеющиеся ограниченные ресурсы и повысить потенциал всех государств в борьбе с терроризмом.

Помимо европейских и американских стран, азиатские государства также пытались наладить более тесное сотрудничество в борьбе с терроризмом. В конце 1970-х годов Бангладеш, Бутан, Индия, Мальдивы, Непал, Пакистан и Шри-Ланка начали обсуждать создание региональной организации для содействия интеграции и развития регионального сотрудничества. В декабре 1985 года была основана Ассоциация регионального сотрудничества стран Южной Азии (SAARC) как межправительственная организация.

Всемирная организация, ООН, также начала действовать в отношении терроризма. В 1970-х годах усилия ООН по борьбе с преступностью были более успешными, в основном потому, что они следовали фрагментарному подходу и концентрировались на конкретных аспектах терроризма, а не на проблеме в целом.

Другая глобальная структура также занимающееся проблемой терроризма - Большая семерка. Она была основана в 1975 году для координации экономической политики крупнейших экономических держав после нескольких серьезных кризисов.

Попытки МО бороться с терроризмом никогда не обходились без проблем. МО часто критиковали за бездействие, "выхолащивание" решений, длительность процессов принятия решений, а также за часто изнурительное балансирование между национальными интересами и общими усилиями. Многие из этих проблем распространялись и на международную кампанию против терроризма.

Как и в большинстве случаев, не было (и нет) идеальных ответов на вопрос о том, как бороться с терроризмом. Хотя чаще всего МО удавалось договориться о тех или иных усилиях, они почти всегда содержали определенные лазейки.

Следует признать очевидную неэффективность резолюций и конвенций ООН. Некоторые политики видели в этих договорах большие перспективы. Прошлые резолюции и конвенции ООН не оказали заметного влияния на конкретные запрещенные способы нападения (например, взрывы, похищение людей или подрыв самолетов).

То есть, среднее значение конкретного запрещенного способа нападения до вмешательства не отличалось от среднего значения после ратификации договора. Это неудивительно, поскольку такие договоры не имеют механизма принуждения, и лишь несколько государств, не соблюдающих договор, могут свести на нет достижения государств, соблюдающих договор.

ООН предлагает форум для взаимодействия с традиционными и нетрадиционными союзниками по целому ряду вопросов борьбы с терроризмом, включая те, которые связаны с противодействием растущей радикализации и экстремизму, подпитывающим исламистский терроризм, и для которых в настоящее время не существует широкого и эффективного форума.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Иванов, В. И. Международный терроризм как глобальная проблема в современном мире / Я. А. Лубенец, В. И. Иванов // Территория науки. 2014. № 6. С. 94-95.

2 Королев, А. А. Международный терроризм на современном этапе [электронный ресурс] // Инфор. гуманит. портал «Знание. Понимание. Умение». 2008. №6. URL: http://www.zpu-journal.ru/e-zpu/2008/6 (дата обращения: 26.09.2022).

УДК 297.17

Гущина Анастасия Николаевна, студентка, Комсомольский-на-Амуре государственный университет
Guschina Anastasia Nikolaevna, student of Komsomolsk-na-Amure State University
Климова Екатерина Викторовна, старший преподаватель кафедры «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Klimova Ekaterina Viktorovna, Senior Lecturer of "Linguistics and Intercultural Communication", Komsomolsk-na-Amure State University

ФЕНОМЕН ТЕРРОРИЗМА

THE PHENOMENON OF TERRORISM

Аннотация. Терроризм – тактика политической борьбы, которая характеризует систематическое применение идеологически мотивированного насилия, чаще всего, выражается в убийствах, диверсии, саботаже и других действиях, которые представляют угрозу безопасности и жизни людей. В данной статье раскрывается определение терроризма, история его возникновения, затрагиваются мотивы действий некоторых экстремистских организаций и уязвимости общества.
Abstract. Terrorism is a tactic of political struggle that characterizes the systematic use of ideologically motivated violence, most often expressed in murders, sabotage, sabotage and other actions that pose a threat to the safety and lives of people. This article reveals the definition of terrorism, the history of its occurrence, the motives of the actions of some extremist organizations and the vulnerability of society are touched upon.
Ключевые слова: терроризм, террор, кибертерроризм, уязвимость, экстремизм.
Key words: terrorism, terror, cyberterrorism, vulnerability, extremism.

In the big legal dictionary, the term «terrorism» is «a crime against public safety, consisting in the commission of an explosion, arson or other actions... for the purpose of violating public safety, intimidating the population or influencing decision-making by the authorities» [1].

The new terrorism takes various types and forms. There is no single understanding of terrorism. This is confirmed by the words of Porter Goss, head of the intelligence Committee of the US House of Representatives: «It's time for us to reconsider the established views on terrorism: if earlier terrorist attacks were organized by order of a particular state, now they are increasingly committed by private individuals who resort to terrorism as a kind of means of persuasion».

The arsenal of the «new» terrorism has such means and methods that make it harder to prevent and harder to fight it. Terrorists have more and more modern equipment and independent sources of financing at their disposal. In addition, the terrorism of the «new wave» is also developing new «spheres of activity». There are even new terms, «cyberterrorism», «bioterrorism» and «ecoterrorism». Which cover various spheres of life, cyberspace, biology and ecology, respectively.

It is important to understand the difference between the concepts of terror and terrorism. The first difference is that terror is the usage of violence to cause a sense of fear of those against whom such violence is directed. It can be personal, massive, elementary or spontaneous. The second difference is the regular usage of rage to achieve specific aims, including political ones.

Although terrorism is hundreds of years old, it has been used as a political means of pressure, especially in the past decades. Since the 60s, terrorism has been gaining strength, especially in connection with the problems of Israel, Palestinian refugees and Arab States. But terrorism is not limited to Northern Ireland and the Near East. The topic of terrorism is also acute in Russia. One of the most terrifying terrorist attacks that took place in Russia was the terrorist attack in Beslan. Innocent people were killed, first of all children. Beslan has become a horror for the country and for the whole world, because nothing like this has ever happened before. Never before has there been a special seizure of a school where the vast majority were children.

In the first century, there was a religious movement of Zealots in Judea, they opposed Roman regulation. The zealous supporters were called sicarii, because they always wore short rapiers in the bends of their clothes. During the holidays of Jerusalem, they mixed with the crowd and killed their opponents by cutting the throats or wounded them in the back.

In 66 AD, a group of Zealots captured the fortress of Masada near the Dead Sea. They brutally destroyed the whole Roman army and made this castle located on the hill their main outpost. During several years they produced bandit attacks from there and frightened the Roman army. In 73 AD, the Tenth Legion under the command of Flavius Silva regained Masada, but he failed to catch the Zealots. According to one scientist of past time, unwilling to give up to Rome, 960 Zealots, with the exception of two women and five children, committed suicide.

Some people believe that the Zealot uprising marked the beginning of what we call terrorism today. Whether this is true or not, but since then, terrorism has not stopped leaving bloody traces in the history of mankind.

Every person who reads news about terrorism tries to figure out what the motives of the terrorists are. Different motives of such groupings are considered below. Most Arab terrorist groups justify their actions by pointing to the need of Palestinian refugees who lost their homeland Palestine when the State of Israel was formed in 1948. For decades, passions have been so inflamed that today the goal of Arab terrorists is not only their own native country, but also something more sinister for Jews: the complete destruction of Israel.

Israeli Ambassador, Benjamin Netanyahu writes: «The cause of terrorism is rooted not in discontent, but in a tendency to unbridled violence. It can lead to a worldview that certain ideological and religious goals justify and even require the rejection of all moral prohibitions» (Terrorism-How the West Can Win). The main purpose of terrorism is to intimidate society. Therefore, the topic of vulnerability should be touched upon.

Neil Livingston, an expert in the United States on terrorism, writes: «As cities grow in our world and it becomes more and more complex, accordingly, we have become increasingly vulnerable to attacks by small groups or even individuals who focus on undermining the lives of the majority or imposing their will on them». Our society is very vulnerable to terrorist actions. «Our delicate vital arteries - water, energy, transport, communication links and sewerage - are at the mercy of insidious terrorists and saboteurs» (Hydra of Carnage) [5].

So, our supply systems are so very vulnerable, a single terrorist today can show the same strength as an entire army in ancient times. Another vulnerable point in modern society is the rapid dissemination of information. Thanks to television, the power of terrorism increases many times. A terrorist wants international publicity for his cause, and thanks to the media, he gets it.

Only about one century ago, a few days passed until the news went around the world. Today, the dissemination of news is an instant affair. In some cases, the terrorist can even see himself on the screen as he plays his role. Often he knows what the other side is doing, while he does not give a look at his cards. Jan Schreiber goes so far as to say that «trying to attract the attention of the public» is «the most successful tactic of terrorists» [3].

The so-called cyberterrorists use modern information technologies for their own purposes. One of their weapons is computer viruses that «eat» information or block the operation of electronic networks. In addition, there are logic bombs - programs that "deceive" computer systems, forcing them to perform operations not provided for them and thus disabling them. According to many, society is becoming less protected from cyberterrorism, since the state of the economy and the security of individual states increasingly depend on computer networks. While the armed forces of most countries have reliable communication systems - even in the event of a nuclear war - civilian systems, be it electricity, transport or financial institutions, do not have such protection against various kinds of sabotage [2].

Not so long ago, a hacker from Sweden penetrated Florida's computer systems and disabled the emergency services' communications network for an hour, so that the police, fire and ambulance services could not respond to calls.

According to some experts, cyberterrorists have such technical means that no security system developed by the security services can resist. This clash of ideologies is revealed in the speech of the Soviet leader Gorbachev, in which he stated: "It should be clear as crystal that international relations can be directed towards normal cooperation only when the imperialists abandon their attempts to resolve the historical disputed issue between the two social systems by military means" (A Time for Peace) [4].

Nowadays terrorism takes new forms and it generates new problems, many points of this kind are being created all over the world. The events of recent years indicate that the number of terrorist acts committed by extremist groups or individual saboteurs is constantly increasing. Although many terrorist attacks are still aimed at military facilities and diplomatic missions, some terrorists choose more «easy» targets, such as public transport, stadiums, hotels, various attractions and other crowded places.

Over the past decade, terrorism has acquired a systemic character, the emergence of which has been facilitated by technological progress, as well as the development of mass media and methods of transmitting information, which has greatly increased the propaganda effect of terrorist acts.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Большой юридический словарь // gufo – Образовательный портал – Раздел сайта «Словари и энциклопедии», подраздел «Большой юридический словарь» - URL: https://gufo.me/dict/law/терроризм (Дата обращения 20.10.22)

2. Раджабов А.С. Рост угрозы терроризма в современном мире: причины возникновения и противодействие терроризму. // Международное сотрудничество евразийских государств: политика, экономика, право. 2021. № 2. С. 47-53.

3. Теракт на рождественской ярмарке в Берлине (2016) // Риа новости – Новостной портал – Раздел «Теракт» – URL: https://ria.ru/20171219/1511180965.html (Дата обращения 19.10.22)

4. Шанько В.В. «Терроризм» как метод политической борьбы (политический терроризм) // Шанько В.В. Философия права. 2022. № 2 (101). С. 116-119.

5. Яковлева Е.А. Религиозный терроризм как основной вид современного терроризма // Сборник статей и тезисов докладов научно-практической конференции, посвященной 25-летию Конституции Российской Федерации. Под ред. Королёвой Е.В., 2019. С. 210-213.

УДК 81.22

Ефимова Мария Евгеньевна, студентка; Комсомольский-на-Амуре государственный университет
Efimova Maria Evgenevna, student of Komsomolsk-na-Amure State University
Малышева Наталья Васильевна, кандидат филологических наук, доцент, Комсомольский-на-Амуре государственный университет
Malysheva Natalia Vasilievna, PhD in Philology, Associate Professor, Komsomolsk-na-Amure State University

ЭКОЛОГИЧЕСКИЙ АКТИВИЗМ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

ENVIRONMENTAL ACTIVISM AS A THREAT TO NATIONAL SECURITY

Аннотация. Цель данной работы рассмотреть негативные стороны влияния экологического движения в контексте современной реальности, когда под угрозой находятся одновременно и человек и природа. Деятельность британской группы активистов по борьбе с изменениями климата Just stop oil, а также участница организации «Fridays for Future» Луиза Неубауер выбраны в качестве показательных примеров для анализа деятельности защитников природы.
Abstract. The purpose of this work is to consider the negative aspects of the impact of the environmental movement in the context of modern reality, when both man and nature are under threat. British climate change activist group Just stop oil and Fridays for Future member Luisa Neubauer are selected as case studies of conservationists.
Ключевые слова: проблемы экологии, экологический терроризм, экологический активизм, Just stop oil, Луиза Неубауер.
Key words: environmental problems, environmental terrorism, environmental activism, Just stop oil, Luisa Neubauer.

Хозяйственная деятельность человечества привела к серьезному загрязнению планеты разными отходами производства. В природе происходят процессы, нарушающие биологическое равновесие, последствия которого вызывает беспокойство определенных групп населения. Все больше людей стремится предотвратить дельнейшее разрушение экосистем и усилить меры по охране окружающей среды. В целях повлиять на общественное мнение природоохранные организации занимаются экотерроризмом, тем самым представляя собой угрозу общественному порядку, а иногда и безопасности граждан.

Обращаясь к вопросу формулировки термина экологического терроризма, возникает двойственность определения. С одной стороны значение экологического терроризма обращает нас к умышленному разрушению окружающей среды. «Экологическим терроризмом, согласно ст. 421-2, признаются действия, преднамеренно осуществляемые лицом или организованной группой, имеющей целью серьезно нарушить общественный порядок путем запугивания или террора, с намерением введения в атмосферу, в почву, подпочву или в воды (включая территориальные морские воды) вещества, способного создать угрозу здоровью людей или животных или природной среде» [1]. С другой стороны, понятие экологического терроризма используется для отрицательной характеристики действий представителей движения зеленых. «Экологический терроризм (экотерроризм, экотаж = экология+саботаж) —радикальные действия групп и лиц, борющихся за права животных, а также любых «зелёных» (энвайронменталистов); ФБР

США определяет экологический терроризм в данном контексте как применение или угроза применения насилия криминального характера против невинных жертв или имуществу граждан со стороны экологически ориентированных, межнациональных групп по эколого-политическим причинам, либо направленных с целью привлечения внимания» [3]. Однако, как отмечает А.А. Пирматова, применение термина «экологический терроризм» для характеристики деятельности защитников окружающей среды недопустимо, так как при действиях террористического характера устрашение – есть самоцель, в то время как защитники природы стремятся остановить эксплуатацию естественных ресурсов [2]. Обозначать движение, выражающееся в радикальных акциях «зеленых» в защиту окружающей среды более корректно термином «экологический активизм». В данной статье пойдет речь о данном явлении как факторе, нарушающем повседневную жизнь граждан в условиях современности.

Все чаще в стремлении привлечь внимание к экологическим проблемам активисты обращаются к весьма пагубным действиям. Зачастую, броские выражения подкрепляются вызывающим поведением. К примеру, британская группа активистов по борьбе с изменением климата Just Stop Oil использует гражданское сопротивление с целью гарантировать, что правительство Великобритании обязуется прекратить лицензирование и производство новых ископаемых видов топлива [4]. Деятельность Just Stop Oil получила известность, действуя смело и провокационно. Летом 2022 г. участники организации привлекли активное внимание СМИ, приклеивая свои руки к известным художественным произведениям в крупных галереях Лондона и Глазго. Они поставили под вопрос ценность искусства, в мире с разрушенной экологией: «What use is art if there is no water?» - Каков смысл искусства, если в мире нет воды? «Is this painting worth more than your life?» - Разве эта картина стоит больше чем ваша жизнь? Данные действия вызывают неоднозначную оценку. Некоторых вдохновляет смелость и радикальность подобной активности, и одновременно с этим многих возмущает порча знаменитых памятников культуры и любых других исторически важных вещей.

На примере дебатов с климатическим активистом на канале Good Morning Britain изложим основные причины ненавистного отношения к движению зеленых. Экоактивистов называют фанатичными и эгоистичными, ведь их протесты (например, перекрытие магистральных путей, вандализм, вред городской инфраструктуре) препятствует привычному ходу жизни и ни в коей степени не предотвращает дальнейшее потребление ресурсов. Их обвиняют в так яро требуемой срочности предпринять какие-либо практические меры, хотя страны уже развиваются в верном направлении и делают все возможное на настоящий момент. Часто встречается сравнение поведения защитников природы с поведением людей в период пубертата, ведь им кажется, что они единственные, кто может спасти целый мир. А массовые забастовки представляют для них лишь возможность большого празднества, ученического слета, где есть возможность выделиться, показать, что я не такой как все. Участников организации Just Stop Oil обвиняют в погрешностях их действий, указывая на тот факт, что все они пользуются вещами, существующими благодаря нефти. Одежда, которую они носят, была привезена в магазин на автомобиле, заправленным бензином. В процессе производства еды, которую они едят, была использована нефть. Даже клей, которым они приклеивают себя к поверхностям, обязан своим существованием нефти. В свою очередь, климатических активистов поражает столь пристальное внимание к деталям и полное игнорирование имеющихся пугающих проблем экологии. Порча городского имущества, как они отмечают, представляет совершенно незначительную долю разрушений, которые обрушатся на нас при неизменности потребительского отношения. [5]

Знаменитая в Германии эко-активистка Луиза Неубауер заявила, что вместе с группой сподвижников намеревается предотвратить строительство самого длинного

нефтепровода в Уганде и Танзании. Идея Луизы о подрыве нефтепровода взбудоражила общественность. В своем выступлении она ссылалась на книгу шведского климатолога Эндрю Мальма «Как взорвать трубопровод», в которой утверждается, что саботаж является логической формой экоактивизма. Позднее она объяснила свою идею о подрыве как шутку, что вызвало ажиотаж и раздражение. В газете «Bild» отмечается, что Неубауер в своем высказывании хотела прокомментировать только идею нового трубопровода. Тем не менее, умышленно было это сделано активисткой или нет, среди публики появилось некоторое беспокойство и неуверенность в безопасности. Здесь действия энвайронменталистов становятся потенциально опасными, тем самым выходят за грани определения экоактивизма, стремясь в сторону террористического характера.

Таким образом, мы видим, что процесс защиты окружающей среды сопровождается риском для людей, и теперь они сами нуждаются в защите. Меры, предпринимаемые экоактивистами, губительно сказываются на человеческой деятельности. Для определения разрушительной активности защитников природы в дискурсе русскоязычного текста корректнее употреблять определение эко-активизм. Однако, если в процессе ограничения губительного влияния на природу, субъект стремиться устрашить публику, то применительно пользоваться терминологическим сочетанием экологический терроризм.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Архипов, А. М. Экологический терроризм как вызов глобальной экологической безопасности / А. М. Архипов // Экономика, право, образование: региональный аспект: сборник научных трудов IX межвузовской научно-практической конференции, Нижний Новгород, 25 июня 2019 года. – Нижний Новгород: Московский университет им. С.Ю. Витте, 2019. – С. 321-332. – EDN VOONVV.

2. Пирматова, А. А. К вопросу о дифференциации "экологического терроризма" и "экологического активизма" / А. А. Пирматова // Право и государство: теория и практика. – 2021. – № 6(198). – С. 83-86. – DOI 10.47643/1815-1337_2021_6_83. – EDN GRBLTD.

3. Экологический терроризм // Wikipedia, the free encyclopedia: онлайн энциклопедия. - URL: https://en.wikipedia.org/wiki/Just_Stop_Oil (дата обращения 11.09.2022). Текст: электронный.https://ru.wikipedia.org/wiki/Экологический_терроризм Just Stop Oil // Wikipedia, the free encyclopedia: онлайн энциклопедия. - URL: https://en.wikipedia.org/wiki/Just_Stop_Oil (дата обращения 01.08.2022). - Текст: электронный.

4. Just Stop Oil // Wikipedia, the free encyclopedia: онлайн энциклопедия. - URL: https://en.wikipedia.org/wiki/Just_Stop_Oil (дата обращения 01.08.2022). - Текст: электронный.

5. Richard Madeley Clashes with Climate Activist in Fiery Oil Protest Debate | Good Morning Britain // YouTube: видео платформа. - URL: https://www.youtube.com/watch?v=-M0jRaOOkT8&ab_channel=GoodMorningBritain (дата обращения 04.08.2022). - Текст: электронный.

УДК 327

Захаров Данил Александрович, студент; Комсомольский-на-Амуре государственный университет
Zakharov Danil Alexandrovich, student, Komsomolsk-na-Amure State University
Мусалитина Евгения Александровна, доцент; Комсомольский-на-Амуре государственный университет
Musalitina Evgenia Aleksandrovna, associate professor, Komsomolsk-na-Amure State University

СОТРУДНИЧЕСТВО СТРАН ШОС ПО БОРЬБЕ С ТЕРРОРИЗМОМ

COOPERATION BETWEEN THE SCO COUNTRIES IN THE FIGHT AGAINST TERRORISM

Аннотация. В современном мире государства столкнулись с глобальной проблемой – международным терроризмом, экстремизмом и сепаратизмом. Всевозможные преступные группировки занимаются захватом заложников, контрабандой наркотиков и оружия, дестабилизацией целых государств. Граждане многих стран попадают под влияние экстремистских идей и оказываются вовлечены в деятельность таких групп. В целях борьбы с подобными проявлениями страны создают международные организации, одной из них является Шанхайская организация сотрудничества (ШОС). В статье рассматривается деятельность ШОС по международному противодействию террористической и экстремистской деятельности.
Abstract. In the modern world, States are faced with a global problem – international terrorism, extremism and separatism. All kinds of criminal groups are engaged in hostage-taking, drug and arms smuggling, and destabilization of entire states. Citizens of many countries fall under the influence of extremist ideas and become involved in the activities of such groups. In order to combat such manifestations, countries are creating international organizations, one of them is the Shanghai Cooperation Organization (SCO). The article examines the SCO's activities in international counteraction to terrorist and extremist activities.
Ключевые слова: противодействие терроризму, безопасность, совместные учения, экстремизм, региональные организации, ШОС.
Key words: countering terrorism, security, joint exercises, extremism, regional organizations, SCO.

В XXI в. тема террористических угроз и способов противодействия им обрела глобальное значение. В связи с международным характером проблемы региональные институты стали важным инструментом взаимодействия стран в контртеррористической политике. Шанхайская организация сотрудничества (ШОС) – это региональная организация, основанная в 2001 г. Китаем, Россией и странами Центральной Азии, такими как Казахстан, Кыргызстан, Таджикистан и Узбекистан, с основной целью – противодействовать терроризму, сепаратизму и экстремизму.

По причине близости государств ШОС к границам Афганистана и Пакистана существует региональная проблема терроризма, также большое количество граждан стран ШОС присоединились к террористическим группировкам. Угрозы терроризма и нестабильность в регионе ШОС достигают высокого уровня. [5]

Противодействие совершению террористических и экстремистских актов является одним из основных направлений деятельности Шанхайской организации сотрудничества. Специализированная организация – Региональная антитеррористическая структура ШОС (РАТС ШОС) имеет главной задачей защиту граждан ШОС от террористических атак преступных группировок. ШОС была основана спустя год после подписания Шанхайской конвенции о противодействии терроризму, сепаратизму и экс-

тремизму согласно соответствующему соглашению от 7 июня 2002 г. Официальное начало работы структуры в Ташкенте состоялось 2 июня 2002 г. Основными органами взаимодействия РАТС ШОС являются Исполнительный комитет и Совет. [2]

В целях борьбы с экстремизмом, сепаратизмом и терроризмом в ШОС приняты следующие положения: 1. Создание и ведение баз данных содержащих информацию о деятельности международных экстремистских, террористических, сепаратистских и организациях. 2. Сотрудничество по подготовке и проведению оперативно-розыскных и прочих мероприятий по борьбе с терроризмом, сепаратизмом и экстремизмом. 3. Взаимодействие по подготовке и проведению контртеррористических учений между странами. 4. Совместное обучение специалистов силовых подразделений ведению контртеррористических действий, а также проведение конференций, направленных на обмен опытом. 5. Сотрудничество с международными организациями, занимающимися борьбой с экстремизмом, терроризмом сепаратизмом. [5]

Странами ШОС проводились различные контртеррористические мероприятия такие как:

1) учения спецслужб и правоохранительных структур.

Совместные учения сотрудников правоохранительных органов «Тяньшань-2», 5-8 мая 2011 г. На территории Китайской Народной Республики отрабатывались действия в условиях массовых беспорядков, был учтен опыт предыдущих событий, происходивших в данном регионе планеты. Участие приняли КНР, Республика Таджикистан, Киргизская республика.

Антитеррористические учения «Восток - Антитеррор-2012», 2-5 июня 2012 г. На территории Узбекистана, Джизакской области прошли тренировки спецподразделений республик Кыргызстана, Казахстана, Узбекистана. Установленной целью была практика уничтожения базы террористов и освобождения заложников, находящихся в одном из зданий.

Антитеррористические учения «Казыгурт - Антитеррор-2013», 13 июня 2013 г.

В Республике Казахстан, городе Шымкент проводились учения правоохранительных органов по пресечению возможных террористических атак в местах массового скопления граждан.

Учения «ЦентрАзия - Антитеррор-2015», 15-17 сентября 2015 г. В Киргизии проводились командно-штабные учения по слаживанию антитеррористических действий стран ШОС. Задачей была отработка действий по пресечению терактов на территории ШОС.

Учения «Тянь-Шань-3 - 2017», 27 июня, 2017 г. На китайско-киргизской границе прошли учения пограничников КНР и Киргизской республики. Совместный координационный штаб управлял операцией по ликвидации условных террористов. Данные учения проводились в 3 этапа.

2) совместные пограничные операции (СПО), проводящиеся на границах стран-членов ШОС. Операция «Восток-2013», 1 апреля – 15 октября, 2013 г. Операция была направлена на пресечение контрабанды наркотиков и организации незаконной миграции. Операция «Восток-2014» 1 мая -31 октября 2014 г. Задачей операции было обеспечение порядка пограничного режима на границе РФ и КНР. Операция «Восток-2015», 15-25 июня, 2015 г. На границе Китая и Киргизии осуществлялась практика пограничных служб двух стран в обеспечении безопасности государственных границ.

3) совместные антитеррористические учения «Мирная миссия».

В таких учениях участвуют вооруженные силы государств - членов ШОС, являются более масштабными чем совместные пограничные операции, о которых упоминалось ранее. Учения «Мирная миссия» проходят в труднодоступных районах с различными видами ландшафтов – горная местность, пустынные территории, а также в условиях городской застройки. Подобные учения отличаются тем, что в них значительно

увеличена численность задействованных подразделений и условия операций являются более тяжелыми, требующими особой слаженности.

Учения «Мирная миссия-2005», 18-25 августа 2005 г. На полуострове Шаньдун осуществлены учения с участием китайских и российских военных, Учения проводились в трех средах: на воде, в воздухе и на суше. Учения «Мирная миссия-2007» 9 августа 2007 г. На территории Синьцзян-Уйгурского автономного района в КНР впервые проведены контртеррористические учения с участием всех стран-участниц на то время. Были отработаны мероприятия по преследованию, захвату и разоружению групп преступников.

Учения «Мирная миссия-2010», 10-25 сентября. На территории Жамбыльской области Казахстана были отработаны навыки взаимодействия в горной местности военнослужащими Китая, России, Таджикистана, Казахстана, Киргизии [3].

Учения «Мирная миссия-2014», 24-29 августа 2014 г. В КНР, провинции Внутренняя Монголия, проводились масштабные учения с применением большого количества боевой техники. По условиям учений граница одного из государств ШОС была нарушена банд формированиями, большая часть была уничтожена авиацией, но часть смогла скрыться в городской черте. На их ликвидацию отправлены спецподразделения вооруженных сил стран-участниц ШОС. «Мирная миссия-2016», 15-21 сентября 2016 г. Учения прошли в Киргизии в ходе которых применялся колоссальный опыт, полученный российскими военными во время операции В Сирийской Арабской Республике. Были отработаны навыки разведки, сопровождения, эвакуации, высадки десанта. [1]

Подобные совместные военные маневры углубляют сотрудничество между Россией, Китаем и другими государствами в сфере обеспечения безопасности. Историческим событием стали учения «Мирная миссия – 2005», две страны впервые отработали совместные действия по высадке морского десанта. В 2007 году участие приняли все страны-член ШОС. Отмечается разная заинтересованность государств в совместных операциях. Например, Россия и Китай не пропустили ни одного такого события, а Узбекистан принял участие лишь однажды. [4]

Таким образом, государства члены СОШ осуществляют тесное взаимодействие по борьбе с проявлениями терроризма и обеспечением безопасности в своих регионах и продолжают наращивать сотрудничество.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Бояренок, К. А. ШОС как модель обеспечения региональной безопасности / К. А. Бояренок // Азиатско-Тихоокеанский регион: история и современность - XV: Материалы научно-практической (заочной) конференции молодых ученых, посвященной 90-летию Бурятского государственного университета имени Доржи Банзарова и 30-летию Восточного института, Улан-Удэ, 10 мая 2022 года / Науч. редактор С.Г. Ошоров. – Улан-Удэ: Бурятский государственный университет имени Доржи Банзарова, 2022. – С. 13-16.

2. Кокошина, З. А. Роль Шанхайской организации сотрудничества в противодействии терроризму и экстремизму на постсоветском пространстве / З. А. Кокошина // Вестник Московского университета. Серия 25: Международные отношения и мировая политика. – 2017. – Т. 9. – № 4. – С. 97-123.

3. Николашвили, Н. Д. Роль Шанхайской организации сотрудничества в борьбе с террористической угрозой на постсоветском пространстве / Н. Д. Николашвили // Постсоветские исследования. – 2020. – Т. 3. – № 8. – С. 633-640.

4. Фань, С. Существующие механизмы Шанхайской организации сотрудничества и проблемы борьбы с нетрадиционными вызовами безопасности / С. Фань // Вестник международных организаций: образование, наука, новая экономика. – 2021. – Т. 16. – № 1. – С. 107-126. – DOI 10.17323/1996-7845-2021-01-05.

5. Ягницын, И. П. Правовая база сотрудничества в сфере безопасности в рамках ШОС / И. П. Ягницын // Россия и Китай: история и перспективы сотрудничества: Материалы IX международной научно-практической конференции, Благовещенск - Хэйхэ, Тяньцзинь, Пекин, 20–28 мая 2019 года / Ответственный редактор Д.В. Кузнецов. – Благовещенск - Хэйхэ, Тяньцзинь, Пекин: Благовещенский государственный педагогический университет, 2019. – С. 176-178.

УДК 343

Захаров Данил Александрович, студент; Комсомольский-на-Амуре государственный университет
Zakharov Danil Alexandrovich, student, Komsomolsk-na-Amure State University
Мусалитина Евгения Александровна, доцент; Комсомольский-на-Амуре государственный университет
Musalitina Evgenia Aleksandrovna, assistant professor, Komsomolsk-na-Amure State University

РОЛЬ КИТАЯ В МИРОВОЙ БОРЬБЕ С КИБЕРТЕРРОРИЗМОМ

THE ROLE OF CHINA IN THE GLOBAL FIGHT AGAINST CYBERTERRORISM

Аннотация. В современных условиях, когда терроризм стал одной из важнейших глобальных проблем человечества, Китай является одним из лидеров по борьбе с этой проблемой. КНР является одним из ключевых участников международных антитеррористических сил и вносит значительный вклад борьбу с международным терроризмом. В статье рассматриваются национальные позиции и принципы Китая по вопросам борьбы с кибертерроризмом. Проводится анализ основных направлений в рамках этой работы: борьбы с терроризмом, с сепаратизмом и экстремизмом.
Abstract. In modern conditions when terrorism has become one of the most important global problems of mankind, China is one of the leaders in fighting this problem. The PRC is one of the key participants in international anti-terrorist forces and makes significant contribution to the fight against international terrorism. The article examines the national positions and principles of China on the issues of fighting cyberterrorism. The analysis of the main directions within the framework of this paper is carried out: the fight against terrorism, separatism and extremism.
Ключевые слова: кибербезопасность, российско-китайское сотрудничество, информационная безопасность, Интернет, Китай.
Key words: cybersecurity, Russian-Chinese cooperation, information security, Internet, China.

В современных условиях, когда терроризм стал одной из важнейших глобальных проблем человечества, Китай является одним из лидеров по борьбе с этой проблемой. КНР является одним из ключевых участников международных антитеррористических сил и вносит значительный вклад борьбу с международным терроризмом.

Кибертерроризм – это относительно новая угроза, влияющая на международный мир и безопасность. Террористические организации используют ресурсы Интернета не только для ведения пропаганды и психологической войны, но также используют Интернет для распространения террористических выступлений и даже планирования терактов [6]. Можно говорить о том, что сфера функционирования кибертерроризма не ограничивается виртуальным киберпространством, а физический реальный мир является главной мишенью его террористических атак. Более того, возможность онлайнового

и офлайнового взаимодействия между членами террористических организаций способствует реализации террористических атак.

Развитие интернет технологий позволяет террористическим организациям делать накопления за счет онлайн-финансирования, что создает проблемы для онлайн-финансового надзора. Что касается онлайн-финансирования, то основные методы, применяемые террористическими организациями, включают публикацию объявлений о сборе средств на своих веб-сайтах, прием онлайн-пожертвований через электронные платежные системы, использование «темной сети» для подпольных транзакций и отмывание денег посредством электронной торговли [4].

В последние два десятилетия предотвращение кибертерроризма и борьба с ним стали целью совместных усилий всех стран. В глобальной модели предотвращения и борьбы с кибертерроризмом Китай придерживается своей национальной позиции и принципов, активно исследует и предлагает нормы, методы управления и модели сотрудничества для предотвращения и борьбы с кибертерроризмом [3].

Террористические организации злоупотребляют научно-техническими достижениями глобализации и информатизации, распространяют насильственно-экстремистские идеи и технологии контроля над насилием через Интернет, что стало одной из самых сложных проблем в сфере международной безопасности. Согласно мировой статистике, большая часть террористической деятельности в современном мире организуется непосредственно в сети.

В марте 2017 года Китай опубликовал «Стратегию международного сотрудничества в киберпространстве», которая определяет участие Китая в международных обменах и сотрудничестве в киберпространстве и заявляет, что он будет «углублять международное сотрудничество в борьбе с кибертерроризмом и киберпреступностью» [1]. Одной из таких мер является расширение партнерства с другими государствами по совместной борьбе с терроризмом, поэтому китайское правительство укрепляет политические обмены и сотрудничество с правоохранительными органами других стран.

Председатель КНР Си Цзиньпин неоднократно заявлял миру о твердой решимости Китая бороться с терроризмом и излагал антитеррористические принципы Китая. Они включают три основные направления: борьба с терроризмом, сепаратизмом и экстремизмом.

В борьбе с кибертерроризмом Китай всегда выступал за соблюдение целей и принципов Устава ООН и за то, чтобы ООН и Совет Безопасности играли центральную координирующую роль в области борьбы с терроризмом. В свою очередь, международная конвенция о борьбе с терроризмом в космосе укрепляет консенсус международного сообщества в отношении борьбы с киберпреступностью и кибертерроризмом [2].

Согласно «Стратегии международного сотрудничества в киберпространстве», обнародованной в 2019 году, указывается, что китайская позиция по этому вопросу направлена на мирное развитие, в основе которого лежит взаимовыгодное сотрудничество, борьба за мир и государственный суверенитет.

Китай делает значительный вклад в международную борьбу с кибертерроризмом, являясь членом Шанхайской организации сотрудничества (далее - ШОС). Одной из главных задач которой стала борьба с терроризмом и поддержание региональной безопасности и стабильности. В целях укрепления сотрудничества правоохранительных органов в сфере киберконтртерроризма ШОС провела три совместных антитеррористических учения в Кита в 2015 г., 2017 г. и 2019 г. Эта серия учений является важной мерой по реализации таких правовых документов, как «Конвенция Шанхайской организации сотрудничества по борьбе с терроризмом» и «Конвенция Шанхайской организации сотрудничества по борьбе с экстремизмом» [5].

Таким образом, Китай постоянно совершенствует меры по борьбе с кибертерроризмом; укрепляет координацию и международное сотрудничество с отделами финан-

совой разведки, правоохранительными органами и разведывательными управлениями; развивает сотрудничество правительства и предприятий и технологических компаний для реализации кибер-антитеррористических операций.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Гао, Ю. Противодействие кибертерроризму в рамках ШОС / Ю. Гао // Вопросы политологии. – 2021. – Т. 11. – № 12(76). – С. 3700-3705. – DOI 10.35775/PSI.2021.76.12.035.

2 Костенко, Н. И. Право международной информационной безопасности (становление, тенденции и проблемы развития) / Н. И. Костенко. – Москва : Издательство "Юрлитинформ", 2019. – 464 с.

3 Саунина, Е. В. Международный опыт правового регулирования противодействия информационному терроризму / Е. В. Саунина, И. Д. Бажина // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2022. – № 1. – С. 108-115. – DOI 10.52452/19931778_2022_1_108.

4 Хань, Ш. Сотрудничество Китая и России в области кибербезопасности / Ш. Хань // Азия и Африка сегодня. – 2022. – № 8. – С. 66-72. – DOI 10.31857/S032150750019782-2.

5 Cheng, Ch. Analysis of BRICS Network Security Governance /Ch. Cheng //. Network Security Technology & Application. Beijing. – 2021. – Issue 4. Pp. 166-168.

6 Lang, P. Greatly Changing International Structure and the Major Power Relationship in the Governance of Cyberspace / P. Lang // Global Media Journal. Beijing. – 2020. – Vol. 7. – Issue 1. – Pp. 70-85.

УДК 32

Контемирова Алиса Константиновна, студент, Благовещенский государственный педагогический университет.
Kontemirova Alisa Konstantinovna, student, Blagoveshchensk State Pedagogical University.

СПЕЦИФИКА ЛЕВОГО ПОЛИТИЧЕСКОГО ЭКСТРЕМИЗМА В РОССИИ НА РУБЕЖЕ XX-XXI ВЕКОВ

THE SPECIFICS OF LEFT-WING POLITICAL EXTREMISM IN RUSSIA AT THE TURN OF THE XX-XXI CENTURIES

Аннотация. В статье рассматривается левый политический экстремизм в Российской Федерации на рубеже XX-XXI веков в качестве социально-политического явления на примере нескольких группировок. И в процессе исследования были установлены особенности изучаемых левых экстремистских организаций и, в целом, определена специфика данного явления.
Abstract. The article examines left-wing political extremism in the Russian Federation at the turn of the XX-XXI centuries as a socio-political phenomenon on the example of several groups. And in the course of the study, the features of the studied left-wing extremist organizations were established and, in general, the specifics of this phenomenon were determined.
Ключевые слова: экстремизм, левые, политика, Россия, экстремистские группировки.
Key words: extremism, leftists, politics, Russia, extremist groups.

На рубеже XX-XXI вв. Россия находилась в упадке – последствия государственного переворота в начале 1990-х гг., невыгодные и безнадежные реформы от новых по-

литических деятелей, которые встали во главе страны, военные кампании на Кавказе, идеологический кризис. Всё это повлекло за собой недовольство масс, недоверие властям и разнообразные народные возмущения. Кроме того, в подобных политических условиях важное место заняла доктрина политического экстремизма. Причина тому ясна – политический экстремизм имеет свойство проявляться в период непростых, контрадикторных изменений во всех сферах социума.

Если обратиться к определению политического экстремизма, то в научной литературе такого понятия не найдётся, поскольку данный термин трактуется различными учёными и публицистами неоднозначно. Так, например, согласно мнению В.Н. Давыдова, политический экстремизм – это некоторый метод борьбы, что отрицает сотрудничество в любом его проявлении с политическими оппонентами [1, С. 22]. Также существует такая точка зрения, согласно которой политический экстремизм представляет собой модификацию ультралевых и ультраправых политических движений [2, С. 241].

Тем не менее, на государственном уровне в Российской Федерации также предпринимались дать толкование термину «политический экстремизм», законно обосновать меры и формы по противодействию ему. В 1999 г. в Государственную Думу России был внесен законопроект «О противодействии политическому экстремизму» (был отклонён в первом чтении). В данном законопроекте понятие политического экстремизма звучит следующим образом: «Политический экстремизм - это деятельность общественных объединений, иных организаций, должностных лиц и граждан, направленная на насильственное изменение конституционного строя Российской Федерации, насильственный захват власти или насильственное удержание власти, нарушение суверенитета и территориальной целостности Российской Федерации, организацию незаконных вооруженных формирований, возбуждение национальной, расовой или религиозной вражды, а также публичные призывы к совершению в политических целях противоправных деяний» [3].

Также существует мнение, что определение политического экстремизма не должно касаться юридической сферы общества. Такие определения должны толковаться в социологии и политологии в то время, как на законодательном уровне будет достаточно лишь того, что многие экстремистские группировки будут запрещены и при необходимости будут применяться узаконенные методы противодействия деятельности подобных объединений [4, С. 5]

Таким образом, по нашему мнению, понятие политического экстремизма – крайне сложное явление, которое отличается своей многоаспектностью. Но всё в итоге сводится к первопричине возникновения политического экстремизма. Речь здесь идет непосредственно об экономическом, политическом и социальном кризисе и о противоречиях идеологического характера. Всё это имеет следующие последствия: народное недовольство, протесты, что впоследствии перерастает в проявления политического экстремизма.

Как уже говорилось авторами ранее, политический экстремизм – это далеко не тривиальное явление, которое содержит в себе определённую структуру. В ходе исследования авторами была рассмотрена классификация по идеологическому признаку.

Существуют такие виды политического экстремизма, как правый и левый [5, С. 38]. В рамках нашего исследования, обратимся к последнему.

Так, левый политический экстремизм есть тентатива установления общественного правопорядка радикальными методами. В левом политическом экстремизме доктрина социальной справедливости зиждется на представлениях о свободном, эгалитарном обществе, которое должно быть построено любым способом [6, С. 34].

Что касается России, то здесь левый политический экстремизм стал развиваться с XIX века, а конкретно с января 1878 г. Это связано с началом работы террористической организации «Народная воля», участники которой планировали совершить пере-

ворот и установить народовластие под социалистическими лозунгами [7, С. 170]. С этого момента, на наш взгляд, развитие левого политического экстремизма набирало обороты, что остро проявляется в период Гражданской войны, когда экстремистские группировки (анархисты, эсеры) активно боролись за власть. Следующий яркий всплеск активности левоэкстремистских группировок в России произошёл уже в 1990-е гг.

Рассматривая наиболее активные экстремистские организации левого толка, что действовали в России на смене XX-XXI вв., следует отметить, во-первых, «Новую революционную альтернативу» (НРА), во-вторых, «Революционный коммунистический союз молодёжи» (РКСМ) и, в-третьих, «Национал-большевистскую партия» (НБП) [8, С. 109].

В 1996 г. была образована «Новая Революционная Альтернатива» (НРА). В данной группировке состояли представители анархистских организаций (Ассоциация Движений Анархистов, Конфедерация Анархо-Синдикалистов). Идеология НРА базировалась на социалистической революционной доктрине и была пронизана анархическими постулатами из-за своего состава [9, С. 167-169]. В целом, НРА – это организация, которая способна выразить сопротивление антинародной политике правящего режима. При этом в борьбе могут быть использованы даже теракты [10]. Итак, Новая Революционная Альтернатива – это одна из крупнейших левоэкстремистских организаций, что была создана в конце XX в., однако свою деятельность не прекратила и в начале XXI в., но уже к 2003 г. почти все активисты данной группировки, в том числе их лидер Александр Бирюков, были заключены под стражу, и организация прекратила открытые попытки экстремистской деятельности.

Чуть ранее была основана ещё одна крупная организация – «Революционный коммунистический союз молодёжи» (РКСМ). Данное движение во главе с Игорем Маляровым изначально пыталось вписаться в государственную систему, были попытки сотрудничества с ещё активной на тот момент Коммунистической партией Российской Федерации. Разумеется, всё это вызвало недовольство у радикально настроенных рядовых членов РКСМ. Вследствие этого внутри организации развивался конфликт, который обострился, поскольку руководство РКСМ поддержало мошенническую финансовую пирамиду, создатель которой впоследствии всеми средствами стремился дискредитировать Российский комсомол. Однако несмотря на внутренние конфликты, активисты всё равно осуществляли политическую деятельность: выходили на пикетирование Госдумы в мае 1998 г., развивали профсоюзную деятельность и пытались сотрудничать рабочим движением, участвовали в забастовках на предприятиях в начале 2000-х гг. [9, С. 172-173]. По нашему мнению, данная молодёжная организация не пошла по пути открытого политического экстремизма, но тем не менее, её члены и по сей день, активно функционируют, отстаивают коммунистическую идеологию, всё также проводя агитацию путём распространения листовок, пикетирований и работы на предприятиях.

Рассматривая ещё одну организацию леворадикального характера – «Национал-большевистскую партию» – стоит отметить, что она, в отличие от всех выше нами перечисленных, пошла по пути радикального и открытого политического экстремизма. Партия не обладает четкой идеологией (что проявляется даже в её названии). Постулаты данной организации звучат следующим образом: социальные гарантии в интересах масс, отмена привилегий для бюрократии. Кроме того, НБП стоит на позиции гражданского общества [11, С. 188-189]. И, по нашему мнению, эту партию стоит относить к леворадикальным. Спектр деяний экстремистского характера у данной организации весьма широк. Так, в 2001 г. лидер партии Эдуард Лимонов был арестован за незаконное приобретение оружия; в 2003 г. члены Национал-большевистской партии ворвались в здание Министерства Юстиции с требованием зарегистрировать их партию на государственном уровне; в следующем 2004 г. активисты-лимоновцы проводили акцию протеста у здания Минздрава. Подобные действия повлекли за собой логичный результат – в 2007 году

«Национал-большевистская партия» в ходе судебного процесса была признана экстремистской и запрещена на территории Российской Федерации [9, С. 251].

Исходя из вышесказанного, следует, что левый политический экстремизм в России на рубеже второго тысячелетия развивался в разных направлениях. Во многих организациях, в том числе и в тех, что мы анализировали ранее, происходили внутренние конфликты, крупные движения распадались на более мелкие группировки. Другие же консолидировались в рамках государства и встроились в политическую систему страны. Есть также и те организации, которые до последнего борются с режимом, стремясь изменить общественный строй и государственный режим. Отсюда проистекает сама специфика левого политического экстремизма в России, начиная с конца XX-начала XXI вв. Все организации такого характера крайне неустойчивы, разрознены. У них нет четкой структуры, программы, иерархии, что тоже крайне важно в любой организации. Но невзирая на все эти факторы, левые экстремистские группировки не исчерпают себя. Напротив, даже на современном этапе, для их появления существуют, по нашему мнению, благоприятные условия. Здесь речь идёт, в первую очередь, о нарастающей социальной несправедливости. Возвращение на капиталистические рельсы, частная собственность на средства производства, кризис как внутри страны, так и в мировом масштабе – всё это дает толчок к появлению левых радикальных группировок экстремистской направленности. По этой причине есть риск, что доктрины левого политического экстремизма могут заинтересовать большое количество людей. И, таким образом, левоэкстремистские организации станут представлять общественную опасность в больших масштабах, но так или иначе, усилиями правительства и госструктур есть возможность сокращения роста и развития деятельности левых политических экстремистских организаций.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Давыдов, В. Н. Военно-политические черты международного терроризма / В.Н. Давыдов, Су Минь. // Вестник Российского университета дружбы народов. – 2006. – № 1 (6). – С. 21-36.

2. Пиджаков, А. Ю. Борьба с политическим экстремизмом и терроризмом: проблемы изучения / А.Ю. Пиджаков. // Правоведение. – 2003. – № 3. – С. 234-244.

3. Проект федерального закона «О противодействии политическому экстремизму» № 99058804-2, внесенный Правительством Российской Федерации 8 июня 1999 года и отозванный им же 19 мая 2002 года (Документ официально не был опубликован). [Электронный ресурс]. – Режим доступа: https://sozd.duma.gov.ru/bill/99058804-2. – Дата обращения: 24.10.2022.

4. Краснов, М.П. Политический экстремизм – угроза государственности / М. Краснов. // Российская юстиция. – 1999. – № 4. – С. 4-7.

5. Ямалитдинов, А.А. Экстремизм: его разновидности и формы / А.А. Ямалитдинов // Вестник Уфимского юридического института МВД России. – 2016. – № 4. – С. 37-40.

6. Витюк, В.В. Левый экстремизм и идеал социальной справедливости / В.В. Витюк, С.А. Эфиров // Социальная справедливость и пути ее реализации в социальной политике. Сборник трудов в 2-х книгах. – М.: АН СССР, Институт социологических исследований, 1982. – Кн.2. – 342 с.

7. Революционное народничество 70-х годов XIX века : в 2 томах / С.Н. Валк [и др.]. – М. : Академия наук СССР, 1965. Т.2. – 472 с.

8. Арчаков, М.К. К вопросу о появлении и деятельности леворадикальных общественных организаций / М.К. Арчаков // Вестник Саратовского университета. – 2010. – № 1. – С. 108-111.

9. Арчаков, М.К. Политический экстремизм: сущность, проявления, меры противодействия / М.К. Арчаков. – М. : Юрайт, 2022. – 295 с.
10. ДЕЛО «НОВОЙ РЕВОЛЮЦИОННОЙ АЛЬТЕРНАТИВЫ» [Электронный ресурс]. – Режим доступа: http://left.ru/2001/7/nra20.html. – Дата обращения: 25.10.2022.
11. Савельев, В.А. Горячая молодежь России : Лидеры. Организации и движения. / В.А. Савельев. – М. : Кванта, 2006. – 287 с.

УДК 327

Курило Олеся Евгеньевна, студентка, Комсомольский-на-Амуре государственный университет
Kurilo Olesya Evgenievna, student, Komsomolsk-na-Amure State University
Лопатина Ольга Ивановна, старший преподаватель, Комсомольский-на-Амуре государственный университет
Lopatina Olga Ivanovna, senior lecturer, Komsomolsk-on-Amur State University

ФАКТОРЫ, ВЛИЯЮЩИЕ НА ВОЗНИКНОВЕНИЕ ТЕРРОРИСТИЧЕСКОЙ УГРОЗЫ

FACTORS INFLUENCING THE EMERGENCE OF THE TERRORIST THREAT

Аннотация. В данной статьи рассмотрено понятие терроризма, проанализированы факторы, влияющие на повышение террористической угрозы в стране, такие как: мультикультурность, сепаратистские движения, а также сделаны попытки описать способы влияние террористов на население с целью склонить на свою сторону.
Abstract. This article examines the concept of terrorism, analyzes factors influencing the rise of the terrorist threat in the country, such as multiculturalism, separatist movements, and attempts to describe the ways in which terrorists influence the population in order to persuade them to take their side.
Ключевые слова. Угроза безопасности, террористическая угроза, мультикультурность.
Key words. Security threat, terrorist threat, multiculturalism.

XXI век – век глобализации. Происходит активное смешение культур, неизбежно вызывая столкновение радикально отличающихся взглядов. Возникают противоречия и конфликты, многие из которых можно уладить словесно и мирно. Однако существует ряд конфликтов настолько серьёзных, что их решение давно вышло за рамки переговоров и попало в руки преступников. Так, начинает проявлять себя терроризм, являющийся одной из наиболее острых проблем всего современного мира.

Терроризм (с лат. «страх», «ужас») – это совокупность чрезвычайных мер, применяемых террористами для устрашения населения и властей. Чаще всего терроризм применяется для влияния на политическую ситуацию, террористы ставят перед государственными деятелями выбор: или выполнение высказанных ими требований, или смерть как невинных граждан, так и влиятельных лиц. Как справедливо отметил В. М. Кулагин, автор книг о современной международной безопасности, «террористы целенаправленно нарушают традиционные и широко принятые в международной практике правила ... запрещающие, в частности, взятие заложников ... нападение на дипломатов и дипломатические учреждения, гражданское население». Нападение на население является главной причиной, по которой терроризм волнует современный мир. Террористы не преследуют целей ослабления военной мощи страны путём нападения на вооружённые силы и военные объекты. Их целью является распространение на территории стра-

ны паники, ощущения беззащитности и кризиса, негативных по отношению к властям настроений.

Российская Федерация является одним из государств с повышенным риском возникновения случаев терроризма, и россияне осознают это. Более 70% граждан опасается того, что могут произойти новые теракты, при этом многие боятся, что они сами или их близкие станут их жертвами. В России запрещено более 90 общественных объединений и религиозных организаций, чьи взгляды и деятельность подразумевают или могут подразумевать совершение терактов.

Несмотря на повышенный уровень террористической активности, Россия находится на 44-м месте в рейтинге стран мира по уровню терроризма, составленном на основе исследования Global Terrorism Index. На первом месте стоит Афганистан, за ним – Ирак и Сомали. Страны Европы также сильно подвержены террористическим атакам, что заставляет нации объединяться в поисках устранения общей угрозы.

Ещё одна причина особой опасности политики терроризма заключается в том, что она активно находит сторонников. Террористические организации владеют определёнными приёмами так называемой «промывки мозгов», при помощи которых они внушают населению свои радикальные идеи. Политические необразованные и подверженные чужому влиянию люди поддаются психологическим махинациям террористов и позже используются в качестве оружия: они добровольно совершают теракты, нередко сами погибая в процессе, выполняя роль смертников, тоже добровольно.

По этой причине одним из главнейших шагов на пути победы над терроризмом является просвещение населения, демонстрация кровожадной сути терроризма и его последствий. Особенно важно просвещать пользователей Интернета, так как именно там современные террористические организации часто находят новых последователей, обычно выбирая молодых людей.

Кроме этого, в каждом государстве должна быть детально разработана система противодействия терроризму – деятельности органов государственной власти и органов местного самоуправления, а также физических и юридических лиц по предупреждению терроризма, выявлению и последующему устранению причин и условий, способствующих совершению терактов, минимизации и ликвидации последствий проявлений терроризма.

Для борьбы с терроризмом международные институты. Среди них выделяются следующие: Контртеррористический комитет СБ ООН, Комитет СБ ООН по санкциям в отношении движения «Талибан», «Аль-Каиды» и «Исламского государства», Целевая группа ООН по осуществлению контртеррористических мероприятий, аппарат Координатора ЕС по борьбе с терроризмом, Международный банк данных по противодействию терроризму и другие.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 spbu.tu: файл PDF: сайт. – URL: https://spbu.ru/sites/default/files/terrorizm_kak_ugroza_globalnoy_regionalnoy_i_nacionalnyo_bezopasnosti.pdf (дата обращения 21.10.2022). – Режим доступа: открытый.

2 CYBERLENINKA: блог: сайт. – URL: https://cyberleninka.ru/article/n/terrorizm-kak-ugroza-mezhdunarodnoy-bezopasnosti-v-globaliziruyuschemsya-mire/viewer (дата обращения 21.10.2022). – Режим доступа открытый.

3 gtmarket.ru : блог : сайт. – URL: https://gtmarket.ru/ratings/global-terrorism-index (дата обращения 21.10.2022). – Режим доступа открытый.

УДК 364.08

Лисоводская Валерия Витальевна, студент, Комсомольский-на-Амуре государственный университет
Lisovodskaya Valeria Vitalievna, student, Komsomolsk-na-Amure State University
Шинкорук Марина Владимировна, кандидат педагогических наук, доцент, Комсомольский-на-Амуре государственный университет
Shinkaruk Marina, Ph.D. in Pedagogy, Associate Professor, Komsomolsk-na-Amure State University

БЕЗОПАСНОСТЬ КАК СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЙ ФЕНОМЕН

SECURITY AS A SOCIO-PSYCHOLOGICAL PHENOMENON

Аннотация. В статье рассматривается понятие «безопасность» в социально – психологическом контексте. Представлен анализ современных исследований понятия «безопасность». Обращается внимание на новые смыслы безопасности, динамику безопасности в области представлений и значимости для личности и общества, выделены состояния безопасности как социально-психологического феномена.
Abstract. The article discusses the concept of "security" in a socio –psychological context. The analysis of modern research on the concept of "security" is presented. Attention is drawn to the new meanings of security, the dynamics of security in the field of representations and significance for the individual and society, states of security as a socio-psychological phenomenon are highlighted.
Ключевые слова: безопасность, угроза, социальная безопасность, психологическая безопасность, социально психологическая безопасность.
Key words: security, threat, social security, psychological security, socio-psychological security.

В современной социокультурной ситуации вопрос о безопасности личности и безопасности общества ставится достаточно остро в связи с возрастанием количества явлений, процессов и событий, представляющих угрозу для человека и человечества. Спектр угроз весьма разнообразен, он касается как физической [6], информационной безопасности личности, так и психологической, социальной. Безопасность граждан Российской Федерации гарантируется на уровне законодательства Федеральным законом «О безопасности» от 28.12.2010 г. № 390-ФЗ [4], однако его полное обеспечение и контроль не всегда становится возможным. Прежде всего, достаточно сложно поддается контролированию психологическая безопасность личности, что обусловлено сложностью и многоуровневостью функционирования психического в целом, и, в частности с особенностями психологического здоровья личности, которые выражаются в позитивном самосознании, в социальном благополучии, в отсутствии эмоционального вреда в условиях социума.

Актуальность проблемы социально психологической безопасности личности выражается в следующих основаниях:

1 Деформация потребностей в социальной безопасности. Это связано со стремительным развитием общества, потребностями, которые испытывает человек, что в результате вытекает в понижение уровня удовлетворенностью настоящим и страхом будущего.

2 Общественная неопределенность, отсутствие уверенности и социальная нестабильность значительно понижают уровень социального настроения, тем самым выставляя «безопасность», как феномен, требующий развития в области переосмысления понятия «психологическая безопасность» [1]. Данные основания обусловливают цель

нашего исследования - выявление социально-психологических смыслов категории «безопасность», изменяющих устоявшееся понятие безопасности личности.

Безопасность в психологическом смысле это, прежде всего внутреннее состояние защищенности человека. Ее можно трактовать в плане субъективного подхода, который отражает совокупность индивидуально психологических, духовно нравственных особенностей личности на макроуровне, и отношение к миру и к себе на микроуровне, где объектом воздействия является сознание, психика. Данный подход рассматривали Антипов Г. А., Донских О. А [3], в качестве условия безопасности они выдвинули наличие опыта субъекта, который выражается в психологической готовности противостоять опасностям.

Психологическая безопасность носит интегративный характер, что позволяет рассматривать ее как процесс. Интеграция в данном подходе заключается в разделении безопасности по уровням. К таковым относятся: безопасность на уровне обществе, на уровне локальной среды и на уровне личности. Такое разделение предоставляет возможность взглянуть на безопасность, как на состояние, обеспечения базовой защищенности личности и общества, а так же как на свойство личности, способной противостоять негативным воздействиям [2].

Таким образом, безопасность как психологический феномен можно рассматривать как способность человека или среды отражать неблагоприятные внешние воздействия.

Безопасность в социальном смысле представляет собой состояние, характеризующееся отсутствием угроз интересам личности и общества. Ее можно рассматривать в рамках: объективного подхода, который трактует социальную безопасность как состояние защищенности кого или чего либо; факторного подхода, предполагающего состояние защищенности личности от внутренних и внешних угроз, которые возникают в процессе жизнедеятельности; функционального подхода, определяющего факторы того, в чем заключается безопасность, что является угрозой для человека [5]. Данные основания позволяют сформулировать следующие особенности социальной безопасности личности:

1 Многоаспектность, выражающаяся в широком понимании социальной безопасности, которая может трактоваться как: совокупность условий, форма отношений, вид защитных средств.

2 Противоречивость, отражающее отношения субъектов, которое выражается в игнорировании интересов других групп, личностей.

3 Двойственность, которая включает в себя одновременно как объект безопасности, так и субъект. В качестве объекта социальной безопасности выступает личность или общество, которое нуждается в благоприятном воздействии, а субъектом выступает система, обладающая человеческими качествами, направленными на защиту личности.

Таким образом, безопасность как социально - психологический феномен имеет отражения в следующих состояниях:

- в свойствах субъекта;
- в свойствах объекта;
- в требованиях среды;
- в жизненных событиях;
- в условиях жизнедеятельности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Бухаров Д. С. Теоритический анализ подходов понятия «психологической безопасности», как фактора психологической безопасности личности в современной психологической литературе / Д. С. Бухаров // Статья в сборнике статей. – 2020. С. 73-76.

2 Данакин Н. С. Логико – методологический анализ понятия «социальная безопасность» / Н. С. Данакин // Статья в сборнике трудов конференции. – 2018. С. 233-239.

3 Молокоедов, Андрей Владимирович. Психологическая безопасность личности [Текст] : основы комплексного анализа / А. В. Молокоедов, И. М. Слободчиков, С. В. Франц. - Москва : Левъ, 2017. - 173 с.

4 «О безопасности» : «Федеральный закон» от 28.12.2010 г. № 390-ФЗ. Доступ из справочно- правовой системы «КонсультантПлюс». – Режим доступа: по подписке.

5 Павлов, М. Ю. Оценка пожарной опасности и противопожарная профилактика в местах массового скопления людей / М. Ю. Павлов, Н. В. Муллер // Научно - техническое творчество аспирантов и студентов : материалы всероссийской научно – технической конференции студентов и аспирантов, Комсомольск-на-Амуре, 09–20 апреля 2018 г. – Комсомольск – на – Амуре : ФГБОУ ВО «КнАГУ», 2018. – Ч. 2. – С. 394-397.

6 Смык Ю. В. Доверие в структуре психологической безопасности личности / Ю. В. Смык // Научная статья. – 2019. № 1 С. 6

УДК 340

Лиханов Руслан Владимирович, студент; Комсомольский-на-Амуре лесопромышленный техникум
Lihanov Ruslan Vladimirovich, student, Komsomolsk-na-Amure Forestry College
Хомякова Екатерина Вячеславовна, преподаватель; Комсомольский-на-Амуре лесопромышленный техникум
Khomyakova Ekaterina Vyacheslavovna, lecturer, Komsomolsk-na-Amure Forestry College

ТРАНСФОРМАЦИЯ ПОНИМАНИЯ БЕЗОПАСНОСТИ В КОНТЕКСТЕ СОВРЕМЕННЫХ СОЦИАЛЬНЫХ УСЛОВИЙ

TRANSFORMATION OF THE UNDERSTANDING OF SECURITY IN THE CONTEXT OF MODERN SOCIAL CONDITIONS

Аннотация. В статье рассматривается «понятие безопасность» и его трансформация и расширение значения в эпоху глобализации. Длительная эволюция человека позволила нам не только приспособиться к природной окружающей среде, но и преобразовать ее. Не стоит забывать, что адаптационные возможности человека не безграничны. Однако даже измененная нами окружающая среда, казалось бы, столь комфортная для человечества, не может быть абсолютно безопасной. И речь идет не только о «физической безопасности» от внешней угрозы, она по-прежнему актуальна. В стремлении к индивидуализации современный человек все меньше чувствует «внутреннюю безопасность», которая тесно соприкасается со всеми сферами его жизни. В работе анализируются основные сферы жизнедеятельности человека с точки зрения безопасности.

Abstract. The article deals with the «concept of security» and its transformation and expansion of meaning in the era of globalization. The long evolution of man has allowed us not only to adapt to the natural environment, but also to transform it. Do not forget that the adaptive capabilities of a person are not unlimited. However, even the environment that we have changed, which would seem so comfortable for humanity, cannot be absolutely safe. And this is not only about «physical security» from an external threat, it is still relevant. In the pursuit of individualization, modern man feels less and less «internal security» which is closely related to all spheres of his life. The paper analyzes the main areas of human life from the point of view of security.

Ключевые слова: безопасность, глобализация, адаптация, сферы жизнедеятельности.
Key words: security, globalization, adaptation, spheres of life.

Понятие безопасности является исходным и первостепенным для нормальной полноценной жизни человека. Безопасность - состояние защищённости жизненно важных интересов личности, общества, государства от внутренних и внешних угроз, либо способность предмета, явления или процесса сохраняться при разрушающих воздействиях[2].

Принято считать, что людей и животных объединяет две первичные потребности - физиологическая и потребность в безопасности, так как они связаны с сохранением нас и животных как вида. И если изначально речь шла скорее о физической безопасности, то сейчас к ней добавились экономическая, социальная, психологическая, информационная и др. подвиды данного понятия. Социолог А. Маслоу писал о том, что потребность в безопасности включает в себя стабильность, защиту, свободу от страха, от хаоса, потребность в структуре, порядке, законе, ограничениях[5]. В эпоху глобализации, с развитием новых технологий, поле значений для этого состояния разрастается, приобретает новые смыслы.

В условиях современного общества и данного исторического периода, вопросы, которые касаются безопасности человека, обострились и приняли черты проблемы выживания человека в социуме. И если раньше первобытный человек в среде соплеменников чувствовал коллективную поддержку и защиту, то сейчас на пути к тотальной индивидуализации, человек может рассчитывать скорее только на себя. С одной стороны, новые технологии, вещи и системы упростили нашу жизнь, стали ее важной составляющей, тем не менее, закрывшись в своем доме, человек не чувствует себя в полной безопасности. Это и есть обратная сторона бешеного ритма истории и бурного развития технологий, последних нескольких десятилетий. Постоянно происходят изменения, которые отдельно взятый человек не может контролировать. Меняется политическая картина и экономика в целом. С развитием технологий многие специальности становятся ненужными, в связи с этим увеличивается рост безработицы и появляется страх в завтрашнем дне. Экономическая безопасность - это ряд показателей, без которых, человек не сможет нормально существовать: возможность благоустроить жилище, прокормить, одеть, вылечить при необходимости себя и свою семью. Качество жизни во многом зависит от стабильного экономического положения. Лишение заработка и любого другого дохода приравнивается к обездоленному существованию, привычный образ жизни радикальным образом меняется. Появляется страх невозможности обеспечить себя и свою семью. Современный человек много работает, так как вся мировая экономика ориентирована на глобальное потребление. Люди скупают не только необходимое, но и «престижное», порой загоняя себя в рамки крупных долговых обязательств, испытывая страх неуверенности перед обществом. При этом экология ухудшается, в мировом пространстве быстро распространяются массовые заболевания (например, ВИЧ, КОВИД и др), от которых становится невозможным укрыться, на фоне всего этого продолжается рост преступности, наркомании, терактов.

Борьба за исчерпаемые ресурсы и сферы влияния может полностью изменить политическую картину мира в ближайшие десятилетия, поэтому человечество находится в напряженном ожидании войн и возможном переделе мира. Невозможно скрыться от «глобализации» - процесса всемирной, экономической, политической, культурной и религиозной интеграции и унификации [1]. Сложность нового глобального вызова связана с необходимостью коренной переоценки самих представлений о природе человека [6] . Ведь, казалось бы, с улучшенными новыми технологиями и научными открытиями, общество должно стать более развитым в культурном, духовном смысле, но картина противоположна. Доступ к любой информации не сделал всех гениальными и процент таких людей не изменился в сравнении с другими историческими периодами.

С начала 2000-х дети ушли с улиц и сели за компьютеры, многие родители подумали, что теперь чадо в безопасности, однако психологи уже доказали, что игры и выдуманный мир таит гораздо больше опасностей, чем реальный. Отсутствие социализации у детей приводит к тому, что они ведут себя очень неуверенно в малознакомой среде, испытывая чувство страха из-за малого опыта выстраивания взаимоотношений. Испытывая чувство опасности во внешнем мире, они все сильнее погружаются в виртуальный мир, где они смелые и значимые. Таким образом, уже с малых лет современный человек взращивает в себе повышенное чувство тревоги и искаженное чувство безопасности, пытаясь компенсировать состояние разного рода зависимостями (играя в компьютерные игры, заедая стресс, употребляя алкоголь, и т. д. Наряду со средой реальных социальных отношений формируется параллельная цифровая реальность, вне которой сложно представить функционирование современной экономики, политики и социокультурной сферы [4]

Отсутствие личной безопасности человека в информационном пространстве также становится проблемой. Теоритически в законодательном плане личная жизнь человека находится под защитой государства. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. [3]. Однако данные о личной жизни с легкостью попадают в информационное поле, долго не могут из него выйти (часто происходит с известными, знаменитыми людьми), и наносят человеку ущерб, иногда даже не сопоставимый с материальным. Несмотря на явные нарушения конституционного права, призвать к ответу бывает некого, так как найти злоумышленника в информационной среде достаточно сложно.

Таким образом, для современного человека физическая безопасность (жизнь и здоровья) тесно связана с экономической безопасностью (работа, финансовое благополучие), с политической безопасностью (отсутствием войн и жесткой политики внутри государства) и также с социальной безопасностью (развития нравственности в обществе, сохранения личного пространства). И чтобы человек чувствовал себя по-настоящему в безопасности ему нужно найти баланс во всех жизненных сферах.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Глебов, Г. И. Современные международные отношения. Учебное пособие. //Пенза: Изд. Пензенского государственного университетата, – 2010. – С 98.

2 Гражданская защита: Энциклопедия в 4-х томах. – Т. I.,// М. – ФГБУ ВНИИ ГОЧС (ФЦ). – 2015. – С. 125.

3 Конституция Российской Федерации //Литера – 2021. – С. 7., ст 23-24

4 Кузнецов, П.Д. Цифровизации экономики России: институциональные драйверы // Теория и практика общественного развития – 2019 №4, – С. 75

5 Маслоу, А. Мотивация и личность // Питер – 2019 – С. 36.

6 Лебедев, И.Ю. Глобальные проблемы человечества: социально-философский взгляд // Теории и проблемы политических исследований – 2016. – С. 63.

УДК 327

Лихтин Семен Владимирович, студент; Комсомольский-на-Амуре государственный университет
Lihtin Semen Vladimirovich, student, Komsomolsk-na-Amure State University
Мусалитина Евгения Александровна, доцент, Комсомольский-на-Амуре государственный университет
Musalitina Evgenia Aleksandrovna, Associate Professor, Komsomolsk-na-Amure State University

К ВОПРОСУ О РАЗВИТИИ РОССИЙСКО-КИТАЙСКОГО СТРАТЕГИЧЕСКОГО СОТРУДНИЧЕСТВА В СФЕРЕ БЕЗОПАСНОСТИ

ON THE DEVELOPMENT OF RUSSIAN-CHINESE STRATEGIC COOPERATION IN THE SPHERE OF SECURITY

Аннотация. Развитие отношений в сфере безопасности и борьбы с терроризмом стало одним из ключевых вопросов двустороннего сотрудничества России и Китая в последнее время. Россия и Китай объединены общими целями по поддержанию мира, суверенности, обеспечению защиты от террористических угроз. В статье анализируются направления двусторонней работы правительства России и Китая по вопросам международной безопасности в современных геополитических условиях. Рассматриваются результаты встречи Н. Патрушева и Ян Цзечи по проблеме стратегического сотрудничества в сфере безопасности.
Abstract. The development of relations in the field of security and the fight against terrorism has become one of the key issues in two-sided cooperation between Russia and China recently. Russia and China are united by common goals of maintaining peace, sovereignty and providing protection against terrorist threats to the citizens of their states.
The article analyzes the directions of two-sided work of the government of Russia and China on international security issues in modern geopolitical conditions. The results of the meeting between N. Patrushev and Yang Jiechi on the issue of strategic cooperation in the field of security are considered.
Ключевые слова: международная безопасность, российско-китайское сотрудничество, саммит ШОС, стратегическое партнерство.
Key words: international security, Russian-Chinese cooperation, SCO summit, strategic partnership.

Развитие отношений в сфере безопасности и борьбы с терроризмом стало одним из ключевых вопросов двустороннего сотрудничества России и Китая в последнее время. Россия и Китай объединены общими целями по поддержанию мира, суверенности, обеспечению защиты от террористических угроз гражданам своих государств.

В рамках взаимодействия в сфере безопасности 19 сентября 2022 г. Секретарь Совета безопасности РФ Н. Патрушев и Ян Цзечи, директор аппарата Комиссии по иностранным делам ЦК КПК провели 17-й раунд российско-китайских консультаций по вопросам стратегической безопасности [5].

На повестке были вопросы углубления взаимодействия по международной безопасности, международных отношений и координации в многостороннем формате. В результате Стороны договорились в дальнейшем эффективно использовать важную платформу механизма консультаций по стратегической безопасности, реализовывать консенсус, достигнутый главами России и Китая в ходе Самаркандского саммита ШОС; укреплять взаимное доверие, поддерживать друг друга в принятии пути развития, который соответствует их национальным условиям; и совместно поддерживать глобальную страте-

гическую стабильность; продолжать консолидировать и обогащать смысл всеобъемлющего стратегического партнерства координации между двумя странами [3].

Ян Цзечи заявил, что скоординированные действия глав государств является фундаментальной гарантией стабильности и долгосрочной жизнеспособности двусторонних отношений. В последние годы под стратегическим руководством председателя КНР Си Цзиньпина и президента России В. В. Путина китайско-российские отношения сохраняют стабильный курс развития. Две страны продолжают углублять стратегическую координацию, твердо поддерживают друг друга в вопросах, касающихся основных внутригосударственных интересов и основных внешних проблем, обогащают коннотацию сотрудничества в различных областях, совместно защищают международный порядок, основанный на международном праве [1].

Российско-китайское сотрудничество подало международному сообществу пример нового типа отношений между крупными странами, характеризующихся взаимным уважением, мирным сосуществованием и взаимовыгодным взаимодействием [6].

Ян Цзечи отметил, что главы двух государств недавно провели вторую в этом году личную встречу в Самарканде. По результатам чего Китайская сторона заявила, что готова сотрудничать с российской стороной для полной реализации консенсуса, достигнутого главами двух государств; дальнейшего углубления политического взаимного доверия и стратегического сотрудничества между двумя сторонами.

Также были обсуждены меры обеспечения дальнейшего развития двусторонних отношений в направлении, заданном главами двух государств для обеспечения безопасности России и Китая; внесения большего вклада в защиту общих интересов двух стран, а также безопасности и стабильности в мире [2].

Н. Патрушев заявил, что российско-китайское всеобъемлющее стратегическое партнерство имеет прочную основу в том числе в форме общественной поддержки двух стран. Россия одобряет принцип «Одного Китая» и решительно поддерживает меры, предпринимаемые китайским правительством по тайваньскому вопросу для защиты суверенитета и территориальной целостности [4].

Российская сторона считает развитие отношений с Китаем приоритетным дипломатическим направлением по вопросам безопасности и готова поддерживать с китайской стороной тесные стратегические связи, углублять практическое сотрудничество в различных областях, еще больше укреплять координацию и сотрудничество в международных организациях.

Стороны также обменялись мнениями по вопросам поддержания глобальной стратегической стабильности, ситуации в сфере безопасности в Азиатско-Тихоокеанском регионе и другим международным и региональным вопросам, представляющим взаимный интерес.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Ашмарина, К. Д. Механизмы сотрудничества России и Китая в сфере безопасности в рамках ШОС / К. Д. Ашмарина // Государство, власть, управление и право : Материалы XII Всероссийской научно-практической конференции, Москва, 06 декабря 2021 года. – Москва: Государственный университет управления, 2022. – С. 277-279.

2 Ли, С. Приоритеты национальных интересов РФ и современные российско-китайские отношения / С. Ли // Scientific achievements of the third millennium: Collection of Scientific Papers based on the results of an XVII international scientific conference, New York, USA, 15 февраля 2022 года. – New York, USA: 2022, 2022. – С. 44-46.

3 Нехорошева, А. Н. Противодействие распространению терроризма в Центрально-Азиатском регионе: новое направление сотрудничества России и Китая? / А. Н. Нехорошева, А. А. Романов // Россия и мир: развитие цивилизаций. Инновации и консерватизм: поиск баланса : Материалы XII международной научно-практической

конференции, Москва, 06–07 апреля 2022 года. – Москва: Институт мировых цивилизаций, 2022. – С. 187-192.

4 Петрунина, Ж. В. Приграничное сотрудничество России и Китая в условиях вызовов начала 2020-х годов / Ж. В. Петрунина, Г. А. Шушарина // Социальные и гуманитарные науки на Дальнем Востоке. – 2022. – Т. 19. – № 1. – С. 197-203. – DOI 10.31079/1992-2868-2022-19-1-197-203.

5 Хо, Д. Политические аспекты сотрудничества китайской народной Республики и Российской Федерации в сфере безопасности в рамках ШОС / Д. Хо // Вопросы политологии. – 2022. – Т. 12. – № 4(80). – С. 1306-1313. – DOI 10.35775/PSI.2022.80.4.033.

6 Патрушев заявил, что Россия и Китай хотят справедливости в мире [Электронный ресурс] – Режим доступа: https://tass.ru/politika/15792445 (дата обращения: 24.09.2022).

УДК 327

Лопатина Ольга Ивановна, старший преподаватель, Комсомольский-на-Амуре государственный университет
Lopatina Olga Ivanovna, senior lecturer, Komsomolsk-on-Amur State University

ОСОБЕННОСТИ ОСВЕЩЕНИЯ ТЕРАКТОВ В СМИ

THE SPECIFICS OF MEDIA COVERAGE OF TERRORIST ATTACKS

Аннотация. В данной статье рассмотрены принципы освещения террористических атак в СМИ, выделена теория о том, что террористические организации чаще совершают атаки при повышенном освещении их в эфире, а так же сделана попытка проанализировать важность контроля информации, появляемой на новых медийных платформах.
Abstract. This article examines the principles of media coverage of terrorist attacks, highlighting the theory that terrorist organisations are more likely to carry out attacks with increased media coverage, as well as attempting to analyse the importance of controlling information appearing on new media platforms.
Ключевые слова: СМИ, террористические атаки, освещение.
Key words: Media, terrorist attacks, coverage.

В 2017 году опрос Фонда Варки, проведенный среди 20 000 молодых людей по всему миру, показал, что 83% респондентов считают, что терроризм заставил их бояться за будущее - больше, чем любой другой фактор, включая изменение климата и войну. Было много спекуляций по поводу гипотезы о том, что освещение террористических групп в СМИ может стимулировать новые атаки.

Многие теракты, которые мы наблюдаем сегодня, по крайней мере, частично задуманы с учетом освещения в СМИ, нацелены не только на реальных жертв, но и на миллионы шокированных и потрясенных зрителей по всему миру. Между тем, огромное давление, оказываемое на СМИ с целью привлечения аудитории - перед лицом продолжающихся волн технологических и финансовых преобразований - может создать мощный соблазн сосредоточиться на насилии и сенсациях, и первыми сообщить свежую информацию и слухи, даже до того, как будет обеспечена достоверность.

Новостные СМИ могут освещать эти аспекты и в то же время подчеркивать подлинный диалог и дискуссии как альтернативу насилию и кровопролитию. Мы не всегда можем предотвратить терроризм, но что мы можем контролировать, так это нашу реак-

цию. Мы можем принять решение не позволять терроризму провоцировать нас жить в страхе, питать наши собственные предрассудки или закрывать доступ к законным мнениям. Другими словами, мы можем не позволить террору разрушить весь тот прогресс, которого мы достигли в развитии демократии, свободы слова и прав человека во всем мире. В противном случае мы рискуем сыграть на руку тем, кто занимается террором, а также тем, кто использует реакцию на теракты для того, чтобы способствовать подозрительности, поляризации и нарушениям прав. Средства массовой информации могут сделать все возможное, чтобы помочь обществу справиться с этими проблемами.

Освещение случаев насильственного экстремизма и терроризма должно быть сбалансированным. То, в какой степени СМИ должны уделять место преступнику и влияющей идеологии, должно быть результатом серьезной редакционной оценки, которая позволит избежать любых обобщений.

В случае распространения языка вражды, паники и страха, СМИ будут использовать доступные инструменты социальных сетей и каналов связи для их подавления.

СМИ должны всегда использовать официальные источники информации, через прямой контакт с лицами, ответственными за связь с общественностью, или через уполномоченные новостные платформы (официальный сайт органов власти, которые могут дать соответствующие ответы на ключевые вопросы).

В ожидании официальной информации не прибегать к непроверенным источникам информации и спекуляциям, которые ведут к сенсациям. Это может привести к распространению паники и страха, что является одной из ключевых целей воинствующих экстремистов и террористов, и таким образом СМИ, ненароком, становятся их союзниками.

СМИ в своих различных формах могут играть ключевую роль в ситуациях политических конфликтов. Радио, телевидение и газеты могут подстегивать или сдерживать политическое насилие; они могут использоваться как инструмент пропаганды или просто как мегафон для распространения информации среди большой аудитории. Например, радиопередачи могли сыграть решающую роль в подъеме нацистов, геноциде в Руанде или недавнем подъеме националистических антисербских партий в Хорватии. Однако потенциальной причинно-следственной связи между освещением событий в СМИ и терроризмом уделяется меньше внимания, хотя многие комментаторы предполагают такую динамику.

В августе 2016 года тогдашний государственный секретарь Джон Керри заметил, что, возможно, СМИ окажут всем нам услугу, если не будут освещать это так часто".

Сегодня более 44 процентов американцев боятся террористической атаки, но только 22 процента боятся умереть. Согласно другому опросу, до половины населения США опасается, что они или их семья станут жертвами терроризма. Одно из интуитивных объяснений этих, казалось бы, иррациональных ответов на вопросы опроса соответствует идее о том, что воздействие СМИ на терроризм усиливает страх перед терроризмом, что обычно играет на руку террористической группе. В частности, повышенное внимание СМИ может принести террористической группе прямую выгоду, распространяя ее послание, вызывая страх у целевого населения и вербуя последователей. Таким образом, освещение в СМИ представляет собой важный, бесценный инструмент для террористов и их кампаний.

Важное различие между ролью СМИ в терроризме и в конфликтных ситуациях касается подразумеваемого механизма. В соответствующих конфликтных ситуациях СМИ могут способствовать распространению пропаганды и информации, чтобы повлиять на политические взгляды и убеждения людей. Террористические организации, однако, выбирают время для того, чтобы привлечь максимальное внимание СМИ" и могут нанести больше ударов, когда внимание СМИ уже приковано к ним. Таким образом, освещение в СМИ не обязательно используется явно для достижения конкретных

целей, но террористические группы могут стремиться использовать ту медийную платформу, которой они располагают в данный момент. Интересно, что эта цель максимального освещения в СМИ может противоречить желанию правительств атаковать "когда мир не смотрит".

Освещение терроризма, как правило, вызывает и другие эмоции и отношение, как к самим актам, так и к их освещению в СМИ. В целом, освещение событий, как правило, вызывает чувство гнева, хотя цель таких чувств может быть разной. Чаще всего враждебные эмоции направлены на преступников. Похоже, что эти чувства присущи освещению. В Израиле освещение теракта вызывает не только гнев у многих израильтян, но и негативные стереотипы о палестинцах и усиление восприятия враждебности противника.

Анализ данных, полученных после событий 11 сентября до конца 2015 года, дает доказательства, которые согласуются с идеей о том, что Аль-Каида систематически совершает больше атак, когда освещение в новостях выше. Этот результат проявляется в отношении внимания СМИ в четырех основных американских СМИ: CNN, NBC, CBS и Fox News. Соответствующая величина значительна: Каждая минута освещения Аль-Каиды в 30-минутной новостной программе в среднем стимулирует примерно одну дополнительную атаку в течение следующих семи дней.

Некоторые наблюдатели обвиняют СМИ в том, что они вдохновляют террористические акты или выступают в качестве добровольных сообщников террористов. Другие утверждают, что СМИ несут ответственность за терроризм лишь в той же степени, в какой гражданская авиация несет ответственность за угон самолетов: "Можно остановить угон самолетов, посадив все гражданские самолеты; возможно, терроризм можно уменьшить путем полного отключения СМИ".

Премьер-министр Великобритании Маргарет Тэтчер заняла менее враждебную позицию. Тэтчер предложила "журналистскую самодисциплину", чтобы лишить будущих террористов "кислорода гласности, от которого они зависят".

Генеральный прокурор Соединенных Штатов Эдвин Миз III поддержал предложение премьер-министра и сделал еще один шаг вперед. Ирландская республиканская армия также была хорошо осведомлена о способности террористов вымогать известность. Один из немногих выпускников университета, вступивших во Временную ИРА, сформулировал, какое значение группа придавала пропаганде. В июле 1974 года анализ шестидесяти взрывов бомб показал, что более восьмидесяти процентов из них были организованы так, чтобы получить максимальное освещение в телевизионных новостях.

Беспокоит и то, что СМИ теряют интерес к освещению теперь уже обыденных угонов и похищений, тогда террористы будут использовать более эффектные методы привлечения внимания общественности. Одним из таких примеров является "фанатичное" нападение на штаб морской пехоты США в Бейруте, Ливан.

В современную эпоху средств массовой информации цифровые платформы играют решающую роль в том, как люди потребляют новости, тем самым создавая новую проблему для этичного освещения терроризма. Цифровые платформы традиционных СМИ обычно придерживаются тех же этических норм, что и вещательные и печатные СМИ. К сожалению, цифровые медиа-источники, не связанные с традиционными СМИ, часто не связаны теми же этическими принципами и не имеют такой же журналистской экспертизы, как традиционные новостные СМИ, хотя эти платформы играют важную роль в фильтрации информации и формировании новостных сюжетов. Это представляет собой серьезную проблему, которую необходимо решить в будущих исследованиях.

СМИ также могут оказать положительное воздействие, выступая в роли миротворца или подчеркивая солидарность между общинами и сообществами. СМИ могут повысить осведомленность общественности об угрозах безопасности и процедурах чрезвычайных ситуаций в недраматической форме, а также стимулировать обществен-

ные разговоры и дебаты о социальных и политических последствиях терроризма. Кристина Арчетти рекомендует, чтобы в современную эпоху СМИ понимали, как "стратегические коммуникации" и "нарративы" могут быть использованы в качестве эффективных инструментов противодействия экстремизму. Она признает, однако, что существует множество проблематичных предположений, которые необходимо преодолеть, чтобы это было реалистично. В конечном счете, самостоятельные рекомендации для СМИ могут помочь снизить потенциальное негативное воздействие освещения терроризма в СМИ.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Ашмарина, А.А. Особенности освещения террористических акций в СМИ / А.А. Ашмарина, Т.В. Баранова // Огарёв-Online. 2016. №7 (72). URL: https://cyberleninka.ru/article/n/osobennosti-osvescheniya-terroristicheskih-aktsiy-v-smi (дата обращения: 01.11.2022).

2 Тараканов, А. В. Терроризм и СМИ: проблема взаимодействия // Вестник Кемеровского государственного университета. – 2008. – № 3. – С.5–9.

3 Shuneyko, A. Media Space as a Regulator of the Global Transformation of Communicative Interaction / A. Shuneyko, O. Chibisova // Media Education. – 2022. – No 1. – P. 109-118. – EDN XYOLRW.

УДК 343.301

Малышев Василий Михайлович, студент, Комсомольский-на-Амуре государственный университет
Malyshev Vasily Mikhailovich, student of Komsomolsk-na-Amure State University
Малышева Наталья Васильевна, кандидат филологических наук, доцент; Комсомольский-на-Амуре государственный университет
Malysheva Natalia Vasilievna, PhD in Philology, Associate Professor, Komsomolsk-na-Amure State University

ТЕХНОЛОГИЧЕСКИЙ ПРОГРЕСС НА СЛУЖБЕ ТЕРРОРИЗМА

TECHNOLOGICAL PROGRESS AS A TERRORISM SERVANT

Аннотация. В списке глобальных проблем человечества особую позицию занимает терроризм, как элемент устрашения населения и инструмент влияния на умы людей, приводящий к жертвам, потрясениям, созданию атмосферы незащищенности и уязвимости системы (государства) и жизни человека. Прогресс, передовые технологии, используемые в террористических целях, способны многократно увеличить последствия его разрушительной деятельности.
Abstract. In the list of global problems of mankind, a special position is held by terrorism as an element of intimidation of the population and an instrument of influence on the minds of people, leading to victims, shocks and creating an atmosphere of insecurity and vulnerability of the system (state) and human life. Progress, advanced technologies used by terrorists and extremists multiply the consequences of their destructive activity.
Ключевые слова: терроризм, технологии, технологический прогресс, развитие, правительство.
Key words: terrorism, technology, technological progress, development, government.

В настоящее время мы являемся свидетелями перехода к демократическому использованию новых и новейших технологий. В прошлом передовые технологии были доступны только ученым, правительственным чиновникам и военным. Сегодня передовые технологии доступны как открытый источник. Современные технологии повсеместны и достаточно просты в использовании.

Хотя технологии могут быть движущей силой развития и процветания, они могут быть использованы в своих целях террористами, непредсказуемым и смертоносным образом. Никогда в истории негосударственные субъекты, применяющие насилие, не были настолько глобально объединены, изобретательны, динамичны, хорошо финансируемы и технологически подкованы. Этому есть три причины. Первая заключается в том, что в прошлом передовые технологии были доступны лишь немногим: сегодня две трети населения мира держат в руках смартфон, который в миллионы раз мощнее, чем компьютеры управления "Аполлона-11", отправившего людей на Луну в 1969 году. Во-вторых, новые технологии резко расширили глобальный охват террористических групп, возможность индоктринации и вербовки мгновенно, без затрат и в относительной анонимности в любой точке мира. В-третьих, террористы теперь имеют доступ к технологиям военного класса. Многие из существующих сегодня технологий являются технологиями двойного назначения, которые можно использовать как в мирных, так и в военных целях.

Представим краткий обзор вышеуказанных причин.

1 Использование современных технологий негосударственными субъектами прослеживается с последних десятилетий 19 века. Террористические группы ранее придерживались двух основных видов оружия: динамита и огнестрельного оружия (в частности, автомата Калашникова). Вскоре после того, как Альфред Нобель изобрел динамит в 1867 году, анархистские движения поделились инструкциями по его использованию, что вызвало волну нападений в более чем 50 странах. Выпуск автомата Калашникова (АК-47) в 1950-х годах способствовал возникновению второй глобальной волны политического насилия. Используемые повстанцами, организованными преступными группировками, террористами и "борцами за свободу", автоматы Калашникова продолжают убивать. Ежегодно в результате применения огнестрельного оружия погибает около миллиона человек.

Таким образом, негосударственные деятели всегда были заинтересованы в получении и овладении инновационным оружием. Согласно "теории расширения возможностей летального исхода", новые технологии быстро принимаются и адаптируются террористами, осуществляющими насилие, если они доступны, дешевы, просты в использовании, транспортабельны, скрыты и эффективны. Террористы заинтересованы в оружии, которое применяется в совершенно разных сферах, "которое усиливает эффект, имеет символический резонанс и может быть использовано в неожиданных целях".

2 Расширение охвата, индоктринации и вербовки через интернет и социальные сети.

В 1991 году представители Национальной академии наук США выступили с заявлением, ставшим пророческим: "Завтрашний террорист сможет нанести больше вреда с помощью клавиатуры, чем с помощью бомбы". Интернет и социальные сети, а также аппаратное обеспечение для доступа к ним - смартфоны - стали новым цифровым оружием войны. Экстремисты используют эти инструменты для проведения психологических операций, вербовки, планирования и проведения атак, финансирования и обеспечения анонимности. Сегодня технологии позволяют террористам получить беспрецедентный доступ к глазам и нейронам миллионов людей через Интернет и социальные сети.

Хотя социальным сетям всего 20 лет, они изменили современную жизнь как в положительную, так и в отрицательную сторону. Социальные сети помогли запустить движения за социальную справедливость #MeToo и BlackLivesMatter. Однако, социаль-

ные медиа и усилили экстремистские группы, подпитывая расовые, гендерные, культурные, политические и религиозные движения, такие как группы белых экстремистов, инцелов, крайних салафитов-джихадистов и другие.

Алгоритмы социальных сетей разработаны таким образом, чтобы апеллировать к человеческой психике и действовать как зеркало наших самых глубоких желаний и увлечений. Создатели контента используют алгоритмы платформ социальных сетей и силу человеческих эмоций, создавая привлекающий внимание контент.

Итак, цель развития в научной, технической, социальной, культурной и других сферах состоит в удовлетворении возрастающих потребностей человечества. Технический прогресс предоставляет такие возможности: появляются новые способы коммуникации, передвижения, производства и изучения. Однако, открытость современного знания делает его эффективным оружием в руках террористов.

Поэтому крайне важно информировать общественность о новых рисках, как это было сделано в 2022 году Министерством внутренней безопасности (DHS), которое предупредило, что внутренние экстремистские группы разработали планы атаки на энергосистему США, или аналогичные предупреждения об атаках ransomware на критическую инфраструктуру Австралии, США, Великобритании и других стран.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED) “The impact of the COVID-19 pandemic on terrorism, counter-terrorism and countering violent extremism” Accessed February 21, 2022. https://reliefweb.int/sites/reliefweb.int/files/resources/cted_covid19_paper_dec_2021.pdf (дата обращения: 22.10.2022).

2 Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) // https://rkn.gov.ru (дата обращения: 22.10.2022).

3 Myanmar Opposition Announces ‘Defensive War’ against Junta | Myanmar | The Guardian. Accessed February 21, 2022. https://www.theguardian.com/world/2021/sep/07/myanmar-opposition-announces-defensive-war-againstjunta (дата обращения: 22.10.2022).

4 Department of Defense Office of Inspector General. “Lead Inspector General for Operation Inherent Resolve Quarterly Report to the United State.” Accessed February 21, 2022. https://www.dodig.mil/reports.html/=Article/2833944/lead-inspector-general-for-operation-inherent-resolvequarterly-report-to-the-u/ (дата обращения: 22.10.2022).

УДК 343.301

Малышева Наталья Васильевна, кандидат филологических наук, доцент; Комсомольский-на-Амуре государственный университет
Malysheva Natalia Vasilievna, PhD in Philology, Associate Professor, Komsomolsk-na-Amure State University

МЕЖДУНАРОДНЫЕ И РЕГИОНАЛЬНЫЕ ОРГАНИЗАЦИИ ПО БОРЬБЕ С ТЕРРОРИЗМОМ И ЭКСТРЕМИЗМОМ

INTERNATIONAL AND REGIONAL ORGANISATIONS TO COMBAT TERRORISM AND EXTREMISM

Аннотация. Усиление террористических движений происходит в результате негативных явлений в экономической, социальной и политической сферах как развитых, так и

развивающихся стран. Совместная работа государств, государственных структур, межгосударственных организаций, направленная на разработку мер противодействия терроризму и экстремизму, проводимая в течение последних десятилетий, привела к снижению уровня смертности в результате террористических актов на 10% за последние два года. Краткий обзор наиболее известных организаций и проводимых ими мероприятий представлен в данной статье.

Abstract. Strengthening of terrorist movements occurs as a result of negative phenomena in the economic, social and political spheres of both developed and developing countries. The joint work of states, state structures, interstate organizations aimed at developing measures to counter terrorism and extremism, which has been carried out over the past decades, has led to a decrease in the death rate as a result of terrorist acts by 10% over the past two years. A brief overview of the noted organizations and their activities is presented in this article.

Ключевые слова: террористическое движение, экстремизм, антитеррористическая программа, глобальный индекс терроризма, международная организация, региональная организация.

Key words: terrorist movement, extremism, anti-terrorist program, global terrorism index, international organization, regional organization.

Террористические движения и экстремизм представляют одну из глобальных угроз современному миру. Согласно Глобальному индексу терроризма (Global Terrorism Index), который ведется Институтом экономики и мира (IEP, Сидней) с 2007 года по настоящий момент, в различных странах произошло свыше 60500 случаев террористических актов, жертвами которых стали от одного человека до трех тысяч (теракт 11 сентября 2009 года, США) в каждом. В Глобальном индексе терроризма от 2022 года приводится статистика по ста семидесяти странам [7]. Она составляется по четырем основным показателям: количество террористических актов, количество смертельных случает, количество пострадавших и уровень материального ущерба.

Таблица 1 – Рейтинг государств согласно Глобальному индексу терроризма за 2022 год

Страна	Рейтинг	Страна	Рейтинг
1 Афганистан	9,109	15 Египет	6,932
2 Ирак	8,55	22 Таиланд	5,723
3 Сомали	8,398	28 США	4,961
4 Буркина-Фасо	8,270	31 Великобритания	4,770
5 Сирия	8,250	33 Германия	4,729
6 Нигерия	8,233	35 Франция	4,562
7 Мали	8,152	41 Новая Зеландия	4,376
8 Республика Нигер	7,856	44 Россия	4,219
9 Мьянма	7,830	60 Австралия	2,438
10 Пакистан	7,825	67 Китай	1,863
12 Индия	7,432	92 Тайвань	0,227

В первой и третьей колонках таблицы указаны страны в порядке убывания от стран с наивысшим уровнем террористической активности до стран с нулевым показателем. Колонка с рейтингом индекса влияния построена по десятибалльной шкале, где 10 – очень высокий уровень влияния, 8 – высокий уровень, 6 – средний, 4 – низкий, 2 – очень низкий, 0 – влияние не выявлено.

Примечательно, что 85% смертельных случаев в результате действий террористических организаций приходится на страны, входящие в первую десятку данного индекса (рис.1)

Рисунок 1 – Количество смертей от террористических действий в 2021 (%)

Несмотря на незначительное снижение смертельных случаев от террористических действий (1,2%) число самих атак выросло на 17% (4458 в 2020 году и 5226 в 2021 году).

Вне сомнения, деятельность по противодействию терроризму и экстремизму, которую ведут страны на национальном и межнациональном уровнях, приводит к некоторым результатам.

К таким организациям можно отнести следующие:

1 Международная организация – Организация Объединенных Наций – ведет активную многостороннюю деятельность в поддержку жертв терроризма, проводит конференции по правам жертв терроризма (The Conference on The Promotion and Protection of the Human Rights of Victims of Terrorism), разрабатывает стратегии по осуществлению контртеррористической деятельности, рекомендованные для всех стран-участников (UN Global Counter-terrorism Strategy) [13].

2 Управление ООН по наркотикам и преступности – the United Nations Office on Drugs and Crime (UNODC) Terrorism Prevention Branch (TPB) – занимается борьбой с незаконным оборотом наркотиков, оружия, организованной преступностью, торговлей людьми и международным терроризмом [12]. В рамках деятельности данной организации запущены образовательные программы и проекты по реинтеграции жертв терроризма, по поддержанию устойчивого развития проблемных регионов [10].

3 Контртеррористический комитет Совета Безопасности ООН – United Nations Security Council – Counter-Terrorism Committee Executive Directorate (CTED) организуют обучение противодействию террористическим действиям в различных регионах. Так, например, в 2019 году был разработана и внедрена многоэтапная обучающая программа для Нигерии [8], поскольку спецификой данного региона является массовое вовлечение женщин различного возраста и девочек в деятельность террористических группировок Боко Харам, западных провинций Африки и других исламских государств.

4 Организация по защите прав детей, включая права ребенка на защиту от насилия, жестокого обращения и эксплуатации – the United Nations International Children's Emergency Fund (UNICEF) – функционирует благодаря финансированию различных государств и частному спонсированию [11]. Организация привлекает внимание общественности к «серьезным нарушениям» прав детей во времена вооруженных конфликтов. Одним из таких нарушений является использование детей в деятельности вооруженных группировок в результате принудительной или добровольной вербовки.

6 Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма – the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) – является региональной организацией и включает объединенную работу девяти государств: Беларуси, Индии, Казахстана, Китая, Кыргыстана, России, Таджикистана, Туркменистана и Узбекистана [6]. В результате исследований выявляются высокорисковые зоны и секторы, информация распространяется в правоохранительные и надзорные органы, проводятся семинары, региональные форумы и тренинги.

7 Организация по безопасности и сотрудничеству в Европе (ОБСЕ) – Organization for Security and Co-operation in Europe – объединяет 57 стран-участников по всему миру, работает как постоянно действующий международный форум их представителей, разрабатывает следующие меры: контроль над вооружением, контртерроризм, борьба с торговлей людьми, предотвращение и разрешение конфликта, кибербезопасность, права человека и др. [9].

На уровне государства каждая страна учреждает организацию по противодействию терроризму, принимает законы, регулирующие деятельность данных организаций и других силовых структур, проводит конференции.

В России учрежден Национальный антитеррористический комитет (НАК) как координатор действий федеральных органов исполнительной власти и органов местного самоуправления 15.02.2006 [3].

Во Франции – Группа вмешательства – элитное антитеррористическое подразделение национальной жандармерии, которое подчиняется Генеральному директору напрямую [2].

Германия разработала большое количество законодательных нормативных актов, предписывающих антитерорристическую деятельность как отдельных ведомств, так и их совместную деятельность, таких как: Центр по борьбе с экстремизмом и терроризмом (2012 год создания), спецподразделения разведслужб и аналитических центров [5].

В качестве вывода, следует отметить активность стран на международном и региональном уровнях по предупреждению опасностей терроризма и экстремизма, по разработке и совершенствованию мер нейтрализации новых вызовов, обусловленных технологическим прогрессом и другими социальными, политическими и экономическими явлениями, происходящими в различных регионах нашей планеты. Открытость, обмен опытом и данными, вовлеченность, активная внутри- и межгосударственная контртеррористическая политика способствуют прогрессу в предотвращении «угрозы XXI века» [4].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Всемирный антикриминальный и антитеррористический форум www.waaf.ru (дата обращения: 20.10.2022).

2 Крутиков Я. О. Институциональная основа борьбы с терроризмом во Франции. Эффективность и методы ее повышения. Вестник РУДН. Серия: Государственное и муниципальное управление. 2017. Vol. 4. No 2. С. 172-179.

3 Национальный антитеррористический комитет http://nac.gov.ru_(дата обращения: 20.10.2022).

4 Национальный антитеррористический комитет. Видеоролик «Терроризм – угроза XXI века» http://nac.gov.ru/dokumentalnye-filmy/terrorizm-ugroza-xxi-veka.html (дата обращения: 20.10.2022).

5 Романовский Г. Б. Противодействие терроризму в Германии: законодательные новеллы / Г. Б. Романовский // Электронный научный журнал «Наука. Общество. Государство». 2019. Т. 7. № 4 (28) https://cyberleninka.ru/article/n/protivodeystvie-terrorizmu-v-germanii-zakonodatelnye-novelly (дата обращения: 20.10.2022).

6 Eurasian Group on Combating Money Laundering and Financing of Terrorism https://eurasiangroup.org/ru (дата обращения: 20.10.2022).

7 Global Terrorism Index 2022 https://www.economicsandpeace.org/wp-content/uploads/2022/03/GTI-2022-web.pdf (дата обращения: 20.10.2022).

8 Nigeria Training Module on Gender Dimensions of Criminal Justice Responses to Terrorism
https://www.unodc.org/pdf/terrorism/Web_stories/UNODC_Nigeria_Gender_Training_Module.pdf (дата обращения: 20.10.2022).

9 Organization for Security and Co-operation in Europe https://www.osce.org/ (дата обращения: 20.10.2022).
10 Preventing Violent Extremism for Children in Conflict with the Law https://www.unodc.org/easternafrica/about/preventing-violent-extremism-for-children-in-conflict-with-the-law.html (дата обращения: 20.10.2022).
11 United Nations International Children's Emergency Fund https://www.unicef.org/nigeria/about-us (дата обращения: 20.10.2022).
12 United Nations Office on Drugs and Crime https://www.unodc.org/ (дата обращения: 20.10.2022).
13 United Nations Global Counter-Terrorism Strategy https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy (дата обращения: 20.10.2022).

УДК 621.9:519.8

Махно Виктория Владиславовна, студентка, Комсомольский-на-Амуре государственный университет;
Makhno Viktoria Vladislavovna, student of Komsomolsk-na-Amure State University
Яковлева Ирина Михайловна, студентка, Комсомольский-на-Амуре государственный университет;
Yakovleva Irina Mikhailovna, student of Komsomolsk-na-Amure State University
Когай Сергей Геннадьевич, старший преподаватель, Комсомольский-на-Амуре государственный университет
Kogai Sergei Gennadevich, Senior lecturer, Komsomolsk-na-Amure State University

РОЛЬ ШОС КАК ЭФФЕКТИВНОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ЕВРАЗИИ

THE ROLE OF THE SCO AS AN EFFECTIVE SECURITY SYSTEM IN EURASIA

Аннотация. Данная статья посвящена деятельности Шанхайской организации сотрудничества. Организация, которая была создана для поддержания мирных отношений на Евразийском континенте и эффективного сотрудничества стран-участников во многих областях общественной жизни. Также рассматриваются цели и задачи ШОС.
Abstract. This article is devoted to the activities of the Shanghai Cooperation Organization. An organization that was created to maintain peaceful relations on the Eurasian continent and the effective cooperation of the participating countries in many areas of public life. The goals and objectives of the SCO are also considered.
Ключевые слова: интернациональный терроризм, Китай, сотрудничество, безопасность, сохранность Евразии.
Key words: international terrorism, China, cooperation, security, safety of Eurasia.

На современных условиях всеобъемлющей интеграции большинство областных и местных проблем приобретают интернациональный характер, и нередко их решение становится невыполнимым действиями исключительно одного государства. Явным образцом представляется увеличение сегодняшних нестандартных и невоенных угроз безопасности. Собственно, по данному фактору появилась потребность сопротивления новым вызовам современности едиными общественными усилиями. Помимо этого, активность эстремизма и пропаганда нелегальных веществ потребовала безотлагательного вмешательства.

Ярким примером такой структуры представляется Шанхайская организация сотрудничества. Сформированная поначалу как политическая организация пяти государств, устанавливающая перед собой стремление уладить пограничные вопросы на участке советско-китайской границы, ныне данная организация переросла в полноценную многостороннюю структуру.

На современном этапе значимость ШОС, как эффективной системы обеспечения безопасности на пространстве Евразийского континента, приобретает более значимый характер. Абсолютно все сферы жизнедеятельности граждан становятся предметами интереса ШОС. Оперируя принципами так называемого «шанхайского духа» обоюдного доверия, справедливости, почитания многообразия культур и рвения к общей модернизации, данная организация может оказывать существенное влияние на сохранность устойчивости региона. Диапазон целей, что ШОС устанавливает перед собой, включает сопротивление нестандартным угрожающим факторам и угрозам безопасности, таким как интернациональная преступность, экстремизм, коррупция, противозаконная торговля наркотиками, преступная миграция, техногенные и природоохранные проблемы.

Как известно, Шанхайская организация сотрудничества одной из первых отреагировала на события апреля и июля 2010 года в Кыргызстане, так как переломные факторы в социально-экономической и политической жизни данной страны могли иметь непоправимый эффект для всего региона, в том числе государств Центральной Азии. Но совместными действиями государств-членов Шанхайской организации сотрудничества стало возможным приостановить нестабильную обстановку в данной государстве и предотвратить в ней общественные столкновения.

Исходя из вышеописанного, говоря о всеобщих и областных вопросах обеспечения сохранности, невозможно не реагировать на вероятность вторжения на территорию опасности интернационального терроризма, культового экстремизма и государственного радикализма. В данной области партнёрство в сфере сохранности в рамках Шанхайской организации сотрудничества ориентировано, в первую очередь, на уничтожение источников роста нынешних опасностей и угроз. Все это дозволяет считать данную организацию, вкупе с иными функционирующими на данной территории разносторонними объединениями и институтами, необходимой составляющей в структуре разнонаправленного партнёрства.

Близость нашего региона с источниками неустойчивости, прежде всего, исходящими с территории Афганистана, делает проблему снабжения общественной сохранности одной из особо животрепещущих и актуальных. Упорядочение обстановки в Афганистане представляется одним из первостепенных течений деятельности описываемой организации. Например, страны, входящие в состав ШОС, пользуясь своим близким географическим расположением, оживленно содействуют спокойному возрождению данного государства. Данный фактор дает крупное превосходство для ШОС конструктивнее прерывать беззаконную преступность на границах, в том числе исходящую с территории Афганистана. В настоящее время Шанхайская организация сотрудничества уже организовывает антинаркотический район безопасности по периметру афганской границы.

В результате, необходимо принять весьма серьезный и значимый факт, а именно то, что Шанхайская организация сотрудничества из локальной компании постепенно преобразуется в объединение, которое расширяет площадь своей ответственности и приобретает транснациональную направленность. Ныне в своём деле данная организация ставит своей целью охватывать массовый диапазон задач, сопряженных с предоставлением сохранности в Евразии.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ
1. ШОС: история создания и особенности организации / РЕН ТВ. URL : https://ren.tv/longread/987748-shos-istoriia-sozdaniia-i-osobennosti-deiatelnosti-organizatsii (Дата обращения 20.10.2022)
2. Роль ШОС в обеспечении Евразийской безопасности / Руслан Изимов. URL : https://ia-centr.ru/experts/iats-mgu/rol-shos-v-obespechenii-evraziyskoy-bezopasnosti/ (Дата обращения 20.10.2022)
3. ШОС и её роль на евразийском пространстве / Студенческая библиотека онлайн. URL : https://studbooks.net/2233125/ekonomika/rol_evraziyskom_prostranstve (Дата обращения 20.10.2022)
4. Петрунина Ж.В. Стратегия «Один пояс - Один путь» как катализатор изучения иностранных языков в Китае // В сборнике: Россия и Китай: история и перспективы сотрудничества. Материалы XI международной научно-практической конференции. Отв. редактор А.В. Друзяка. Благовещенск, 2021. С. 513-516.

УДК 316

Мусалитина Евгения Александровна, доцент, Комсомольский-на-Амуре государственный университет
Musalitina Evgenia Aleksandrovna, Associate Professor, Komsomolsk-na-Amure State University

АРХИТЕКТУРНАЯ ЗАЩИТА УЧЕБНЫХ ЗАВЕДЕНИЙ ОТ СКУЛШУТИНГА (НА ПРИМЕРЕ США)

ARCHITECTURAL PROTECTION OF EDUCATIONAL INSTITUTIONS FROM SCHOOLSHOOTING (ON THE EXAMPLE OF THE USA)

Аннотация. За последние 10 лет в Америке значительно вырос уровень террористических атак на общеобразовательные учреждения. Свободная продажа оружия, доступность радикальной информации в сети интернет, неустойчивая психика молодых людей приводит к тому, что стрельба в школах становится регулярным явлением. В статье рассматривается комплекс государственных мер по модернизации архитектуры зданий уже существующих учебных заведений и строительства новых с учетом инженерной антитеррористической защиты.
Abstract. Over the past 10 years the level of terrorist attacks on educational institutions has increased significantly in America. The free sale of weapons, the availability of radical information on the Internet, the unstable psyche of young people leads to the fact that school shootings become a regular occurrence. The article discusses a set of state measures to modernize the architecture of buildings of existing educational institutions and the construction of new ones, taking into account engineering anti-terrorist protection.
Ключевые слова: терроризм, стрельба в школе, США, архитектурная защита безопасности.
Key words: terrorism, school shooting, The USA, security architectural protection.

Соединенные Штаты – единственная развитая страна, где регулярно повторяются школьные перестрелки. За последние 10 лет в Америке значительно вырос уровень террористических атак на общеобразовательные учреждения. В новом отчете исследовательского отдела Министерства образования США, опубликованном в 2021 г., говорится о 93 случаях стрельбы в школах за 2020-2021 учебный г. в начальной и средней школе, и это на 93% больше, чем 10 лет назад. Из 93 случаев стрельбы, зафиксирован-

ных в этот период, 43 случая со смертельным исходом и 50 случаев стрельбы, в результате которой были получены травмы разной степени тяжести [2].

Несмотря на новые меры по обеспечению порядка, безопасности и некоторые улучшения в этом вопросе, уровень преступности в школах вызывает тревогу у американского правительства. В 2021 г. Дж. Байден подписал закон о регулировании огнестрельного оружия в Соединенных Штатах, что, как предполагается, будет способствовать уменьшению случаев террористических атак на учебные заведения в стране [5]. Поскольку американским школам в среднем 44 года, их архитектура спланирована без учета защиты от террористических атак [1].

Американское правительство серьезно озабочено данной проблемой, совершенствуя систему антитеррористической борьбы. Одной из таких мер является внесение изменений в архитектуру зданий уже существующих учебных заведений и строительство новых с учетом инженерной антитеррористической защиты. Согласно разработанным рекомендациям необходимо оснащать новые школы биометрическими считывателями, наружным освещением, оптимизированным для видеонаблюдения, и устройствами распознавания звука, способными обнаруживать конкретные акустические признаки, указывающие на угрозу, такие как агрессия или паника в голосе людей.

Инженерные изменения по защите от стрельбы вводились постепенно, но в настоящий момент они являются обязательными при проектировании каждой новой школы в Соединенных Штатах, и, очевидно, их влияние на архитектуру учебных заведений будет длиться десятилетиями. Например, в Шелбивилле, штат Индиана, в новой средней школе учителя должны носить с собой тревожные кнопки. Также в холлах заведения установлены датчики движения и задымленности [1].

Во Фрутпорте, штат Мичиган, здание новой средней школы является одним из самых оснащенных системами безопасности заведений в стране. На каждом этаже установлены перегородки, за которыми учащиеся смогут спрятаться, двери с датчиком блокирования в учебных кабинетах.

В связи с резким ростом случаев стрельбы в учебных заведениях, например, в Колумбиане, Технологическом институте Вирджинии, Сэнди-Хук и Портленде, школьные комитеты по безопасности разработали систему стандартов и рекомендаций по конструктивно-архитектурным изменениям зданий с целью повышения уровня безопасности [3]. Однако исполнение этих рекомендаций в каждом штате зависит от решений местного самоуправления, организации работы на местах.

В Чарльстоне, Южная Каролина, компания «Tony Deering», производитель бронетранспортеров, открыла новую дочернюю компанию, производящую пуленепробиваемые двери. Таким образом, компания обеспечила дверями три школы в этом районе. Однако, индустрия школьной безопасности требует больших финансовых затрат. В настоящий момент государство ежегодно выделяет на это 2,7 млрд долларов.

Особое внимание удалятся проблеме обеспечения возможности беспрепятственно покинуть помещение в случае опасности. Предполагается, что для достижения этой цели школы должны обеспечить свободный проход в холлах и лестничных пролетах. Однако несколько штатов проигнорировали эту рекомендацию и изменили локальные законы, разрешив установку систем баррикад в школах, которые могут включать железные заграждения, системы пропускного входа.

В результате введенных правительством мер по модернизации архитектурной среды школ, отмечается повышение уровня их безопасности.

Таким образом, в период с 2019 – 2020 гг. увеличился процент государственных школ, усиливших следующие меры безопасности и охраны: контроль доступа в школьные здания (с 92% до 97%), использование камер видеонаблюдения (с 61 % до 91%), обязательное ношение преподавателями и сотрудниками школы бейджей или удостоверения личности с фотографией (от 63% до 77%) [*4]*.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Акуленко, Н. Е. Развитие скулшутинга. его природа и сущность / Н. Е. Акуленко // Актуальные проблемы противодействия экстремизму и терроризму на современном этапе : Сборник научных статей I Всероссийской научно-практической конференции с международным участием, Новосибирск, 17–18 февраля 2022 года. – Новосибирск: Новосибирский военный институт имени генерала армии И.К. Яковлева войск национальной гвардии Российской Федерации, 2022. – С. 6-9.

2 Винниченко, Е. О. Международный опыт противодействия экстремизму: возможна Ли эффективная профилактика? / Е. О. Винниченко, Е. Б. Абдрасулов // Право и государство. – 2019. – № 2(83). – С. 99-113.

3 Гараганов, А. В. Социально-психологические причины школьного шутинга / А. В. Гараганов // Гуманизация образования. – 2022. – № 1. – С. 145-156. – DOI 10.24411/1029-3388-2020-10223.

4 Мурадян, В. Г. Стрельба в школах. Причины и способы предотвращения / В. Г. Мурадян, П. П. Филипкова, О. Н. Кажарская // Исследование инновационного потенциала общества и формирование направлений его стратегического развития : Сборник научных статей 11-й Всероссийской научно-практической конференции с международным участием, Курск, 30 декабря 2021 года / Редколлегия: М.Г. Клевцова (отв. ред.). – Курск: Юго-Западный государственный университет, 2021. – С. 307-310.

5 Перминов, Ф. В. Феномен "стрельбы в школе": причины и нравственное воспитание обучающихся как возможный способ его предупреждения / Ф. В. Перминов // Нравственные императивы в праве, образовании, науке и культуре : Материалы V международного молодежного форума, проводимого по благословению митрополита Белгородского и Старооскольского Иоанна, Белгород, 12 мая 2017 года. – Белгород: Курский институт кооперации (филиал) Автономной некоммерческой организации высшего профессионального образования "Белгородский университет кооперации, экономики и права", 2017. – С. 318-323.

УДК 340

Мухридинов Шахзод Фархатович, студент; Комсомольский-на-Амуре государственный университет
Mukhridinov Shahzod Farkhatovich, student, Komsomolsk-na-Amure State University
Мусалитина Евгения Александровна, доцент, Комсомольский-на-Амуре государственный университет
Musalitina Evgenia Aleksandrovna, associate professor, Komsomolsk-na-Amure State University

ПРАВОВЫЕ АСПЕКТЫ МЕЖДУНАРОДНОЙ СИСТЕМЫ БОРЬБЫ С ТЕРРОРИЗМОМ

LEGAL ASPECTS OF INTERNATIONAL SYSTEM OF FIGHTING AGAINST TERRORISM

Аннотация. Терроризм является глобальной проблемой, поскольку несет многочисленные человеческие жертвы, наносит ущерб экономической деятельности и развитию государства в целом. В последнее время проблема правовых аспектов борьбы с международным терроризмом приобрела особую актуальность. Международное сообщество признает необходимость усиления глобального реагирования системы уголовного правосудия на терроризм. В статье рассматривается международная правовая база по борьбе с терроризмом, которая регулирует направления этой деятельности.

Abstract. Terrorism is a global problem since it causes numerous victims, damages economic activity and the development of the state as a whole. Recently, the problem of legal aspects of the fight against international terrorism has become of special importance. The international community declares necessity to strengthen global criminal justice response to terrorism. The article discusses the international legal framework for the fight against terrorism which regulates the course of this activity.
Ключевые слова: терроризм, уголовное преследование, правовые аспекты, стратегическое партнерство.
Key words: terrorism, criminal prosecution, legal aspects, strategic partnership.

Терроризм является глобальной проблемой, поскольку несет многочисленные человеческие жертвы, наносит ущерб экономической деятельности и развитию государства в целом. Под термином «терроризм» понимается «социально опасное явление, для которого характерны радикальная идеология…сопровождаемое устрашением населения и иными противоправными насильственными действиями» [5].

Негативное воздействие терроризма на развитие особенно заметно проявляется в странах, находящихся в состоянии военных конфликтов, регионах со слабыми системами управления, неэффективными системами уголовного правосудия и экономической нестабильностью. Терроризм и провоцируемая им экономическая нестабильность осложняет инвестиции и международную торговлю. Отечественные и иностранные инвесторы часто рассматривают терроризм и уязвимость страны как признак нестабильности и угрозу безопасным инвестициям. Кроме того, терроризм ослабляет социальный и человеческий капитал страны, поскольку террористические атаки снижают качество жизни и могут вытеснить квалифицированных специалистов из страны. Террористические атаки и вызванные ими страхи также мешают гражданам пользоваться основными гражданскими правами, включая свободу передвижения, доступ к новым возможностям трудоустройства и образования. В силу этого, укрепление потенциала системы уголовного правосудия по борьбе с терроризмом является ключевым элементом всеобъемлющей стратегии развития любого государства.

В последнее время проблема правовых аспектов борьбы с международным терроризмом приобрела особую актуальность и нашла отражение в работах многих исследователей. В существующих работах можно выделить несколько направлений. Одно из них исследует юридические аспекты проблемы финансирования терроризма (А. Ю. Павшукова, М. Г. Ажибаев, Д. А. Акбарализода) [4], второе направление занимается изучением международно-правовых аспектов соблюдения прав и свобод на фоне кибертерроризма (И. А. Гуляева, В. В. Боровиков) [3]; следующее направление занимается исследованием уголовно-правовых аспектов террористической деятельности (Д. М. Куклина, А. А. Саенко, Я. А. Шаповалов) [6].

Исследователи отмечают, что эффективный ответ на терроризм должен включать подход, основанный на уголовном правосудии, руководствующийся нормативной базой, основанный на верховенстве закона и уважении прав человека [2]. Это требует совершенствования национальных систем уголовного правосудия для привлечения преступников к суду или экстрадиции; организации судебных разбирательств в разных странах в полном соответствии с глобальной правовой системой по борьбе с терроризмом.

Международное сообщество признает необходимость усиления глобального реагирования системы уголовного правосудия на терроризм. В связи с этим международное сообщество разработало общую правовую базу по борьбе с терроризмом, которая в настоящее время состоит из 16 конвенций и протоколов. Эти правовые документы вместе с резолюциями Совета Безопасности по вопросам терроризма составляют универсальный правовой режим борьбы с терроризмом.

В настоящее время действительно несколько международных правовых документов, регламентирующих борьбу с терроризмом. Это «Конвенция о борьбе с актами ядерного терроризма», принятая В 2005 г. Генеральной Ассамблеей ООН.; «Конвенция о борьбе с незаконными актами, направленными против безопасности морского судоходства» и др [1]. Эти правовые документы составляют основную часть глобального правового режима борьбы с терроризмом. Они были разработаны главным образом в качестве ответных мер на конкретные террористические акты или угрозы и охватывают следующие террористические акты: угон самолета; действия, направленные на саботаж авиации; насилие в аэропорту; действия, угрожающие безопасности морского судоходства; действия, угрожающие безопасности стационарных платформ, расположенных на континентальном шельфе; преступления против международного персонала (например, похищение дипломатов); незаконное приобретение и владение ядерным материалом; организация взрывов; финансирование и поддержка террористических актов и террористических организаций; ядерный терроризм.

Таким образом, учитывая появление новых форм и проявлений терроризма, необходимо постоянно совершенствовать правовые акты, устанавливающие регламент борьбы с террористическими преступлениями.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Ажибаев, М. Г. Вопросы привлечения лиц к ответственности за финансирование терроризма и экстремизма: правовые аспекты отечественного и международного законодательства / М. Г. Ажибаев // Вестник Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан. – 2022. – № 2(24). – С. 16-21. – DOI 10.52425/25187252_2022_24_16.

2 Акбарализода, Д. А. Теоретико-правовые аспекты противодействия терроризму / Д. А. Акбарализода // Законодательство. – 2021. – № 2(42). – С. 152-157.

3 Гуляева, И. А. Заведомо ложное сообщение об акте терроризма: международно-правовой аспект / И. А. Гуляева // Актуальные проблемы международного сотрудничества в борьбе с преступностью : Международная научно-практическая конференция, приуроченная к 65-летию со дня принятия Устава Международной организации уголовной полиции (Интерпола), Москва, 29 октября 2021 года. – Москва: Московский университет МВД России имени В.Я. Кикотя, 2021. – С. 20-22.

4 Павшукова, А. Ю. Международно-правовые аспекты регулирования борьбы с финансированием терроризма / А. Ю. Павшукова // Оригинальные исследования. – 2020. – Т. 10. – № 7. – С. 36-45.

5 Сыли, В. Н. Уголовно-правовое регламентирование преступлений террористического характера / В. Н. Сыли // Геополитическая картина мира: угрозы и вызовы : Сборник материалов Международной научно-практической конференции, Москва, 09–11 декабря 2020 года. – Москва: Московский государственный лингвистический университет, 2022. – С. 250-258.

6 Шаповалов, Я. А. Становление и динамика антитеррористической защиты объектов: частноправовой аспект / Я. А. Шаповалов // Гуманитарные и юридические исследования. – 2021. – № 3. – С. 124-130. – DOI 10.37493/2409-1030.2021.3.17.

УДК 621.9:519.8

Наливайко Наталья Сергеевна, студент; Комсомольский-на-Амуре государственный университет
Nalivayko Natalia Sergeevna, student of Komsomolsk-na-Amure State University
Когай Сергей Геннадиевич, старший преподаватель Комсомольский-на-Амуре государственный университет
Kogai Sergei Gennadevich, senior lecturer of Komsomolsk-na-Amure State University

ЭВОЛЮЦИЯ МЕТОДОВ КИТАЯ ПО БОРЬБЕ С ТЕРРОРИЗМОМ И ЭФФЕКТИВНОСТЬ ИХ ПРИМЕНЕНИЯ

EVOLUTION OF CHINESE COUNTERTERRORISM METHODS AND EFFECTIVENESS OF THEIR APPLICATION

Аннотация. В нашей статье мы рассматриваем эволюцию методов и подходов Китая в борьбе с терроризмом. Каким образом, и какие способы применяет правительство для противодействия террористическим актам и провокациям. Анализируем эффективность их внедрения и применения, а так же разбираем преимущества и негативные стороны проведения подобной политики, затрагивая их важность и необходимость для безопасности международного сообщества.
Abstract. In our article, we examine the evolution of China's methods and approaches in countering terrorism. How and what methods the government uses to counter terrorist acts and provocations. We analyze the effectiveness of their implementation and application, as well as the advantages and disadvantages of such policies, touching upon their importance and necessity for the security of the international community.
Ключевые слова: Китай, терроризм, безопасность, эффективность, экстремизм, борьба.
Key words: China, terrorism, security, effectiveness, extremism, fighting.

В окончании XX столетия поменялась геополитическая обстановка по всему свету, что воплотилось ростом террористической опасности, установив проблемы международной, а также региональной защищенности в нескольких основных приоритетах интернациональной политической деятельности государств.

Актуальность темы особенно характерна для таких стран, как Китай, который хорошо наслышан о терроризме, и борется с этой проблемой уже не один год, в связи с тем, что на западной территории Синьцзян-Уйгурской автономном районе (СУАР) функционируют террористические группировки. К их числу относятся «Исламская освободительная организация Восточного Туркестана» и «Информационный центр Восточного Туркестана», которые осуществили многочисленные теракты на территории, как Китая, так и в ряде других стран. В соответствии со сведениями, изученными в Европейском совете по части международных взаимоотношений, с 2004 по 2016 гг. по вине террористов погибли свыше 40 граждан Китайской народной республики. «Исламское государство» в 2015 г. требовало выкуп, а потом совершило казнь над гражданином Китайской народной республики Фань Цзинхуэем. В октябре 2013 г. на пекинской площади Тяньаньмэнь с множеством туристов в толпу людей выехал внедорожник, затем машина врезалась в ограждения и взорвалась, унеся жизни 5 человек, а 40 человек получили тяжелые травмы. Через 4 месяца было произведено новое оглушительное нападение с ещё большим количеством жертв. В марте на Куньминском вокзале в 8 террористов при помощи обычных кухонных ножей убили 29 граждан за 12 минут, и ранили ещё 143 человека. После этого борьба с экстремизмом стала одним из приоритетов китайской внутренней политики.

Началом этой политики стали решения по территории Синьцзяна, которая на данный момент времени является стратегически необходимым для страны с 40% угольным запасом КНР и с примерно ⅓ её нефтяных месторождений. Одновременно этот регион является самым беспокойным. За минувшие семьдесят лет там многократно вспыхивали волнения, преимущественно при поддержке Талибы в Афганистане и ИГИЛ, которая запрещена в Российской Федерации, на Ближнем Востоке поставляли уйгурам оружием и инструкторов. Рост войск и повальная китаизация не помогли, а только озлобляло местное население. Изменения произошли, когда в регион был назначен новый управляющий, который ранее заведовал ещё одной проблемно областью Китая Тибетом, Чэнь Цюаньго, прозванный «Железным Чэнем». Под его руководством через каждые 500 м в городах были установлены полицейские блокпосты. Число стражей правопорядка значительно возросло. За один только 2016 г. в Синьцзяне было набрано 90 тыс. правоохранителей. Все переходы из блоков были оборудованы системой Контрольно-пропускных пунктов, на которых предусмотрели средства сканирования радужной оболочки глаза. Десятки тысяч видеокамер, системы распознавания лиц – были направлены на отслеживание и передвижения в автоматическом режиме, в том случае если подозрительная личность отклонилось от привычного маршрута, полицейские посты были сразу же об это предупреждены.

С декабря 2017 г. начался собор образцов ДНК у всех жителей Синьцзяна. В регионе заблокировали все иностранные соцсети, а за их использование грозит уголовное преследование. Запреты распространились и на кухонные ножи, с помощью которых был произведён один из терактов, а теперь приобрести их можно лишь в специальных магазинах, предъявив для этого удостоверение личности, при этом на лезвие приобретаемого ножа гравируется QR-код с информацией о покупателе.

На момент 9 октября правительство Китая анонсировало документ «Положение о борьбе с экстремизмом в СУАР», таким образом, признав законным существования «лагерей перевоспитания», в которые, в свою очередь, помещали за соблюдение запрещенных религиозных обрядов, отказ от изучения китайского языка, чтение запрещённой литературы, и т.д. Однако к 2014 году после волны терактов, в Китае всё-таки дали согласие на ведение религиозной деятельности, но только в специально отведенных для этого учреждениях. Регламентированию подвергался и внешний вид, так например, запретили, как ношение хиджабов, так и «чересчур длинной бороды». В иных государствах подобные жестокие запреты имели возможность спровоцировать протест, но в Синьцзяне ровным счетом ничего такого не произошло, и Пекин добился собственной цели, учитывая то, что в 2012 г. произошло около 200 терактов, то в 2018 г. не зарегистрировано ни единого случая.

Современные методы борьбы с терроризмом в Китае к нынешним годам всё же претерпели изменения. Так в июне 2019 года в городе Бишкек прошёл саммит главнейших членов Шанхайской Организации Сотрудничества. В рамках этой встречи председатель Китая Си Цзиньпин произвел особый упор не только на проблематике региональной безопасности, но и на усилении борьбы с терроризмом. Акцентируя внимание на три базисных положения в борьбе с терроризмом, КНР предложил международному сообществу взаимообмен данными, укрепление киберборьбы с терроризмом, перерезать каналы аккумуляции финансов террористов, а также направить все силы на избавление от экстремизма. Данные позиции стали, своеобразной базой подходов китайского правительства по борьбе с терроризмом. Поднебесная осуждает подход запада к противодействию международному терроризму, а также дает отрицательную оценку «моральному превосходству» европейских государств в интернациональных взаимоотношениях, кроме того порицает вторжение во внутренние процессы. Пекин настаивает на сражении с ключевыми первопричинами терроризма, которые скрываются в бедности и определённых конфликтах, одновременно поддерживая международный диалог и

наращивая общественную интеграцию. Пекин в 2015 году принял закон по борьбе с терроризмом, который позволил Народной вооруженной милиции Китая, по сокращению НВМ, и Народно-освободительной армии, по сокращению НОАК, принимать участие в контртеррористических миссиях за пределами государства. Закон не очерчивает строгих масштабов таких миссий, благодаря чему обеспечивается предельная гибкость для вооруженных сил Китая при проведении любых операций. Утверждение закона повергло к решающим переменам в применении военной силы КНР заграницей. Перемены коснулись проведения учений, закупки оборудования, базирования и деятельности дипломатического характера, а также новейших разработок НОАК в границах утвержденной военной доктрины. Изменился и подход китайской столицы к международному сотрудничеству, Пекин стал активно вести диалог по обмену разведданными со своими новыми партнерами. В марте 2019 г. Госсовет КНР принял документ регламентирующий приверженность вести борьбу против терроризма в СУАР, уделяя внимание к обмену опытом и участию в международном сотрудничестве. Как доказательство эффективности, ВВП провинции значительно увеличился. Были предоставлены около 5 миллионов мест для рабочих. Почти 3,06 миллиона человек вышли из бедного положения, собственно которое Китай и называет одной из основных причин терроризма, – именно такая политика смогла официально преодолеть бедность в Синьцзяне. Увеличилось в два раза и число рабочих заводов, предприятий, частных и государственных, около 2,21 миллиона. Самое важное, это рост "индекса безопасности" – почти 99,13 % опрошенных жителей. Один из самых очевидных результатов – это как раз то, что регион превратили в едва ли не самую открытую внешнему сообществу провинцию КНР. Итоговый документ по десятилетнему развитию упоминает, что сотруднические связи у СУАР есть со 176 регионами и странами мира из почти двухсот имеющихся государств. Однако, исходя из этого, взаимоотношения между Китаем и его европейскими партнерами могут существенно ухудшиться в связи с различающимися взглядами на подходы по эффективному противодействию терроризму

Терроризм в Китае наряду с сепаратизмом, а так же экстремизмом воспринимаются как «три силы зла» – 三股势力, и они являются идейно неделимыми. Вследствие, проблемы связанные с темой сепаратизма в СУАР Китайской Народной Республики учитываются в пределах проблематики международного терроризма и способны спровоцировать непонимание всемирного общества. Китайская форма борьбы с терроризмом базируется на концепции «верховенства закона с китайской спецификой», что добавляет преграду для сопоставления интернационального, а также китайского опытов борьбы с терроризмом. Противодействие терроризму со стороны КНР хорошо заметно на примере проводимых учений. Таким образом, КНР активно принимает всестороннее участие, как оказывая противостояние терроризму в Юго-Восточной Азии, так и участвуя в учениях в рамках ШОС, сотрудничая с Пакистаном.

Важно отметить, что ранее учения, проводимые КНР имели преимущественно региональный характер до недавнего времени. Однако нынешняя география учений, проводимых Китаем и его партнерами, напрямую пересекается маршрутами с инициативой «Пояса и Пути», что дает возможность заявлять о соединении инициативы борьбы с терроризмом с развитием китайской инициативы и указывает на двойную эффективность проводимой политики. Бесспорно и понимание того, что дальнейшее развитие контртеррористической стратегии Китая будет связано именно с развитием инициативы «Пояса и Пути», поскольку для государства крайне важно поддерживать безопасности новых сухопутных и морских маршрутов.

И сегодня работники силовых структур КНР все непрерывно наращивают усилия в сражении с преступлениями террористической, экстремисткой и сепаративной ориентированности. Общегосударственная система борьбы с преступными группировками все время развивается, становиться гибче и приобретает все более глобальный ин-

тернациональный характер. Для диалога в противодействии с террористическими и экстремистскими организациями подключают все заинтересованные международные организации и государства. Сегодня Китай как-никогда готов возглавить это противостояние.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Терроризм в Китае // [Электронный ресурс] URL: https://student.zoomru.ru/history/terrorizm-v-kitae/43951.338007.s1.html (дата обращения 08.10.2022)

2. Позиция Китая в вопросе борьбы с внутренней и внешней террористической угрозой// [Электронный ресурс] URL: https://author.nbpublish.com/knt/article_25425.html (дата обращения 08.10.2022)

3. Анализ социально-экономических и этнополитических причин проявления международного терроризма в Китае // [Электронный ресурс] URL: https://vaael.ru/ru/article/view?id=817 (дата обращения 08.10.2022)

4. Терроризм в КНР и противодействие ему на примере Синьцзян-Уйгурского автономного района // [Электронный ресурс] URL: http://www.dslib.net/globrazvitie/terrorizm-v-knr-i-protivodejstvie-emu.html (дата обращения 08.10.2022)

УДК 81

Наливайко Наталья Сергеевна, студент; Комсомольский-на-Амуре государственный университет
Nalivayko Natalia Sergeevna, student of Komsomolsk-on-Amure State University
Кортун Екатерина Александровна, старший преподаватель Комсомольский-на-Амуре государственный университет
Kortun Ekaterina Aleksandrovna, senior lecturer of Komsomolsk-on-Amure State University

ЯЗЫК КАК СПОСОБ МАНИПУЛИРОВАНИЯ СОЗНАНИЕМ МИРНЫХ ГРАЖДАН ТЕРРОРИСТИЧЕСКИМИ ОРГАНИЗАЦИЯМИ ЧЕРЕЗ СРЕДСТВА МАССОВОЙ ИНФОРМАЦИИ

LANGUAGE AS A MEANS OF MANIPULATING THE MINDS OF CIVILIANS BY TERRORIST ORGANISATIONS THROUGH THE MEDIA

Аннотация. В статье исследуются особенности применения языка для воздействия на общественность. Рассматривается языковое манипулирование СМИ и правительствами стран, которые незаметно для себя играют на продвижение терроризма и увеличение числа участников террористических организаций. А так же предлагается метод ослабления подмены понятий и установления холодной беспристрастной лексики в средствах массовой информации.

Abstract. The article explores the specifics of using language to influence the public. It examines the linguistic manipulation of the media and governments of countries that are quietly playing to promote terrorism and increase the participation of terrorist organizations, as well as a method of weakening the substitution of concepts and establishing a cold, impartial vocabulary in the media.

Ключевые слова: язык, терроризм, языковое манипулирование, воздействие, СМИ
Key word: language, terrorism, language manipulation, influence, media

Терроризм, особенно в его негативном восприятии, в последнее время остается на переднем плане основных глобальных дискурсов. Не то чтобы терроризм был новым явлением, поскольку он так же стар, как и человеческая политика, но скорее из-за того, какое измерение он принял в последнее время. Из-за его кажущейся угрозы глобальному миру и безопасности он остается главной темой основных дискурсов. Особенно после исторической атаки на Всемирный торговый центр в Соединенных Штатах Америки 11 сентября 2001 года, совершенной группировкой "Аль-Каида". С этого дня, кажется, не проходит и дня без истории о террористической акции в той или иной стране. От Пакистана до Ирака, от Сомали до Египта, Кении, Сирии, Мали и многих других стран терроризм не прекращается. Во всех этих случаях терроризм принимает различные формы и приводит к различным разрушениям. В Нигерии это является наболевшей социальной угрозой. Начиная с вооруженной борьбы молодежи дельты Нигера за управление и контроль над нефтяными богатствами, борьбы, которая в какой-то момент была перехвачена социальными злоумышленниками, и, заканчивая непрекращающимися похищениями людей, охватившими другие регионы страны, особенно Юго-Восток, терроризм сохраняется.

Однако в нашей статье нас интересует не какая-то страна конкретно. Делать упор мы будем именно на язык, благодаря которому и производится основная нагрузка на умы населения. И так как английский язык является международным языком, он и станет главной темой для исследования в этой статье.

Язык относится к числу естественных явлений человеческой природы, которые привлекают пристальное внимание ученых. Однако в большинстве научных взглядов повторяется одна черта: язык - это средство коммуникации. Несомненно, язык важен для человека в плане социального выживания, как вода и пища для биологического и химического пропитания. Функции языка в социальной жизни человека огромны. Он это связующая сила, объединяющая и сплочающая механизм. Фактически, общество существует потому, что существует язык. Уберите язык, и общество распадется и разрушится. Эффективность языка заключается в его смысловом потенциале. Язык экспрессивно проявляется как сборник слов, фраз, клаузул и предложений, но они выбираются пользователями и систематически нанизываются друг на друга, чтобы выразить значения, уместные в определенном контексте. По сути, использование языка интерпретируется на фоне его контекста. Заимствуя слова Финегана, "люди используют язык в основном как инструмент для совершения действий: просят об услуге, дают обещание, сообщают новости, дают указания, предлагают приветствие, ищут информацию, направляют приглашение, просят о помощи и делают сотни других вещей...

То, что человек делает с помощью языка, может привести к положительным или отрицательным последствиям. Поэтому знание языка - это не просто умение выстраивать слова во фразы и предложения для кодирования сообщений и передачи их второй стороне, которая затем расшифровывает их, чтобы понять, что было задумано. Аналогично, использование языка не просто включает в себя кодирование и декодирование сообщений или просто достижение грамматической компетенции, где каждое предложение будет иметь фиксированную интерпретацию независимо от контекста его использования. Оно также воплощает в себе нашу способность использовать язык точно, уместно и гибко, чтобы отразить контекст и сообщение. Оно включает в себя способность заставить язык выполнять потребности пользователя предполагаемых рамках.

Если рассматривать его более подробно, то можно задеть следующие примеры. Утром 11 сентября 2001 года Мохамед Атта пролетел над балконами квартир мирного населения в Ист-Виллидж прямо над рейсом одиннадцатой авиакомпании American Airlines. Ужас, печаль и страх того трагического дня быстро разворачивались и остаются ощутимыми для жителей даже сейчас. Однако уже через неделю появился невероятно отстраненный язык для описания того, что произошло 11 сентября. Рассмотрим со-

общение, которое компания Verizon оставила в ящике голосовой почты жителей 19 сентября: «During this time of crisis, we are asking all customers to review and delete all current and saved messages that are not essential» ,- заявила безымянная женщина-диктор (В это кризисное время мы просим всех клиентов пересмотреть и удалить все текущие и сохраненные сообщения, которые не являются для вас жизненно-важными). «This request is necessary due to extensive damage that was recently sustained in the World Trade Center district» (Эта просьба необходима в связи с большим ущербом, который недавно был нанесен району Всемирного торгового центра).

Время кризиса? Неужели приливная волна вызвала «recently sustained» (недавно нанесенные) разрушения в Манхэттене? Аналогично, компания под названием «Tullet & Tokyo Liberty» ссылается на «the disaster that has hit New York and Washington» (катастрофу, обрушившуюся на Нью-Йорк и Вашингтон). Использование пассивного залога в этих и подобных случаях позволяет предположить, что Всемирный торговый центр и Пентагон были разрушены неуправляемыми, возможно, природными силами.

Компания под названием «Kinko's» была еще более многозначной. Вскоре после массового убийства компания по производству фотокопий разместила в своих магазинах несколько очень красочных плакатов со звездами и полосами, наложенными на контур сорока восьми нижних штатов США. Графика также включала в себя прискорбную надпись: «The Kinko's family extends our condolences and sympathies to all Americans who have been affected by the circumstances in New York City, Washington, D.C., and Pennsylvania» (Семья Kinko's выражает соболезнования и сочувствие всем американцам, которых затронули обстоятельства в Нью-Йорке, Вашингтоне, округ Колумбия, и Пенсильвании). «Circumstances» (обстоятельства) - это слово может описывать отключение электричества, но не кровопролитие террористов.

Точно так же постоянно в англоязычных СМИ мелькает, что люди «died» (погибли) в башнях-близнецах или в Пентагоне. Нет, люди «die»(умирают) в больницах, часто в окружении своих близких, пока врачи и медсестры предлагают помощь и утешение. Невинные люди во Всемирном торговом центре, в Министерстве обороны и на поле в Шанксвилле, штат Пенсильвания, были убиты в результате тщательно срежиссированного акта массового убийства. Чем больше пассивного, слабого, эвфемистического языка появлялось по мере того, как начиналась борьба с терроризмом, тем больше люди задумывались, что жизненно важно обратить пристальное внимание на слова, символы и образы, которые управляют этим новым и неотложным конфликтом. Цивилизованный мир сегодня сталкивается с самым антисемитским врагом с тех пор, как Адольф Гитлер и Йозеф Геббельс совершили самоубийство в Берлине почти 60 лет назад. Воинствующий ислам - самая кровожадная идеология со времен красных кхмеров, уничтоживших треть населения Камбоджи.

Исламо-фашизм - это всемирное явление, которое уже коснулось этой страны и многих других государств. Однако мусульманские экстремисты редко имеют армии, которые можно наблюдать, истребители, которые можно сбить с неба, или легко идентифицируемые штаб-квартиры, такие как рейхсканцелярия 1940-х годов. Однако в их руках более мощное оружие, с помощью которого они воздействуют на умы человечества. Языковое манипулирование вот, чем обладают эти далеко не малообразованные люди, а скорее наоборот.

Действия террористов с каждым годом переходят в более спланированную и подготовленную акцию, которая учитывает все, в том числе последствия, влияние их действий на общество и СМИ. Описание террористов как «одиноких волков» или «вдохновителей» и прозвища, такие как «Битлз», только прославляют их. Исламское государство» — это не государство, это группа людей, творящих ужасные вещи. Зои Александер, чей брат, 35-летний Ник Александр, был убит во время теракта в «Батаклане» в Париже в 2015 году, сказала, что термины, которые изображают ИГИЛ или

подобные организации как «гламурные», являются «крайне контрпродуктивными». Это, вероятно, деструктивный способ использования слов, когда необходимо быть более беспристрастными и более холодными в отношении репортажей. Такие термины, как солдат, одинокий волк и инициатор, подразумевают, что атаки были совершены по законным причинам. Злоумышленники используют терминологию, что «они с нами воюют». Это не война, а они не солдаты. Это пропаганда, которую они используют, чтобы затуманить мышление граждан, воздействуя, на то к чему все прислушиваются, заставляя звучать гораздо более легитимно, отстраненно, чем оно есть на самом деле.

Фонд мира Тима Пэрри Джонатана Болла, созданный в память о двух детях, ставших жертвами взрыва бомбы в 1993 году в Уоррингтоне, даже составил словарь «Counter-Daesh», который призывает использовать «lone actor»(одинокий актер), а не «lone wolf»(одинокий волк). «Волк имеет положительное, почти героическое значение. Следует проявлять осторожность, чтобы не прославлять преступную деятельность», — говорится в нем. «Mastermind(s)» (инициатор/ы), что подразумевает признание заслуг преступника, и «soldier(s)» (солдат/ы) следует заменить словом «perpetrator(s) » (преступник/и). Слово «caliphate» (халифат) придает ложную легитимность, поскольку это не государство, и его следует заменить на «Daesh-held territory» (территория, удерживаемая ИГИЛ), советует он. Он также предостерегает от использования таких слов, как «джихад», «джихадист» и «джихадистская невеста», которые часто игнорируют сложный религиозный смысл джихада. «Если в репортажах настаивают на его использовании, убедитесь, что это обозначено как «насильственный джихад», — говорится в нем.

Таким образом, можно будет избежать, пропаганды, которую умышленно проводят террористический группировки, умело манипулируя СМИ. Однако на деле это оказывается не так легко, как могло бы показаться, потому что в нынешней современности все лишь набирает обороты.

СМИ играют важную роль не только в освещении терроризма, но и в его формировании и развитии на мировой арене. Атаки 11 сентября 2001 года на нью-йоркские башни Всемирного торгового центра стали поворотным моментом в дискурсе о терроризме и значительно повлияли на то, как СМИ сообщают о террористических актах и кого называют террористом. Исследователи данной проблемы называют это собственными терминами и говорят о таком явлении, как «медиаориентированный терроризм». Совокупность актов, которые направлены на привлечение внимания Средств Массовой Информации, а благодаря СМИ — и внимания общественности. Террористам необходима особая публичность, и эту публичность им предоставляют СМИ, и в то же время они являются необходимыми для драматизации события, чтобы привлечь широкую аудиторию. Терроризм — это не просто источник новостей, а мощный инструмент информационного манипулирования сознанием и пропаганды. Медиа помогают продвигать политические интересы и формировать общественное мнение.

После взрыва 26 августа в аэропорту Кабула президент Байден сказал: «Мы этого не простим. Мы не забудем. Мы выследим вас и заставим заплатить.…Эти террористы ИГИЛ не победят». Ссылка Байдена на терроризм вряд ли была неожиданной. После 11 сентября слово «терроризм» стало центральным элементом политического нарратива, изображающего Соединенные Штаты как полностью вовлеченных в экзистенциальную борьбу против «оси зла». Два десятилетия спустя язык «терроризма» пронизывает политику стран по всему миру. 20 лет, прошедшие после 11 сентября, демонстрируют, как язык нанес побочный ущерб в виде расширения насилия против всех форм оппозиции. А правительства разных стран, продолжают использовать язык терроризма для оправдания политики, которая имеет мало общего с борьбой с «террором».

Название акта террористическим играет большую роль, устанавливая особое политическое и социальное значение. На примере всё тех же Соединённых Штатов Америки, событие 11 сентября и террористическая угроза использовались как оправдание

вторжения в Ирак. Террористическая угроза использовалась и Дональдом Трампом как оправдание запрета на въезд в США граждан шести мусульманских стран, подписанный президентом 27 января 2017 года.

Риторика, что для победы в войне в Ираке потребуется предпринять «морально опасные действия», изображающая терроризм как неминуемую угрозу, требующую решительных мер, помогла повысить общественную поддержку пыток и в глазах общественности «борьба с терроризмом» стала допустимой до любой жестокости, которую США совершали на Ближнем Востоке.

Как итог можно подвести, что язык напрямую оказывает самое главное влияние, манипулируя сознанием граждан. И угроза его использование во благо оправдания действий правительства, или для смягчения обстоятельств только усугубляет положение и призывает других людей к агрессии, подмене понятий об истинном зле и убийствах мирного населения. И таким образом языковое манипулирование только порождает новый терроризм, успешно играя в сторону террористической пропаганды, позволяя вербовать все большее количество людей с затуманенным сознанием, воспринимающим действия злоумышленников как норму или называя их оправданными.

Здесь, дома, мы можем побеждать сложившуюся обстановку с помощью вечной бдительности. Одним из наших главных оружий всех граждан должно стать то, что легко доступно каждому из нас – язык и умение здраво мыслить..

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Lexicon: The Language of Terrorism is Falling US // [Электронный ресурс] URL: https://www.theringer.com/2017/10/6/16431794/lexicon-terrorism-las-vegas (дата обращения 08.10.2022)

2. Terrorism and the Media: A Dangerous Symbiosis // [Электронный ресурс] URL: https://www.e-ir.info/2012/07/22/terrorism-and-the-media-a-dangerous-symbiosis/ (дата обращения 08.10.2022)

3. The Phrase "Islamic Terrorism" and the Power of Words// [Электронный ресурс] URL: https://digitalresource.center/resource/islamic-terrorism-and-power-words-0 (дата обращения 08.10.2022)

4. How Terrorists Are Creating a New Language // [Электронный ресурс] URL: https://areomagazine.com/2017/09/21/how-terrorists-are-creating-a-new-language/ (дата обращения 08.10.2022)

5. Translating Terrorism // [Электронный ресурс] URL: https://www.languagerealm.com/articles/translating_terrorism.php (дата обращения 08.10.2022)

6. Eagles of Death Metal Merch Manager Nick Alexander Killed in Paris Attack // [Электронный ресурс] URL: https/www.rollingstone.com/music/music-news/eagles-of-death-metal-merch-manager-nick-alexander-killed-in-paris-attack-50447/

7. No ‘lone wolf’: media urged to take care over terrorism vocabulary // [Электронный ресурс] URL:https/www.theguardian.com/uk-news/2018/sep/24/no-lone-wolf-media-urged-to-take-care-over-terrorism-vocabulary

8. Шушарина Г.А. Репрезентация ценностей в дискурсивном пространстве разового политического дискурса // Ученые записки Комсомольского-на-Амуре государственного технического университета. 2020. № 4 (44). С. 20-26.

УДК 621.9:519.8

Огнева Анастасия Андреевна, студентка, Комсомольский-на-Амуре государственный университет
Ogneva Anastasia Andreevna, student of Komsomolsk-na-Amure State University
Шахова Олеся Александровна, студентка, Комсомольский-на-Амуре государственный университет
Shakhova Olesya Aleksandrovna, student of Komsomolsk-na-Amure State University
Когай Сергей Геннадьевич, старший преподаватель, Комсомольский-на-Амуре государственный университет
Kogai Sergei Gennadevich, Senior Teacher of Komsomolsk-na-Amure State University

СИСТЕМА ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В КИТАЕ

CYBERSECURITY SYSTEM IN CHINA

Аннотация. Данная работа освещает проблему кибертерроризма на территории Китая и принятые китайским законодательством способы защиты информационного поля во избежание утечки данных и личной информации. Раскрывается суть используемых методов и их эффективность, а также упоминаются применяемые в настоящее время системы киберзащиты.
Abstract. This work highlights the problem of cyberterrorism in China and the ways adopted by Chinese legislation to protect the information field in order to avoid leakage of data and personal information. The essence of the methods used and their effectiveness are revealed, as well as the cyber defense systems currently used are mentioned.
Ключевые слова: система безопасности, кибербезопасность, кибертерроризм, информационная безопасность в Китае, закон о распространении личных данных.
Key words: security system, cybersecurity, cyberterrorism, information security in China, the law on the dissemination of personal data.

В современном мире киберпространство является областью жизни и работы людей, каналом для распространения информации, средством для коммуникации и сотрудничества, а также служит источником культурного богатства. Однако по мере развития Интернета и информационных технологий в мировом сообществе растёт угроза кибертерроризма.

В борьбе за национальную безопасность в киберпространстве в Китае объединены военные и гражданские органы управления, разработана соответствующая юридическая база, регулирующая их функции. Ведущую роль в информационной политике КНР занимает КПК (Коммунистическая партия Китая), что отличает Китай от большинства стран мира.

Китай добился значительного прогресса во внедрении всеобъемлющей нормативно-правовой базы с помощью трех законов о кибербезопасности и регулировании распространения персональных данных. К этим законам относятся Закона о кибербезопасности, вступивший в юридическую силу 1 июня 2017 г.; Закона о защите данных, действующий с 1 сентября 2021 года, и Закона о защите личной информации, который был принят незначительно позднее - 1 ноября 2021 года.

С момента принятия в 2017 году Закона о кибербезопасности Китай быстро развил свой режим регулирования технологий и обработки информации. В 2018 и 2019 годах был введен ряд стандартов и руководящих принципов для дальнейшего определения сферы применения правил и их требований. В 2020 году, после двух лет поддержки нормативных актов и разработки проектов по их корректированию, регулирующие органы, в частности Министерство общественной безопасности, переключило свои усилия на обеспечение соблюдения нормативных требований.

В Китае значительно возросла котнролирующая риски активность, связанная с сертификацией Многоуровневой схемы защиты (MLPS) - стандартом кибербезопасности, основанном на соображениях национальной безопасности и социальной стабильности.

Более современным стандартом является система MLPS 2.0, представляющая собой комплексный технологический стандарт, требующий от компаний оценки текущего состояния своих информационных и операционных технологических систем и связанных с ними возможных рисков. Требования к контролированию определенных факторов не ограничиваются технологиями; они включают деловые и управленческие функции, такие как распоряжение человеческими ресурсами.

Как и более ранняя версия системы MLPS, ее последующая замена устанавливает пять уровней кибербезопасности в зависимости от риска. Отдельным системам предварительно присваивается “уровень”, основанный на потенциальном воздействии утечки данных или компрометации системы. По большей части, это анализ рисков, что является одним из ключевых различий в подходе к кибербезопасности со стороны китайских и международными стандартов.

Уровни варьируются от 1 до 5, где 5 предназначен для чувствительных правительственных объектов и систем. Уровень систем будет определять требования к контролю безопасности в нескольких доменах. Более высокие уровни предъявляют более строгие требования к безопасности.

Помимо этого, к базовым документам, обеспечивающим внутригосударственную информационную безопасность КНР, относится Антитеррори-стический закон, принятый в 2015 г. Он предполагает дешифровку интернет-трафика, изъятие у иностранных компаний информации, используемой для террористических целей, а также введение цензуры для СМИ на территории Китая.

Во все более неопределенном мире политики Китая предпринимают решительные шаги по снижению рисков кибербезопасности, которые они рассматривают как угрозу экономике, обществу и национальной безопасности. Учитывая, что программа MLPS является наиболее зрелым и всеобъемлющим регулированием, направленным на устранение общих рисков кибербезопасности, это одновременно важная инициатива и серьезная проблема соблюдения требований для компаний, работающих в Китае и вынужденных соответсовать выбранной системе.

Национальная стратегия безопасности в киберпространстве КНР определяет информационную безопасность как основу стабильности в стране, для поддержания которой необходимо предотвращать любые виды вмешательства в политическую, социальную и культурную жизнь государства. Данная стратегия реализует защиту законных прав своих граждан в сети Интернет. В сфере обеспечения кибербезопасности был определен главный проект - "Золотой щит" - система фильтрации интернет-контента в Китае. "Золотой щит" — это один из ведущих проектов КНР в области создания электронного правительства, за реализацию которого отвечает бюро общественной информации и надзора за сетевой безопасностью.

"Щит" применяется провайдерами для защиты компьютерных систем от хакерских атак и интернет-вирусов, а также для ограничения доступа к информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Cyberattack on Google Said to Hit Password System / NY Times. URL : http://www.nytimes.com/2010/04/20/technology/20google (Дата обращения 10.10.2022).

2. Enforcement of China’s Multi-Level Protection Scheme - The rapid roll-out of cyber security compliance / Jim Fitzsimmons. URL : https://www.controlrisks.com/campaigns/china-business/enforcement-of-chinas-multi-level-protection-scheme (Дата обращения 10.10.2022).

3. Is China's Xinhua the Future of Journalism? / Newsweek. URL : https://www.newsweek.com/chinas-xinhua-future-journalism-71961 (Дата обращения 10.10.2022).
4. Ministry of Industry and Information Technology / Reporters without borders. URL : http://english.www.gov.cn/state_council/2014/08/23/content_281474983035940.htm (Дата обращения 10.10.2022).
5. Number Resources / IANA official website. URL : http://www.iana.org/numbers (Дата обращения 10.10.2022).
6. Open letter to the Yahoo! Chairman / Reporters without borders. URL : http://archives.rsf.org/article.php3?id_article=2959 (Дата обращения 10.10.2022).

УДК 327.28+327.3+316.42

Пиллер Илья Константинович, студент, Благовещенский государственный педагогический университет
Piller Ilya, student, Blagoveshchensk State Pedagogical University
Буяров Дмитрий Владимирович, к.ф.н., доцент, зав. кафедры всеобщей истории, философии и культурологии, Благовещенский государственный педагогический университет
Buyarov Dmitriy Vladimirovich, Ph.D., Associate Professor, Head of the Department of General History, Philosophy and Cultural Studies, Blagoveshchensk State Pedagogical University

ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ

INFORMATION TERRORISM ON THE GLOBAL INTERNET

Аннотация. В статье рассматриваются крупнейшие проблемы распространения информационного терроризма в сети Интернет и их виды, а также способы их решения. Под данным тезисом подразумеваются различные виды шантажа, глобальные мошеннические аферы, взломы баз данных и последующая публикация их в интернете, взлом сайтов государственного значения, вмешательство в политические события стран мира.
Abstract. The article discusses the problems of the spread of terrorism in the information sphere on the Internet and their types, as well as ways to solve them. This thesis implies various types of blackmail, global fraudulent scams, database hacks and their subsequent publication on the Internet, hacking of sites of national importance, interference in political events of countries around the world.
Ключевые слова: информационный терроризм, кибертерроризм, киберпреступность, Интернет, фишинг.
Key words: information terrorism, cyberterrorism, cybercrime, Internet, phishing.

Целью статьи является рассмотрение информационного терроризма в Интернете в общественно-политическом аспекте. Задачи поставлены следующие: оценить степень влияния на социальную сферу, определить возможности снижения уровня киберпреступности, описать последствия информационного.

Понятие информационного терроризма сложилось еще в 1980-ые годы Барри Коллином, старшим научным сотрудником Института безопасности и разведки и подразумевало оно распространение терроризма на киберсреду. Если мы рассматриваем современное понятие, то конкретной формулировки не существует. Информационный терроризм (далее по тексту – кибертерроризм) как таковой – это совокупность различных преступных деяний в отношении как физических лиц, так и юридических в киберпространстве.

В наше время тема информационного терроризма актуальна, поскольку происходит повсеместная компьютеризация многих сфер жизни. Ввиду отсутствия курсов

компьютерной грамотности для людей кибертеррористы пользуются данной брешью в человеческом разуме, тем самым наращивая масштабы своих преступлений.

Изначально информационный терроризм заключался в основном в различных мошеннических схемах по типу фишинга (прим. – фишинг – это тактика рассылки мошеннических электронных писем и попытка обманом заставить получателей нажать на вредоносную ссылку или скачать зараженное вложение, чтобы затем украсть их личную информацию). Данный способ крайне прост, поскольку не требует особых действий для привлечения внимания потенциальных жертв, поскольку они сами из-за неумения фильтровать поступающую информацию попадаются на уловку. Одним из популярных примеров фишинга был следующий случай: The Daily Swig сообщила о фишинговой атаке, произошедшей в декабре 2020 года на американского поставщика медицинских услуг Elara Caring, которая произошла после несанкционированного компьютерного вторжения, нацеленного на двух его сотрудников. Злоумышленник получил доступ к электронной почте сотрудников, в результате чего были раскрыты личные данные более 100 000 пожилых пациентов, включая имена, даты рождения, финансовую и банковскую информацию, номера социального страхования, номера водительских прав и страховую информацию. [1].

На 2022 год пришлось также крайне много фишинговых атак. Самые крупные из них:

- Публикация данных «Яндекс.Еда» – ФИО, адрес, номер телефона. Примерно 6,9 миллионов данных, 50 миллионов заказов.
- Публикация данных «Гемотест» – все личные данные клиентов. 31 миллион строк информации, 554 миллиона заказов [2].

Еще одним способом информационного терроризма является распространение компьютерных вирусов. Так, например, вирус WannaCry в 2017 году стал самым массовым за XXI век и нанес ущерб примерно на 1 миллиард долларов.

Почему происходят подобные кибератаки? Дело в социальной инженерии. Люди, не особо отличая настоящие письма от поддельных успешно им доверяют и переходят по прикрепленным ссылкам. Здесь мошенники в большинстве своем играют на интересах пользователей, используют так называемые кликбейтные (прим. – то, на что успешнее всего среагирует человек и перейдет по ссылке) заголовки и тексты. Ловко используя психологические приемы, киберпреступники вымогают баснословные деньги. Чаще всего именно деньги являются основным мотивом в информационном терроризме, после этого идут уже какие-то собственные цели, очевидно преследуемые не столько самими хакерами, а скорее определенными лобби, которые заинтересованы дестабилизации какой-то страны или же всего мира.

Можно сказать о «нигерийских письмах», которые получили свое распространение в 2000-ых. Это электронные письма, которые написаны якобы от банкира нигерийского принца, который оставляет наследство адресату. Тот, в свою очередь, наивно веря, что получил легкие деньги, переходит по ссылке и становится жертвой мошенника.

Информационный терроризм наносит серьезный вред по социальной и политической сфере общества везде, где есть Интернет, поскольку кибертеррористы способны влиять на процессы внутри общества через взломы социальных сетей и последующую агитацию, но пока это успешно пресекается государственными службами безопасности, поскольку деятельность подобных группировок противоречит законодательству.

В современной политике существует понятие хактивизма (прим. – использование незаконными способами компьютеров и компьютерных сетей для продвижения политических идей, свободы слова, защиты прав человека и обеспечения свободы информации). Хактивисты не являются интернет-террористами, поскольку своей целью ставят привлечение внимания к их лозунгам, а не кибертеррор, но нередко они становятся соучастниками крупных преступлений.

Так, например, огромный резонанс вызвал арест 7 декабря 2010 года основателя портала «WikiLeaks» Джулиана Ассанжа. Почти сразу хакеры атаковали сервисы, которые, по их мнению, провинились перед Ассанжем.

Портал известной платежной системы MasterCard приостановил свою работу из-за хакерской атаки. Нападение на сайт было совершено в отместку за арест Ассанжа. Кроме того, хакеры обрушились на сайт платежной системы PayPal, отказавшейся принимать пожертвования для WikiLeaks, и на сайт швейцарского банка Swiss Post Office, где были заморожены счета австралийца.

По данным, опубликованным на сайте информационного агентства «РИА Новости», атака была проведена группой анонимных активистов, которая называет себя «Anonymous» (прим. – общее название хакерских групп по всему миру, особой связи между собой они не имеют). [3, с. 4].

Anonymous называют себя «интернет-собранием» с «очень свободной и децентрализованной структурой управления, которая основана на идеях, а не директивах» [5].

Также хактивисты не только заявляют о себе, но и успешно провоцируют социальные события. Anonymous не был на слуху в течение многих лет после перезапуска операции Darknet в 2017 году. Но о ней снова заговорили в 2020 году, когда группа выступила против коррупции в полиции после смерти Джорджа Флойда. В поддержку крупнейшего общественно-политического движения Black Lives Matter группа опубликовала в Twitter видео, в котором специально критикует полицейское управление Миннеаполиса. В результате аккаунт Anonymous в Твиттере взорвался популярностью, обеспечив приток 3,5 миллионов новых подписчиков в течение нескольких дней после публикации видео [6].

Одной из серьезных проблем информационного терроризма можно отметить крайне быстрое распространение слухов, в том числе фейковой информации, несущей в себе деструктивный характер [4, с. 2]. Так, к примеру, случилось в ситуации с пожаром в ТРЦ «Зимняя вишня» в 2018 году. Тогда правительство Кемеровской области долго не сообщало точные данные касаемо погибших и раненых, в результате чего начали появляться различные фейки. Вследствие вбрасывания ложной информации в обществе начались волнения, которые затронули, буквально говоря всю Россию. В 2019 году был подписан так называемый закон о фейках, который вводил уголовную ответственность за распространение неверной информации, вводящей в заблуждение население РФ [7].

Среди молодежи стал популярен так называемый скамминг (прим. – вид интернет-мошенничества, реализуемый через фейковые продажи вещей; наивные покупатели переводят деньги скамеру, тот перестает выходить на связь – буквально говоря, классика данного вида мошенничества). Это является серьезной проблемой и масштабы начинают поражать, поскольку данный вид преступлений популяризируется через рэп-индустрию.

На данный момент проблема информационного терроризма периодически решается, но хакеры находят новые бреши в системе, тем самым вызывая все более крупные и резонансные события, влияющие на общество.

Способы решения проблемы информационного терроризма:

- привлечение молодых IT-специалистов, способных внести новые корректировки в систему безопасности и отслеживания потенциальных кибертеррористов;
- использовать теорию социальной инженерии, влияя на слабые стороны хакеров;
- корректирование юридической базы с целью недопущения распространения в Интернете слухов, которые могут привести к общественным волнениям.

В качестве заключения стоит сказать о том, что очень многое можно подвязать к информационному терроризму, но его рамки имеют собственный минимум, поскольку если киберпреступления затрагивают лишь локально обозначенную малую часть, не выходя за рамки территориального региона, тогда это является своего рода хулиган-

ством. Да, это влияет на общество, но гораздо в меньшей степени, нежели бы это было в рамках целой страны или мира. Точно так же и со слухами.

Информационный терроризм несет за собой серьезные последствия. Помимо того, что публикуются личные данные миллионов пользователей, что уже само по себе противоречит нормам права, так еще это приводит к общественным волнениям, которые могут нести за собой серьёзные последствия для государства.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. 11 типов фишинга и их примеры из реальной жизни [Электронный ресурс]. URL: https://www.cloudav.ru/mediacenter/tips/types-of-phishing/ (дата обращения: 25.10.2022).

2. 14 компаний, откуда утекли данные пользователей в 2022 году [Электронный ресурс]. URL: https://www.sravni.ru/text/14-kompanij-otkuda-utekli-dannye-polzovatelej-v-2022-godu/ (дата обращения: 25.10.2022).

3. Акопов Г.К. Политический «хактивизм» в эпоху информатизации социума // Научно-культурологический журнал «Relga». 2014. №1, 7 с.

4. Григорьев Н.Ю., Родюков Э.Б. Информационный терроризм // Вестник Университета. 2015, 6 с.

5. Основные мировые события, хактивизм и #OpOlympicHacking [Электронный ресурс]. URL: https://habr.com/ru/company/dell_technologies/blog/308334/ (дата обращения: 25.10.2022).

6. Что такое хактивизм? Кампании, которые сформировали движение [Электронный ресурс]. URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/348956.php (дата обращения: 25.10.2022).

7. Федеральный закон о внесении изменений в статью 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_320401/ (дата обращения: 25.10.2022).

УДК 327

Пустовит Никита Евгеньевич, студент, Комсомольский-на-Амуре государственный университет
Pustovit Nikita Eugenevich, student of Komsomolsk-na-Amure State University
Мусалитина Евгения Александровна, кандидат культурологии, доцент, Комсомольский-на-Амуре государственный университет
Musalitina Evgenia Alexandrovna, Candidate of Cultural Sciences, Associate Professor, Komsomolsk-na-Amure State University

ВОЕННО-ТЕХНИЧЕСКОЕ СОТРУДНИЧЕСТВО РОССИИ И КИТАЯ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ВНУТРЕННЕЙ И ВНЕШНЕЙ БЕЗОПАСНОСТИ В РАМКАХ ШОС

MILITARY-TECHNICAL COOPERATION BETWEEN RUSSIA AND CHINA TO ENSURE INTERNAL AND EXTERNAL SECURITY IN THE FRAMEWORK OF THE SCO

Аннотация. В статье рассматриваются этапы становления военно-технического сотрудничества России и Китая, сферы такого сотрудничества, предпосылки образования Шанхайской организации сотрудничества, а также совместные действия стран, реали-

зуемые в рамках антитеррористических мероприятий. Указываются проблемы и перспективы работы по борьбе с терроризмом стран – участников ШОС.
Abstract. This report examines the stages of formation of military-technical cooperation between Russia and China, examples of such cooperation, prerequisites for the formation of the Shanghai Cooperation Organization, as well as joint actions of the countries carried out within the framework of anti-terrorist activities. The problems and prospects of work in the fight against terrorism of the SCO member countries are indicated.
Ключевые слова: военно-техническое сотрудничество, Шанхайская организация сотрудничества, безопасность, совместные учения.
Key words: military-technical cooperation, Shanghai Cooperation Organization, security, joint exercises.

Поставки вооружений являются важным показателем уровня стратегического доверия между странами. За последние 70 лет отношения между Китаем и Советским Союзом/Россией проходили через этапы, которые характеризовались кардинально разными уровнями военно-промышленного сотрудничества. Последствия крымского кризиса 2014 г. повлияли на российско-китайские отношения в сфере торговли оружием на фоне истории, когда Россия стремилась ограничить поставки оружия в Китай. Санкции, введенные против Китая после боевых действий на Тяньаньмэнь в 1989 г. и против России с начала 2014 г., имели последствие в виде стимулирования более тесного российско-китайского сотрудничества в сфере оружейной промышленности.

Изменившиеся после 2014 г. стимулы способствовали беспрецедентному китайско-российскому оружейно-промышленному сотрудничеству, которое способствует развивающемуся российско-китайскому военному взаимодействию, и, в конечном итоге, может привести к более равноправным отношениям в совместной разработке вооружений.

В период с 2005 по 2012 гг. объем российско-китайской оборонной торговли заметно снизился. Китайский оборонный импорт в целом сократился примерно на 58% с 2007 по 2011 гг.; в то время как страна начала проявлять большую активность на рынке экспорта вооружений с 2001 по 2011 гг., китайский оборонный экспорт вырос на 95%. Для многих экспертов это свидетельствовало о растущем чувстве самодостаточности китайских производителей оружия и уменьшении степени зависимости от российских систем и российской технической поддержки. Еще одним фактором, способствовавшим снижению объемов поставок российских вооружений в Китай в этот период, были трения, возникшие в связи с обвинениями России в китайском реинжиниринге и незаконном копировании российских систем [3].

Кроме того, китайцы неоднократно обращались к России за помощью в решении технических проблем с закупленными радиолокационными системами, которые, как выяснилось после проверки, были вызваны неудачными попытками заменить оригинальные российские компоненты китайскими аналогами.

С момента вступления на пост главы государства Си Цзиньпина в 2012 г. российско-китайское оборонно-промышленное сотрудничество вновь начало развиваться, достигнув высоко уровня.

Исходя из предположения, что российская оборонная промышленность может оказаться неспособной эффективно компенсировать потерю доступа к западным технологиям с 2014 г., Китай и Россия могут вскоре поменяться традиционными ролями, при этом Китай будет все больше становиться поставщиком для России.

Активизация российско-китайского военно-технического сотрудничества должна рассматриваться на фоне общего усиления политической и стратегической координации между администрациями Си Цзиньпина и В. Путина, которая включает в себя не просто декларации на уровне риторики, а существенные обмены в нескольких стратегически важных сферах, включая торговлю нефтью и газом, геополитическую коорди-

нацию в Центральной Азии, совместные военные учения, контроль информационной сферы и взаимную поддержку в международных организациях.

После десятилетий блокирования российско-китайских оружейно-промышленных контактов экономическое давление после распада Советского Союза создало для России сильные стимулы для более тесного сотрудничества с Китаем. В то время у Китая не было альтернативных вариантов из-за западного эмбарго на поставки оружия. Эти обстоятельства нашли отражение на политическом уровне: в 1996 г. Россия и Китай сформировали «стратегическое партнерство координации», а в 2001 г. совместно основали Шанхайскую организацию сотрудничества (ШОС) для более тесной координации действий в Центральной Азии [2].

Что касается общемировых проблем, таких как борьба с терроризмом, Китай и Россия приняли резолюцию ООН. Так, например, ШОС действует в русле Контртеррористического комитета Совета Безопасности ООН. ШОС придает большое значение доработке в ООН проектов Международной конвенции по борьбе с актами ядерного терроризма и Конвенции по борьбе с международным терроризмом.

В целях подготовки и отработки навыков противодействия новым террористическим угрозам Россия и Китай провели антитеррористические учения в 2021 г. В Оренбурге открылись крупные многонациональные антитеррористические учения «Мирная миссия 2021» с участием стран-членов Шанхайской организации сотрудничества. Около 4000 офицеров и солдат из восьми стран-членов ШОС, включая Россию, Китай, Казахстан, Пакистан и Индию, принимали участие в учениях на полигоне. Народно-освободительная армия Китая направила 558 военнослужащих и 130 единиц техники для участия в 14-х совместных учениях, организованных ШОС [1].

В Манесаре (Индия) прошли многонациональные совместные антитеррористические учения (JATE) «Манесар-Антитеррор 2022» в рамках мероприятий Шанхайской организации сотрудничества, в ходе которых страны-участницы обменялись инновационными методологиями и передовым опытом в борьбе с экстремизмом и терроризмом. В мероприятии приняли участие представители антитеррористических сил шести стран-членов РАТС-ШОС, в том числе Казахстана, Кыргызской Республики, Узбекистана, Таджикистана, Российской Федерации и Индии [3].

Во время последнего саммита в Самарканде лидеры стран ШОС впервые собрались вместе лично после периода виртуальных встреч. Это было широко ожидаемое событие, особенно из-за двух ключевых лидеров ШОС: Президента России В. Путина и его китайского коллеги Председателя Си Цзиньпина, которые встретились в кулуарах саммита - впервые после пандемии.

Си Цзиньпин призвал к расширению сотрудничества в области безопасности по таким традиционным угрозам, как борьба с терроризмом, сепаратизмом, экстремизмом, наркотрафиком и транснациональной организованной преступностью. Это давние цели ШОС и «Шанхайской пятерки», которая предшествовала ШОС и существовала в период с 1996 по 2000 гг.

Российско-китайские отношения постулируются в зависимости от отношений между США и Китаем, как заявляет Э. Сун, старший научный сотрудник Сингапурского института международных отношений. «Если отношения между США и Китаем ухудшаются, то Россия и Китай еще больше сблизятся. В настоящее время отношения между США и Китаем претерпевают не лучшие времена, поэтому вполне естественно, что отношения между Россией и Китаем улучшатся» [1].

Международный форум по борьбе с терроризмом «Великая стена-2022», спонсируемый Народной вооруженной полицией Китая (НВП) завершился 31 августа. Этот двухдневный форум, организованный Специальной полицейской академией РАР, собрал более 170 представителей вооруженных полицейских сил или вооруженных сил подобного рода из 30 стран, включая Китай, Россию, Пакистан, Бразилию и Италию.

Участники форума обменялись мнениями и провели открытые и конструктивные дискуссии по проблемам международного сотрудничества в борьбе с терроризмом между жандармерией, полицией или вооруженными силами мира и применение беспилотного и интеллектуального оружия в контртеррористических операциях в различных условиях, например, в городских/горных районах [4].

В начале сентября 2022 г. Китай присоединился к российским военным учениям в дальневосточном регионе России. Глава Китая предложил продолжать проводить совместные антитеррористические учения, жестко пресекать терроризм, сепаратизм и экстремизм, незаконный оборот наркотиков, а также кибер- и транснациональную организованную преступность. Китай готов в ближайшие пять лет подготовить 2000 сотрудников правоохранительных органов для государств-членов ШОС и создать китайско-ШОСовскую базу для подготовки сотрудников по борьбе с терроризмом, чтобы усилить наращивание потенциала правоохранительных органов государств-членов ШОС.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Кабасакалова, М.Г. Внешняя политика США как фактор сближения России и Китая // Вестник Российского университета дружбы народов, 2015. – № 1. – С. 70-78.

2 Топычканов, П. В. Трансформация регионального сотрудничества в области безопасности (на примере Шанхайской организации сотрудничества // Вестник Московского университета. – 2013. – № 4. – С. 84-96.

3 Фаткулин, С. Т. Сотрудничество правоохранительных органов государств-участников ШОС по противодействию международному терроризму и экстремизму / С. Т. Фаткулин, М. В. Мулюкова // Правопорядок: история, теория, практика. – 2019. – № 4(23). – С. 109-114.

4 Чжэн, Ж. Сотрудничество России и Китая в борьбе с международным терроризмом (в рамках ШОС) : специальность 23.00.04 "Политические проблемы международных отношений, глобального и регионального развития" : автореферат диссертации на соискание ученой степени кандидата политических наук / Чжэн Жуньюй. – Москва, 2008. – 26 с.

УДК 327

Роскольчук Вадим Игоревич, студент, Комсомольский-на-Амуре государственный университет
Roskolchuk Vadim Igorevich, student, Komsomolsk-na-Amure State University
Лопатина Ольга Ивановна, старший преподаватель, Комсомольский-на-Амуре государственный университет
Lopatina Olga Ivanovna, senior lecturer, Komsomolsk-on-Amur State University

СЕПАРАТИСТСКИЕ ДВИЖЕНИЯ КАК ПРОЯВЛЕНИЕ ТЕРРОРИЗМА

SEPARATIST MOVEMENTS AS A MANIFESTATION OF TERRORISM

Аннотация. В данной статье рассмотрено определение сепаратизма, его связь с религиозными, политическими и культурными взглядами. Необходимость в характеристике возникла уже давно, поскольку его часто намеренно заменяют правом народа на самоопределение. В конфликтах можно наблюдать умелое вмешательство во внутренние дела государства, провоцирующее внутригосударственные беспорядки, которые могут привести к нарушению территориальной целостности. Сделана попытка обобщить информацию о связи этнического терроризма, сепаратизма и экстремизма.

Abstract. This article examines the definition of separatism and its relationship to religious, political and cultural attitudes. The need for a characterisation has been around for a long time, as it has often been deliberately substituted for a people's right to self-determination. In conflicts, one can observe skillful interference in the internal affairs of the state, provoking internal disturbances that can lead to the violation of territorial integrity. An attempt has been made to summarise the information on the links between ethnic terrorism, separatism and extremism.
Ключевые слова: сепаратизм, этнотерроризм, национализм.
Key words: separatism, ethno-terrorism, nationalism.

Общепринятое определение сепаратизма заключается в том, что это пропаганда состояния культурного, этнического, племенного, религиозного, расового, правительственного или гендерного отделения от более крупной группы. Хотя часто речь идет о полном политическом отделении, сепаратистские группы могут добиваться не более чем большей автономии.

Террористы-сепаратисты (также называемые националистическими террористами) используют акты террора, чтобы заставить создать новое государство или присоединиться к другому существующему государству, с которым тесно связана сепаратистская община.

Этнический терроризм значительно отличается от насилия, совершаемого по идеологическим, религиозным или финансовым мотивам. Этнические террористы часто стремятся повлиять на свой собственный электорат больше, чем на страну в целом. Этнические террористы часто стремятся укрепить общинную идентичность, в отличие от идентичности, предлагаемой государством. Этнические террористы часто нападают на потенциальных посредников, которые в противном случае могли бы пойти на компромисс в вопросах идентичности. Вторичной целью атак является создание атмосферы страха среди населения конкурирующей группы.

Этнический терроризм создает сложную проблему для государства: обычные контрмеры могут вызвать более широкую поддержку повстанческого или сепаратистского движения, даже если они препятствуют или побеждают конкретную террористическую группу. Поскольку государственные стратегии часто дают обратный эффект, идеальной стратегией является политика "внутри группы" - поощрение умеренных этнических групп с помощью пряников и кнутов для наказания радикальной активности.

Сепаратизм, как его традиционно представляют, имеет долгую историю в Европе. Хотя он ассоциируется преимущественно с известными военизированными группами, такими как Временная Ирландская республиканская армия и ее ответвления, а также с такими группами, как Баскское отечество и Свобода, сепаратизм не всегда ассоциируется с терроризмом и политическим насилием. В Европе значительно больше сепаратистских групп, участвующих в политической ненасильственной борьбе и стремящихся к автономии, чем тех, кто предпочитает прибегать к насилию. Примеры ненасильственных сепаратистских движений можно найти в Северной Италии, Корсике, Кипре, Дании, Чешской Республике, Франции, Германии, Нидерландах, Испании и Великобритании. Важно отметить, что общественно-политические движения, ориентированные на различные виды сепаратизма в Европе, в основном не связаны с какими-либо экстремистскими движениями или действиями; терроризм и политическое насилие не являются неизбежным путем от сепаратистских идей.

Однако идеологические основы того и другого, наряду с построением исторически, этнически, экономически, расово или религиозно мотивированных границ, являются взаимосвязанным явлением. Рапопорт зафиксировал взаимосвязь, хотя и косвенную, между волнами терроризма с начала двадцатого века и до настоящего времени. В каждой из волн террора сепаратизм выступал в различных обличьях. Опять же, говоря о сепаратизме, следует подчеркнуть, что применение или угроза насилия являются исключением. Однако в некоторых кампаниях применение террористической тактики как средства достижения сепаратистских целей было более распространено, чем в других.

Тем не менее, по-прежнему сохраняется тенденция смешивать терроризм и сепаратизм, в первую очередь из-за того, что сепаратистские движения якобы стремятся бросить вызов статус-кво политической власти и тем самым бросают прямой вызов государству. Покалова отмечает, что после событий 11 сентября, когда угроза терроризма часто представлялась как стратегическая и экзистенциальная для западных обществ, правительствам было свойственно рассматривать сепаратизм как часть глобальной борьбы с терроризмом.

Конечно, есть отдельные лица и группы, которые действительно занимаются экстремистской деятельностью - как идеологически, так и поведенчески, опираясь на сепаратистские нарративы для оправдания и мотивации своих действий. В данном контексте экстремизм определяется как поведение и идеи/отношения/убеждения, которые находятся вне социальных, политических, культурных и правовых норм данной территории.

Сепаратизм как экстремизм осложняется еще и тем, что экстремизм понимается как нарушение норм общества. Неточность такого определения затрудняет определение того, что считать экстремизмом, а что нет. Все становится более ясным, если сузить толкование экстремизма до включения только применения насилия или угрозы насилия, заимствуя, таким образом, определение терроризма для категоризации этого термина.

В качестве альтернативы, это может быть предпочтение использования термина терроризм (а не сепаратизм); этот вопрос мы обсудим позже. Аналогичным образом, исследования сепаратизма в мире также немногочисленны, но это вполне можно объяснить возникшей гибридизацией, когда сепаратизм и терроризм (преимущественно исламистский экстремизм) смешиваются, что служит для сокрытия сепаратистских мотивов движений, которые в прошлом могли бы рассматриваться как полностью сепаратистские.

Понимание сепаратизма как экстремизма предполагает понимание гибридности сепаратизма, как этот термин используется в настоящее время, и признание того, что он возникает в ответ на изменение социальных норм, а не в ответ на традиционные территориальные границы и границы идентичности в Европе.

Юго-Восточная Азия предлагает хороший пример для изучения проблемы этнического сепаратизма и религиозного экстремизма, а также последствий этих процессов для монополии государства на применение силы. Этот регион иллюстрирует, как применение силы все больше распространяется за пределами досягаемости государства и в оппозиции к нему. Этот регион является классической иллюстрацией основных выводов Группы глобального анализа по вопросу "монополии государства на применение силы", а именно, что эта монополия является скорее мифом, чем реальностью, в частности потому, что государство, за очень редким исключением и при очень ограниченных обстоятельствах как на Глобальном Севере, так и на Глобальном Юге, столкнулось с распространением или гибридизацией обеспечения безопасности. Это развитие обусловлено целым рядом факторов, включая этнический сепаратизм - во многом сформированный западной колонизацией, которая сопровождалась произвольным установлением государственных границ, расколовших некогда относительно однородные этнические сообщества - и религиозный экстремизм.

Коренные причины различаются в разных культурах и регионах, хотя их объединяет реальность растущего социального неравенства, формы отчуждения и более общие недостатки социальных, экономических и политических систем управления.

Как бы ни были различны Шри-Ланка, российский Кавказ и север Испании в географическом, политическом и этническом плане, нынешний статус их соответствующих сепаратистских движений удивительно похож. Все они характеризуются асимметричной войной. Военные возможности России, Испании и Шри-Ланки превосходят возможности их противников, однако во всех трех случаях государства еще не добились значительного прогресса в разрешении или даже подавлении конфликтов с помощью силовых военных действий.

Российские военные участвуют в событиях в Чечне уже несколько десятилетий. После вторжения российских войск в 1994 году, они были вынуждены уйти - потерпев

унизительное поражение - через 18 месяцев. Плохо мотивированные и сталкивающиеся с постоянными засадами чеченских партизан, российские войска сильно деморализованы, в неделю гибнет от 30 до 40 российских солдат. Конфликт привел к перемещению от 300 000 до 400 000 человек и унес тысячи жизней. Несмотря на численное превосходство российских войск над чеченцами, России пока не удалось добиться реального прогресса.

Ситуация в Шри-Ланке привела к таким же ужасным последствиям, унеся жизни более 65 000 шриланкийцев. Поучительным примером является попытка захвата города Паллай. В ходе наступления, получившего название "Огненный жезл", шриланкийские военные попытались захватить этот город, стратегически расположенный рядом с важным Слоновьим перевалом. Даже располагая ресурсами централизованного правительства, армия понесла сотни потерь по сравнению с десятками потерь тамилов, которые в итоге отбили атаки. Подобно российским солдатам в Чечне, военным Шри-Ланки пришлось сражаться против хорошо укоренившейся оппозиции на внутренней территории, которая, тем не менее, оказалась крайне враждебной, незнакомой и чужой.

Пример Испании представляет собой аналогичный сценарий. К счастью, испанское правительство не взяло на себя обязательства по серьезному военному участию в конфликте с баскскими сепаратистами.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Карпович, О. Г. Сепаратизм и сепаратистские движения в современном мире (на примере Бельгии и Великобритании): сравнительный анализ / О. Г. Карпович // Право и политика. – 2016. – № 4. – С. 449-457. – DOI 10.7256/1811-9018.2016.4.18693. – EDN VSXJMV.

2 Савинов, С. С. Внутренние и внешние факторы сепаратистских движений в Каталонии на современном этапе / С. С. Савинов // Актуальные проблемы международных отношений, международного права и безопасности. – Москва : Информационно-внедренческий центр "Меридиан", Российское общество политологов, 2021. – С. 654-656. – EDN BZEXEO.

УДК 32.019.5

Руденко Валерия Андреевна, студент, Комсомольский-на-Амуре государственный университет
Rudenko Valeria Andreevna, student of Komsomolsk-na-Amure State University
Кортун Екатерина Александровна, Старший преподаватель кафедры «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Kortun Ekaterina Alexandrova, Senior Lecturer, Department of Linguistics and Intercultural Communication", Komsomolsk-na-Amure State University

ЗАРОЖДЕНИЕ И СТАНОВЛЕНИЕ ТЕРРОРИЗМА В РОССИИ

THE ORIGIN AND FORMATION OF TERRORISM IN RUSSIA

Аннотация. В данной статье будут рассмотрены основные моменты становления терроризма в царской России современной России. Так же будут рассмотрены ключевые террористические акты, их лидеры и пособники, повлиявшие на способы борьбы с терроризмом в России, и принятые на их основе законы по противодействию терроризму.
Abstract. This article will consider the main points of the formation of terrorism in tsarist Russia of modern Russia. The key terrorist acts, their leaders and accomplices who influenced the ways of combating terrorism in Russia, and the laws adopted on their basis on countering terrorism will also be considered.

Ключевые слова: терроризм, история, Беслан, террористические организации.
Key words: terrorism, history, Beslan, terrorist organizations.

В истории России отдельная роль отводиться деятельности террористических группировок, движений связанных с политической жизнью в XIX - начале XX веков. История терроризма в России началась 4 апреля 1866 года. В этот день неизвестный выстрелил в Александра II, когда он садился в карету после прогулки. Вовремя появившийся крестьянин, Осип Комиссаров, попал убийце в руку, и пуля пролетела мимо императора. Убийцу схватили, им был Дмитрий Каракозов, дворянин из Саратовской губернии. Каракозов входил в тайный кружок народников в Москве, возглавлял его двоюродный брат Николай Ишутин. Целью общества было свергнуть законных властей путем государственного переворота. В ходе судебного процесса Каракозова и Ишутина приговорили к суммарной казни. Впоследствии Ишудин был спасен от смерти и провел остаток своей жизни в Шлиссельбургской тюрьме.

Партия социал-революционеров стала одной из важной террористической организации в начале XX века, которая появилась заграницей в 1901 году. За террористическую часть в партии отвечали Г.А. Гершуни, Е.Ф. Азеф и Б.В. Савинков.

Первый теракт был совершен социал-революционерами в 1901 году. Карпович из Словацкой Республики серьезно ранил министра национального образования Н.И. Боголепова. Следующей жертвой, выбранной эсерами, стал министр внутренних дел Сипягин. Его преемником стал Плев, который также был убит бомбой, брошенной старшим эсером Созоновым. Почти все убийства, совершенные социал-революционерами, оправдываются в либеральной прессе. Героизм террористов даже получил высокую оценку общества.

Покушение на Столыпина совершенное 12 августа 1906 года стало самым кровавым актом террора В Санкт-Петербурге. В связи с этим правительство было вынуждено выпустить указ, суть которого состояло в том, чтобы завершить всю деятельность военного суда за последующие 48 часов. И в соответствии с основным законом России, точнее со статьёй 87, все решения принятые военокомандующим округа должны быть обязательно исполнены в течение следующих суток.

Петр Аркадьевич Столыпин предпологал, что такие действия наиболее эффективны для поддержки безопасности общества, и пологал, что насилие необходимо побеждать насилием.

Петр Столыпин был убит, после того как его усилиями с массовым террором было покончено. 1 сентября 1911 года, когда царская семья была в Киеве, в здании местной оперы Столыпин был смертельно ранили. В него стрелял эсер Дмитрий Богов. Этим убийством и закончился в России Большой террор.

Когда в 1917 году к власти пришли большевики, В.И Ленин принял на вооружение тактику красного террора против врагов советской власти. При И.В Сталине терроризм стал не только средством борьбы с политическими противниками, но и способом утверждения режима собственной власти.

Большинство террористических актов в России произошло в 1990-е годы и в первой половине XXI века. Одной из самых страшных страниц стал инцидент с захватом заложников в школе в Беслане 1 сентября 2004 года. В результате теракта погибли 333 человека, в том числе 186 детей. В школу ворвались 3 сентября, и этот день был выбран как День солидарности в борьбе с терроризмом. С 2005 года в России вспоминают жертв терактов, когда-либо совершенных не территории страны.

Для чеченских боевиков Беслан стал кульминацией нескольких лет террористической деятельности. В 2000 году их "полевая армия" была разгромлена в Грозном, Аргунском ущелье и селе Комсомольское. В 2002 и 2003 годах нападения партизан также прекратились. Нет никакой замены тем, кто был убит или захвачен в плен, и многие предпочли бы сложить оружие или отправиться в эмиграцию. Лидеры сепаратистов совершенно ясно понимают, что в ближайшие годы они потерпят полное поражение.

Для того чтобы у их движения был шанс выжить, радикалам необходимо изменить не только свою тактику, но и весь стиль ведения войны. В 1990-х годах их стратегия претерпела два ключевых изменения. Во-первых, война выходит за пределы Чечни. Теперь их усилия сосредотачивались ещё и на Дагестане, Ингушетии, Кабардино-Балкарии.

После этого подполье решило поменять второй элемент стратеги и это было изменение ключевых целей. Акты террора и раньше использовались в обороте террористов, но только в дополнении на нападения российских офицеров и солдат.

Оставшиеся в живых лидеры сепаратистов, особенно Шамиль Басаев, помнили разрушительные последствия нападения на Будённовск во время первой войны. Настало время превратить отдельные террористические акты во всеобъемлющую кампанию.

В России с 2002 и 2003 года постоянно происходили акты террора в отдалённых регионах. В эти года происходили - захват театрального центра на Дубровке, атаки смертниц, взрывы бомб в кавказских республиках за пределами Чечни — боевики рьяно воплощали в жизнь свою новую стратегию. Однако пиком террористической кампании стал 2004 год.

По мнению террористов, школа – это хороший вариант для атаки. Дети меньше способны к сопротивлению, поэтому теракт умножает психологическое давление на них. Также охрана школы более слабая, чем на заводах или АЭС. Из-за конфликта между осетинами и ингушами, который был вызван вооружённым конфликтом ещё в начале 1990-х годов, террористы выбрали Беслан.

Утром 1 сентября 2004 года, во время праздничной линейки, отряд террористов численностью более 30 человек захватил школу №1 в Беслане. Террористы захватили 1128 заложников в спортивном зале школы и удерживали их там в течение трех дней без воды и пищи. Около полудня 3 сентября в школе прогремел взрыв, и началась беспорядочная стрельба. Дети и женщины выпрыгивали из окон и дыр в стене спортзала.

Переговоры с террористами проходили плохо, только наследующей день после захвата, Хучбаров согласился отпустить только грудных детей: малыши не понимали угроз и кричали, их вывел президент Ингушетии Руслан Аушев.

Беслан стал самым катастрофическим террористическим актом в современной российской истории. Басаев совершил поистине идеальное убийство - безжалостно, на глазах у всех, под пристальным взглядом телекамер. И на этот раз жертвами стали дети. Однако переломного момента в войне не произошло. Сожженные руины Бесланской школы № 1 - жуткий памятник человеческой жестокости и человеческим страданиям - но после Беслана, Басаев и Масхадов не достигли никаких политических целей, а побежали навстречу собственному позорному концу. Жертвами этой трагедии стали 334 человека, из которых 186 были детьми. Погибли также сотрудники правоохранительных органов и МЧС. В общей сложности 810 человек получили различные ранения.

Беслан стал самым жестоким проявлением бесчеловечности и жестокости террористов. О трагедии в Беслане помнят до сих пор, выжившие приезжают каждый год 1 сентября почтить память умершим. Но ещё до Беслана, Басаев пытался изменить положение в Чечне, не желая видеть там российские войска.

Как пример ещё одного из массового захвата была история с оккупацией города Будённовск в 1995 году. Тогда террористы взяли в плен 1200 жителей города. Данным захватом руководил Шамиль Басаев. Жителей сгоняли в местную больницу, а кто отказывался - расстреливали. С начала захвата террористы выдвигали огромное количество требований, но главное из них было, чтобы российские войска были выведены из Чечни. Либер террористок, Шамиль Басаев, активно вёл переговоры с журналистами, одновременно держа заложников в больнице. Все россияне следили за развитием событий ты Будённовске, которое транслировали по телевизорам.

После этого прецедента, в 2006-м в России приняли закон «О противодействии терроризму». В 16-й статье говорится, что ведение переговоров возможно, но «специально уполномоченными на то руководителем контртеррористической операции». Во время теракта в Буденновске погибли 129 человек.

Как итог, можно сделать вывод, что в борьбе террористов с властью жертвами всегда становятся невинные люди, женщины, старики, дети. В данный момент в России всё меньше и меньше происходит террористических актов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Гирфанов А.Р., Сергеев С.А. Терроризм в современной России: причины возникновения и способы противодействия // Вестник Казанского технологического университета. 2014. №17. URL: https://cyberleninka.ru/article/n/terrorizm-v-sovremennoy-rossii-prichiny-vozniknoveniya-i-sposoby-protivodeystviya (дата обращения: 16.12.2022).

2 Ратке А. Е. Международное сотрудничество в борьбе с терроризмом // Правопорядок: история, теория, практика. 2017. №4 (15). URL: https://cyberleninka.ru/article/n/mezhdunarodnoe-sotrudnichestvo-v-borbe-s-terrorizmom (дата обращения: 16.12.2022).

3 Батулов В.И. Понятие «терроризм» в отечественной и зарубежной науке // Скиф. 2021. №4 (56). URL: https://cyberleninka.ru/article/n/ponyatie-terrorizm-v-otechestvennoy-i-zarubezhnoy-nauke (дата обращения: 16.12.2022).

УДК 297.17

Рыбакова Кристина Валерьевна, студент, Комсомольский-на-Амуре государственный университет
Rybakova Kristina Valerevna, student of Komsomolsk-na-Amure State University
Климова Екатерина Викторовна, старший преподаватель, кафедры «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Klimova Ekaterina Viktorovna, Senior Lecturer of “Linguistics and Intercultural Communication”, Komsomolsk-na-Amure State University

РАДИКАЛИЗАЦИЯ ИСЛАМА В СОВРЕМЕННОМ МИРЕ

RADICALIZATION OF ISLAM IN THE MODERN WORLD

Аннотация. Статья посвящается исследованию проблем радикализации ислама в современном мире как одной из глобальных угроз современной международной безопасности. В статье рассматриваются формы исламского радикализма и факторы распространения этой угрозы в современном обществе и молодежной среде. Определены основные цели сторонников радикальных движений: строгое соблюдение традиций ислама, замене светских законов, для достижения поставленных целей представители радикального движения используют агрессивные методы воздействия на общество.

Abstract. The article is devoted to the study of the problems of radicalization of Islam in the modern world as one of the global threats to modern international security. The article examines the forms of Islamic radicalism and the factors of the spread of this threat in modern society and the youth environment. The main goals of supporters of radical movements are defined: strict observance of the traditions of Islam, the replacement of secular laws, to achieve their goals, representatives of the radical movement use aggressive methods of influencing society.

Ключевые слова: радикализация, ислам, экстремизм, терроризм, современный мир, общество.

Key words: radicalization, Islam, extremism, terrorism, modern world, society.

Internal armed conflicts and terrorism have traditionally been a frequent threat to international security. Terrorism is often taken as the «number 1» threat to the entire international security, and at all levels: at the universal and at the regional levels. This is primarily due to the fact that terrorism has gradually turned from a local problem into a global one that knows no borders, it becomes international.

One of the conditions for the existence of terrorism of any kind is the presence of a certain level of approval or support at any level. This is especially true for nationalist and religious terrorism, and is also important for terrorism in the political field, especially in cases where it is used by groups or organizations that are in opposition to the official government. We can talk about different types of assistance and support: material and financial, providing protection to leaders or a number of groups. Terrorism in our time has already become a famous and very common term – «the plague of the XXI century» [7].

Unfortunately, this is true, the «plague of terrorism» has affected almost all countries around the world, the disease of terrorism brings with it pain, destruction and massive human losses. Today, terrorism is the most fundamental threat to security and stability in the international field. Unfortunately, currently the ideological basis of international terrorism is most often Islamic radicalism [8].

Islamic radicalism is an extreme demonstration of political Islam, which uses voluntarist methods of conducting political struggle. Radicalism itself is a variation of fundamentalism. Islam, like many religions, cannot be the root cause of a form of conflict. The radicalization of Islam is associated with the process of its politicization. Radicalism itself is peculiar not only to Islam, it can also be found in other religions. The final configuration of radicalism is terrorism.

From a philosophical point of view, radicalism means a departure from traditionalism, and is understood as a special trend towards reforms in solving complex political, economic and social problems [10].

Currently, scientists distinguish two forms of radicalization of Islam. The first form is constructive radicalism, which has its main goal, the transformation of a real social system qualitatively and progressively. In this form, radicalism is represented by a social revolution, the construction of a perfect social order. This form of radicalism can be characterized as a «healing» way of saving the socio-political system, which does not require the complete destruction of all spheres of the social system [9].

The second form of radicalization of Islam is destructive radicalism, which resolutely and mercilessly destroys the existing social system, primarily such radicalism is aimed at preserving or restoring social relations that are categorically outdated. Destructive forces are aimed at destroying the existing socio-political system, such a form of radicalization can be described as a «violent» way to save the social body.

In modern society, radicalism, which is associated with Islam, is represented by a real factor of opposition to the world ideological and political force. Muslim believers are revealed as radical strata of society and quite allow the use of terror, in their opinion, the only true way to achieve their goals, most often such goals have political overtones [2].

The destructive forces of radical Islam are aimed at destroying the «ignorant» society of the Western world. Such a form despises all generally accepted international rights, ignores territorial integrity, does not recognize the rights and freedoms of people[3].

The creed of Islamism expresses the following saying from the Koran: «Fight the infidels until only one faith remains on Earth, faith in Allah alone and the whole Earth becomes an Islamic world». Its strategic goal is to create a global Islamic empire, or a worldwide caliphate, arranged according to Sharia law.

The extremist trend of radical Islam poses the highest danger to the social stratum. In achieving their goals, representatives of this trend are trying to destroy the global socio-political balance throughout the world, as well as in certain regions [1].

Supporters of extremist radical Islam do not recognize the existing values in society, according to their worldview, the recognized form of secular state does not correspond to the Muslim religion.

Representatives of extremist radical Islam are most often young people, they absorb radical ideas like sponges and try to bring them to life. This age group is most susceptible to the harmful influence of extremist organizations, young people are full of energy and support the changes taking place in society. The greatest danger to the national security of progressive youth is posed by extremist movements that hide behind «pious thoughts» and actively spread pseudo-Islamic teachings among young people [4].

The position of modern radical Islam is based on a distorted theological model, radical ideology is represented by apostates of faith who have invented and invented their ideas based on the Koran. The radicalization of Islam in modern society and the world is associated with a negative attitude towards the values promoted by Western society. The cultural, political and moral ideas of the modern West degrade traditional Muslim values. The inability of the Islamic position to adapt to global processes and «moving forward» leads to the growth of radical Islamists [5].

Currently, Islamists consider the overthrow of corrupt and decadent regimes in Muslim countries, the elimination of the American military presence in them, countering the penetration of Western values and Western lifestyle into Muslim society and the economy of Muslim countries, the establishment of Muslim control over the use of energy resources in the Islamic geographical space, the fight against Israel and its domination in Palestine.

In this regard, the main goals of the supporters of radical Islam are: the destruction of «pro-Western», «non-Islamic» political regimes existing in a number of Islamic states, the creation of a single nation, the extension of the most radical version of the laws of Islam to the entire Muslim world.

To achieve their goals, extremists and terrorists use the Internet as a global source of information dissemination. Thus, terrorists collect information, funds, propaganda and spread the ideas of radical Islam [6].

Thus, radical Islam is widely spread all over the world and poses a huge danger to modern society, timely identification of signs of radical Islam in society, youth and the global Internet network will ensure security in the modern world.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Васильев Ю. В. Социально-политическая триада: гражданское общество, исламский радикализм, православное христианство; основы конкуренции и ее последствия // Современное общество: к социальному единству, культуре и миру : Материалы международного форума, Ставрополь, 21–22 апреля 2016 года. – Ставрополь: Издательский дом "Тэсэра". 2016. С. 93-98.

2. Грановский Г. А. Борьба с исламским радикализмом в Королевстве Марокко на рубеже XX–XXI вв // Молодой ученый. 2017. № 6(140). С. 370-373

3. Гятов Т. Т. Исламский "ренессанс" и экспансия исламского радикализма в Кабардино - Балкарии и Карачаево - Черкесии // Этносоциум и межнациональная культура. 2013. № 9(63). - 137 с.

4. Добаев И. П. Блокирование исламского радикализма в условиях Северного Кавказа // Отечественные записки. 2003. № 5. С. 136-148.

5. Излученко Т. В. Методология исторической антропологии в исследовании исламского радикализма (на примере "Исламского движения Узбекистана") // Известия Иркутского государственного университета. Серия: Политология. Религиоведение. 2017. Т. 22. С. 255-266.

6. Имаков, Т. З. Влияние исламского радикализма на экстремизм и терроризм в современной России / Т. З. Имаков, Г. А. Корнилов. – Махачкала : ИП Овчинников Михаил Артурович (Типография Алеф). 2016. - 192 с.

7. Кашкаров А. А. К вопросу об общественной опасности исламского радикализма в современном светском обществе // Гуманитарные, социально-экономические и общественные науки. 2018. № 2. С. 79-83.
8. Семедов С. Исламский радикализм в современном мире: сущность и причины возникновения // Россия и мусульманский мир. 2010. № 4. С. 149-158.
9. Цуркан А. А. Европа: исламский радикализм vs. модернизация религии // Современная Европа. 2014. № 2(58). С. 131-142.
10. Цуркан А. Классификация политических моделей исламских стран с учетом фактора исламского радикализма // Россия и мусульманский мир. 2014. № 8(266). С. 169-181.

УДК 297.17

Рыбакова Кристина Валерьевна, студент, Комсомольский-на-Амуре государственный университет
Rybakova Kristina Valerevna, student of Komsomolsk-na-Amure State University
Климова Екатерина Викторовна, старший преподаватель, кафедры «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Klimova Ekaterina Viktorovna, Senior Lecturer of "Linguistics and Intercultural Communication", Komsomolsk-na-Amure State University

«СВЕТОФОР» ТЕРРОРИСТИЧЕСКОЙ ОПАСНОСТИ

«TRAFFIC LIGHT» OF TERRORIST DANGER

Аннотация. Статья посвящена исследованию «цветной» схемы классификации уровней террористической угрозы, принятой в России. Каждому уровню террористической опасности соответствует определенный цвет: синий, желтый и красный. Синий уровень террористической опасности обозначает повышенный уровень готовности населения к угрозе теракта, желтый цвет обозначает высокий уровень опасности террористической угрозы, красный цвет уровня террористической опасности сигнализирует о критической угрозе жизни населения.
Abstract. The article is devoted to the study of the «color» scheme's classification of terrorist threat levels, adopted in Russia. Each level of terrorist danger corresponds to a certain color: blue, yellow and red. The blue level of terrorist danger indicates an increased level of readiness of the population for the threat of a terrorist attack, yellow color indicates a high level of danger of a terrorist threat, red color indicates a critical threat to the life of the population.
Ключевые слова: светофор, уровень, террористическая опасность, население, контртеррористическая операция.
Key words: traffic light, level, terrorist danger, population, counter-terrorist operation.

For the first time, the system of terrorist threat levels was developed in the United States after the events of September 11, 2001 in response to numerous complaints from citizens of the country that government agencies did not provide explanations about the degree of such danger. The American system consists of five levels - green, blue, yellow, orange and red.

This practice has already operated in more than 70 countries around the world, and the number of danger levels varies from three to five.

In Russia, the concept of introducing a similar terrorist threat system has been discussed since 2004. Its main lobbyist was the National Antiterrorist Committee headed by FSB Director, Alexander Bortnikov.

In accordance with Federal Law No. 35-FZ of March 6, 2006 «On Countering Terrorism» for the purpose of informing the population about the threat of a terrorist act and organizing activities to counteract its commission carried out by the National Anti-Terrorist Committee in cooperation with federal executive authorities, state authorities of the subjects of the Russian Federation, local authorities local governments. According to the Decree of the President of the Russian Federation No. 851 of June 14, 2012, levels of terrorist danger may be established, they provide for the adoption of additional measures to ensure the security of the person, society and the state [1].

The following levels of terrorist danger can be established on the territory of the Russian Federation, sites, and individual objects:

a) an increased level of terrorist danger (blue) - in the presence of information that requires confirmation of the real possibility of committing a terrorist act;

b) a high level of terrorist danger (yellow) - if there is confirmed information about the real possibility of committing a terrorist act;

c) the critical level of terrorist danger (red) - if there is information about a committed terrorist act or about the commission of actions that pose an immediate threat of a terrorist act.

Table 1. «Color» classification's scheme of terrorist threat levels

Blue level	Yellow level	Red level
information about the possibility of a terrorist attack is received	information about the preparation of a terrorist attack is confirmed	the regime of the counterterrorist operation is announced
Actions		
information about a possible terrorist attack is being checked	stricter control of the pass-port mode is carried out	mass verification of documents is carried out
coordination of plans for the protection of objects that may be subjected to acts of terrorism	protection of life support facilities is being strengthened	listening to telephone conversations
conducting training to repel the terrorist threat	control over the movement of transport across administrative borders; checks of infra-structure objects	resettlement of local residents; restriction of traffic and pedestrians; access of law enforcement agencies to any premises

One or another level of danger is established in order to inform the population in a timely manner about the threat of a terrorist attack and to counteract its accomplishment [3].

Only the head of the anti-terrorist commission of the region has the right to introduce, change or cancel the blue and yellow danger levels in coordination with the head of the FSB department. The red level is set and removed by the Chairman of the National Anti-Terrorist Committee on the recommendation of the head of the regional anti-terrorist Commission [5].

The introduction of the blue level of danger practically does not affect the life of an ordinary citizen.

The features of the blue level of danger include additional inspections of infrastructure facilities to identify possible places of laying explosives. In public places, such as parks, squares and train stations, enhanced patrols are put up. Inspection measures are strengthened in public places [4].

When the danger level is blue, citizens are advised to immediately report all suspicious objects and situations, such as strange behavior of people, unusual finding of objects, to the police. People should not accept any items, such as bags, boxes, packages, from strangers. Citizens need to have identity documents with them, as well as follow the news from official sources of information [8].

The introduction of the yellow danger level affects people whose official duties (police officers, military personnel, etc.) are associated with the prevention of a terrorist attack or the

elimination of its consequences. Migration control and registration of citizens (residence permit, place of residence) are strengthened at the borders. The authorities conduct trainings and working out possible actions to stop the terrorist attack and rescue people. Medical organizations are put on high alert [2].

At the yellow danger level, citizens are advised to follow all the rules of behavior at the blue danger level. People should refrain from visiting public places, such as train stations, cinemas, shopping malls [7].

The introduction of a red danger level affects the life of a citizen, as his habitual lifestyle may temporarily change, such as the availability of certain services, transport routes, etc. The State is taking urgent measures to save people, all forces involved in the counter-terrorism operation are put on alert. The State is creating temporary accommodation facilities for people, they are provided with water and food. All medical institutions are put on emergency alert.

At the red level of danger, citizens are advised to observe all rules of behavior at the blue and yellow levels of danger. People are forbidden to approach the place of a terrorist attack during a counter-terrorist operation. It is necessary for the population to refuse to visit places of mass stay of people, to cancel any types of trips. People should prepare documents, basic necessities and prepare for possible evacuation [6].

Thus, the «color» scheme of classification of the levels of terrorist threat makes it possible to determine the level of threat of terrorist danger in a particular subject of the Russian Federation - increased, high and critical. Each of these levels is assigned its own color – blue, yellow and red.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Адамбеко К. С. Актуальные вопросы правового обеспечения противодействия терроризму // Право и государство. 2013. № 4(61). С. 24-28.

2. Бару С. Е. Эффективный способ снижения уровня террористической опасности // Вопросы оборонной техники. Серия 16: технические средства противодействия терроризму. 2019. № 3-4(129-130). С. 66-71.

3. Гайнуллин Д. Е. Показатели уровня террористической опасности в системе индикаторов национальной безопасности государства // Актуальные проблемы противодействия идеологии терроризма и экстремизма в современном обществе : материалы городской научно-практической конференции, Казань, 20 апреля 2018 года. – Казань: Казанский государственный технический университет им. А.Н. Туполева. 2018. С. 60-63.

4. Иванец Г. Оценка уровня опасности угроз террористического характера на потенциально опасном объекте // Научный журнал власть и общество (история, теория, практика). 2017. № 1(41). С. 198-223.

5. Кувырченкова Т. В. Контртеррористические операции: новая реальность // Защита прав и охраняемых законом интересов граждан : факультетские Научные чтения им. профессора Р.Е. Гукасяна, Тверь, 01–31 мая 2022 года. Тверь: Тверской государственный университет. 2022. С. 48-54.

6. Кузнецов А. Е. К проблеме измерения и оценки уровня террористической опасности // Известия Института инженерной физики. – 2013. – № 4(30). – С. 47-51.

7. Плотников В. В. Об организационных аспектах противодействия терроризму в муниципальных образованиях Московской области // Противодействие терроризму. Проблемы XXI века - COUNTER-TERRORISM. 2012. № 3. С. 25-36.

8. Шалягин Д. А. Особенности установления уровней безопасности объектов транспорта при угрозе террористического акта // Высокие технологии, наука и образование: актуальные вопросы, достижения и инновации : сборник статей XII Всероссийской научно-практической конференции, Пенза, 07 сентября 2021 года. Пенза: Наука и Просвещение. 2021. С. 104-107.

УДК 343.301

Себелева Алина Денисовна, студент; Комсомольский-на-Амуре государственный университет
Sebeleva Alina Denisovna, student of Komsomolsk-na-Amure State University
Малышева Наталья Васильевна, кандидат филологических наук, доцент; Комсомольский-на-амуре государственный университет
Malysheva Natalia Vasilievna, PhD in Philology, associate professor, Komsomolsk-na-Amure State University

МИГРАЦИЯ КАК УГРОЗА МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ В ЕВРОПЕ И КИТАЕ

MIGRATION AS A THREAT TO INTERNATIONAL SECURITY IN EUROPE AND CHINA

Аннотация. В условиях современности миграция населения все больше становится предметом внимания руководства многих государств. По мере роста ее масштаба и причин, которые заставляют или вынуждают население покинуть привычную им среду, миграция может стать серьезной угрозой для национальной безопасности государства. В статье рассматриваются проблемы, связанные с глобальными перемещениями населения. Раскрываются миграционные проблемы в Европе и Китае.
Abstract. In modern conditions migration of the population is increasingly becoming the subject of attention of the leadership of many states. To the extent of its scale and the reasons that force parts of the population to leave their usual environment, migration can become a serious threat to the national security of the state. The article discusses the problems associated with global population movements. Migration problems in Europe and China are revealed.
Ключевые слова: миграция, международная безопасность, нелегальная миграция, Китай, Европа, Россия.
Key words: migration, international security, illegal migration, China, Europe, Russia.

На протяжении последних лет международная миграционная политика вышла на первое место в области безопасности стран. Современный мир рассматривает усиление миграционных потоков как угрозу международной безопасности в связи с глобальным характером и чрезвычайно серьезными последствиями для стран. Основная причина миграции – это противоречие уровня развития человека, его потребностей и условий его удовлетворения на что влияют среда и социальные нормы [4]. В самом общем смысле термина безопасность означает отсутствие угроз.

Миграция является процессом, обусловленным самыми разными факторами и причинами, которые возникают в странах вывода и приёма. Она помогает отдающим и принимающим странам решать свои насущные проблемы (экономика, демография, политика, геополитика), то есть минимизирует угрозы безопасности по данным направлениям. С другой стороны, этот же самый процесс порождает новые вызовы и угрозы безопасности. Миграция влияет на самые различные сферы, аспекты и виды национальной, региональной и международной безопасности.

Более того, отечественная и иностранная литература всё чаще рассматривает «миграцию» в контексте «миграции и национальной безопасности страны». В связи с этим все страны интересуются национальной безопасностью, удовлетворением и соблюдением национальных приоритетов, и неконтролируемый миграционный поток может привести к существенным изменениям в социальной и экономической жизни государства и изменению привычного для населения образа жизни.

Итак, цель данного исследования состоит в описании последствий незаконной миграции в принимающие страны, являющиеся центрами миграционного притяжения.

Цель определяет следующие задачи:

1) рассмотреть угрозы безопасности, связанные с миграцией в европейские страны;

2) описать угрозы безопасности Китая, связанные с миграцией.

Рост нелегальной миграции в последние десятилетия является серьезной угрозу для национальной безопасности и требует комплексных подходов к ее регулированию, согласованность действий национальной экономики с их интересами, поиск новых способов решения проблем, возникающих в настоящее время.

Миграция как угроза международной безопасности в Европе

Террористические акты 11 сентября привели к тому, что угрозы, связанные с миграцией, ассоциировались в общественном дискурсе главным образом с феноменом терроризма. Это объясняется тем фактом, что терроризм как метод распространения массового страха используется не только авторитарными и диктаторскими государствами, но и негосударственными субъектами. Примером стали террористические акты 11 сентября, когда группа из девятнадцати террористов (иностранцев) в 2000 и 2001 годах законно пересекла границу Соединенных Штатов для проведения скоординированных террористических атак после нескольких месяцев пребывания и подготовки. Террористический акт 7 июля 2005 года, произошедший в Лондоне, где группа из четырех террористов взорвала три бомбы в лондонском метро и одну в общественном транспорте [2].

Помимо прямого взаимодействия между миграцией и терроризмом, международные потоки населения влияют на террористическую деятельность косвенным образом. Приток иммигрантов нередко приводит к усилению радикальных, расистских и ксенофобских настроений и к развитию различных форм политического экстремизма. Наиболее впечатляющим и в то же время трагическим проявлением этого были нападения в Осло, совершенные норвежским экстремистом, сторонником Андреасом Берингом Брейвиком, который 22 июля 2011 года совершил два скоординированных нападения, в результате которых в общей сложности погибло 77 человек. Брейвик изложил мотивы своего поведения в манифесте под названием "2083: Европейская декларация независимости"[7]. Его наполненное ненавистью содержание направлено как против иммигрантов-мусульман, так и против демократии, мультикультурного общества и политиков, пропагандирующих религиозную и этническую терпимость. Манифест провозглашает необходимость расовой войны и предлагает способы, как Европа может освободиться от иммигрантов. В этой связи следует подчеркнуть, что случай Норвегии, возможно, не является изолированным. Неконтролируемая вспышка насилия в отношении иммигрантов или террористический акт, подобный тому, что произошел в Норвегии, могут произойти, где угодно.

Присутствие большого числа иммигрантов, особенно выходцев из других культурных и цивилизационных кругов, плохо интегрированных в принимающее общество, может вызвать сильную социальную напряженность, часто проявляющуюся в форме протестов и беспорядков, которые являются серьезными нарушениями общественного порядка. Такие ситуации часто возникали в странах с различным этническим, религиозным и национальным составом.

Примером могут служить события во Франции, где беспорядки переросли в конфликты с правоохранительными органами. Они начались в октябре и ноябре 2005 года в районах, где преобладают иммигранты, после того, как двое подростков, спасавшихся от полиции, были непреднамеренно убиты. Демонстрации, проходившие в знак протеста против жестокости органов правоохранительной власти, быстро переросли в беспорядки и распространились на другие французские агломерации [6].

Как террористические действия, так и беспорядки являются проявлением сильных антагонизмов, происходящих в мультикультурных обществах, где, с одной стороны, существуют общины иммигрантов, а с другой - сторонники ультраправых, стремящихся сохранить национальную, культурную, религиозную, а иногда даже расовую однородность. Сегодня эта дихотомия проявляется наиболее ярко, в частности, в отношении иммигрантских мусульманских общин, функционирующих в странах Западной Европы. В целом, однако, отмечается, что для многих современных иммигрантских сообществ характерно сохранение индивидуальности, часто сопровождающееся попыткой воссоздать свои коренные социальные и культурные условия в странах проживания [3].

В дополнение к обвинениям, сформулированным в отношении иммигрантов, обвиняющих их в подрыве социальной и культурной сплоченности, их также нередко обвиняют и в увеличении масштабов социальных проблем, таких как безработица, снижение реальной заработной платы, мошенничество с пособиями или ухудшение доступности государственных услуг.

Миграция как угроза международной безопасности в Китае

Китайская Народная Республика - самая густонаселенная страна мира. Мотивы, уровень напряженности, основные характеристики антикитайского настроения в России нельзя понять вне контекста определенного перечня мотивов, обстоятельств и мотивов. Россия столкнулась со спонтанным, массовым и высококонцентрированным притоком трудовых мигрантов. Эти мигранты отличались от россиян по культурным особенностям, структуре и образу жизни, поведению и привычкам. В основном жители Китая мигрировали на Дальний Восток России. Далее, этот регион граничил с Китаем – “спящим гигантом” в представлениях того времени. Это привело к сильным антимигрантским настроениям [1].

На сегодняшний день миграция граждан Китая в РФ представлена почти всеми формами: трудовым, коммерческим, образовательным, приездом на работу, туризмом и так далее.

Один из факторов негативного влияния на российскую экономику, и прежде всего на Сибирь и Дальний Восток, - это использование граждан Китая российскими коммерческими организациями для осуществления финансовой и хозяйственной деятельности с нарушениями Федерального закона "Об иностранных инвестициях в РФ". Китайцы стремятся получить право предпринимательства через российские подставные компании, преследуя такие цели: сокрыть факт и объем инвестиций в предпринимательские объекты в России, а также размер полученной прибыли в налоговые органы, приглашаемых на работу в российские предприятия. Следует отметить, что на территории России мигранты КНР, в основном нелегальные, входят в криминальную деятельность. Кроме того, безвизовый туризм стал устойчивым каналом экспорта наркотических веществ и наркотических препаратов, различных видов контрабанды. Так, например, по данным Дальневосточной оперативной таможни, почти 85% китайских граждан, задержанных при попытке провоза указанного препарата, входят в безвизовые группы. Из всех вышеперечисленных явно, что незаконные мигранты являются огромной опасностью для безопасности России.

Из всего вышесказанного очевидно, что нелегальные мигранты представляют огромную опасность для безопасности РФ. Они представляют собой категорию мигрантов, которые чаще всего легально въезжают в Россию, но впоследствии занимаются незаконным трудом.

Много экспертов и аналитиков называют проблему незаконной миграции одной из наиболее серьезных в нашей стране. И это именно потому, что нелегальная миграционная деятельность, которая сама по себе является труднорегулируемой, ведет к негативным процессам во всех сферах жизнедеятельности человека, перерастая в итоге в угрозы безопасности РФ.

В настоящее время основными вызовами внутренней безопасности государства являются терроризм, политический экстремизм и кризисы, которые могут привести к разрыву или ослаблению социальных связей. Все эти угрозы тесно связаны с миграционными потоками. В последние годы именно терроризм стал особенно серьезной угрозой. Сохранение социальной сплоченности представляет собой еще одну важную проблему. Приток иммигрантов, как правило, влияет как на социальные отношения, так и на отношения между властями и обществом. Появление иммигрантских меньшинств приводит к плюрализации обществ, в результате чего, как показывает опыт стран Западной Европы, ставится под сомнение нынешнее понимание национального и политического сообщества. Отсутствие согласованности в этих областях является почвой для развития экстремистской деятельности, проявляющейся в беспорядках или террористических актах. Это, в свою очередь, создает благодатную почву для деятельности популистских и крайне правых партий, которые строят свой политический капитал на антииммигрантских лозунгах. Что насчёт России, она должна иметь ясную, последовательную и долгосрочную миграционную политику, основываясь на четком понимании, какие мигранты заинтересованы в стране, какие права и обязанности они имеют. Также законодательным органам власти Российской Федерации необходимо выработать механизм экономического стимулирования или остановки миграции, исходя из потребностей собственного хозяйства.

Поэтому возникает вопрос, как современные демократические государства могут смягчить указанные выше угрозы, связанные с миграцией. Следует иметь в виду, что эти опасности никогда не могут быть полностью устранены. Однако, что можно сделать, так это ограничить возможность их возникновения путем применения соответствующих стратегий, методов и инструментов. Эффективная защита границ, контроль за притоком иностранцев, действия полиции и разведки, а также адекватная политика интеграции имеют здесь стратегическое значение.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Китайская миграция и политика КНР по её регулированию // Анохина Е.С. // Томский государственный университет, 2012. URL: https://cyberleninka.ru/article/n/kitayskie-diaspory-i-novaya-kitayskaya-migratsiya-v-stranah-yugo-vostochnoy-azii (дата обращения 18.10.2022).

2. Lebowitz, L. and I. Podheiser. “Summary of the Changes in Immigration Policies and Practices After the Terrorist Attacks of September 11, 2001: The USA Patriot Act and Other Measures” // University of Pittsburgh Law Review 63, 2001-2002. P. 873-888.

3. Самсонова Л.О. Политика Европейского союза в сфере противодействия нелегальной миграции в контексте национальной безопасности России / Л.О. Самсонова // Историческая и социально-образовательная мысль. 2016.

4. Софронова Е.Г. Актуальные вопросы миграционной политики РФ / Е. Г. Софронова // ДНК Права. 2015.

5. Амирова Д.Р. Регулирование миграционных процессов как фактор обеспечения национальной безопасности страны / Д.Р. Амирова, А.И. Храмова // Современные научные исследования и инновации. 2016.

6. Андерс Брейвик убил 77 человек. URL: https://lenta.ru/articles/2021/07/22/10_years_breivik/ (дата обращения 18.10.2022)

УДК 008

Солодовников Роман Вячеславович**,** студент**,** Сибирский государственный университет путей сообщения
Solodovnikov Roman Vyacheslavovich, student of Siberian State Transport University
Юшкова Лариса Ананьевна, кандидат психологических наук, доцент, доцент кафедры "Общей психологии и истории психологии", Новосибирский государственный педагогический университет
Yushkova Larisa Ananievna, Candidate of Psychological Sciences, Associate Professor, Associate Professor of the Department of General Psychology and History of Psychology, Novosibirsk State Pedagogical University

РОЛЬ СОЦИОКУЛЬТУРНОЙ ИНТЕГРАЦИИ В УРЕГУЛИРОВАНИИ КОНФЛИКТОВ. ПРОЦЕСС МЕЖКУЛЬТУРНОЙ КОММУНИКАЦИИ

THE ROLE OF SOCIO-CULTURAL INTEGRATION IN CONFLICT RESOLUTION. THE PROCESS OF INTERCULTURAL COMMUNICATION

Аннотация: Целью работы является рассмотрение сущности и роли социокультурной интеграции как механизма урегулирования этнических и национальных конфликтов в контексте межкультурной коммуникации. В процессе работы сделаны выводы о прикладной пользе социокультурной интеграции и ее влиянии на гражданское общество.
Abstract: The aim of the work is to consider the essence of socio-cultural integration as a mechanism for resolving ethnic and national conflicts in the context of intercultural communication. In the course of the work, conclusions were drawn about the applied benefits of socio-cultural integration and its impact on civil society.
Ключевые слова: социокультурная интеграция, межкультурная коммуникация, коммуникация, цель социокультурной интеграции, понятие межкультурной коммуникации, урегулирование этнических и национальных конфликтов.
Key words: sociocultural integration, intercultural communication, communication, the purpose of sociocultural integration, the concept of intercultural communication, settlement of ethnic and national conflicts.

Выбранная для статьи тема актуальна на сегодняшний день, исходя из объективных тенденций мировой глобализации, миграционной политики отдельно взятых стран и террористических актов с религиозно-этнической направленностью.

Общение или коммуникация в контексте межкультурной среды - это трудный и многогранный процесс для установление контакта между носителями разной культурной идентичности, сопровождающийся непониманием верований, традиций и обычаев друг друга - не разрешение которого ведет к конфликту и его эскалации. Требуется немало когнитивных ресурсов и прошлого опыта взаимодействия для эффективной коммуникации с представителем другой культурной общности, что несет за собой прикладной характер вышеупомянутой темы, привлекая научных специалистов в области социокультурной интеграции и адаптации к изучению данной проблематики.

Социокультурная интеграция - это процесс адаптации субъектов социальной общности с определенной национально-культурной принадлежностью к отличной от нее культурной среде. Она базируется на создании плюралистической межкультурно-коммуникативной среды, основанной на принципах инклюзии, толерантности, объединения и сопричастности. [5]

Межкультурная коммуникация - это взаимодействие и передача информации носителями разной культурной среды, что значительно влияет на результат их комму-

никации. Такая дисциплина, как теория межкультурной коммуникации изучает вышеупомянутое взаимодействие в рамках теории межкультурной коммуникации [1].

Культура же имеет множество определений, включающее в себя широкий спектр конъектуры жизнедеятельности человека. В обобщенном смысле, термин культура определяется тем, что создано и создается человеком, в частности, материальные объекты (скульптуры, картины, художественные произведения), а также и нематериальные (регламентируемые нормы поведения, обычаи, традиции.)

Культура - это система, созданных материальных и нематериальных объектов человечества в процессе его жизнедеятельности, на протяжении всей его истории. Наука, изучающее данное направление обрело название - культурология [2]

Подходы к изучению межкультурной коммуникации:

– Функциональный подход. Сравнение методов общения разных культур, что позволяет отметить их различия и особенности в коммуникативной среде.

– Объяснительный подход. Суть объяснительного подхода - описать и проанализировать конкретную группу людей с разным культурным кодом, не ставив перед собой цель спрогнозировать поведенческие факторы человека. Приверженцы подхода считают, что не культура определяет человеческое поведение, а человеческое поведение культуру, то есть носит субъективный характер.

– Критический подход. Как и объяснительный использует метод анализа, но рассматривает межкультурную коммуникацию через исторический контекст. Поведение определено культурой, которое приравнивается к силовому доминированию. Если объяснительный подход не ставит перед собой цель спрогнозировать поведение, то критический подход ставит перед собой именно эту цель для изменения жизни людей. Также, данный подход не предусматривает контакта с испытуемыми коммуникантами, а использует анализ текста и средств массовой информации.[3]

Целью социокультурной интеграции является достижение равного положения в обществе граждан с разной культурно - этнической и религиозной идентичностью, внедрение социальной сплоченности и плюрализма. Интеграция всех членов общества в социальные гражданско-правовые процессы. Что противопоставляется идее насильственной ассимиляции и сегрегации, которые являются основным источником конфликта.

Социокультурная интеграция, решая основную проблематику в урегулировании этнических и национальных конфликтов, выделяет несколько задач в соответствии с вышеупомянутой целью:

– Выявление сущности и взаимосвязи понятий: интеграция, культурная идентичность, конфликт;

– Трактовка социокультурной интеграции как механизма по предотвращению межкультурных противоречий;

– Определение факторов национальной напряженности.

Выявление сущности и взаимодействия понятий: интеграция, идентичность, конфликт:

– Идентичность - это осознание субъектом самого себя в качестве носителя определенных ценностей, традиций, верований, определяющее его отношение к миру и ближайшему кругу взаимодействия;

– Конфликт идентичностей - совокупность противоречий, между представителями нетождественных культур, возникающие в процессе их самоидентификации и социализации.

Трактовка социокультурной интеграции как механизма по предотвращению культурных противоречий сводится к социальной сплоченности, базирующейся на определении общих целей, толерантности, плюрализме. Также интеграция граждан разной культурной самоидентификации в социально - политические и гражданско-

правовые процессы, обеспечение безопасности для общего пространства взаимодействия, что приведет к снижению эскалации внутренних конфликтов.

Определение факторов национальной напряженности. Факторы национальной напряженности носят локальный, региональный характер, иными словами, внутренне - политический конфликты, приобретающие этнический характер. К причинам национальной напряженности относят: социальное неравенство, отчуждение социальных групп определенного этноса и конфессии, потребность в безопасности и защиты своих интересов. Играет роль и экономически - политическая ситуация, в частности: военные действия, коррупция, инфляция, безработица, преступность, насильственная ассимиляция; вытеснение гражданских ценностей этническим радикализмом и его пропаганда в средствах массовой информации.[4]

Процесс социокультурной интеграции и решение экономически - политических проблем приведет к урегулированию межкультурных конфликтов, минимизируя факторы их возникновения.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Основы теории межкультурной коммуникации - [Электронный ресурс]. Режим доступа: https://elar.urfu.ru/bitstream/10995/34793/1/978-5-7996-1517-8.pdf, свободный

2. Природа и сущность межкультурной коммуникации - [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/priroda-i-suschnost-mezhkulturnoy-kommunikatsii-1,свободный

3. Теоретические основы межкультурной коммуникации. Формы проявления - [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/teoreticheskie-osnovy-mezhkulturnoy-kommunikatsii-suschnost-i-formy-proyavleniya, свободный

4. Авксентьев В.А., Гриценко Г.Д., Дмитриев А.В. Региональная конфликтология: концепты и российская практика. – М.: Альфа-М, 2008. – 368 с.

5. Венедиктова Т. Д. Основы теории коммуникации : учебник и практикум для академического бакалавриата / Т. Д. Венедиктова [и др.] ; под редакцией Т. Д. Венедиктовой, Д. Б. Гудкова. – М. : Издательство Юрайт, 2019. – 193 с

УДК 327.83

Сэм Готфред, студент магистратуры Государственного университета управления
Sam Godfred, Master Degree Student of the State University of Management
Талалова Лариса Николаевна, доктор педагогических наук, доцент, лектор магистерской программы «Управление международным бизнесом», Государственный университет управления
Talalova Larissa Nikolaevna, Doctor of Pedagogical Sciences, Docent, Lecturer of Master's Degree Program "International Business Management", the State University of Management

ПОЛИТИЧЕСКАЯ ДОКТРИНА ПАНАФРИКАНИЗМА ГАНЫ

GHANA'S PAN-AFRICANISM POLITICAL DOCTRINE

Аннотация. В материалах рассмотрены механизмы привлечения инвестиций в экономику Ганы средствами тур-отрасли под маской Программы «Год Возвращения – 2019», задуманной правительством как тур-проект, но позиционировавшейся как манифестация политической доктрины панафриканизма первого президента Кваме Нкрумы по предоставлению равных возможностей для бывших соотечественников в возвращении на родину. Программа была ориентирована на достижение стратегий: долгосрочной – налаживание взаимодействия с диаспорой за рубежом; краткосрочной – превращение республики в главное тур-направление африканского континента, привлечение инвестиций.

Abstract. The paper analyzes the mechanisms of the investment policy in Ghana by means of tourist sector within “The Year of Return”, Ghana – 2019” campaign which was originated as a mere tour project. Nevertheless, the campaign is closely connected with the country’s Pan-Africanism political doctrine of the first president Kwame Nkrumah, the basic dimensions of which are the equal rights for the ex-compatriots to come back. The program had both long- and short-term strategies: to collaborate with the diaspora abroad and making the republic under investment the key tourist destination at the African continent.
Ключевые слова: панафриканизм, региональная интеграция, африканская диаспора, инвестиции, краткосрочные/долгосрочные стратегии, политическая доктрина, африканская идентичность.
Key words: pan-africanism, regional integration, african diaspora, investment, short/long-term strategies, political doctrine, african nationalist identity.

“The Year of Return”, Ghana – 2019” is a major landmark spiritual and birth-right journey inviting the Global African family, home and abroad, to mark 400 years of the arrival of the first enslaved Africans in Jamestown, Virginia (1619) [3]. The arrival of enslaved Africans marked a sordid and sad period, when strong black men were forcefully taken away from Africa into years of deprivation, humiliation, and torture. While August 2019 marks 400 years since enslaved Africans arrived in the United States, “The Year of Return, Ghana – 2019” celebrates the cumulative resilience of all the victims of the Trans-Atlantic slave Trade who were scattered and displaced through the world in North America, South America, the Caribbean, Europe, and Asia.

This event brought lot of Africa Americans and Europeans around the world to Ghana which contributed positively to Ghana’s economy. One of the main goals of “The Year of Return” campaign is to position Ghana as a key travel destination for African Americans/Europeans and the African Diaspora. Today “the tourism sector has grown to become the fourth foreign exchange earner after cocoa, gold and remittances.” [1, p. 2].

In 2019, the events planned throughout the year serve as a launch pad for a consistent boost in tourism for Ghana in the near and distant years. Beyond tourism, this initiative supports one of the President’s key developmental initiatives knowing that tourism can be a leading indicator to business and investment. The National Tourism Development Plan for 2013–2027 is a testament to government recognition of the industry's importance.

This paper examines the impact of “The Year of Return” on Ghana’s international tourism which was based on the analysis of field data from mixed-format survey questionnaires collected in Accra, Kumasi, Cape Coast and Ho, four of Ghana’s major tourist destination cities. Tourists were attracted to Ghana’s rich offerings in culture and natural environment, including the UNESCO listing Cape Coast Castle, Elmina Castle, Kwame Nkrumah Mausoleum, Wli water falls, Kakum and Mole National Parks as key point of visit, even though it was a successful event in the history of Africa there were some challenges faced by tourists which include visa acquisition process and mobility within the country, especially with regard to limited public transportation options and deficient highway infrastructure. This paper will throw more illumination not only on the impacts of “The Year of Return” program but on some of the challenges as well.

As soon Ghana got its independence in 1957, the Prime Minister and then the President Kwame Nkrumah started advocating for regional integration within the African continent. Pan-Africanism became the political doctrine oriented for the unity of Independent Africa, and the period itself is comprehended as “the golden age of high Pan-African ambitions”. In 1958 there has taken place the first All-African Peoples’ Conference in Ghana. The conference collected political leaders from main African countries. This conference marked the Pan-African movement as an important event with the effect of African Nationalist identity which

was manifested later. The pivot of Nkrumah's Pan-African thoughts was to unite black Africa under the political motto of regionalism.

"The Year of Return, Ghana – 2019", was linked to the 400th anniversary of slaves landing in the US which was said to be the first recorded arrival of enslaved Africans in the Americas. Ghana was a key transit point for transporting slaves and the President of Ghana Nana Akufo-Addo said his country felt a responsibility to welcome all those who could trace their ancestry to Africa. At the beginning of 2019, the Ghana Tourism Authority predicted that, "The Year of Return" program would attract 500,000 extra visitors. Official data from January to September 2019 indicates an additional 237,000 visitors – a rise of 45% compared with the same period the previous year – with significant increases in visitors from the US and UK. "The country recently unveiled a 15-year-long tourism plan that seeks to increase the annual number of tourists to Ghana from one million to eight million per year by 2027." [2].

This first ever event in Africa attracted number of celebrities to Ghana, including international model Naomi Campbell, actor Idris Elba, comedian Steve Harvey, American rap singer Cardi B and a lot to mention. "The Year of Return" program in Ghana according to the Minister of Tourism Barbara Oteng Gyasi has injected about $1.9 bn (£1.5 bn) into Ghana's economy. Ghana Tourism Authority however informed that there was an estimate which was based on multiplying total visitor arrivals, 763,545 between January and September. And by that figure, the average spend per tourist was $2,590. Despite all these positive contributions there were some challenges these tourists faced before and during their visits.

Tourism is a huge business. And globally, it accounts for more than 10% of GDP. According to the World Travel & Tourism Council, 1 out of 5 of all jobs created in the last 5 years was in a tourism sector. But on the African continent, it accounts for only 3.6% of GDP. With its massive growth and job creating potential, it's no wonder why African governments are trying to increase tourism to their nations. None has done it as well as Ghana. The "Year of Return" has hit a chord. One of the significant impacts "The Year of Return" program had on Ghana's tourism was promoting Ghana's image internationally, it has drawn the wider attention of Ghana and positively influenced international media reports. Most of these tourists who visited Ghana and still visiting purchase properties, invested, and set up businesses which boost the country's economy.

"The Ghana Year of Return" is undoubtedly momentous because of its tourism sector and communities in the Americas that, for so long, were robbed of histories and cultures and subjugated to racial and ethnic discrimination. However, it was an important event that did not only positively impact Ghana's tourism sector but tells the story of Africa as a whole, the people, cultures, and regions. Africa's popular image is one-sided and most often mired with poverty, violence, and the perpetual paternalistic stories of aid which the Ghana's historic Year of Return vividly shows and narrates the other side of Ghana and Africa to the world. Financially "The Year of Return" program had injected about $1.9 bn (£1.5 bn) into the economy which was an added advantage in revenue wise.

Even though "The Year of Return" contributed greatly to Ghana's economy, positioning of some of the events were lacking, lot of tourist's sites were not fully exploited in other regions, and this was due to poor transport services to these destinations visiting tourists complain bitterly about the situation which some think it could've been avoided.

Furthermore, a lot of concerns have been expressed about the cost of visa acquisition and air transportation to Ghana. Ghana is seen as a relatively expensive destination in terms of cost of travel and its living standards compared to other Africa countries and the Caribbean. Tourists during the visits lamented so much about this problem and asked government to take a second look at this situation.

Ghana government over the years has been trying to improve its tourism sector by heavily investing and promoting it to the outside world but there are some key relevant obstacles that need to be considered and tackled. Marketing positioning is very important in this

modern day of business and Ghana government in collaboration with the Ghana tourism board needs to find a peculiar way to promote and position the countries tourism sector in the minds of individual tourists, create more enabling environment for this tourists by constructing and developing the country's road channels for this tourists to fully exploit other regions in the country with all this been done the government will generate more revenue from other sectors in various regions. Furthermore, visa acquisition should be made easy for international travelers who want to visit Ghana for tourists' purposes, curbing this problem will greatly influence airline companies to direct more of their flights route to Ghana instead of the Caribbean countries. Здесь можно указать ссылки на грант и другие финансируемые проекты, в рамках которых выполнялось исследование.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Bentum-Ennin, I. Determinants and Economic Impact of International Tourist Arrivals in Ghana. African Economic Research Consortium. August 2019. N 580. URL: https://aercafrica.org/wp-content/uploads/2019/09/Policy-brief-Isaac-580-r.pdf (the date of access: 20.10.22).

2. Busari, S., Siaw, L. Ghana Is Being Heralded as the Next Big Tourist Destination. Here Is Why. CNN. February 7, 2019, URL: https://edition.cnn.com/travel/article/ghana-year-of-return-tourism-intl/index.html (date of access: 22.10.2022).

3. Diakite, P. How Ghana's Year of Return Campaign Put Black Destinations in the Spotlight. Jacksonville Free Press. April 28, 2020, URL: https://jacksonvillefreepress.com/how-ghanas-year-of-return-campaign-put-black-destinations-in-the-spotlight/ (date of access: 22.10.22).

УДК 343.301

Турбанов Илья, студент; Комсомольский-на-Амуре государственный университет;
Turbanov Ilya, student of Komsomolsk-na-Amure State University
Малышева Наталья Васильевна, кандидат филологических наук, доцент; Комсомольский-на-Амуре государственный университет
Malysheva Natalia Vasilievna, PhD in Philology, Associate Professor, Komsomolsk-na-Amure State University

ПРОБЛЕМА ЭФФЕКТИВНОСТИ ВООРУЖЕННОЙ БОРЬБЫ С МЕЖДУНАРОДНЫМ ТЕРРОРИЗМОМ (ОПЫТ США)

THE PROBLEM OF THE EFFECTIVENESS OF THE ARMED FIGHT AGAINST INTERNATIONAL TERRORISM BASED (THE USA PRACTICE)

Аннотация. В данной статье рассматривается эффективность вооруженных сил в борьбе с террористической деятельностью, особенно с международным терроризмом, на примере США. Соединенные Штаты Америки в начале XXI в. столкнулись с проблемой безопасности всей страны. С целью противодействия угрозам руководством страны были разработаны и реализованы экономические, политические, информационные, военные и другие мероприятия, показавшие свою эффективность на данном этапе развития современного мира.

Abstract. This article examines the effectiveness of military forces in combating terrorist activity, especially international terrorism, using the United States as an example. The United States in the early twenty-first century faced a nationwide security challenge. In order to counteract the threats, the country's leadership has developed and implemented economic, political, informational, military and other measures, which have shown their effectiveness at this stage in the development of the modern world.

Ключевые слова: международный терроризм, США, антитеррористическая кампания, война против терроризма
Key words: international terrorism, the USA, antiterrorism campaign, war against terrorism

После террористических актов 9 сентября 2001 года Соединенные Штаты Америки начали деятельность, направленную на ликвидацию международного терроризма и названую впоследствии «Войной против терроризма». Правительством США эта война ведется уже более 20 лет. Согласно отчету от сентября 2021 года проекта "Стоимость войны" Института международных и общественных отношений имени Ватсона при Университете Брауна общее число жертв войны с терроризмом в Ираке, Афганистане и Пакистане составляет от 518 000 до 549 000 человек. Согласно проекту "Издержки войны" Института Ватсона при Университете Брауна, война с терроризмом обойдется в 8 триллионов долларов на операции в период с 2001 по 2022 год плюс 2,2 триллиона долларов на будущие расходы на обслуживание ветеранов в течение следующих 30 лет.

В данной статье мы изучим эффективность применения вооруженных сил в борьбе против международного терроризма на примере США.

Исходя из цели были поставлены следующие задачи:

- изучить цели США в войне с терроризмом;
- изучить методы борьбы с терроризмом;
- изучить эффективность вооруженных сил в войне с терроризмом.

На протяжении всей войны с терроризмом цели США в ней оставались неизменными. Согласно официальным заявлениям Белого Дома, она подразумевает под собой защиту американцев от угрозы терроризма, предотвращение террористических актов, ликвидация террористических группировок, а также разрешение различного рода проблем, являющихся основой для формирования радикальных движений. Так, Джордж Буш поставил целью уничтожение Аль-Каиды и прочих международных террористических группировок, позже Барак Обама повторил данные цели и добавил к ним еще и уничтожение Исламского государства.

В ответ на увеличение числа террористических актов, направленных против американских военных, в вооруженных силах США были созданы контртеррористические структуры. Основная их цель – заблаговременное и детальное планирование, подготовка и осуществление мер по борьбе с терроризмом. В настоящее время, стратегия США по борьбе с террористической деятельностью основана на использовании вооруженных сил США без объявления при этом полномасштабной войны, а также на укреплении международного антитеррористического сотрудничества [1].

Кроме того, США проводят подготовку местных вооруженных сил для дальнейшей борьбы с терроризмом на территории их страны, создав программу для обучения местных специалистов через систему различных центров. Так, в 2003 году был создан «Центр по противодействию террористическим угрозам», а позже в 2004 году «Национальный контртеррористический центр» для интеграции и анализа всей информации о терроризме как внутри страны, так и за рубежом.

Что касается противодействию терроризму внутри самих Соединенных Штатов, то за него отвечает подразделение ФБР «Команда по спасению заложников» (Hostage Rescue Team) [3]. Таким образом, ответственность за террористические акты во всех случаях несут федеральные власти. Согласно данным исследования Эрика Гепнера, можно сказать, что существует явная корреляция между увеличением усилий США в войне с терроризмом и ухудшением террористической ситуации в мире. Так, на каждый потраченный миллиард долларов и тысячу американских военнослужащих, отправленных на борьбу с террором, количество террористических актов в мире увеличивается на 19. Если рассматривать данный вопрос в глобальном плане, то можно видеть,

что в 2001 году в целом было совершено 1880 террористических актов, однако к 2014 году их число возросло до 16818 [4]. В августе 2021 американские войска покинули Афганистан в результате экстренного вывода войск с территории страны [2]. Вывод войск сопровождался оставлением оружия и техники, которые впоследствии были захвачены силами Талибана, запрещенной во многих станах мира террористической организацией. В августе того же года талибами был захвачен Кабул, а вскоре вся территория Афганистана перешла под их контроль.

В заключение можно сказать, что, несмотря на активные действия США по предотвращению террористической деятельности и на уже имеющиеся конкретные задачи по ее предотвращению, террористические группировки международного масштаба, такие как Аль-Каида, до сих пор не были уничтожены, а число террористических актов в мире за последнее время не сильно сократилось. Напротив, имеется связь между вмешательством США, в частности, с применением вооруженных сил, и увеличением числа террористических актов по всему миру. Помимо этого, несмотря на почти 20 лет военного присутствия в Афганистане, сразу после вывода американских войск, радикальными исламистами был взят контроль над страной, что может говорить о том, что созданное США правительство Афганистана держалось исключительно на военной поддержке Соединенных Штатов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Устинова Т. С., Солсоев И. Н. Роли и методы США в борьбе с терроризмом // Социально-экономическая география. 2017. С. 9-11.

2 Галстян К. А. Военная операция НАТО в Афганистане (2001-2021) // История и археология. 2022. С. 488-490.

3 Воронин Ю. А., Беляева И. М., Кухтина Т. В. Стратегия борьбы с терроризмом в США: Современные тенденции // Государство и право. Юридические науки. 2019. Том 19. № 4. С. 7-13.

4 Гепнер Э. В. Измерение эффективности войны Америки с террором. 2016. № 1. С. 108-120.

УДК 621.9:519.8

Турбанов Илья, студент; Комсомольский-на-Амуре государственный университет;
Turbanov Ilya, student of Komsomolsk-na-Amure State University
Когай Сергей Геннадьевич, старший преподаватель, Комсомольский-на-Амуре государственный университет
Kogai Sergei Gennadevich, senior lecturer, Komsomolsk-na-Amur State University

БОРЬБА КНР С МЕЖДУНАРОДНЫМ ТЕРРОРИЗМОМ В РАМКАХ ИНИЦИАТИВЫ «ОДИН ПОЯС, ОДИН ПУТЬ»

PRC'S COUNTERING INTERNATIONAL TERRORISM UNDER THE "ONE BELT, ONE ROAD INITIATIVE"

Аннотация. В данной статье исследуются методы борьбы Китая с международным терроризмом в рамках инициативы «Один пояс, один путь». Цель статьи – оценить масштабы угрозы и меры, принимаемые Пекином для защиты своих граждан и бизнеса и для противодействия террористической угрозе в целом. Ставится также задача проанализировать новые тенденции в политике Пекина в вопросах международной безопасности.
Abstract. This article examines how China is combating international terrorism through the One Belt, One Road initiative. It aims to assess the scale of the threat and the measures taken

by Beijing to protect its citizens and businesses and to counter the terrorist threat in general. It also aims to analyse new trends in Beijing's international security policy.
Ключевые слова: «Один пояс, один путь», борьба с терроризмом, Китай, международный терроризм.
Key words: One Belt, One Road, counter-terrorism, China, international terrorism.

В 2013 году китайское правительство предложило инициативу «Пояса и пути», на пути реализации которой возникло определенное количество проблем, в том числе и проблемы безопасности. В настоящее время терроризм стал основной из такого рода проблем, влияющей на плавный ход реализации инициативы Китайской Народной Республики «Один пояс, один путь». Развитие инициативы «Один пояс, один путь»на разных этапах, начиная от строительства «Экономического пояса Шелкового пути», и заканчивая «Морским Шелковым путем XXI века» сталкивается со значительной угрозой терроризма. Вдоль «Пояса и пути» проходит более 70 стран, имеющих различные социальные системы, верования, традиции и уровень экономического развития. Те страны или регионы, в которых имеются различные экономические проблемы, общественное неравенство и острые межэтнические конфликты, чаще всего сталкиваются с внутренними социальными волнениями, а как следствие с появлением терроризма. Целью данного исследования является деятельность КНР, направленная против терроризма, в рамках инициативы «Один пояс, один путь». Исходя из цели, были поставлены следующие задачи:

- рассмотреть цель антитеррористической деятельности вдоль «Пояса и Пути».
- изучить правовую основу КНР в борьбе с международным терроризмом.
- рассмотреть сотрудничество Китая с другими странами в борьбе с террористической деятельностью.

В законе Китайской Народной Республики о борьбе с терроризмом, принятого Китаем в 2015 году, указаны основы, принципы и соответствующие юридические процедуры для осуществления международного сотрудничества в борьбе с терроризмом. Международное сотрудничество Китая в борьбе с террористической детальностью направлено не только на беспрепятственную реализацию инициативы «Один пояс, один путь» и защиту национальных интересов страны, но и на обеспечение международного сотрудничества для политической, экономической и социальной безопасности стран, расположенных вдоль «Один пояс и один путь». Однако, учитывая международный характер терроризма, интернациональное сотрудничество Китая в борьбе с ним также основывается на действующем международном праве. Как член Организации Объединенных Наций и постоянный член Совета Безопасности, а также как сторона, подписывающая или ратифицирующая международные антитеррористические договоры, Китай не только берет на себя международные обязательства по борьбе с терроризмом, но и пользуется широкими правами [4]. Китай, осуществляя международное антитеррористическое сотрудничество в рамках существующего международного правопорядка, реализует свои интересы и разрешает связанные с этим конфликты в рамках, допускаемых международным правом [2]. Также, международное право предоставляет Китаю юридическую гарантию осуществления международного сотрудничества в борьбе с терроризмом в странах и регионах вдоль «Пояса и пути». Несколько резолюций по кибертерроризму, принятых Советом Безопасности ООН, обеспечивают международно-правовую основу для сотрудничества стран вдоль «Пояса и пути» в целях предотвращения кибертерроризма и борьбы с ним. В настоящее время Китай ведет активное сотрудничество с ШОС, в рамках которой было создано действующее антитеррористическое агентство в соответствии с «Шанхайской конвенцией о борьбе с терроризмом, сепаратизмом и экстремизмом» [3]. КНР также расширяет сотрудничество в борьбе с терроризмом, а также пресекает террористическую деятельность в Восточном Туркестане и Тибете [1]. В то же время он активно способствует более широкому меж-

региональному сотрудничеству по вопросам совместной борьбы с терроризмом между другими странами или региональными организациями вдоль «Пояса и пути» и Шанхайской организации сотрудничества.

Исходя из приведенной выше информации, можно сделать вывод о том, что в настоящее время Китай, являясь членом международных организаций, ведет сотрудничество между странами по борьбе с терроризмом. Развитие инициативы «Один пояс, один путь» создало для КНР явные террористические угрозы более серьезного характера. В настоящее время Китай пользуется возможностью внести свой вклад в борьбу с международным терроризмом, а также укрепляет свою позицию и роль в международной борьбе с террористической деятельностью со странами вдоль «Пояса и пути». Созданный правовой механизм в борьбе с терроризмом ставит закон во главе сотрудничества в борьбе с террористической деятельностью.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Чжао М., Ван Ш. Оценка ситуации в области национальной безопасности и контрмеры вдоль «Пояса и пути» // Китайской академии наук. 2016. № 6. С. 21-32.

2 Ши Х. О реакции Китая на создание международного антитеррористического правового механизма на фоне «Одного пояса и одного пути» // Журнал Юньнаньского университета управления. 2017. № 4. С. 27-36.

3 Го Ц. «Один пояс один Путь» предоставляет новые возможности для уничтожения почвы терроризма // Политика и политические науки. 2019. С. 21-23.

4 Кирьянов А.В. Противодействие международному терроризму в рамках ООН // Государство и право. Юридические науки. 2017. С. 213-218.

УДК 340

Турмачева Анастасия Эдуардовна, студентка, Комсомольский-на-Амуре государственный университет
Turmacheva Anastasia Eduardovna, student, Komsomolsk-na-Amure State University
Мусалитина Евгения Александровна, доцент, Комсомольский-на-Амуре государственный университет
Musalitina Evgenia Aleksandrovna, associate professor, Komsomolsk-na-Amure State University

СИСТЕМА ГОСУДАРСТВЕННЫХ МЕР ПРОФИЛАКТИКИ ТЕЛЕФОННОГО ТЕРРОРИЗМА В РОССИИ

THE SYSTEM OF STATE MEASURES FOR PREVENTION OF TELEPHONE TERRORISM IN RUSSIA

Аннотация. Телефонный терроризм стал глобальной проблемой национальной безопасности не только в России, но и во многих европейских и азиатских странах. Масштаб телефонного терроризма наносит существенный ущерб социально-экономической сфере государства. В статье рассматриваются юридические аспекты, законодательные акты и меры по борьбе и профилактике преступности в сфере телефонии. Рассматривается их легитимность в контексте международных стандартов по правам человека.
Abstract. Telephone terrorism has become a global national security problem not only in Russia, but also in many European and Asian countries. The scale of telephone terrorism causes significant damage to socio-economic sphere of the state. The article deals with legal aspects, legislative acts and measures to fight and prevent crime in the field of telephony. Its legitimacy is considered in the context of international human rights standards.

Ключевые слова: телефонный терроризм, профилактика терроризма, Россия, безопасность, террористические атаки.
Key words: telephone terrorism, prevention of terrorism, Russia, security, terrorist attacks.

Телефонный терроризм стал глобальной проблемой национальной безопасности не только в России, но и во многих европейских и азиатских странах. Многие крупные города России в последнее время подвергаются телефонным террористическим атакам с информацией о заложенной бомбе. Так, согласно данным УМВД России по Московской области, в период с января по сентябрь 2022 г. по причине ложных телефонных звонков было эвакуировано около 45 тыс. человек [5].

Телефонные атаки направлены на образовательные организации дошкольного, школьного, средне специального и высшего образования, органы судебной власти, медицинские учреждения и др. Очевидно, что масштаб телефонного терроризма наносит существенный ущерб социально-экономической сфере государства.

В связи с ростом телефонного терроризма в России правительством был разработан ряд мер по борьбе и профилактике. В рамках этой работы особое внимание уделяется проблеме влияния мобильной связи на рост телефонной преступности. В период появления систем мобильной телефонии в России отсутствовала законодательная база, регулирующая правовые аспекты услуг мобильной связи физическими лицами [3]. В результате, появилось большое количество так называемых «серых» абонентов, то есть номеров, зарегистрированных на не идентифицированных лиц. Такая ситуация увеличивает рост потенциальных преступлений, связанных с телефонным терроризмом.

Эффективное пресечение терроризма требует привлечения к уголовной ответственности тех, кто планирует, организует и руководит террористическими актами, в том числе телефонным терроризмом. Возникшая потребность в урегулировании законодательства деятельности провайдеров мобильной связи обусловила разработку ряда проектов. Один из них – решение, в соответствии с которым операторы телекоммуникационных предприятий должны регистрировать учетную запись пользователя, проводить истинную идентификацию при обработке различных операций пользователей по доступу к сети [1]. При регистрации пользователя проверяется его идентификационная информация. Согласно постановлению, отказавшемуся от идентификации абоненту, услуга не предоставляется.

Наряду с этими правилами все телекоммуникационные компании обязаны принять меры, чтобы предотвратить агентский выпуск и обслуживание сим-карт в неограниченном количестве. Согласно «Закону о борьбе с терроризмом» проводится перерегистрация старых пользователей, не идентифицированных в системе ранее [6]. Для пользователей, не завершивших процедуры регистрации в установленный срок, базовая телекоммуникационная компания приостанавливает предоставление услуг связи (за исключением экстренных служб, таких как вызов пожарной службы, полиции, скорой медицинской помощи и дорожно-патрульной службы).

Разработка законодательства по борьбе с терроризмом, в том числе, с телефонным терроризмом, связана с проблемой соблюдения прав человека. Это означает, что должен соблюдаться баланс между эффективностью уголовного преследования и соответствия мер международным стандартам в области прав человека [4]. Таким образом, при разработке инфраструктуры безопасности, которая ограничивает осуществление прав человека, и реализует ее, оно должно продемонстрировать, что соблюдаются следующие принципы:

- принцип законности: ограничительные меры должны быть установлены или предписаны в соответствие с законодательством;

- принцип законной цели: законодательство о борьбе с терроризмом, направленное на ограничение прав человека, не должно применяться к действиям, не являющимся терроризмом;

- принцип необходимости и соразмерности: меры, нарушающие права человека, должны быть направлены на применение к конкретному лицу. Необходимо определить, как эта мера связана с противодействием реальной или потенциальной террористической угрозе государству и его вкладу в международные и региональные механизмы борьбы с терроризмом;

- принципы равенства и не дискриминации: эти два принципа являются фундаментальными элементами международного права в области прав человека [2].

В заключении можно сделать вывод о том, что регулирование сферы мобильной телефонии способствует повышению эффективности организации профилактики и борьбы с телефонным терроризмом. Разработанная в РФ регламентация этой сферы позволила ликвидировать рынок «серой» телефонии, который служил технической и финансовой базой телефонного терроризма.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Агузарова, В. М. Телефонный терроризм и его предупреждение / В. М. Агузарова, М. Р. Бадтиева // Конкурс лучших студенческих работ : сборник статей X Международного научно-исследовательского конкурса, Пенза, 15 октября 2021 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2021. – С. 145-147.

2 Акбарализода, Д. А. Теоретико-правовые аспекты противодействия терроризму / Д. А. Акбарализода // Законодательство. – 2021. – № 2(42). – С. 152-157.

3 Жерновой, М. В. Законодательное обеспечение борьбы с "телефонным терроризмом" в России / М. В. Жерновой // Российская юстиция. – 2018. – № 6. – С. 53-54.

4 Косовская, Д. В. Актуальные проблемы борьбы с телефонным терроризмом / Д. В. Косовская // Евразийский юридический журнал. – 2022. – № 4(167). – С. 396-398.

5 Савинский, А. В. Общественная опасность телефонного терроризма заслуживает адекватной уголовно-правовой оценки / А. В. Савинский // Юридическое образование и наука. – 2022. – № 1. – С. 22-25. – DOI 10.18572/1813-1190-2022-1-22-25.

6 Тимощук, А. С. Общественное сознание как мишень терроризма / А. С. Тимощук // Пенитенциарное право: юридическая теория и правоприменительная практика. – 2019. – № 2(20). – С. 130-136.

УДК 323.2

Тырышкин Сергей Игоревич, студент Комсомольского-на-Амуре государственного университета.
Tyryshkin Sergey Igorevich, student of Komsomolsk-on-Amur State University.
Подкич Светлана Александровна, старший преподаватель Комсомольского-на-Амуре государственного университета.
Podkich Svetlana Alexandrovna, senior lecturer at Komsomolsk-on-Amur State University.

ПРОФИЛАКТИКА ТЕРРОРИЗМА И ЭКСТРЕМИЗМА В МОЛОДЕЖНОЙ СРЕДЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

PREVENTION OF TERRORISM AND EXTREMISM AMONG YOUNG PEOPLE OF THE RUSSIAN FEDERATION

Аннотация. Для всего человечества и для Российской Федерации проблемами, препятствующими наиболее опасным явлениям 21 века, считаются экстремизм и терроризм. Эти проблемы особенно актуальны для молодежных кругов. На основе обобщения положений, сформулированных в учении о криминалистике, и анализа законов и практи-

ки в правоприменительной деятельности выявлены наиболее распространенные проблемы, связанные с распространением среди подростков этих негативных социальных явлений, и способы их решения заключается в практике правоприменения. правоохранительных органов и предлагает наиболее репрезентативные проблемы и решения, связанные с распространением этих негативных социальных явлений среди подростков.

Abstract. For all of humanity and for the Russian Federation, extremism and terrorism are considered to be the most dangerous phenomena of the 21st century. These problems are particularly relevant for youth circles. On the basis of a generalization of the provisions formulated in the doctrine of criminology, and an analysis of laws and practice in law enforcement, the most common problems associated with the dissemination of these negative social phenomena among adolescents have been identified, and the ways to solve them are in the practice of law enforcement. Law enforcement agencies and offers the most representative problems and solutions associated with the spread of these negative social phenomena among adolescents.

Ключевые слова: терроризм, экстремизм, профилактика, молодежная среда, законодательство.

Key words: terrorism, extremism, prevention, youth environment, legislation.

Если мы обратим внимание на социальные тенденции, проявляющиеся в молодежной среде в последнее время, то станет очевидно, что экстремизм как общественно опасное явление начинает проявляться среди молодежи гораздо чаще, чем в XX веке. [7]. Молодое поколение исторически относится к группе риска. В силу возраста для молодых людей характерны такие психологические особенности, как юношеский максимализм, неустойчивость мировоззрения, стремление к объединению в группы, трудности в самоопределении, что при определенных условиях и создании благоприятной среды становится исходным механизмом антисоциальной активности. Эти факторы, присущие данной возрастной группе, накладываются на определенные социальные, культурные и исторические особенности, что в итоге может привести к возникновению определенной напряженности – психологической, если мы говорим о конкретном индивиде, или социальной, если мы пронаблюдаем некоторую выборку представителей.

Сегодня мы можем наблюдать проявление характера молодежного экстремизма в отношении очернения или отрицания закона. Другим проявлением экстремизма, которое может быть отмечено как одно из наиболее широко проявляющихся, является нетерпимость к гражданам России, которые представляют разные социальные и этнические группы. Именно недостаточная социальная адаптированность, которая проявляется у представителей молодежи при взаимодействии с носителями разных общественно-политических, правовых, экономических, нравственных, эстетических и религиозных представлений, может быть выделена как один из основных факторов, способствующих формированию и проявлению экстремистских настроений. Формирование экстремистских настроений у молодежи свидетельствует о недостаточной социально адаптированности данной категории населения и о том, что антисоциальные установки в сознании могут привести к противоправному поведению [4].

Молодежная культура стремительно меняется, и повсеместное внедрение интернета только ускоряет эти изменения. Отслеживать социальные, философские, психологические тенденции становится все сложнее. Не существует исторического прецедента, которой позволил бы отследить внутренние процессы, характерные для определенной возрастной и/или социальной группы в условиях глобализации и полной доступности информации. Между тем, именно эти внутренние процессы зачастую становятся причиной тех проявлений нетерпимости, напряженности и конфликтов, которые могут превратиться в экстремистские инциденты с участием молодежи.

Разговоры о реализации национальной молодежной политики в сфере предотвращения и противодействия терроризму и экстремизму менее эффективны и часто ведут к участию молодежи в экстремистской деятельности. В результате часть молодежи находится под влиянием определенных кругов, в которых в отличие от них существуют государственные институты и государство в целом. Важное значение для профилактики ювенального экстремизма имеет Федеральный закон от 24 июня 1999 г. № 24. № 120-ФЗ «Основы системы профилактики безнадзорности и правонарушений несовершеннолетних» [1]. Данный нормативный акт призван регулировать деятельность различных государственных органов в сфере профилактики безнадзорности и правонарушений среди молодежи.

Стоит отметить, что, несмотря на то, что количество подобных инициатив с каждым годом увеличивается, и существует явный успешный прецедент их реализации, в основном данные инициативы призваны перекрывать те или иные отдельные аспекты озвученной проблемы и не имеют единой системы координации при реализации. Таким образом, одной из основных тем, требующих детального рассмотрения, становится объединение данных инициатив с целью более рациональной и эффективной профилактики проявлений экстремизма в молодежной среде. Кроме того, безусловно необходима адаптация существующих решений к новым, цифровым и интернет-реалиям, в которые представители молодого поколения погружены гораздо больше, чем иные возрастные группы.

Менее эффективны меры по отношению к несовершеннолетним и отбывающим наказание в колониях. Работа с этой категорией неизменно осложняется специфическими социальными и психологическими особенностями, которые необходимо тщательно продумывать на этапе планирования и разработки любых профилактических программ, а также своевременно актуализировать в процессе их реализации. Кроме того, среди этой категории молодых людей наиболее заметна тенденция к рецидивирующему поведению, что может быть обусловлено как индивидуальными особенностями каждого представителя группы, так и общими, характерными для группы, стремлениями оставаться частью коллектива, не выделяться, следовать за авторитетами и т.п. Все эти факторы могут, ввиду большого количества возможных конфигураций, складываться в определенный психосоциальный профиль, уникальный для каждого конкретного представителя. Работу по профилактике проявления экстремистских настроений в таком случае следует планировать и реализовывать индивидуально, учитывая весь спектр факторов, выявленных в каждой разбираемой ситуации.

До сих пор планомерно проводилась работа по предупреждению терроризма и экстремизма на законодательном уровне. Так, Постановлением Правительства РФ от 3 апреля 1996 г. № 387 «Дополнительные меры поддержки молодежи в Российской Федерации», дата: 12.07.999 г. Принят № 795 «Задача Государственного комитета Российской Федерации по молодежной политике». Данный нормативный акт был призван утвердить порядок регулирования и координации деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления по реализации Комплексного плана противодействия идеологическому терроризму Российской Федерации на 2019-2023 годы.

Также в рамках данного направления были разработаны различные программы, направленные на патриотическое воспитание молодежи, в частности программы по борьбе с экстремизмом и предупреждению терроризма. В пример успешной реализации этого направления можно привести Всемирный благотворительный фонд «Дети и молодежь против терроризма и экстремизма». Он направлен на развитие борьбы с терроризмом и регулирования. Указом Президента Российской Федерации от 29 мая 2020 г.

утверждена Единая стратегия Российской Федерации по противодействию экстремизму до 2025 г. [3].

Все вышеперечисленные меры активно применяются и демонстрируют достижение определенных результатов и положительную динамику в воспитательных и профилактических моментах работы с молодежью. Между тем, стоит отметить, что они во многом носят теоретический характер, и не всегда соответствуют актуальным на данный момент способам убеждающего воздействия на молодое поколение. Кроме того, при разработке данных мероприятий не всегда уделяется должное внимание этнокультурным особенностям регионов Российской Федерации.

Возникновение новой антисоциальной субкультурной молодежной системы можно рассматривать как своего рода рецидивирующее явление. Одной из основных причин его появления является отсутствие программы блокирования экстремистских настроений нового поколения, которая в достаточной степени отвечала был современным экономическим, социальным и культурным явлениям нашего общества, и особенно его молодежной составляющей. Существующие программы противодействия проявлениям терроризма и экстремизма требуют тщательного изучения в контексте этих аспектов, что в перспективе позволит нам определить масштабы проблемы и более детально проработать пути ее решения. На сегодняшний день отмечается некоторая недостаточность разработки программ профилактических действий с учетом психологических и социокультурных особенностей социальных групп молодежи.

По нашему мнению, бережное отношение к мультикультурным особенностями многонационального государства, развитие терпимого и уважительного отношения в среде молодежи, должно сплотить все народы Российской Федерации, формируя идеалы межнационального согласия, дружбы и сотрудничества народов [5].Поэтому профилактика молодежного терроризма и экстремизма должна осуществляться путем достаточной проработки на законодательном уровне, в государственных учреждениях и вузовской администрации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Основные принципы безнадзорности несовершеннолетних и предупреждения правонарушений: Федер . Акт 24 июня . 1999 г. 120-ФЗ: В редакции. перо . Закон от 24 апреля 2020 г. № 147-ФЗ // Росс . Джиа . 1999. 30 июня ; 29 апреля 2020 г.

2. Борьба с терроризмом: Перо . Закон от 6 марта 2006 г. 35-ФЗ: Изменено. перо . Закон от 26 мая 2021 г. № 155-ФЗ // Росс . Джиа . 10 марта 2006 г.; 31 мая 2021 г.

3. Об утверждении Стратегии противодействия экстремизму Российской Федерации до 2025 года: Указ Президента Российской Федерации от 29 мая 2020 г. № 344 // звонок. Росс Лоу. Союз. 1 июня 2020 г.

4. Дробизева Л., Страдающая Е. Политический терроризм и экстремизм // Эпоха толерантности. 2003. Нет. 5. С. 33-37. 5. Совкова И. Ю. Служебная активность деструктивного поведения личности в кризисной ситуации // Психовоспитание правоохранительных органов. 2003. Нет. 1(19). 73-81 стр.

6. Ольшанский Д.В. Психология терроризма. СПб .: Питер, 2002.

7. Чурков Б.Г. Мотивационно-идеологические основы современного терроризма // Социальный конфликт: экспертиза, навыки прогнозирования и разрешения. 2013. № 4. С. 27–34.

УДК 340

Цирукина Дарья Кирилловна, студент, Комсомольский-на-Амуре государственный университет
Tsirukina Daria Kirillovna, student, Komsomolsk-na-Amure State University
Мусалитина Евгения Александровна, доцент, Комсомольский-на-Амуре государственный университет
Musalitina Evgenia Aleksandrovna, associate professor, Komsomolsk-na-Amure State University

ДЕЗИНФОРМАЦИЯ КАК ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ В СОВРЕМЕННОМ ОБЩЕСТВЕ

DISINFORMATION AS INFORMATION TERRORISM IN MODERN SOCIETY

Аннотация. Терроризм является острой и важной проблемой в мире, поскольку он затрагивает самые разные аспекты жизни общества, нанося огромный урон по всем сферам. В нынешнее время он обрел множество направлений, одним из которых является информационный терроризм. В век постиндустриального общества, в котором самым главным фактором влияния является информация, проблема данного направления терроризма обрела особую актуальность. Многие авторы рассматривали данную тему, однако аспект дезинформации – одного из главных понятий, относящихся к кибертерроризму – остался недостаточно освещенный. В статье рассматриваются особенности роли дезинформации в современном обществе.
Abstract. Terrorism is undoubtedly an acute and important problem in the world, as it affects all aspects of society, causing huge damage in all spheres. In modern times, it has taken many directions, one of which is information terrorism. In the age of post-industrial society, in which the most important factor of influence is the information, the problem of this direction of terrorism has gained particular relevance. Many authors have addressed the subject, but the aspect of disinformation, one of the main concepts related to cyberterrorism, has remained underreported. This article discusses the peculiarities of the role of disinformation in modern society.
Ключевые слова: терроризм, кибертерроризм, информационный терроризм, дезинформация.
Key words: terrorism, cyberterrorism, information terrorism, disinformation.

В настоящее время терроризм приобрел разнообразные формы, охватывая с каждым годом все больше сфер жизни. В информационном обществе самой главной ценностью соответственно является информация. «Кто владеет информацией, тот владеет миром…», – утверждал Н. Ротшильд [3]. Если информация попадает в руки террористов, это становится глобальной проблемой. В глобализированном мире существование интернет-коммуникаций стирает коммуникационные границы суверенных государств, создавая отсутствие информационных барьеров и создавая условия для развития терроризма и экстремизма в разных частях света путем воздействия на сознание пользователей интернета.

Обратимся к понятию информационного терроризма. Итак, информационный терроризм – это, прежде всего негативное воздействие на личность, общество и государство всеми существующими видами информации [1]. Он используется для создания ложного представления общества о различных аспектах жизни. Чаще всего такой терроризм используется в политической сфере, оказывая огромное влияние на население страны, формируя их настроения по отношению к власти, другим народам, истории и т.д. Примером может служить любого рода пропаганда, распространенная СМИ.

Средства массовой информации нельзя недооценивать, за годы пропаганды ложная информация может сформировать определенное мировоззрение, необходимо

террористам. Она может настроить людей на переворот, на насилие и даже убедить их самих примкнуть к террористам. Примерами тому служат перевороты в некоторых республиках бывшего СССР, а также стран Средней Азии и Ближнего Востока [3]. СМИ из-за этого часто называют четвертой властью. Периодически террористы захватывают каналы телевещания, распространяя дезинформационную пропаганду.

Кибертерроризм – использование компьютерных и телекоммуникационных технологий в террористических целях. Корни понятия кибертерроризма можно проследить до начала 1990-х годов, когда быстрый рост использования Интернета и дебаты о зарождающемся «информационном обществе» вызвали ряд исследований потенциальных рисков, с которыми сталкиваются высокоразвитые сети, высокотехнологичные страны [2]. Информационный терроризм отличается низким уровнем раскрываемости. Кибертеррористы практически не оставляют следов, способных помочь в обнаружении преступников [4].

Помимо социально-политического направления дезинформация также активно действует в экономической направленности, дестабилизируя государственную экономику изнутри. В последнее время участились акты ложного минирования различных структур: заводов, учебных заведений, супермаркетов. Вынужденная проверка этой информации на достоверность приводит к огромным экономическим убыткам.

Информационный терроризм – самое опасное противообщественное явление. Дезинформация проникает в сознание незамедлительно и мгновенно воздействует на позитивное восприятие психики, негативно влияя на нервную систему. Человек уже не может ничего воспринимать без сомнений, недоверия, он начинает подозревать ложь везде и предвзято относится к любой информации. В данной обстановке тяжело мыслить объективно. Такой терроризм порождает злобу, ненависть, и даже вызывает межнациональную вражду.

Помимо влияния на рассудок, дезинформация может наносить огромный вред физическому здоровью людей. Лживые сведения в области здравоохранения о вакцинах, лекарствах, способах лечения различных болезней способны вызвать большое количество жертв среди обычных людей.

Несовершенство законодательства касательно кибертерроризма, несомненно, еще больше осложняет возможность поимки и наказания дезинформаторов. Термин кибертерроризм запрещён законодательно лишь в двух странах мира: США и Украине. Тем не менее, для борьбы с информационным терроризмом имеется развёрнутая международная правовая система, основанная на соответствующих актах ООН и ОБСЕ, договорённостях в рамках ШОС и ЕС. Международное сотрудничество в этой области продолжает усиливаться [5].

Таким образом, дезинформация и информационный терроризм в целом являются угрозой национальной безопасности мирового уровня. Оказывая влияние на различные сферы жизни, дезинформация дестабилизирует государство и мировое сообщество, а также психику и здоровье простых людей. В связи с этим, очевидна необходимость улучшения средств и методов борьбы с данным видом терроризма, а также усовершенствования способов установления личности информационных террористов. Мы также видим необходимость реформирования системы наказания за дезинформационную пропаганду.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Аношкина, А. А. Информационный терроризм как угроза национальной безопасности / Аношкина А. А. – Текст: непосредственный // Молодой ученый. – 2020. – № 20 (310). – С. 245-247.

2 Иванов, Д. В. Информационный терроризм как угроза безопасности России / Д. В. Иванов // Актуальные вопросы теории и практики в деятельности подразделений

полиции по охране общественного порядка и иных служб ОВД : Материалы вузовской научно-практической конференции, Волгоград, 11–12 августа 2022 года. – Москва: ООО "Издательство "Спутник+", 2022. – С. 63-67.

3 Цыплаков, А. Ю. Информационные войны. Российская Федерация в условиях информационной войны / А. Ю. Цыплаков // Актуальные вопросы становления российской государственности: генезис, проблемы, тенденции : Материалы региональной научно-практической конференции студентов и молодых ученых с международным участием, Таганрог, 31 мая 2019 года. – Таганрог: Издательско-полиграфический комплекс РГЭУ (РИНХ), 2019. – С. 384-388.

4 Шарыпова, Т. Н. Кибертерроризм: сущность, опасность, методы борьбы / Т. Н. Шарыпова, В. В. Винкерт // Аллея науки. – 2019. – Т. 2. – № 2(29). – С. 886-888.

5 Шарыпова, Т. Н., Сиваков В. Н. Киберпреступления. цели, последствия и методы защиты. Научно-практический электронный журнал Аллея Науки. №1(28) 2019.

УДК 323

Чувеева Александра Анатольевна, студент, Комсомольский-на-Амуре государственный университет
Chuveeva Aleksandra Anatolievna, student, Komsomolsk-na-Amure State University
Мусалитина Евгения Александровна, доцент, Комсомольский-на-Амуре государственный университет
Musalitina Evgenia Aleksandrovna, Associate professor, Komsomolsk-na-Amure State University

ЯВЛЕНИЕ ТЕЛЕФОННОГО ТЕРРОРИЗМА В СФЕРЕ ОБРАЗОВАНИЯ

THE PHENOMENON OF TELEPHONE TERRORISM IN THE SPHERE OF EDUCATION

Аннотация. Терроризм – это стратегия и намерение преступника организованно применять насилие или угрожать насилием в отношении безоружных людей и достигать определенной политической цели путем запугивания определенного объекта. Общей формой проявления являются акты насилия, которые целенаправленно создают панику, преднамеренно нападают на гражданских лица или игнорируют их безопасность в религиозных, политических или идеологических целях. Такие действия, как правило, спровоцированы неправительственными организациями. В статье рассматривается явление телефонного терроризма в образовательной сфере, его частота и последствия.
Abstract. Terrorism is the strategy and intention of a criminal to use violence or threaten violence against defenseless people in an organized manner and to achieve a certain political goal by frightening a certain object. A common form of manifestation is acts of violence that intentionally create panic, deliberately attack civilians or ignore their safety for religious, political or ideological purposes. Such actions are usually provoked by non-governmental organizations. The article examines the phenomenon of telephone terrorism in the educational sphere, its frequency and consequences.
Ключевые слова: телефонный терроризм, заведомо ложное сообщение об акте терроризма, «минирование» детских садов, школ и университетов.
Key words: "telephone terrorism", deliberately false report of a terrorism act, "mining" kindergartens, schools and universities.

Терроризм – это использование насилия, шантажа или угроз против правительств, общественности или отдельных лиц. Это одно из самых опасных явлений в обществе, так как подвергает его психологическому стрессовому воздействию, вызывает страх и как следствие всего этого - массовую панику. Посредством этого происходят

попытки донести послание террористов и выдвинуть требования. Одним из самых распространенных видов терроризма в мире и, особенно, в России является так называемый «телефонный терроризм». Под этим термином понимается «психологическое воздействие, вызывающее массовую панику, практически срывающее работу учреждений и организаций на весь рабочий день, в любом проявлении выполняя свою социально разрушительную задачу» [2]. В России рост данной проблемы наблюдается с девяностых годов и по сей день не утрачивает своей актуальности.

Данное явление затрагивает различные сферы общественной жизни, нанося ущерб не только психологическому состоянию общества, но и деятельности различных организаций страны, срывает процесс обучения, а также работу банков, крупных торговых центров и магазинов. Для передачи заведомо ложного сообщения об акте терроризма по телефону характерны три этапа совершения этого преступления:

1) подготовка;

2) непосредственная передача сообщения;

3) сокрытие преступления.

К подготовке к преступлению также относится выбор адресата, которому будет передано сообщение.

Исходя из анализа уголовных дел, наиболее распространенными объектами «минирования» считаются:

а) учебные заведения – 34%;

б) жилые здания и помещения – 20,8%;

в) лечебные учреждения – 13,2%;

в) железнодорожные, автобусные вокзалы, аэропорт,

метро – 11,2% [5].

Масштабная волна ложных угроз взрыва по всей России возникла осенью 2017 года, когда в общей сложности 2,6 миллиона человек были эвакуированы из 75 регионов по всей стране. Поскольку террористы используют анонимные IP-адреса и различные технологии, чтобы скрыть свое истинное местоположение для ложного сообщения о минировании, полиции трудно их вычислить.

Несмотря на то, что волна таких сообщений не привела ни к каким жертвам, она оказала влияние и поколебала психологию российского народа. Последние результаты опроса Российского фонда изучения общественного мнения показывают, что, хотя более половины опрошенных не считают, что “телефонный терроризм” представляет угрозу для их жизни, 43% из них знают о “телефонном терроризме" и 28% слышали о нем. С недавних пор звонки от неизвестных с угрозами минирования, а также с «предупреждениями» о наличии в зданиях бомб начали терроризировать детские сады, школы и университеты страны особенно активно. С каждым годом частота звонков лишь учащается.

В связи с этим многие исследователи обозначили эту проблему в своих работах. Среди них есть исследующие телефонный терроризм и меры по его пресечению (Ю. И. Жарикова, А. В. Лосяков) [4], рассматривающие это явление и состав данного преступления (А. М. Жиляева) [3] и анализирующие его на примере двух стран: России и США (М. В. Евгеньева) [1]. 19 декабря 2019 года в Хабаровском крае было эвакуировано более 40 детских садов после акта «телефонного терроризма». В начале января 2022 года прошла самая масштабная волна минирований. 20 января сообщения о минировании поступили в школы Тюмени, Челябинска, Магадана, Барнаула и Сахалина. Занятия прерывались почти во всех средних школах страны. 14 октября 2022 года из-за поступивших писем об угрозе безопасности были прерваны занятия в таких крупных вузах Хабаровска, как ТОГУ и ДВЮИ МВД РФ.

Вопреки тому, что в России заведомо ложное сообщение об акте терроризма уголовно наказуемо (статья 207 Уголовного кодекса Российской Федерации), случаи такого рода преступлений продолжают увеличиваться и по сей день. Более того были предприняты необходимые меры государственного реагирования – ужесточение статьи 207 УК РФ.

В заключение, хотелось бы отметить, что пока нет способа, который бы гарантировал поимку террористов, а значит массовые эвакуации продолжатся и будут подрывать работу в различных общественных сферах. Не реагировать на это невозможно, так как однажды среди потока ложных сообщений может оказаться одно правдивое и это будет стоить невинным людям жизни.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Евгеньева, М. В. Институт телефонного терроризма на примере Российской Федерации и Соединенных штатов Америки / М. В. Евгеньева // Пермский период : Сборник материалов V Международного научно-спортивного фестиваля курсантов и студентов, Пермь, 14–19 мая 2018 года. – Пермь: Пермский институт Федеральной службы исполнения наказаний, 2018. – С. 159-161.

2 Жарикова, Ю. И. Проблема «телефонного терроризма» в России и меры по его предупреждению / Ю. И. Жарикова, Ю. В. Болтенкова // Наука молодых - будущее России : сборник научных статей 6-й Международной научной конференции перспективных разработок молодых ученых, Курск, 09–10 декабря 2021 года. Том 2. – Курск: Юго-Западный государственный университет, 2021. – С. 242-246. – EDN QQUVPY.

3 Жиляева, А. М. Телефонный терроризм / А. М. Жиляева // Форум молодых ученых. – 2019. – № 1-1(29). – С. 1262-1265.

4 Лосяков, А. В. Проблема "телефонного терроризма" в современной России и меры по его предупреждению / А. В. Лосяков // Ученые труды Российской академии адвокатуры и нотариата. – 2020. – № 4(47). – С. 67-70.

5 Михалева, Д. А. Криминалистическая характеристика преступлений, связанных с заведомо ложным сообщением об акте терроризма / Д. А. Михалева // Бизнес в законе. – 2008. – № 1. – С. 279-281. – EDN JWSJGP.

6 Хаматова, С. Х. Заведомо ложные сообщения об акте терроризма: проблемы предупреждения и противодействия / С. Х. Хаматова // VII Международный молодежный юридический форум "Экстремизму – отпор" : Сборник научных статей материалов Международной научно-практической конференции, Владикавказ, 22–24 ноября 2018 года / Под редакцией Кокоевой Л.Т., Цалиева А.М.. – Владикавказ: Северо-Кавказский горно-металлургический институт (государственный технологический университет), 2021. – С. 142-151.

УДК 343.712.3

Шаповалов Алексей Артемович, студент, Комсомольский-на-Амуре государственный университет
Shapovalov Alexey Artemovich, student of Komsomolsk-na-Amure State University
Кортун Екатерина Александровна, старший преподаватель Комсомольский-на-Амуре государственный университет
Kortun Ekaterina Aleksandrovna, senior lecturer of Komsomolsk-na-Amure State University

ПОХИЩЕНИЕ КАК ВИД ТЕРРОРИЗМА

KIDNAPPING AS A TYPE OF TERRORISM

Аннотация. Цель исследования – раскрытие темы похищения, в чем его суть. В данной статье акцентируется внимание на психологии поведения заложника и похитителя. Рассказывается о мерах предосторожности нахождения в подобной ситуации. Проявление

Стокгольмского синдрома, его признаки, опасности, которые он несет и меры по восстановлению ментального здоровья.
Abstract. The purpose of the study is to reveal the topic of abduction, what is its essence. This article focuses on the psychology of hostage and abductor behavior. It tells about the precautions of being in a similar situation. The manifestation of Stockholm syndrome, its signs, the dangers it carries and measures to restore mental health.
Ключевые слова: похищение, удержание в заложниках, Стокгольмский синдром, опасность, секта.
Key words: abduction, hostage-taking, Stockholm syndrome, danger, sect.

Непосредственно терроризм воплощается в виде террористического акта - совершения преступления террористического характера, являющегося завершающим этапом террористической операции. Существуют не колько видов терроризма. В данной статьерассмотрим такой вид, как похищение.

Похищение – это противоправное действие по отношению к человеку с изъятием его из социальной среды и удержанием против его воли в ином месте.

Как правило, это происходит из корыстных целей, чтобы получить выкуп, либо для выполнения требований похитителей.

Меры предосторожности

Попытка убежать или вырваться будет оценена террористами агрессивно. Следует успокоиться и ожидать освобождения.

1. Приготовиться к долгому ожиданию. Специалистам необходимо время, для вашего освобождения.

2. Постараться мысленно отвлечься от происходящего: вспомнить стихи, любимые книги, фильмы, мультфильмы, решить задачи в голове.

3. Стараться не раздражать террористов: не кричать, не плакать, не сердиться.

4. Не конфликтовать с террористами, делать все, что они говорят. Важно помнить: это вынужденная мера, вы спасаете себя и других.

5. Помнить, что возможно, придется долго обходиться без воды и еды – стоит беречь силы.

6. Если в помещении душно, стараться меньше двигаться, чтобы сберечь кислород.

7. Если воздуха достаточно и по зданию запрещено передвигаться, делайте простые физические упражнения – напрягайте и расслабляйте мышцы рук, ног и спины. Не делайте резких движений.

Гай Юлий Цезарь

Примечание из истории: Великий император Римской империи сам стал жертвой похищения. В 76 году до н. э. он отправился на остров Родос, где хотел обучиться ораторскому мастерству у Аполлония Молона - у известного оратора. По пути на остров на корабль Цезаря напали пираты. Они поняли, что в их руках оказался богатый римский патриций и запросили 20 талантов серебра (около 620 кг). Бандиты ожидали, что пленный начнет торговаться за свою жизнь и будет сбивать цену. Однако в ответ на это, Цезарь только рассмеялся и сказал, что цена его оскорбляет. Он потребовал, чтобы выкуп повысили до 50 талантов серебра (около 1,5 тонн). После этого Цезарь отправил своих подчиненных в разные города, чтобы собрать нужную сумму. 38 дней его удерживали на небольшом острове Фармакусса, и все эти дни он делал все, что хотел.

Как только люди Цезаря отдали выкуп, Цезаря мгновенно освободили.

Но сразу после своего освобождения он собрал флот кораблей, и отправился на битву с пиратами, которые рискнули его похитить.

Стокгольмский Синдром

Стокгольмский Синдром – является проявлением симпатии жертвы к своему похитителю.

Данный термин появился в 1973 году, когда во время ограбления на один из шведских банков захваченные работники внезапно прониклись симпатией к грабителям и сами начали им помогать.

Общие признаки:

Жертва импонирует к агрессору, и вместе с тем неприязнь к тем, кто хочет помочь ей выйти из этих отношений. Это могут быть правоохранительные органы, которые желают помочь привлечь обидчика к ответственности, или близкий человек, который акцентирует внимание на деструктивное поведение партнера и предлагает прекратить продолжать отношения с ним.

Жертва начинает оправдывать его действия, видеть в своем мучителе нравственность, искать достоинства.

Механизм стокгольмского синдрома кроется в инстинкте самосохранения и держится на надежде жертвы, что если она будет проявлять послушание, то получит снисхождение от агрессора.

Опасность синдрома

Опасность как раз таки зависит от самого заложника, так как он действует против своих интересов, например, в предотвращении его освобождения. Известны такие случаи, когда во время спасательной операции заложники предупреждали захватчиков о появлении спецназа и даже прикрывали террориста своим телом. Однако случалось и так, что террорист притворялся заложником и сами заложники умалчивали об этом. Как правило, стокгольмский синдром проявляется после первого убитого заложника.

Лечение

Для лечения стокгольмского синдрома в настоящее время используются общепринятые методы работы с жертвами насилия. Здесь хорошо справляются когнитивная психотерапия, разного рода адаптированные способы работы с горем, с чувством вины и нормализации пройденного опыта.

Секта, как пример стокгольмского синдрома

Секта Бога Кузи

Люди уже состоящие на службе секты сами вербовали знакомых в свои ряды. Самым эффектным методом считалось объявление на приеме на работу в павильон. Проводили оценку соискателей, чтобы понять можно ли на этого человека влиять. Также на выставках адепты искали людей в крайне угнетенном состоянии, и вербовали их в свои ряды. Примером этого является женщина, пришедшая заказать панихиду по умершему мужу. Злоумышленники понимали состояние женщины и быстро ее «обрабатывали» - рассказывали о не ком человеке – чудотворце.

Людей, которых вырвали из семей, секта внушала им что их родня представляет демонов, которые не позволяют им обрести собственного счастья.

Попов, он же Бог Кузя, держал последователей в достаточно жёсткой дисциплине, им внушалась вина в собственных болезнях. Он также склонял всех своих последователей на развод с любимыми, призывал прекратить отношения с родителями, а детей отдать на воспитание родственникам или в интернат. Согласно Попову, родственников нужно заставлять переписывать на себя имущество и обманывать всеми доступными способами, в том числе и уничтожать физически, поскольку это «демоны, которые должны гореть в аду».

Развитие правовой базы уголовной ответственности за данные виды преступлений позволит изменить в положительную сторону криминогенную ситуацию в стране. Уважение к человеку, признание его достоинства и самоценности должны стать главной предпосылкой успешного развития общества.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Смертин А. Н. Экстремизм и терроризм: некоторые подходы к определению понятий // Вестник Санкт-Петербургского университета МВД России. 2009. №1. URL: https://cyberleninka.ru/article/n/ekstremizm-i-terrorizm-nekotorye-podhody-k-opredeleniyu-ponyatiy (дата обращения: 18.10.2022).

2. Коффман, Б. И., Миронов, С. Н., Сафаров, А. А., Сафиуллин, Н. Х. Терроризм: история и современность / Б. И. Коффман [и др.]. - Казань : Тейс, 2002.

3. "Учение" Бога Кузи: как любитель Шекспира основал прибыльную секту [Электронный ресурс] РИА Новости. – URL: https://ria.ru/20180716/1524552378.html (дата обращения: 17.10.2022).

4. Цезарь в плену [Электронный ресурс] WAS – Журнал історій, що вражають. – URL: https://was.media/microformats/cezar-v-plenu/ (дата обращения: 18.10.2022).

5. Что такое стокгольмский синдром и как его лечат [Электронный ресурс] Статьи - медицинский блог Подольска. – URL: https://www.gdp1podolsk.ru/blog/chto-takoe-stokgolmskij-sindrom-i-kak-ego-lechat/ (дата обращения: 19.10.2022).

УДК 1234.56

Шинкорук Милена Денисовна, студент, Комсомольский-на-Амуре государственный университет
Shinkoruk Milena Denisovna, student, Komsomolsk-on-Amur State University
Шинкорук Марина Владимировна, кандидат педагогических наук, доцент, доцент кафедры «Педагогика, психология и социальная работа», Комсомольский-на-Амуре государственный университет
Shinkoruk Marina Vladimirovna, Candidate of Pedagogical Sciences, Associate Professor, Associate Professor of Pedagogy, Psychology and Social Work Department, Komsomolsk-on-Amur State University

ФЕНОМЕНОЛОГИЯ БЕЗОПАСНОСТИ В СУБЪЕКТИВНЫХ ПРЕДСТАВЛЕНИЯХ РЕСПОНДЕНТОВ

PHENOMENOLOGY OF SAFETY IN THE SUBJECTIVE REPRESENTATIONS OF RESPONDENTS

Аннотация. В статье предпринята попытка исследования феноменологии безопасности через анализ результатов опроса респондентов о безопасности; представлены результаты анализ выявленных субъективных представлений респондентов о безопасности; выделены ключевые феномены в субъективных описаниях безопасности; определены аспекты безопасности на основе феноменологического анализа ответов респондентов.
Abstract. The article attempts to study the phenomenology of security through the analysis of the results of a survey of respondents about security; the results of the analysis of the identified subjective perceptions of respondents about safety are presented; key phenomena in sub-

jective descriptions of safety are highlighted; safety aspects are defined on the basis of the phenomenological analysis of respondents' answers.
Ключевые слова: безопасность, феноменология, субъективные представления, феномены безопасности, аспекты безопасности
Key words: security, phenomenology, subjective ideas, security phenomena, security aspects

Толковый словарь определяет слово «безопасность» как состояние, при котором «не угрожает опасность, есть защита от опасности» [9]. В этом значении подчеркивается смысл безопасности как свойства субъекта (человека) или объекта (предмета, вещи, механизма, информации) быть в условиях отсутствия опасности или иметь потенциал её отражения. Данное значение получило своё развитие в дифференциации и выделении множества плоскостей исходного понятия.

Сегодня, анализируя опыт исследования безопасности, можно выделить такие контексты её рассмотрения, как: физический [6], психический [3]; психологический [8]; национальный[4; 5]; государственный[4]; средовый [8]; гендернный [2; 10]; профессиональный[8]; продовольственный[1]; информационный [7]; транспортный[4]; и другие.

В рамках данного исследователя нас интересовал личностный контекст безопасности, с целью исследования которого мы попросили респондентов дать своё понимание слова «безопасность». В исследовании приняли участие 110 человек. Группу респондентов составили жители Хабаровского края - представители различных профессиональных сообществ, студенты и пенсионеры. Возраст респондентов: от 18 до 65 лет.

Анализ ответов позволил нам выделить основные феномены, вокруг которых строится понимание безопасности у опрашиваемых. Среди таких феноменов мы выделили:

1) Чувства: безопасность раскрывается с использованием категорий, обозначающих эмоции и чувства: страх, счастье, сохранность, тревога, и т.п.;
2) Действие: безопасность характеризуется возможностью предпринимать действия, быть активным;
3) Состояние: для определения безопасности используются слова, характеризующие психические состояния - опорность, сохранность, уверенность, спокойствие и т.п.;
4) Окружающая среда: под безопасностью подразумевается определенное состояние окружающей среды, условия, созданные извне: гарантии права, мир на Земле, устойчивость экономики и т.д.;
5) Знание: безопасность трактуется как наличие у субъекта определенных представлений о себе и мире;
6) Место: безопасность связывается с присутствием в определенном месте, определенных физических обстоятельствах;
7) Объекты: безопасность раскрывается через обладание чем-то;
8) Взаимодействие: безопасность представляется через описание характера взаимодействия с другими и с миром в целом.

Выделенные в описании субъективных представлений респондентов феномены могут быть рассмотрены в качестве аспектов безопасности личности. Ниже, в таблице представлено соотношение выделенных нами аспектов понимания безопасности личности и ответов респондентов.

Таким образом, осуществлённое исследование позволило нам взглянуть на личностную безопасность как многоаспектное понятие, раскрывающееся через феномены, описывающие чувства, состояния, действия, знания, обладание, место, общение. Опыт этого подхода может быть использован как в расширении представлений о личностной безопасности, так и в разработке способов поддержки безопасности личности в практике помогающих профессий.

Таблица 1 – Соотношение аспектов описания безопасности личности и ответов респондентов

Аспекты описания безопасности	Ответы респондентов
Безопасность как чувство	«отсутствие страха», «спокойствие», «счастье», «уверенность в завтрашнем дне», «чувство полной сохранности», «не бояться за свою жизнь», «отсутствие тревоги», «есть ЗАВТРА, нет страха за свою жизнь и свободу и за свою семью»,
Безопасность как возможность действовать	«спокойно ходить по улицам, быть рядом со своей семьей», «возможность реализации своих жизненных целей, мыслей», «возможность планировать»
Безопасность как внутреннее состояние	«защищенность, комфорт», «сохранность жизни и здоровья», «состояние уверенности, что завтра будет», «защищённость психики», «целостность личности», «защита душевного здоровья и духовности»
Безопасность как ответ окружающей среды	«защита и опора из вне»,» нет опасности, исходящей от других», «гарантии права», «Мир на Земле», «отсутствие угрозы», «устойчивость экономики», «отсутствие угрозы текущему здоровью, свободе, благополучию себя и близких», «когда мое государство меня охраняет»
Безопасность как знание о себе и мире	«знание, что есть на кого положиться», «знание, что мне ничего не угрожает»
Безопасность как место	«это то место, где находятся мои близкие люди», «там, где я чувствую себя уверенно и понимаю, что никто меня не тронет»
Безопасность как обладание объектами	«когда много денег»
Безопасность как характер взаимодействия с миром	«спокойное, мирное взаимодействие с окружающим миром», «создание условий, в которых возможно самовыражение, ощущение комфорта и защищенности»

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Katusov D.N., Shatov A.A. Продовольственная безопасность – основа национальной безопасности страны // Сборник докладов X Международной научно-практической конференции молодых ученых. 2015. С. 203-207.

2. Виноградова С.М., Рущин Д.А. Гендерные проблемы социальной и личностной безопасности // Вестник Ленинградского государственного университета им. А.С. Пушкина. 2015. Т. 2. № 3. С. 170-180.

3. Гайдамашко И.В., Жемерикина Ю.И., Пугачева Е.В. Психическая устойчивость как феномен безопасности личности // Актуальные направления научных исследований: от теории к практике. 2015. № 4 (6). С. 124-127.

4. Дюмина А.А. К вопросу о соотношении понятий "Безопасность", "Национальная безопасность", "Транспортная безопасность" // В сборнике: Наука и образование: отечественный и зарубежный опыт. Шестнадцатая международная научно-практическая конференция. 2018. С. 260-264.

5. Запыленова Д.А. Безопасность личности как фактор национальной безопасности // В сборнике: Актуальные направления развития города Москвы и его связей: Современные тренды и тенденции. Сборник научных статей. 2018. С. 19-23.

6. Капуста В.А., Младова Т.А. Оценка риска для здоровья населения от факторов среды // В книге: Научно-техническое творчество аспирантов и студентов: материалы 46-й научно-технической конференции студентов и аспирантов. Комсомольский-на-Амуре государственный технический университет; Э.А. Дмитриев (отв. ред.). 2016. С. 247-249.

7. Лызь Н.А., Веселов Г.Е., Лызь А.Е. Информационно-психологическая безопасность в системах безопасности человека и информационной безопасности государства // Технические науки. 2014. № 8 (157). С. 58-66.
8. Мартыненко К.А., Фадеев В.И. Психологическая безопасность образовательной среды как определяющий компонент сохранения психического здоровья и позитивного развития его участников // NovaInfo.Ru. 2016. Т. 3. № 44. С. 364-367.
9. Неведомский А.Д., Муллер Н.В. Действия персонала во время чрезвычайных ситуаций // В сборнике: Молодежь и наука: актуальные проблемы фундаментальных и прикладных исследований. Материалы V Всероссийской национальной научной конференции молодых учёных. Комсомольск-на-Амуре, 2022. С. 317-318.
10. Толковый словарь Ожегова // Электронный ресурс. – URL: https://slovarozhegova.ru/
11. Шконда Д.Н., Муллер Н.В. Особенности безопасности труда женщин // В сборнике: Молодежь и наука: актуальные проблемы фундаментальных и прикладных исследований. Материалы V Всероссийской национальной научной конференции молодых учёных. Комсомольск-на-Амуре, 2022. С. 355-356.

УДК 81-1/-9

Шушарин Никита Станиславович, студент, Комсомольский-на-Амуре государственный университет
Shusharin Nikita Stanislavovich, student, Komsomolsk-on-Amur State University
Шушарина Галина Алексеевна, кандидат филологических наук, доцент, Комсомольский-на-Амуре государственный университет
Shusharina Galina Alexeyevna, PhD in Philology, Associate Professor, Komsomolsk-on-Amur State University

ПОНЯТИЙНЫЕ КОНЦЕПТУАЛЬНЫЕ ПРИЗНАКИ КОНЦЕПТА «*THREAT*»

CONCEPTUAL FEATURES OF THE CONCEPT «*THREAT*»

Аннотация. Исследование посвящено выявлению понятийных признаков концепта *threat* в английском языке на основе лексикографических толкований слова-имени концепта и анализа его словообразовательного потенциала. Исследование осуществляется в рамках когнитивно-дискурсивной парадигмы, доминирующей в контексте полипарагматизма современной лингвистической науки.
Abstract. The study is devoted to identifying the conceptual features of the concept *threat* in English based on lexicographic interpretations of the word-name of the concept and the analysis of its derivational potential. The study is carried out within the framework of the cognitive-discursive paradigm, which dominates in the context of the polyparagmatism of modern linguistic science.
Ключевые слова: концепт, понятийные концептуальные признаки, угроза.
Key words: concept, conceptual conceptual features, threat.

Концепт *threat* относится к базовым концептам, поскольку ежедневно и повсеместно современный человек сталкивается с различными угрозами от бытового типа (угроза пожара в квартире, угроза дорожно-транспортных происшествий, угроза потери работы и т.д.) до глобальных угроз, а именно, угрозы потери национальной идентичности, угрозы террористических актов, вооруженных конфликтов, применения ядерного оружия и пр.

Исследование посвящено выявлению понятийных признаков концепта *threat* в английском языке и осуществляется в рамках когнитивно-дискурсивной парадигмы, доминирующей в контексте полипарагматизма современной лингвистической науки.

В настоящее время в науке представлено значительно количество работ, повещённых изучению тех или иных концептов [5; 6]. Сам термин «концепт» получил и продолжает получать значительное количество интерпретаций. В настоящем исследовании под концептом мы понимаем «единицу коллективного знания или сознания, имеющую языковое выражение и отмеченную этнокультурной спецификой» [2, с. 51].

Изучение представленных в современном научном знании статей и тезисов демонстрирует, что концепт как ментальное образование обладает сложной структурой. Согласимся с позицией отечественного лингвиста Н.Н. Болдырева, который выделяет в структуре концепта определённые характеристики или концептуальные признаки [1, с. 29], которые могут быть выражены эксплицитно и отражены в дефинициях лексикографических источников и определяются как понятийные концептуальные признаки [4; 7].

Проведем вычленение понятийных концептуальных признаков концепта *threat* в общенациональном английском языке с использованием данных лексикографических источников на английском языке. Выделение сем, присутствующих в дефиниции слова *threat*, является для нас основным при определении понятийных признаков одноименного концепта. При этом нас интересует весь массив значений.

В толковых словарях современного английского языка Oxford Advanced Learner's Dictionary, Cambridge Dictionary и др. у слова *threat* выделяется 4 значения, которые могут быть сведены к следующим [8; 9; 10]:

Threat n. 1. A statement in which you tell somebody that you will punish or harm them, especially if they do not do what you want. 2. The possibility of trouble, danger or disaster, something bad. 3. A person or thing that is likely to cause trouble, danger, damage, etc. 4. a situation or an activity that could cause harm or danger. На основе приведенных словарных значений слова мы определили понятийные концептуальные признаки, которые обозначают денотаты реальной действительности и раскрывают содержание концепта *threat*:

1. Утверждение, в котором звучит возможность наказания или причинения вреда в случае невыполнения некоторых действий.
2. Возможность неприятностей, опасности или катастрофы, чего-то нехорошего.
3. Человек или предмет / явление, которые могут причинить неприятности, опасность, ущерб и т. д.
4. Ситуация или действие, которые могут причинить вред или опасность.

Выделенные семы исследуемого имени концепта рассеиваются по его дериватам, фиксируя «кванты информации» [3, с. 23], позволяющие наглядно представить результат предметно-познавательной, интерпретационной деятельности человека. В рамках словообразовательного гнезда с исходным существительным *threat* образовались следующие производные слова, принадлежащие к различным частям речи: threaten, threatening, threateningly. Все производные слова сохранили прямое (прототипическое) значение своего производящего слова.

Таким образом, мы определили понятийные концептуальные признаки концепта *threat* на основе лексикографических толкований слова-имени концепта и анализа его словообразовательного потенциала.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Болдырев Н.Н. Когнитивная семантика. – Тамбов. Изд-во Тамбовского ун-та, 2001. 123 с.

2. Воркачев С.Г. Счастье как лингвокультурологический концепт. – М.: Гнозис, 2004. – 236 с.

3. Кубрякова Е.С. Возвращаясь к определению знака. Памяти Р. Якобсона // Вопросы языкознания. 1993. №4. С.23-31.
4. Лебедько М.Г. Время как когнитивная доминанта культуры. Сопоставление американской и русской темпоральных концептосфер. Монография. – Владивосток. Изд-во Дальневосточного университета, 2002. – 240 с.
5. Малышева Н.В. Концепты "устойчивость" и "sustainability" в отечественном и зарубежном лингвокультурном пространстве // Ученые записки Комсомольского-на-Амуре государственного технического университета. 2022. № 4 (60). С. 38-43.
6. Навицкайте Э. А. Лингвистические средства создания образа исламской угрозы в англоязычном медиадискурсе. Дисс… к.филол.н. Иркутск, 2012. URL: https://www.dissercat.com/content/lingvisticheskie-sredstva-sozdaniya-obraza-islamskoi-ugrozy-v-angloyazychnom-mediadiskurse/read
7. Пименова М.В. Концепты внутреннего мира. Дисс… доктора филол.наук. – СПб, 2001.
8. Cambridge Dictionary. URL: https://dictionary.cambridge.org
9. Macmillan Dictionary. URL: https://www.macmillandictionary.com/dictionary
10. Oxford Advanced Learner's Dictionary. URL: https://www.oxfordlearnersdictionaries.com/definition/english

УДК 323

Шугай Анна Васильевна, студентка Комсомольского-на-Амуре государственного университет
Shugai Anna Vasilyevna, student at Komsomolsk-on-Amur State University
Шушарина Галина Алексеевна, кандидат филологических наук, доцент, Комсомольский-на-Амуре государственный университет
Shusharina Galina Alexeyevna, PhD in Philology, Associate Professor, Komsomolsk-on-Amur State University

НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ В ЯПОНИИ

NATIONAL SECURITY IN JAPAN

Аннотация. Статья посвящена анализу внешней политики правительства С. Абэ в сфере обеспечения национальных интересов страны и основных положений принятой Стратегии национальной безопасности Японии В современном мире ни одна страна не может поддерживать свой собственный мир и безопасность в одиночку. Япония, включая ее Силы самообороны, в максимально возможной степени вносит свой вклад в усилия по поддержанию и восстановлению международного мира и безопасности, например в рамках миротворческих операций ООН.
Abstract. The article analyzes the foreign policy of the Abe government in securing the country's national interests and the main provisions of Japan's National Security Strategy In today's world, no country can maintain its own peace and security on its own. Japan, including its Self-Defense Forces, contributes as much as possible to efforts to maintain and restore international peace and security, for example as part of UN peacekeeping operations.
Ключевые слова: Япония, Абэ Синдзо, внешняя политика, стратегия национальной безопасности.
Key words: Japan, Abe Shinzo, foreign policy, national security strategy.

Агентство обороны Японии является юридическим лицом, принадлежащим к базе данных ООН. Агенство было официально преобразовано в министерство в тот же день, когда Агентство обороны Японии представило созданный правительством законопроект, разрешающий внесение поправок в конституцию.

Премьер-министр Японии Абэ заявил, что бюджет вооруженных сил Японии не должен сокращаться. Он начал работать над выполнением своих предвыборных обещаний после избрания в ноябре 2012 года. Оба финансовых года с 2013 по 2014 год показали увеличение военного бюджета по сравнению с 2012 годом. Стокгольмский международный институт исследования проблем мира сообщает, что военный бюджет Японии вырос на 2,2% по сравнению с предыдущим годом.

В течение многих лет у Японии не было прочной основы для своей политики безопасности. В 1967 году японский парламент принял Три принципа, которые регламентировали экспорт оружия в страны, находящиеся под властью коммунистов; и поставлять оружие в страны, не подпадающие под запрет ООН. В 1976 г. Токио ввел 35-летний запрет на экспорт товаров военного назначения. Однако в 1976 г. он был распространен на все без исключения страны, не оставив места для военного экспорта. Этот запрет распространяется на все страны, участвующие в активных боевых действиях. Японское правительство рассматривало возможность создания оружия следующего поколения, когда принимало решение о производстве истребителя В-35. Они приняли это важное решение после консультации с японским патентным ведомством, которое является государственным ведомством. Позже они передумали в связи с необходимостью страны создавать и производить оружие в сотрудничестве с другими странами, включая Австралию и Южную Корею.

В октябре 2013 года премьер-министр Японии Синдзо Абэ создал неофициальную группу экспертов по безопасности. В задачу специального комитета входило рассмотрение того, как Япония реализует принципы анализа экспорта вооружений.

Чтобы существовать, Совет национальной безопасности Японии должен быть одобрен японским парламентом. Закон о нем был принят 27 ноября 2013 года. Совет национальной безопасности Японии подчиняется премьер-министру Японии. Закон о Совете национальной безопасности был введен в действие в январе 2014 года. В результате в том же месяце секретариат канцелярии премьер-министра стал Агентством национальной безопасности.

После тесного сотрудничества с США в 2013 году Совет сыграл важную роль в разработке многих важных аспектов политики национальной безопасности. Это инструкции по совершенствованию вооруженных сил страны, а также пятилетний план военной обороны. Для защиты своих целей и интересов в сфере международных отношений японское правительство создало первый документ о стратегии национальной безопасности. В документе изложены военные, дипломатические, экономические и другие меры страны, призванные защитить Японию от угроз и потрясений.

Таким образом, политика национальной безопасности Японии фокусируется на решении ряда проблем, которые предстают перед государством в целом мире. С другой стороны, премьер министру легко удается проводить реваншистскую политику, которую соседи по АТР не поддерживают.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Бунин В.Н. Современное состояние оборонного потенциала Японии. – М.: Ин-т Дал. Востока, 2019. – 152 с.

2. Бунин В. Н. Японско-американский союз безопасности: История и современность: (К 50-летию со дня основания). – М.: ИДВ РАН, 2017. – 331 с.

3. Ковалев С. И. Силы самообороны Японии – М.: Международные отношения, 2018. – 335 с.

4. Панов А. Н. Внешнеполитические приоритеты премьер-министра Японии Абэ Синдзо / А. Н. Панов // Япония 2017. Ежегодник / А. Н. Панов. – М.: АИРО-XX1, 2017. – С. 7-42.

5. Japan Security Watch. The Japanese Election, the LDP's Manifesto, and Defense: [Электронный ресурс] / - Электрон. дан. – Режим доступа: http://jsw.newpacificinstitute.org/?p=10614 - Загл. с экрана.

УДК 327

Щеголев Станислав Максимович, студент Комсомольского-на-Амуре государственного университета
Shchegolev Stanislav Maksimovich, student at Komsomolsk-on-Amur State University
Непочатова Валерия Михайловна, старший преподаватель Комсомольский-на-Амуре государственный университет
Nepochatova Valeria Mikhailovna, senior lecturer of Komsomolsk-na-Amure State

УГРОЗЫ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ, ВЫЗВАННЫЕ ТЕРРОРИЗМОМ

THREATS TO INTERNATIONAL PEACE AND SECURITY CAUSED BY TERRORIST ACTS

Аннотация. В данной статье рассматривается проблема терроризма как угрозы номер 1 для международной безопасности и способы защиты. Объектом моего высказывания является терроризм как угроза международной безопасности. Предмет - условия возникновения терроризма и угрозы, которые он несет. Цель - рассмотреть причины возникновения терроризма и проблемы борьбы с ним. Для достижения поставленной цели необходимо рассмотреть следующие задачи: - изучить понятие терроризма и его причины; - выявить проблемы борьбы с терроризмом в России и мире; - рассмотреть способы защиты от терроризма как угрозы международной безопасности государств и человечества.
Abstract. This article deals with terrorism as the number 1 threat to international security and how to defend it. The object of my statement is terrorism as a threat to international security. The subject is the conditions under which terrorism emerges and the threats it poses. The aim is to consider the causes of terrorism and the problems of combating it. In order to achieve the goal, the following tasks need to be considered: - examine the concept of terrorism and its causes;
- identify the problems of combating terrorism in Russia and the world; - consider ways of defending against terrorism as a threat to the international security of states and humanity
Ключевые слова: терроризм, виды терроризма, международная безопасность, глобализация, индекс глобального терроризма.
Key words**:** terrorism, the types of terrorism, international security, globalization, global terrorism index.

Hijackings of planes, buildings, explosions in the subway, on the street, the death of people - this is no longer footage from a cool action movie - this is the reality of our modern life. And the words "terrorist", "terrorist", "terrorism" has long been included in our lexicon.

Today, when the international situation can hardly be called stable, the topic of international terrorism is very relevant. This is the "number 1" threat to the entire system of international security and from a regional problem it has turned into a global problem that knows no borders. It is noteworthy that terrorist attacks, with few exceptions, are not directed against armed forces or military installations, but against the civilian population and the most vulnerable pieces of infrastructure. The question of why innocent people suffer, who are in no way connected with ideological warfare, much less political questions, remains rhetorical and unanswered. We all remember the explosions of houses in Moscow, Volgodonsk, the hostage-taking in Beslan, and the recent explosion of a strategic bridge in Crimea. Therefore, the problem of combating terrorism in Russia has become very relevant both inside the country and outside its borders.

According to statistics for 2021, 65 terrorist crimes were prevented in Russia, 23 bandits were neutralized, 312 militants and 821 accomplices were detained. The activities of 211 criminal groups were suppressed, 236 illegal workshops for the production and alteration of weapons were liquidated. FSB officers together with law enforcement agencies carry out the

fight against terrorist gangs in Russia, even Roskomnadzor employees take an active part in the fight against terrorism, protecting the information space from propaganda of the ideology of terrorism. They blocked 6.5 thousand and deleted 50 thousand materials containing terrorist propaganda on the Internet. The national anti-terrorist committee coordinates the work of all special services to combat terrorism.

But, despite the work and good results of our special services, the fear of terrorist attacks in Russia among the population remains high.

From the survey it follows that two-thirds of the respondents surveyed, and this is 84% fear that they themselves or their relatives may be victims of a terrorist attack and only 16% exclude this possibility. Therefore, Russia, as one of the largest states in the world, which has taken a place in world politics befitting its potential, has not remained aloof from the problem of combating terrorism within the framework of international security. Our priority is to form a system of ensuring international security that meets the new realities of the modern world. According to the latest relevant data, which were published in March 2022, Russia is on the 44th place in the ranking of countries in terms of terrorism. Its global terrorism index is 4.271.

The Global Terrorism Index is a comprehensive study that measures the level of terrorist activity in countries around the world. It was developed by an international group of experts under the auspices of the Institute of Economics and Peace of the University of Sydney, Australia and measures the level of terrorist activity by four main indicators: the number of terrorist incidents, the number of deaths, the number of victims, the level of material damage. I would like to note that the first place in the ranking is occupied by Afghanistan (9,109), Syria - in fifth place (8, 25), Turkey in 23rd place (5, 651), the United States in 28th place (4,961), the UK - 31st place (4, 77).

All this once again gives us the right to assert that terrorism has become a global threat. The main directions of which are the aggression of terrorist forces on some countries, provoking political and military conflicts between states, creating instability within countries that can lead to civil war, inciting mutual hatred of peoples of different nationalities and beliefs, mass death of people because of terrorist attacks.

So what is terrorism? What is its nature and driving force? Attempts to give a clear definition of terrorism were unsuccessful, since for some terrorism is a crime, for others - the struggle for a "just cause". One thing is for sure – this is the most dangerous form of resolving social and political conflicts, a new non-traditional type of war, manifestations of globalization. This is a complex phenomenon, an identification that should be carried out by three interacting components. The first component is ideology, the second organizational process aimed at the materialization of terrorist ideas and the third is terrorist activity. The ideological component can be called basic. It plays a kind of pivot, forms a terrorist worldview, on the basis of which an organizational component appears, and activity manifests itself in the form of terrorist acts. It is also ideology that makes a person a fanatic. At the same time, it should be noted that terrorism has a wide range of negative properties, such as: a misanthropic essence, cruelty, the division of the world into "us" and "them", the substitution of concepts. We are always dealing with different manifestations of terrorist ideology, which is actively parasitizing. At the same time, in the interests of terrorist organizations, concepts are being replaced, facts are being manipulated, and postulates are being "pulled" out of the general context. Nationalism, separatism, left- and right-wing extremism can be the basis of terrorism. From individual phenomena, it has turned into a systemic problem that threatens the future of entire countries and regions.

Today we see the chaotization of international relations and the intensification of world disorder, which leads to an acute crisis in the system of international security. This has significantly complicated the tasks of forecasting the situation and planning measures to ensure international and national security. At a time when the West is resolutely nominating NATO for the role of a military-power instrument of global politics, on which they are de facto trying to entrust new missions to ensure international peace and security. The initiator of

these changes is Washington, which secretly supports terrorist groups entrenched in Iran, Libya, Syria, etc., which leads to even greater instability in the world. Europe is bogged down in the problems of uncontrolled migration, has also become an important object of international terrorism and is unable to confront new challenges and threats. And against this background, the attempts of Russia and some countries to form a new system of international security that meets modern requirements are not successful because of the US desire for global dominance. Washington's rejection of treaties that form the foundation of international relations (the Treaty on Strategic Missile Defense, Intermediate-Range and Shorter-Range Missiles, Strategic Offensive Weapons) further destabilizes the international situation, which leads to an increase in the scale of activities of terrorist organizations. And so the first reason for the emergence of terrorism is globalization.

The second no less important reason for the emergence of terrorism is the relations between social, national groups and peoples, problems arising as a result of the internal policies of individual states. And here a serious problem is the use of terrorist organizations as an instrument of pressure on their rivals. As an example, I can cite the attempts of individual states to counteract the strengthening of Russia as one of the centers of influence in a multipolar world, to prevent the realization of national interests and to weaken its position in Europe, the Middle East, and Central Asia.

And the third reason that gives rise to terrorism is its financing. Modern terrorism is characterized by sharply increased technical equipment, has powerful human, material and organizational resources. Terrorist organizations are closely intertwined with organizational crime and receive income from drug trafficking, sales of people and weapons.

How can we resist international terrorism! The first, of course, at the state level (controlled migration, the exclusion of the policy of "double standards", raising the standard of living of the population and eradicating unemployment, control over the availability of weapons). The second is the legal framework, starting with the Constitution of the Russian Federation and the Federal Law "On Countering Terrorism", ending with international documents.

In the conditions of international instability, society must face the truth: it is impossible to defeat international terrorism alone for one state, relying only on state structures and forceful methods. Victory over terrorism is possible only together with the coordinated efforts of the special services of all countries, armed forces, political and international public organizations. I would also like to note that an important place among the measures to prevent terrorism belongs to civil control. In the face of terrorist threats, society should remember that no matter how strong the state is, it cannot protect itself from modern threats and terrorism.

In conclusion, I would like to note that, based on the international practice of communication between states, often the conscientious cooperation of states in the field of countering terrorism is only declared, in reality, the actions of a number of states do not contribute to the effective fight against threat No. 1 - terrorism.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Mikhalenko, A. A. NBIKS - technologies and terrorism: new risks and mechanisms of counteraction [Electronic resource]: vykhodnaya qualificationnaya rabota magistra / A.A. Mikhalenko; Russian State Social University; Faculty of Humanities; Department of Political Science and International Relations. – Moscow, 2018. – 104 p. URL: http://biblioclub.ru/index.php?page=book&id=491855

2 Sidnenko, Gennady Fedorovich. Information counteraction to terrorism in the Russian Federation: ideological and content analysis [Text] / G. F. Sidnenko, V. Kh. Akhmedov // Mir obrazovanie - obrazovanie v mir. – 2015. – № 3 (59). – S. 101-110.

3 Tamaev, R. S. Extremism i natsional'naya zabeda [Elektronnyi resurs]: pravozhnye problemy : monografiya / R.S. Tamaev. – Moscow: UNITY-DANA: Law and Law, 2015. – 263 p. URL: http://biblioclub.ru/index.php?page=book&id=446573

4 Criminal-legal counteraction to terrorism and extremism [Electronic resource]: uchebnoe posobie /; sost. R. M. Uzdenov ; Ministry of Education and Science of the Russian

Federation; Federal State Autonomous Educational Institution of Higher Education "North Caucasus Federal University". – Stavropol': NKFU, 2016. – 156 p. URL: http://biblioclub.ru/index.php?page=book&id=467405

5 Bartosh, A. A. Osnovy mezhdunarodnaya zabad. Organizations of International Security: A Textbook for Universities / A. A. Bartosh. – 2nd ed., rev. and add. – Moscow: Yurayt Publishing House, 2022. – 320 p. – (Higher education). – ISBN 978-5-534-11783-7. – Text: electronic // Educational platform Yurait [site]. – URL: https://urait.ru/bcode/493387 (date of access: 10.10.2022).

6 Kaftan, V. V. Counteraction to terrorism: a textbook for universities / V. V. Kaftan. – 2nd ed., ispr. and add. – Moscow: Yurayt Publishing House, 2022. – 261 p. – (Higher education). – ISBN 978-5-534-00322-2. – Text: electronic // Educational platform Yurait [site]. – URL: https://urait.ru/bcode/489436 (date of access: 14.10.2022).

УДК 341.46

Ясинская Софья Валентиновна, студент, Комсомольский-на-Амуре государственный университет
Yasinskaya Sofya Valentinovna, student, Komsomolsk-on-Amur State University
Подкич Светлана Александровна, старший преподаватель, Комсомольский-на-Амуре государственный университет.
Podkich Svetlana Alexandrovna, Senior Lecturer, Komsomolsk-on-Amur State University.

ФЕНОМЕН ТЕРРОРИЗМА С ИСПОЛЬЗОВАНИЕМ СМЕРТНИКОВ: СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКАЯ ИНТЕРПРЕТАЦИЯ

THE PHENOMENON OF SUICIDE BOMBERS: A SOCIAL AND PSYCHOLOGICAL INTERPRETATION

Аннотация: Терроризм в современном обществе все чаще показывает себя через индивида – террориста-смертника. Анализ культурных и психологических корней суицидального терроризма представляет наличие как культурно-специфичных, так и общекультурных оснований, которые в той или иной степени способствуют росту данного явления.
Abstract: Terrorism in modern society increasingly represents itself through an individual - a suicide bomber. An analysis of the cultural and psychological roots of suicidal terrorism reveals the existence of both culturally specific and general cultural grounds that, to a certain or other degree, contribute to the escalation of this phenomenon.
Ключевые слова: террорист-смертник, суицидальный терроризм, психология террористов, корни терроризма, технологии вербовки террористов.
Key words: suicide bomber, suicidal terrorism, terrorist psychology, terrorism roots, terrorist recruitment technologies.

Terrorism is a constant companion of humanity, one of the most dangerous phenomena of the modern era, which is taking on increasingly diverse forms and threatening scales. Terrorism leads to mass casualties, destroys mental and physical health, destroys material and spiritual values, cultural monuments, which sometimes cannot be restored, provokes wars, hatred and distrust between social and national strata of the population, which sometimes cannot be overcome for a long time, most often more than one generation sees hatred for to yourself because of national, racial or social affiliation.

Terrorism as a mass and political phenomenon is the result of widespread "de-ideologization", when society begins to doubt the legality and rights of the State, and this justifies their turning to terrorism to achieve their goals. Various criminal groups are engaged in

terrorist activities aimed at intimidating and destroying competitors, as well as influencing State bodies in order to ensure favorable conditions for their terrorist activities.

Recently, a dangerous weapon has appeared in the hands of terrorists - sacrificial terrorism using suicide bombers.

Why do suicide bombers appear at all? First of all, a suicide bomber does not like the idea that he and his loved ones, as well as ethnic and religious groups to which he belongs, are being subjected to injustice and humiliation. The next stage of this process is to enter into a certain organizational mechanism with this thought.

Factors such as being in constant conflict or a constant traumatic and humiliating experience also contribute to becoming a suicide bomber. At the same time, everyone has their own history and their own psychology. Therefore, it is difficult to give an exact definition that would unambiguously explain the occurrence of this phenomenon.

Previously, it was believed that suicide bombers mainly belong to the poorest strata of society, but an analysis of the document "Sacred Lake Mungo of the Two Rivers", posted on an Islamist Internet forum, which presents 430 biographies of Al-Qaeda suicide bombers, shows that many of them were highly educated people with well-paid jobs. A study of 32 suicide bombers showed that their only common feature was the lack of strong social ties and susceptibility to external influence. This factor is reinforced by the almost complete isolation of the suicide bomber from external social contacts immediately before the terrorist attack.

The devaluation of life, which contributes to the suicidal act, is most often caused by the desire to get rid of the loneliness experienced by a person who has physically or mentally lost all his loved ones, the stigma of shame, feelings of humiliation for his ethnic group. It is known that young people who survived the war and grew up in refugee families make up a significant proportion of suicide bombers. Ideologists of suicide jihad often emphasize that these are acts of sacrifice aimed at drawing attention to their humiliation. With social norms approving the commission of terrorist acts as a means of struggle, the mechanisms of imitation (for example, a suicide bomber) and conformity (following the instructions of religious or party authorities) are strengthened.

Criminal gangs often try to convince teenagers to become suicide bombers because they are more suggestible than adults. For example, in early 2006, Hamas created a website for children that glorifies teenage "Shahids" (i.e. suicide bombers) and encourages children to "take the path of the Shahid".

Yaron Blum, a former employee of the General Security Service, who spent 7 years as head of the El Al flight safety staff in Munich, Rome and Paris, and now an employee of the Institute for Combating Terrorism, has an excellent idea of the psychological profile of many Palestinian juvenile prisoners. "It is a deep mistake to believe that a child of 12 or 13 years old, and even more so older teenagers, will always prefer to play games or go to the movies alone or in company, rather than look for random victims whom they can stab with a knife, a sharpener or a screwdriver," Blum shares his opinion. experience. of course, in order for a young man or, especially, a child to go and kill, risking his own life, and sometimes even certain death, several elements must come together. First, propaganda pushes a person on the path of terror. "There is no doubt that the knife is one of the main motives of the Islamic State propaganda, and traces of this can be seen in the current wave of terror," Dr. Shaul Shai, a specialist in terrorist profiling, expresses his opinion. "Brothers, we do not want a repeat of the events of September 11, let each of you commit a terrorist attack with the means at your disposal, even with your mother's kitchen knife.

It is a mistake to think that the parents of suicide bombers and suicide bombers support the actions of their wayward children. Most, of course, mourn and condemn such actions. Marari's book tells about the parents of a young terrorist who blew himself up among the passengers at a bus stop. "I would have tied my son to the bed and would not have let him go anywhere," said the unhappy head of this family with tears in his eyes, "and if he had escaped, I

would have caught up and held him so tightly that my life would belong to him. The mother of the suicide bomber supported her husband: "I would tear open my heart, push it into the chest and sew it up, then he would understand that you can't do this. The father of another suicide bomber in a fit of grief posted a photo of his son and resolutely refused to go to his funeral. Can parents keep children who have embarked on the path of terror from their last destructive step? Dr. Boris Polishchuk does not give an unambiguous answer to this question. In his opinion, a lot depends on the relationship in the family. It is characteristic that the research department of the Israel Defense Intelligence Agency believes that adherence to terror is a "contagious disease" spread both through the media and via the Internet. "If parents, relatives and families succeed in defeating the lies of propagandists," Dr. Polishchuk continues, "then their sons or daughters will not want to die and will not become terrorists. I think that a somewhat modified appeal of the famous Czechoslovak anti-fascist journalist Julius Fuchik is appropriate here: "Parents! Be vigilant!"[3]

In an interview with Hamas representatives, the Arab newspaper Al-Sharq Al-Awsat describes how they select people to commit suicide attacks in Palestine: "There are four criteria by which we determine who is suitable," says a Hamas spokesman. And fourthly, his death should illuminate the general idea: The sacrifice of fire at the center of their life is a readiness for a holy war leading to them and others.

It should also be borne in mind that the families of the deceased suicide bombers often receive financial assistance from both terrorist organizations and sympathizers. Therefore, a certain percentage goes on the path of suicide bombers consciously in order to improve the welfare of their family

Terrorism is usually caused by:

1. The presence of social, national and religious problems of existential importance for a given social, national or other group and related to its self-esteem, spirituality, fundamental values, traditions and customs;

2. War and military conflicts in which terrorist acts become part of military operations;

3. The presence of class and social inequality. The presence of social groups that differ from their near and far neighbors by a high level of material well-being and culture and, by virtue of their political, economic and military power or other capabilities, dictate their will to other countries and social groups. The former cause envy and hatred and are endowed with all the characteristics of the most dangerous and insidious enemy, which, if it is impossible to defeat in open combat, can be subjected to a painful attack in private;

4. The existence of secret or semi-secret societies and organizations, especially religious or sectarian ones, which endow themselves with magical and messianic abilities, developing what, in their opinion, is the only true doctrine for the salvation of mankind or the radical improvement of its life, the creation of a system of universal goodness, justice and prosperity, eternal salvation of the soul, etc.

5. Unresolved important economic and financial issues, including at the legislative level.

It is necessary to combat such a phenomenon as "motivation" to join a terrorist organization as a "suicide bomber". At the moment, there are several "types" of the fight against terrorism. All measures aimed at combating terrorism can be divided into law enforcement, legal, external and internal. They are the most effective.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Соснин, В.А. Современный терроризм: социально-психологический анализ //В.А.Соснин, Т.А Нестик.- М.2008г.-239с.

2. Боднар, Э. Л. Психология терроризма : учеб.-метод. пособие //Э.Л.Боднар. – Екатеринбург: Министерство образования и науки Рос.Федерации,Уральский федеральный университет: Издательство Уральского университета, 2013. –76 с.

3. Мельникова, А.А. Террорист-смертник: культурно-психологические корни явления в исторической проекции//А.А.Мельникова. - М. 2019 г.-84с.

РАЗДЕЛ 2
THE RIGHT TO PRIVACY IN THE DIGITAL AGE
ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ В ВЕК ЦИФРОВИЗАЦИИ

УДК 347.23

Белкин Александр Константинович, студент, Комсомольский-на-Амуре государственный университет
Belkin Aleksandr Konstantinovich, student of Komsomolsk-na-Amure State University
Шибико Ольга Сергеевна, кандидат культурологии, доцент, Комсомольский-на-Амуре государственный университет
Shibiko Olga Sergeyevna, PhD in Culture Studies, associate professor, Komsomolsk-on-Amure State University

ЦИФРОВОЙ СЛЕД: ПОНЯТИЕ И ЗНАЧЕНИЕ ДЛЯ ЭКОНОМИКИ

DIGITAL FOOTPRINT: CONCEPT AND SIGNIFICANCE FOR THE ECONOMY

Аннотация. В данном докладе поднимается тема цифрового следа, его роли для личности человека и экономики. Проведенная работа показывает, как цифровой след определяет человеческий образ в сети, дает характеристику цифрового следа, а также показывает, какие негативные и положительные стороны есть у этого явления современного мира.
Abstract. This article raises the topic of the digital footprint, its role for the individual and the economy. The work shows how the digital footprint determines the human image in the network, gives a characteristic of the digital footprint, as well as gives the idea of the negative and positive sides of this phenomenon of the modern world.
Ключевые слова: цифровой след, Интернет, данные, информация.
Key words: digital footprint, the Internet, data, information.

Хотя Интернет может показаться местом, где можно анонимно переходить с сайта на сайт, на самом деле все, что делает пользователь, создает след данных, или цифровой след, который может многое о нем рассказать. Создание массивных баз данных потребительских профилей в последние годы стало проще благодаря достижениям в области технологий искусственного интеллекта, которые позволяют лучше сопоставлять и корректировать данные. Именно поэтому защитники конфиденциальности цифровых данных выступают за ограничение того, какие типы данных могут собирать компании, как долго они могут их хранить и с кем они могут ими делиться [6].

Что такое цифровой след? Цифровой след – это след из данных, как намеренных, так и ненамеренных, которые оставляет пользователь во время работы в сети Интернет, например, посещаемые им веб-сайты, отправляемые электронные письма и информация, которую человек предоставляет в Интернете. Цифровой след может быть использован для отслеживания действий человека в Интернете и его данных. Пользователи Интернета создают свой цифровой след как активно, так и пассивно [1].

В настоящее время существует основное разделение цифрового следа на активный и пассивный.

Активный след можно определить как намеренный след данных, который человек оставляет после себя, например:

1. Отправка кому-либо электронного письма.
2. Публикации в социальных сетях.

3. Заполнение форм, предполагающих подписку на электронные письма или текстовые обновления.

4. Другое.

Пассивный след определяется как непреднамеренные следы, которые человек создает в Интернете, например:

1. Использование приложений и веб-сайтов, которые используют геолокацию для определения местонахождения пользователя.

2. Просмотр продуктов и действий, которые рекламодатели собирают и анализируют, чтобы составить профиль пользователя и предоставить контекстную рекламу [2].

Таким образом, очевидно, что практически любое действие пользователя в сети Интернет создает его цифровой след. В связи с этим вполне закономерен вопрос, почему цифровой след важен и почему этот феномен заслуживает тщательного изучения?

Цифровой след относительно постоянен, и как только данные становятся публичными, владелец практически не может их контролировать, а также то, как другие будут этим пользоваться.

Цифровой след может определять цифровую репутацию человека, которая в настоящее время считается такой же важной, как и его репутация вне сети. Работодатели могут проверять цифровой след своих потенциальных сотрудников, в частности, их социальные сети, перед принятием решения о найме. Колледжи и университеты также могут проверять цифровые следы своих будущих студентов, прежде чем принять их. Слова и фотографии, которые пользователи размещают в Интернете, могут быть неправильно истолкованы или изменены, что может привести к непреднамеренному результату. Контент, предназначенный для частной группы лиц, может распространиться в более широком кругу, потенциально разрушая отношения и дружбу. Киберпреступники могут воспользоваться цифровым следом, используя его в таких целях, как «фишинг» для получения доступа к учетной записи или создание фальшивых личностей на основе украденных данных пользователя.

По этим причинам стоит задуматься о том, что цифровой след говорит о каждом конкретном пользователе. Многие люди пытаются управлять своим цифровым следом, осторожно относясь к своей деятельности в Интернете, чтобы контролировать данные, которые могут быть собраны в первую очередь [1]. Есть ли возможность узнать, какой цифровой след у того или иного пользователя? Для этого можно провести инвентаризацию того, что находится в открытом доступе, чтобы быть в курсе того, к какой информации имеют доступ другие. Можно настроить оповещения Google так, чтобы этот инструмент периодически отправлял пользователю уведомления о каждом сообщении, в котором фигурирует его имя.

Не вызывает сомнений то, что пользователь должен защищать свои личные данные, не раскрывать свой личный адрес, номер телефона, пароли или номера банковских карт, использовать псевдоним вместо настоящего имени, хранить информацию для входа в систему под замком, никогда и никому не сообщать свои имена пользователей и пароли и т. п.[5].

К неблагоприятным последствиям могут привести не только действия мошенников, в руки которых незаконным путем могут попасть личные данные пользователя, но и сам цифровой след, если он имеет негативный характер.

Какой тип контента работодатели меньше всего хотят видеть в онлайн-профилях и истории кандидата? Наличие в цифровом следе любого из перечисленных ниже материалов может оттолкнуть от 45% до 85% работодателей и комиссий по найму. Во-первых, упоминания о незаконном употреблении наркотиков и документально подтвержденное употребление алкоголя. Упоминания об оружии и использование ненормативной лексики. Даже плохая орфография и грамматика могут оттолкнуть потенциального работодателя.

В сфере трудоустройства могут возникать случаи, когда неуместное и неосторожное поведение в социальных сетях может привести к досрочному увольнению. Утечка конфиденциальной информации (например, если младший сотрудник отдела маркетинга преждевременно расскажет о новом клиенте до официального старт работы), написание предвзятых сообщений (например, расистских или сексистских), распространение непристойного контента (например, обнаженной натуры или употребления наркотиков) – примеры таких необдуманных и неосторожных действий, которые могут привести к негативным последствиям [2].

Как видим, цифровой след – важный компонент многих сфер жизни современного человека, не мыслящего себя вне сети Интернет. Какова же роль цифрового следа в экономике?

Наличие положительного цифрового следа пользователя может иметь следующие преимущества:

1. Расширение возможностей для бизнеса: Люди с большей вероятностью будут доверять индивиду или организации, имеющим положительный цифровой след, что приведет к расширению возможностей для роста.
2. Более высокая прибыль: Бренды с отличной репутацией в Интернете обычно легче продают свою продукцию. Люди с большей вероятностью будут покупать у таких компаний и рекомендовать их другим.
3. Меньше риска: Если цифровой след пользователя плохой, это может закрепить негативное отношение к нему, которое будет трудно преодолеть.
4. Финансовые учреждения используют цифровой след в качестве параметра для выдачи кредитов. Большинство финансовых компаний, которые активно работают в сфере розничного кредитования, используют цифровые отпечатки своих клиентов для оценки их кредитоспособности. Это помогает сократить время выдачи кредитов и уменьшения количества мошеннических заявок [4].

Цифровой мир никуда не денется в ближайшее время, поэтому следует думать о его развитии на протяжении всей жизни. Пользователю имеет смысл использовать преимущества цифровых платформ, чтобы представить себя в хорошем свете и продемонстрировать свои лучшие качеств. Разумно поддерживать позитивный цифровой след, чтобы быть уверенными в том, что не возникнет непредвиденных проблем вследствие неосторожности в действиях и взаимодействии в сети.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. What is a digital footprint? And how to protect it from hackers – Kaspersky // [Электронный ресурс] URL: https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint (дата обращения 24.11.2022)
2. What is a digital footprint? Definition – Meaning – Examples / [Электронный ресурс] URL: https://blog.reputationx.com/digital-footprint (дата обращения 24.11.2022)
3. Что такое цифровой след и как мы его оставляем в сети // [Электронный ресурс] URL: https://решение-верное.рф/What-is-digital-footprint-how-do-we-leave-it-online (дата обращения 24.11.2022)
4. Learn with ETMarkets: Why a digital footprint is crucial // [Электронный ресурс] URL: https://economictimes.indiatimes.com/markets/stocks/news/learn-with-etmarkets-why-a-digital-footprint-is-crucial/articleshow/53924552.cms (дата обращения 24.11.2022)
5. Your Digital Footprint: What Is It and How Can You Manage It? // [Электронный ресурс] URL: https://www.rasmussen.edu/student-experience/college-life/what-is-digital-footprint/ (дата обращения 24.11.2022)
6. Your Digital Footprint: It's Bigger Than You Realize – CNET // [Электронный ресурс] URL: https://www.cnet.com/news/privacy/features/your-digital-footprint-its-bigger-than-you-realize/ (дата обращения 24.11.2022)

УДК 347.23

Белобородов Анатолий Анатольевич, студент, Комсомольский-на-Амуре государственный Университет
Beloborodov Anatolii Anatolievich, student of Komsomolsk-na-Amure State University
Шибико Ольга Сергеевна, кандидат культурологии, доцент, Комсомольский-на-Амуре государственный университет
Shibiko Olga Sergeyevna, PhD in Culture Studies, associate professor, Komsomolsk-on-Amure State University

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ БРАУЗЕРОВ В УСЛОВИЯХ ВЗАИМОДЕЙСТВИЯ С ИНОСТРАННЫМИ ЯЗЫКАМИ

SECURE USE OF BROWSERS IN A FOREIGN LANGUAGE ENVIRONMENT

Аннотация. С каждым днём технологии и методы их использования совершенствуются. Те способы, которые использовал человек год назад для уверенного и безопасного путешествия по просторам интернета, уже сегодня могут не работать. В условиях повсеместной цифровизации очень важно не потерять персональные данные и, тем более, не выдать их в руки злоумышленников. Проблема становится наиболее острой, когда пользователь взаимодействуют с иноязычными сайтами. Языковой вопрос в данном вопросе может подвергнуть человека опасности при покупках в интернете и ещё множестве ситуаций. В данной статье поднимается вопрос безопасного использования браузеров, а также приводятся основные пути по повышению уровня персональной защищённости.
Abstract. Every day, technology and methods of its use are improving. Those ways that people used them a year ago for a safe and secure surfing through the internet may fail to work today. In the context of widespread digitalization, it is very important not to lose personal data and, moreover, not to hand it over to grifters. The problem becomes most acute when a user interacts with foreign language sites. The language issue in this question can expose people to danger when buying online and many more situations. This article raises the issue of safe browsers, as well as provides basic ways to improve the level of personal security.
Ключевые слова: безопасность, персональные данные, иностранный язык, браузер, покупки в интернете, защита данных.
Key words: security, personal data, foreign language, browser, internet shopping, data protection.

Возможно ли оценить степень безопасности того, как человек пользуется интернетом? Под безопасностью использования подразумевается его умение определять опасные источники, которые лучше не посещать, а также знания о том, что делать, если данные были утеряны или украдены злоумышленниками, переведена сумма денег мошенникам и т. п. [1]. Удивительно, но ещё несколько лет назад до появления смартфонов люди могли выходить в Интернет только с помощью стационарных компьютеров. А ещё раньше, до эпохи «персональных» компьютеров людям было необходимо идти в компьютерные клубы, где риски возрастали ещё больше.

Браузер – программа для поиска и просмотра на экране устройства информации из компьютерной сети [3]. Как известно, интернет объединяет пользователей со всей планеты. Безусловно, есть сайты, предназначенные только для пользователей конкретной страны – они оформлены на языке этой страны, для покупок используется валюта этой страны, при регистрации в личных кабинетах необходимы местные номера телефонов. Таких признаков может быть значительно больше, но их все объединяет то, что они помогают отнести пользователя к той группе, в которой он сможет наиболее комфортно выполнить своё целевое действие, ради которого он вышел в Интернет.

Дискомфорт и трудности начинаются тогда, когда человеку по той или иной причине необходимо взаимодействовать с иноязычными страницами в интернете или даже при общении на иностранном языке.

В 2022 году почти каждое устройство, будь то компьютер (персональный или ноутбук), смартфон, планшет и т.д., оснащены антивирусными программами, которые защищают пользователей устройства от различных вирусов, которые попадают на устройство. Компьютерный вирус – это программа, способная создавать свои копии, внедрять их в различные объекты или ресурсы компьютерных систем, сетей и производить определенные действия без ведома пользователя. Такие вирусы могут выполнять различные деструктивные действия, мешающие пользоваться устройством или, более того, используют данные пользователя для собственных целей.

В браузерах, как правило, есть свои заранее прописанные в программу антивирусы и протоколы безопасности [1]. Таким образом помечаются неблагоприятные или слабо защищённые сайты (рисунок 1).

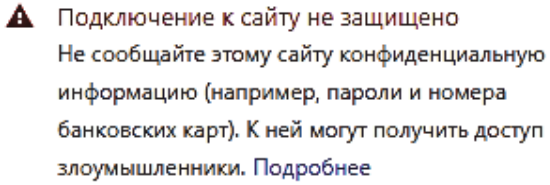

Рисунок 1 - Уведомление в браузере Google Chrome

Пользователи интернета взаимодействуют с иностранными языками по разным причинам. Кто-то ради поиска информации, так как, например, на английском языке количество важной и проверенной временем информации, как предполагают пользователи, значительно выше, чем на русском языке. Кто-то ради покупок иностранных вещей за границей, так как иногда это выходит дешевле, чем у розничных продавцов в их стране. Другие же общаются в социальных сетях с иностранцами на их языке – ради улучшения навыков владения языком, делового взаимодействия или по более личным причинам.

Для безопасного интернет-серфинга [3] необходимо соблюдать ряд универсальны правил, которые помогут обезопасить пользователя от злоумышленников или от неприятных ошибок, влекущих за собой долгосрочные последствия. Нет сомнений в том, что Интернет облегчает жизнь современного человека. Но он также угрожает нам спамом, кражей личных данных, вторжением в частную жизнь. Именно поэтому безопасность в Интернете (также известная как онлайн-безопасность или электронная безопасность) важна. Список необходимых правил допустимо свести к десяти [2]:

1) Использовать программные переводчики.

Для начала необходимо понять, что вообще написано. Многие сайты поддерживают интегрированную функцию перевода, чаще всего при помощи сервиса Google Translate. В подобных переводчиках широкий список переводимых языков. Так, в Google Translate их 133. Однако нужно учитывать, что данный перевод осуществляется компьютерной программой, и при переводе сложных текстов она может допускать ошибки. Для предотвращения недопонимания следует переводить один и тот же текст в разных переводчиках.

2) Своевременно обновлять браузер.

Запуск устаревшей версии веб-браузера равнозначен отсутствию некоторых из новейших функций. Обновление браузера позволяет использовать самые последние меры безопасности, а обновленные браузеры лучше распознают угрозы и блокируют нежелательные всплывающие окна. Игнорирование обновления может привести к заражению браузера с целью завладеть информацией из истории поиска. Время от време-

ни необходимо проверять наличие обновлений. Однако важно не перепутать это окно с рекламным баннером об обновлении браузера [4].

3) Выбрать строгие настройки конфиденциальности и безопасности в браузере.

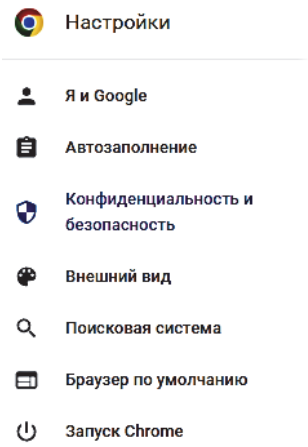

Рисунок 2 - Настройки конфиденциальности

Многие люди не могут оптимизировать настройки безопасности своего браузера. Но это жизненно важный шаг в использовании Интернета. От браузера к браузеру пути до этой вкладки отличаются, но принцип поиска везде одинаково логичен. В Google Chrome данная вкладка выглядит так (рисунок 2).

4) Не посещать сайты без протокола HTTPS.

HTTP - это протокол для компьютеров, но он не зашифрован. HTTPS - это другой протокол, и он зашифрован с помощью Secure Sockets Layer (SSL). Если браузеры используют HTTPS для передачи информации, а данные попадают в руки злоумышленников, они не смогут прочитать информацию. Необходимо убедиться, что веб-сайты являются безопасными, а для этого следует обратить внимание на левую сторону веб-адреса, иногда в качестве иконки безопасности там изображён знак закрытого замка, но для большей точности следует смотреть на адрес сайта. Если там в начале есть необходимый протокол, то такой сайт безопасен (рисунок 3).

Рисунок 3 - Протокол безопасности

5) Быть осторожным с тем, какие файлы и приложения загружать.

Большое количество людей используют интернет для развлечений – скачивают игры, приложения, изображения и музыку. Такое действие может быть источником заражения вирусом или вредоносным ПО. Чтобы избежать неприятных сюрпризов, следует скачивать необходимые файлы только из надежных источников. Кроме того, сканировать файлы на наличие вирусов, прежде чем скачать и открыть их. Если есть подозрения о небезопасности скачиваемого файла, то в панели загрузок можно отменить процесс скачивания.

6) Использовать блокировщик рекламы.

Сегодня в Интернете слишком много объявлений. Именно это мотивирует 42% пользователей во всем мире устанавливать блокировщик рекламы. Блокировщик рекламы - простой инструмент. Он интегрируется с браузером и использует ряд фильтров для блокировки определенного контента. Блокировщик рекламы удаляет отвлекающую рекламу, облегчает чтение страниц и блокирует поддельные новости. Многие объявления содержат вредоносную информацию, что является мошенническим актом сокрытия вредоносных программ в цифровой рекламе. Использование блокировщика рекламы удаляет вредоносный шум и предотвращает пользователя от опасного контента.

7) Запретить браузеру сохранять пароли.

Несмотря на то, что такая функция браузеров очень удобна и позволяет автоматически заходить на любимые сайты, это довольно рискованно. Веб-браузеры оснащены встроенным управлением паролями, которое позволяет сохранять пароли для посещаемых веб-сайтов. Эта функция позволяет пользователю не запоминать все пароли. Однако это влечёт за собой потерю безопасности, потому что данные могут быть украдены по одному щечку мыши.

8) Использовать различные поисковые системы.

Такие гиганты как Google и Яндекс имеют собственные поисковые системы и постоянно отслеживают перемещения пользователя по Интернету. Это и не хорошо и не плохо, так как сбор таких данных может помочь в дальнейшем выдавать пользователю при поиске необходимую информацию гораздо точнее и быстрее. Но есть и другие поисковые системы, которые обеспечат необходимый уровень конфиденциальности. Среди таких поисковых систем можно назвать DuckDuckGo, Ecosia, Qwant, Mojeek и Startpage. Самое большое преимущество использования этих поисковых систем состоит в том, что они не хранят IP-адреса и информацию о пользователях.

9) Использовать надёжные и сложные пароли, подключить двухфакторную аутентификацию (2FA).

Чем сильнее пароль, тем больше защита от вредоносной деятельности. Пользователю желательно завести привычку не использовать один и тот же пароль для разных сайтов. Если произойдёт взлом на одном сайте, то по этим же реквизитам могут взломать и на другом. Кроме того, не рекомендуется использовать даты, номера телефонов, любимые фильмы и имена спортивных команд в качестве пароля. Сильная комбинация паролей должна содержать буквы разных регистров, а также специальные символы и цифры.

Помимо этого следует включить 2FA и повысить безопасность цифровых счетов пользователя. Даже если кто-то угадает пароль, он не сможет получить доступ к учетной записи пользователя. Для входа в аккаунт потребуется не только знание пароля, но и подтверждение через мобильный телефон.

10) Использовать VPN, если это возможно.

В 2020 году безопасность (49%) и конфиденциальность (40%) были двумя наиболее часто упоминаемыми причинами для использования VPN [5]. VPN обычно работает как прерывистый сервис между пользователем и его хостингом. Он шифрует данные и скрывает IP-адрес. Когда информация не зашифрована, ее может просмотреть любой, у кого есть доступ к сети. Но когда включен VPN, киберпреступники не могут расшифровать информацию.

Подводя итог, можно сказать, что невзирая на то, иноязычный это сайт или нет, список правил практически не изменен. Интернет – это глобальная библиотека, наполненная разными данными и знаниями. Миллионы пользователей взаимодействуют между собой ежедневно. Нужно учиться пользоваться интернетом и браузерами, повышать уровень собственной интернет-грамотности, чтобы быть уверенным в том, что использование цифровых технологий не только помогает находить то, что нужно, но и не способствует потере того, что важно.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Семенько Т. В. Безопасность в сети Интернет // Интерактивная наука. 2016. № 9. URL: https://cyberleninka.ru/article/n/bezopasnost-v-seti-internet (дата обращения: 26.11.2022). – Режим доступа: свободный.

2. How to Browse the Internet // swisscyberinstitute.com : информац. ресурс. – URL: https://swisscyberinstitute.com/blog/10-tips-on-how-to-browse-the-internet-safely/ (дата обращения: 26.11.2022). – Режим доступа: свободный.

3. Oxford Languages and Google // languages.uop.com : информац. ресурс. – URL: https://languages.oup.com/google-dictionary-ru/ (дата обращения: 26.11.2022). – Режим доступа: свободный.

4. Мошенники придумали новый способ кражи денег // nsn.fm : информ. агент. 2013. 17 апр. URL: https://nsn.fm/society/moshenniki-pridumali-novyi-sposob-krazhi-deneg-cherez-obnovlenie-brauzera (дата обращения: 26.11.2022).

5. 3rd Annual VPN Market Perot: 2022 // security.org : информац. ресурс. – URL: https://www.security.org/resources/vpn-consumer-report-annual/ (дата обращения: 26.11.2022). – Режим доступа: свободный.

УДК 327

Будерацкий Богдан Денисович, студент, Комсомольский-на-Амуре государственный университет
Buderatsky Bogdan Denisovich, student, Komsomolsk-na-Amure State University
Лопатина Ольга Ивановна, старший преподаватель, Комсомольский-на-Амуре государственный университет
Lopatina Olga Ivanovna, senior lecturer, Komsomolsk-on-Amur State University

ЗАКОНОДАТЕЛЬНАЯ БАЗА РОССИИ В СФЕРЕ ЧАСТНОГО ПРАВА В ЦИФРОВОЙ СРЕДЕ

THE RUSSIAN LEGAL FRAMEWORK FOR PRIVATE LAW IN A DIGITAL ENVIRONMENT

Аннотация. В статье рассматриваются поправки в законодательство, принятые недавно в Российской Федерации, - так называемые "закон Яровой", "фейковые новости" и "неуважение". Раскрывается суть и проблемы применения вышеуказанных правовых документов, дается их оценка с точки зрения прав человека. Установлено, что анализируемые достаточно сложные законы создают значительные угрозы правам человека и основным свободам личности, включая неприкосновенность частной жизни, защиту данных и свободу выражения мнения, а также вносят другие дополнительные негативные эффекты в российское общество и экономику.
Abstract. The article deals with the legislative amendments that have been recently adopted in the Russian Federation, the so-called ‘Yarovaya’ law, the ‘fake news’ law and the ‘disrespect’ law. It explains the essence and problems of implementation of the above-mentioned legal instruments and assesses them from the human rights angle. It is established that the rather complex laws under analysis pose significant threats to the human rights and fundamental freedoms of individuals, including privacy, data protection and freedom of expression, and introduce other additional negative effects to the Russian society and economy.
Ключевые слова: право на частную жизнь, законодательство, цифровизация, контроль над распространением информации.
Key words: right to privacy, legislation, digitalization, information dissemination controls.

Киберпространство глубоко вошло в нашу жизнь: в настоящее время невозможно представить существование современного человека без разнообразных технических средств, включая смартфоны, планшеты и компьютеры, которые постоянно подключены к всемирной паутине и используются на ежедневной основе. Киберпространство не только открывает множество новых возможностей в борьбе за демократию и соблюдение прав человека, но и создает широкий спектр проблем и может использоваться и злоупотребляться в сфере национальной безопасности. Оно представляет собой уникальное поле боя, где правительства - часто при содействии различных частных субъектов - ведут новые виды войны, включая борьбу за умы людей, сферу, которая все более глубоко влияет на развитие нашей экономики и гражданского общества.

В последние годы информационная война (далее: ИВ) в киберпространстве стала основным инструментом России в ее конфликте с Западом. С помощью ИВ, особенно пропагандистских усилий в киберпространстве, Россия якобы неоднократно вмешивалась в избирательные процессы и внутренние дела США, Германии, Великобритании, Украины и ряда других стран. Кроме того, по сообщениям, с помощью ИВ Россия стремится бросить вызов стабильности ведущих западных стран.

Китай и Россия продвигают цифровой суверенитет для защиты своей национальной безопасности и стабильности режимов, как утверждают соответствующие режимы. Обе страны стремятся к большему контролю над собственным киберпространством и, следовательно, к большему контролю над потоками информации, игнорируя конфиденциальность данных и свободу слова. Более того, эти усилия могут побудить другие страны, такие как Иран, Турция, Саудовская Аравия, Египет и многие другие, усилить строгий контроль над своими "частями" киберпространства и нарушить основные права человека в киберпространстве. Следовательно, последние усилия по "суверенизации" киберпространства увеличивают разрыв между западно-либеральными демократиями (прежде всего ЕС и США), с одной стороны, и ключевыми недемократическими странами, такими как КНР и Россия, с другой стороны, в области киберрегулирования и особенно защиты данных и реализации основных прав человека, таких как свобода выражения мнения в цифровой сфере.

Эти события формируют новый импульс в сфере неприкосновенности частной жизни, защиты (сохранения) данных и свободы выражения мнений в киберпространстве и смещают баланс в пользу государственных субъектов в ущерб уважению и защите основных прав и свобод человека, таких как право на неприкосновенность частной жизни, защиту данных и свободу выражения мнений. Более того, различия между подходами к соблюдению вышеупомянутых прав и свобод человека и защите национальной безопасности в разных странах порождают новые вопросы относительно защиты персональных данных в глобальном контексте, особенно с учетом трансюрисдикционных потоков личной информации. В частности, актуальным становится ответ на вопрос, как ЕС должен относиться к последним изменениям в российском законодательстве и регулировании в области защиты данных и свободы выражения мнений в киберпространстве.

В то же время российское руководство убеждено, что Москве угрожают внутренние и внешние враги, стремящиеся бросить вызов национальной безопасности России, в том числе в информационном секторе. С точки зрения Москвы, интернет и свободный поток информации в целом угрожают российской национальной безопасности. Таким образом, чтобы предотвратить возможные попытки Запада дестабилизировать Россию с помощью ИВ в киберпространстве, Москва должна принять необходимые меры предосторожности.

Соответственно, Москва стремится держать информационный поток в российском киберпространстве под своим строгим контролем. Таким образом, она стремится предотвратить или сдержать, насколько это возможно, распространение информации, которая может создать негативный образ страны и ее руководства, или любую деятельность, которая может поставить под угрозу стабильность режима.

Поэтому с помощью законодательства и регулирования Москва пытается усилить контроль над информационным потоком в российском сегменте киберпространства и, соответственно, сохранить стабильность существующего режима. В этой связи следует особо отметить ряд законов/поправок, принятых российским парламентом и подписанных президентом в последние годы: "закон Яровой", "фейковые новости" и "неуважение", которые будут рассмотрены ниже. Широкой общественности это законодательство представляется как необходимая мера для сохранения общественной безопасности и как антитеррористическая мера.

В целом, российское законодательство, принятое в области защиты персональных данных и свободы выражения мнений в киберпространстве, воспринимается как недостаточно изученное, аналогично сравнительному исследованию этого регулирования и правил и процедур, установленных в ЕС. Не так много внимания эксперты в области права уделили трем вышеупомянутым российским законодательным актам, которые не подвергались широкому анализу. В своей публикации Михаил Журавлев и Та-

тьяна Бражник сосредоточились на требованиях к хранению данных, введенных законом "Яровой", но не обсудили два других закона, которые оцениваются в настоящем материале. Более того, необходимо исследовать соответствие новой российской законодательной базы европейским стандартам в области прав человека. Кроме того, эта законодательная база должна быть сопоставлена с требованиями по защите данных, введенными в Общем регламенте по защите данных, которые не смогут выполнить многочисленные организации, обрабатывающие персональные данные. В целом, таким образом, существует необходимость провести более глубокое исследование трех российских законодательных актов и сравнить их совместимость с европейскими стандартами в области защиты данных и свободы выражения мнений.

В последние годы российские власти приняли ряд законов и поправок, которые демонстрируют их решимость значительно усилить контроль над информационными потоками в российском секторе интернета. Эти усилия в основном оправдываются соображениями противодействия терроризму и обеспечения общественной безопасности. Показательным примером такого законодательства является Федеральный закон от 6 июля 2016 года № 374-ФЗ (также известный как "закон Яровой"), вносящий изменения в Федеральный закон, регулирующий меры по противодействию терроризму и обеспечению общественной безопасности. В частности, статья 15 этого закона включает изменения в Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации", а именно в его статью 10.1. Статья 10.1 измененного закона № 149-ФЗ обязывает распространителей информации, таких как интернет- и телекоммуникационные компании, мессенджеры, сервисы электронной почты, форумы и другие платформы, позволяющие обмениваться информацией в интернете, хранить на территории Российской Федерации следующую информацию:

Информацию о фактах приема, передачи, доставки и/или обработки голосовой информации, письменного текста, изображений, звуков, видео или иных электронных сообщений пользователей сети Интернет и информацию об этих пользователях в течение одного года после окончания таких действий;

Текстовые сообщения пользователей сети Интернет, голосовая информация, изображения, звуки, видео и другие электронные сообщения пользователей сети Интернет до шести месяцев с момента окончания их приема, передачи, доставки и/или обработки.

Кроме того, распространители информации в сети Интернет обязаны предоставлять указанную ранее информацию уполномоченному органу исполнительной власти (например, Федеральной службе безопасности (далее - ФСБ)), осуществляющему оперативно-розыскную деятельность или обеспечивающему безопасность Российской Федерации, в случаях, установленных федеральными законами.

Распространители информации в сети Интернет обязаны при использовании дополнительного шифрования электронных сообщений для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет, а также для предоставления пользователям сети Интернет дополнительного шифрования электронных сообщений передавать в федеральный орган исполнительной власти в области обеспечения безопасности информацию, необходимую для декодирования принятых, переданных, доставленных и (или) обработанных электронных сообщений.

Согласно закону, за неисполнение любого из этих обязательств операторы (распространители информации) могут быть заблокированы на территории России. Отметим, что по сравнению с распространенной западной практикой правоприменения, российский закон наделяет спецслужбы гораздо более широкими полномочиями. Например, для получения доступа к персональным данным пользователей, как правило, западным спецслужбам необходимо предоставить судебный ордер оператору связи или интернет-оператору. Получив такой документ, оператор обязан самостоятельно передать необходимую информацию правоохранительным органам. Однако российские

спецслужбы действуют иначе. Каждый оператор связи или интернета по закону обязан установить специальное программное и аппаратное обеспечение, называемое СОРМ или Система оперативно-розыскных мероприятий, которое позволяет ФСБ получать доступ к персональным данным пользователей. В этом случае доступ к информации осуществляется спецслужбами без ведома телекоммуникационных или интернет-компаний. Сотрудник ФСБ просто вводит команду через панель управления СОРМ, которая подключена к серверам оператора. В результате только сотрудник ФСБ и его начальство видят ордер, выданный судом, разрешающий доступ к информации. Учитывая низкий уровень верховенства закона в России и фактическое подчиненное положение судов по отношению к исполнительной власти, спецслужбы, такие как ФСБ, пользуются абсолютной свободой действий и отсутствием надзора. Ситуация усугубляется отсутствием общественного или парламентского контроля за работой спецслужб.

В целом, Россия служит интригующим примером того, как усилия авторитарного режима по сохранению стабильности приводят к подрыву репутации внутри и за пределами государства, значительному прямому и косвенному экономическому ущербу, а также бесконтрольному доступу спецслужб к конфиденциальной частной и коммерческой информации с широкими возможностями для злоупотреблений.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Радченко, А. С. "Пакет Яровой" и "Акт Патриота": общее и частное / А. С. Радченко, А. А. Кнышов // Научный альманах. – 2017. – № 3-1(29). – С. 334-336. – DOI 10.17117/na.2017.03.01.334. – EDN YMZZLH.

2 Кемпф, В. А. Правовые и технические проблемы реализации"пакета яровой" / В. А. Кемпф, С. А. Сорокина // Вестник Барнаульского юридического института МВД России. – 2021. – № 1(40). – С. 100-102. – EDN FAFGZD.

УДК 1234.56

Бурико Екатерина Дмитриевна, студент, Комсомольский-на-Амуре государственный университет
Buriko Ekaterina Dmitrievna, student of Komsomolsk-na-Amure State University
Шушарина Галина Алексеевна, кандидат филологических наук, доцент, заведующий кафедрой «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Shusharina Galina Alekseevna, Candidate of Philological Sciences, Associate Professor, Head of Department “Linguistics and intercultural communication”, Komsomolsk-na-Amure State University

ИНФОРМАЦИОННАЯ КУЛЬТУРА КАК ТРЕБОВАНИЕ ИНФОРМАЦИОННОГО ОБЩЕСТВА

INFORMATIONAL CULTURE AS A REQUIREMENT OF INFORMATIONAL SOCIETY

Аннотация. В условиях современности информационная культура стала неотъемлемым элементом нашего общества. Данная статья посвящена вопросам информационной культуры, её основным критериям и аспектам. Большое внимание уделено взаимосвязи информационной культуры и информационной безопасности, а также информационной компетентности как одному из ключевых звеньев информационной культуры.
Abstract. In modern conditions informational culture has become an essential part of contemprorary society. The article is dedicated to questions of informational culture, its main cri-

teria and aspects. Considerable attention is paid to connection of informational culture and informational safety and informational competence as a sagnificant part of informational culture.
Ключевые слова: информационное общество, информационная культура, информационная компетентность, информационная безопасность, компьютерные технологии, СМИ.
Key words: informational society, informational culture, informational competence, informational safety, computer technologies, mass media.

В условиях современности мы не проводим ни дня без получения огромного потока информации, который мы даже не всегда успеваем проанализировать. Это связано с тем, что мы живём в информационном общества, главным ресурсом которого является информация. В информационном обществе от каждого из нас требуется способность к творчеству и при этом возрастает спрос на знания. Важно отметить, что главными компонентами в информационном обществе являются интеллект и знания, что приводит к увеличению доли умственного труда в отличие от индустриального общества, в центре внимания которого производство и потребление товаров.

Информационное общество обладает своими собственными признаками:

1) осознание информации как главного приоритета общества;
2) отношение к информации как к предмету купли – продажи;
3) равный доступ к информации для всех слоёв населения;
4) обеспечение безопасности информационного общества и информации в целом;
5) профессиональное взаимодействие государственных структур с помощью средств ИКТ.

Информационные ресурсы и информационные продукты являются важными компонентами информационного общества. Информационный продукт значительно отличается от своего предшественника, материального продукта, и является одной из отличительных черт информационного общества. Он не потеряет в качестве и уникальности, даже если мы будем неоднократно его использовать.

Что касается понятия информационной культуры, то можно сказать, что оно довольно комплексное и многогранное. Рассмотрим некоторые из них. Информационная культура представляется как совокупность знаний, которые получает человек, а также умение применять их в своей практической деятельности. Информационная культура – отдельная область культуры, напрямую связанная с функционированием информации в обществе и образованием информационных качеств конкретного индивида. Большинство специалистов полагает, что именно информационная культура является критерием для оценивания конкретных наций и национальностей, их культурного развития.

Однако самым распространённым определением информационной культуры является следующее: совокупность навыков и умений человека, которые позволяют ему успешно взаимодействовать с окружающей его информационной средой. Называть же владение какой-то одной системой знаний информационной культурой определённо не верно. К тому же информационная культура может быть определена как концепция личностного развития, как совокупность ценностных ориентаций и как мировоззрение, в общем и целом.

Если рассматривать информационную культуру с точки зрения истории её развития, то можно выделить пять главных информационных революций:

1. открытие языка
2. открытие письменности
3. изобретение книгопечатания
4. изобретение электричества
5. внедрение современных компьютерных технологий.

Информационная культура подразделяется на технологическую, организационно-производственную, управленческую, научно-познавательную и информационную культуру словесного общения согласно областям информативной деятельности.

Информационная культура также обладает своими критериями, такими как:

a. навык грамотного формулирования поискового запроса
b. навык успешного поиска нужной информации в огромном информационном поле
c. навык переработки существующей информации и создание новой
d. навык отбора и оценки информации
e. навык осуществления информационного общения
f. обладание информационной грамотностью.

Информационная компетентность является важным компонентом информационной культуры. Информационная компетентность – это умение работать с большими и разными по своим характеристикам объёмами информации. Рассмотрим основные элементы информационной компетентности.

Знание информационно-коммуникационных технологий и умение работать с ними является первым элементом.

Множество знаний, умений и навыков, касающихся функционирования необходимого программного обеспечения, является вторым элементом.

Целевые установки и ценностные ориентации, связанные с работой с информацией, являются третьим элементом.

Однако кроме позитивных аспектов, связанных с информационным обществом, присутствуют также и опасные тенденции и прогнозы, связанные с ним. Рассмотрим их более подробно. Одной из самых опасных тенденций является всё большее влияние на общество средств массовой информации, что особенно актуально в нынешних условиях информационной войны. Возможность делиться своим мнением и освещать мировые события из любой точки мира – это несомненно прекрасно, однако в связи с огромным количеством недостоверных источников информации и созданием так называемых фейков (распространение абсолютно ложной информации) ориентироваться в информационном поле становиться порой очень сложно, а иногда и вовсе невозможно, ведь для большинства проще прочитать и поверить ложной информации, чем проанализировать её на предмет объективности. В связи с этим проблема отбора качественной и достоверной информации является крайне важной.

Ещё одним важным аспектом является разрушительное влияние информационных технологий на частную жизнь людей и организаций. Каждый из нас уже не раз слышал или читал истории об утечке персональной информации через социальные сети и иные средства информационных технологий. С этим очень сложно бороться, но всё же можно.

Чтобы избежать всех вышеописанных ситуаций, нужно развивать и совершенствовать в каждом члене общества и в социуме в целом не только информационную культуру, которая уже давно стала неотъемлемым условием информационного общества 21 века, в котором мы живём, но и информационную безопасность.

Информационная безопасность является таким состоянием общества, при котором защищена информационная сфера общества от разного рода информационных угроз. Таким образом, информационная безопасность является довольно глобальным понятием, так как связано с потреблением, преобразованием и созданием информации, которая пронизывает всю нашу планету.

Формирование информационной культуры и информационной безопасности важно начинать развивать с самого детства, ведь именно в школьном возрасте личность наиболее восприимчива к внешнему информационному воздействию, которое, к сожалению, часто может наносить весьма существенный вред психоэмоциональному состоянию ребёнка.

Для этого нужно вычленить основные направления формирования информационной культуры у всех индивидов нашего социума.

Одним из самых главных направлений является формирование понятия о том, что информационная среда – это не хаотичная, а чётко структурированная система со своей иерархией и законами.

Развитие критического отношения к информации и умение оценивать её качество и достоверность также немаловажны.

Таким образом, разрозненные знания и умения работы за компьютером не могут называться информационной культурой. В нынешнее время информативная направленность целостной личности, которая обладает чёткой мотивацией к применению и усвоению данных, четко отражает значение информационной культуры личности. Большинство учёных считают информационную культуру одной из граней личностного развития, являющейся при этом путём к универсализации качеств человека.

Поэтому точно ясно одно: только успешное и эффективное умение применять информационные ресурсы и новейшие прогрессивные достижения в сфере СМИ на практике по-настоящему определяет суть информационной культуры, которая является обязательным требованием информационного общества и без которой невозможно успешное функционирование и развитие каждого человека как личности в реалиях современности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Дука С. И., Информационная компетентность личности как условие развития современного общества // Инновации. 2011. №1 (147). С. 102-104

2. Северцов Н.А., Бецков А.В. Информационная безопасность и принципы её обеспечения // Труды Международного симпозиума «Надёжность и качество». 2018. Т.1. С. 92-96

3. Уразова А.В., Информационная культура личности и информационная культура общества в России // Наука. Инновации. Технологии. 2010. №71. С. 154-158

4. Яковлева Ю.В., Взаимосвязь информационной безопасности и информационной культуры // Международный научный журнал «ВЕСТНИК НАУКИ» № 1 (46) Т. 1 С. 77-81

УДК 323.2

Бучнев Евгений Владимирович, преподаватель кафедры политологии и прикладной политической работы, аспирант, Российский Государственный Социальный университет
Evgeny Vladimirovich Buchnev, Tutor of Department of Political Science and Applied Political Work, PhD student, Russian State Social University

ДОСТУПНОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ: ПОЛИТИЧЕСКИЙ АСПЕКТ

ACCESSIBILITY AND PRIVACY IN SOCIAL MEDIA: THE POLITICAL DIMENSION

Аннотация. Развитие информационных технологий в современном мире влечет за собой интенсивную социализацию общества. В цифровое пространство переходят многие отрасли деятельности человека: медицина, образование, путешествия и социализация. Однако не стоит забывать, что современные социально-политические процессы в некоторых государствах ведут к изменению государственной политики в киберпространстве. Воспринимая цифровое пространство как поле для политического диалога, граждане государства могут участвовать как в политической агитации, так и действиях,

подпадающих под уголовную или иную ответственность. Изучение таких аспектов как доступность и конфиденциальность этой информации формируют правильную и выверенную политику государственного присутствия в цифровом пространстве. Автор рассматривает конфиденциальность информации в социальных сетях как политический аспект взаимоотношений между государством и населением.
Abstract. The development of information technology in today's world entails an intense socialization of society. Many sectors of human activity are moving into the digital space: medicine, education, travel and socialization. The development of social networks, their initial accessibility and ease of use lead to the formation of a person's social information personality. However, it should not be forgotten that modern socio-political processes in some states are leading to a change in public policy in cyberspace. Perceiving the digital space as a field for political dialogue, citizens of the state can participate both in political agitation and in actions that fall under criminal or other liability. Examining aspects such as the accessibility and confidentiality of this information forms the correct and calibrated policy of state presence in the digital space. The author considers social media privacy as a political aspect of the relationship between the state and the population.
Ключевые слова: конфиденциальность, безбарьерная среда, социальные сети, кибербезопасность, политическая агитация, оппозиция, правовой режим информации.
Key words: privacy, barrier-free environment, social media, cybersecurity, political campaigning, opposition, legal information regime.

Для современного человека наличие аккаунта хотя бы на одной социальной платформе или в одной социальной сети становится не просто нормой, а скорее необходимым условием его социализации. Воспринимая изначально сам феномен социальных сетей как внутренний и достаточно ограниченных для сторонних участников клуб для общения, социальные сети сейчас вытесняют не только общение оффлайн, но и заменяют многие аспекты жизнедеятельности человека. С развитием социальных сетей повысилась доступность образования, путешествий, информации, в частности новостей, и скорость передачи этих данных. Принимая во внимание такой позитивный аспект данного развития как “безбарьерность”, не стоит забывать о серьезном цифровом следе, который остается после присутствия человека в киберпространстве. Доступность и легкость обмена информацией, идеями, мнениями через социальные сети делает их не нормой, скорее обязательным условием продуктивности современного человека. По собственным данным компании ВК количество пользователей социальной сети ВКОНТАКТЕ за 1 квартал 2022 года составило 74,5 млн человек, что соответствует почти половине населения Российской Федерации (ссылка).

Ежедневное общение, обмен информации и другими данными между участниками одной социальной группы или родственниками, которые являются основной неотъемлемой функцией социальных сетей ранее, в силу своей замкнутости и ограниченного круга лиц, были покрыты тайной частной жизни. Однако современное общество вместе с развитием технологий развивает другие ориентиры моды и влияния. В последнее десятилетие появляются новые профессии, виды деятельности, огромное количество консультантов и педагогов переходят в цифровое пространство. Это рождает интерес и к социальным медиа как предмету социализации, так и как социальному лифту.

Социальное пространство как социально-политический актор

В современном обиходе все чаще встречаются понятия “инфлюенсер” и “фолловер”, которые составляют огромную часть информационного и социального пространства. Инфлюенсеры - это современные selfmade персоны, которые становятся знаменитостями в социальных сетях за счет самих социальных сетей. Их влияние и статус базируется на признании их своеобразной власти, правильнее даже, моде к чему-то определенному в информационном пространстве. Для современной молодежи, к примеру,

такие личности могут вызывать интерес чаще в государствах с медленно действующими или труднодоступными социальными лифтами. Тем не менее современные “социальные кумиры” формируют определенную базу почитания, которая чаще именует себя “фолловерами” и пристально следит за идеями и нравственными ориентирами своего кумира [1]. Причем образ социального кумира не всегда имеет ярко выраженную и хорошо читаемую позитивную риторику.

Анализируя образ Г.Тунберг в контексте усиления интернет-запросов о экологических проблемах, отечественные ученые приходят к двоякому выводу. Понимая, что социальные сети могут смело брать на себя роль своеобразного актора молодежных мнений, в том числе и политических, тот же актор чаще всего перестает быть личной персоной: его образ и его мысли растворяются в данной социальной повестке, приводят к моменту, когда сама проблема ассоциируется с образом персоны и происходит уничтожение личности персоны в угоду повышению интереса к затрагиваемой им проблеме[2].

Таким образом социальные сети не просто средство общения, а собственный мир со своими правилами, кумирами, законами и своей цифровой моралью. Однако, в отличие от традиционного мира оффлайн, онлайн мир формирует в процессе работы огромное количество данных и персонализированный цифровой след каждого участника данного сообщества. Подобная трансляция все чаще выходит за рамки интимного общения и может быть открыта для широкого круга лиц, что затрагивает большое проблемное поле данной информации: частность, правдивость, доступность, формируемую оценку и влияние на аудиторию.

В современном обществе все чаще возникает проблема утечки данных, которые провоцируют за собой ряд крупных скандалов. И если в одном случае такие скандалы и утечки привели к восстановлению законности и наказанию преступника, то в другом случае они нарушают право на неприкосновенность частной жизни.

Анализируя наиболее распространенные социальные сети, можно составить список актуальных личных данных практически любого. Как правило, при регистрации необходимо указать свое имя, фамилию, дату рождения. Разумеется, никто не гарантирует, что каждый будет использовать верные данные, однако суть социальных сетей именно в актуальной социализации по определенным признакам.

Например, социальная сеть “Одноклассники”[4] предлагает каждому зарегистрированному участнику найти своих знакомых и друзей со школы, места жительства, места работы или благодаря каким-то интересам. В совокупном исчислении на этом формируется маркетинговая работа самих социальных сетей, однако с другой стороны это огромный массив данных, который могут использовать как во благо, так и для развития определенных противоправных действий. По подобному принципу работают и другие социальные сети и платформы.

В современном российском правовом поле существуют трактовки понятий “конфиденциальность информации” и “обеспечение безопасности данных”. Согласно российским законам, под конфиденциальностью понимается прежде всего специальное свойство информации, при котором оно не может быть получено и/или использовано неавторизованными лицами или в случае неавторизованных процессов. Нарушение конфиденциальности не всегда приводит к нарушению безопасности, чаще всего отражая именно моральные аспекты общения или персоны. В последнее время именно нарушение конфиденциальности становится громкой темой в новостях. Согласно заявлению замглавы Роскомнадзора М. Вагнера с января по август 2022 года в Российской Федерации было зарегистрировано 46 случаев нарушения конфиденциальности данных, повлекших их попадание в открытый доступ интернета. Что повлекло к компрометации более 300 млн записей [5].

Под безопасностью, согласно законодательству РФ, понимается комплекс мер, нацеленных на выполнение требований законов России, которые затрагивают обработ-

ку, хранение, передачу данных граждан РФ. Согласно законодательству обязанность по обеспечению безопасности лежит на операторах данных, к которым относятся государственные и муниципальные органы, а также юридические или физические лица, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Заключение

В контексте российской политической культуры цифровое пространство понимается, с одной стороны, как субъект политических отношений, в котором формируется поле взаимодействия государства с населением и, также, как область развития системных и несистемных реакций на государственную политику. С другой стороны, киберпространство воспринимается как объект государственной политики национальной безопасности. Принимая во внимание доступность и неподконтрольность интернета, государственная политика стремится очертить рамки цифрового присутствия и в тоже время использовать само пространство для своих целей. Отсюда можно смело говорить, что социальные сети как одно из проявлений киберпространства должны восприниматься государственной политикой как неотъемлемая часть жизнедеятельности общества.

Защита личной информации для граждан Российской Федерации реализуется согласно Конституции РФ. Однако понятие защиты и конфиденциальности так или иначе затрагивает политику безопасности государства. А отсюда и сложная, порой противоречивая деятельность государства по защите или обереганию интересов граждан в цифровом пространстве.

В своей статье “Поиск через социальные медиа и разумные ожидания конфиденциальности” Б. Мунд затрагивает политическую составляющую конфиденциальности. Изучая законодательный нарратив США, автор приходит к выводу, что современные государства достаточно развили законодательную платформу для восприятия конфиденциальности данных человека как его личной собственности, а население в свою очередь готово к необходимым издержкам в данном направлении[3].

Принимая во внимание многосмысловость киберпространства и его многозадачность, государственная политика сама формирует проблемное поле цифрового пространства. Реализуя политику защиты конфиденциальности, институты власти затрагивают сложную составляющую права на конфиденциальность.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Захаркин Р.А., Аргылов Н.А. Инфлюенсеры как медиазначимые другие: современные тренды вторичной социализации // Власть. 2021. №6. С. 27-38.

2. Ефанов А. А. Деконструкция образа инфлюенсера в современном медиапространстве //Мониторинг общественного мнения: экономические и социальные перемены. 2021. № 5. С. 32—46. https://doi.Org/10.14515/monitoring.2021.5.1958.

3. Mund B. Social media searches and the reasonable expectation of privacy // Yale journal of law and technology. - New-Heaven, 2018. - Vol. 19, N 1, Art 5. -P. 239-273. - Mode of access: http://digitalcommons.law.yale.edu/yjolt/vol19/iss1/5

4. Социальная сеть Одноклассники. Электронный ресурс. Точка доступа:https://ok.ru. Дата обращения: 10.10.2022 г

5. Штейнбах К. Новости. Сноб.РУ. Точка доступа: https://snob.ru/news/roskomnadzor-v-otkrytyj-dostup-s-nachala-2022-goda-popalo-ne-menee-40-baz-dannyh-rossiyan/. Дата обращения: 10.10.2022

УДК 004.738.5

Войтус Антон Михайлович, студент Поволжского института управления им. П. А. Столыпина-филиал РАНХиГС
Voytus Anton Mikhailovich, student at the Volga Institute of Management. P. A. Stolypin - branch of the RANEPA
Менькова Анастасия Михайловна студент Поволжского института управления им. П. А. Столыпина-филиал РАНХиГС
Menkova Anastasia Mikhailovna student at the Volga Institute of Management. P. A. Stolypin - branch of the RANEPA
Антонюк Екатерина Юрьевна, доцент, кандидат культурологии Поволжского института управления им. П. А. Столыпина-филиал РАНХиГС
Antonyuk Ekaterina Yurievna, Associate Professor, Candidate of Culturology, Volga Region Institute of Management. P. A. Stolypin - branch of the RANEPA

АНАЛИЗ ФАКТОРОВ, ВЛИЯЮЩИХ НА КОНФИДЕНЦИАЛЬНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ

ANALYSIS OF FACTORS AFFECTING PRIVACY IN SOCIAL NETWORKS

Аннотация. Социальные сети стали частью обыденной жизни человека. Первоначальной целью социальных сетей являлось общение, в данный момент существует тенденция закрытых профилей, что в значительной степени мешает поставленной цели. В данной работе рассмотрено значение социальных сетей. Проведен опрос среди студентов Поволжского института управления с целью получения информации об осведомленности о базовых факторах, которые влияют на конфиденциальность. Предоставлены авторские рекомендации, которые помогут пользователям защитить свои данные.
Abstract. Social networks have become part of everyday life. The original purpose of social networks was communication, now there is a trend of closed profiles, which greatly interferes with the goal. In this paper, the importance of social networks is considered. A survey was conducted among students at the Volga Institute of Management to obtain information about awareness of the basic factors that affect confidentiality. Author's recommendations are provided to help users protect their data.
Ключевые слова: безопасность, конфиденциальность, опрос, персональные данные, социальные сети, факторы.
Key words: security, privacy, survey, personal data, social networks, factors.

С появлением социальных сетей жизнь человека стала намного разнообразнее. В ВКонтакте многие переписываются со своими друзьями, листают ленту в поисках различной тематической информации, многие выкладывают свои фото, которыми хотят поделиться со своими знакомыми пережитыми эмоциями, а YouTube всегда можно найти интересное видео, которое поможет скоротать унылый вечер, а в Telegram обязательно есть тот самый канал, который публикует промокоды и скидки в различных магазинах. Трудно представить обыденную жизнь без социальных сетей.

Актуальность выбранной темы заключается в том, что каждый человек в той или иной степени ежедневно пользуется социальными сетями, однако в современных реалиях существуют риски потерять свою конфиденциальную информацию.

При использовании социальной сети человек может столкнуться со следующими проблемами:

1) Взлом социальной сети с целью получения конфиденциальной информации с целью шантажа. Обычно это происходит с помощью использования специального

ПО, жертвой мошенников могут стать все личные переписки пользователей, фотографии, а также файлы. В основном это происходит по виде самого пользователя, так как многие особо не задумываются о составлении индивидуального пароля каждой социальной сети прикрываясь тем, что так проще запомнить пароль, другие пользователи ставят максимально простые пороли, например 12345qwe, такие пароли запросто подбираются специальным ПО за несколько секунд.

2) Создание сайтов клонов с целью кражи персональных данных, в том числе реквизитов банковских карт, данных паспортов и т.д. Данный способ обычно проявляется следующим образом, пользователи получают сообщения от профиля, который был создан по образу знакомого человека, сообщение содержит просьбу перейти по ссылке и забрать приз, либо поучаствовать в каком-либо опросе, либо какое-нибудь ещё уникальное предложение, увидев которое пользователь не сможет отказаться, обычно данное предложение подбирается исходя из увлечений, хобби, привычек пользователя, которые он показывает на всю аудиторию.

Таким образом, исходя из проблем, описанных выше, было проведен опрос среди учащихся 1–5 курсов факультета Экономики и Управления Поволжского института управления им. П. А. Столыпина. В данном опросе приняло участие 142 человека.

Среди опрошенных 67% относятся к женскому полу, остальные 33% к мужскому.

На вопрос о том “ежедневно ли вы пользуетесь социальными сетями?” все 142 респондента ответили положительно,

К основным причинам относились: общение с друзьями, семьей-86%; поиск информации-60%; просмотр видео, блогеров-74%; чтение научных статей-11%; прослушивание музыки-49%; опубликовать фото, поделиться интересной новостью со своими друзьями-37%.

Среди студентов, которые прошли опрос 54% проводят в социальных сетях более 4-х часов, 26% проводят от 2-х до 4-х часов, 17% проводят 1–2 часа и всего 3% уделяют социальным сетям менее 1 часа.

Реальные персональные данные указывают 78% опрошенных, также 80% иногда публикуют свои фотографии, 69% опрошенных указывают информацию о своем месте обучения, 17% опрошенных рассказывают о своих увлечениях, любимых книгах и т. п.

Среди опрошенных 84% так или иначе попадались на уловки мошенников, остальные 16% получали уведомление, но игнорировали их.

По итогам опроса 76% используют ОС Windows, остальные 24% используют Mac OS.

У 64% респондентов стоят одинаковые пароли во всех социальных сетях, ещё 27% используют разные пороли для каждой сети, а оставшиеся 9% стараются различными способами и знаками усложнить свой пароль.

Среди респондентов 42% ответили, что в большинстве случаев пользуются социальными сетями от Wifi, 31% использует социальные сети через прямое подключение через LAN, остальные 27% используют для выхода в сеть мобильный интернет.

Среди опрошенных на учебе 70% выходят в социальные сети с помощью общедоступных сетей wifi, 28% выходят в социальные сети с помощью мобильного интернета, оставшиеся 2% не пользуются социальными сетями в процессе обучения.

Таким образом, мы понимаем, что многие респонденты в силу своей неграмотности или халатности подвергают себя и свои данные риску.

В современном мире оставаться анонимным и защищенным на сто процентов просто невозможно, так как если кто-то захочет взломать ваш аккаунт, он это сделает, вопрос будет заключаться лишь в материальных средствах и приложенных усилиях. Для того, чтобы максимально утруднить эту задачу необходимо знать базовые факторы:

1) Грамотно подходить к выбору ОС, ведь именно она является первоначальной ступенью, которая помогает выйти в социальную сеть. У каждой ОС есть свои минусы и плюсы, так, например, Windows логирует большинство приложений и просто

невозможно отследить то, что отправляется на сервера Microsoft. Именно поэтому касаемо данного критерия ОС Linux гораздо лучше, но у этой ОС тоже есть ряд недостатков, по которым она уступает Windows.

2) Следующей ступенью к обеспечению своей конфиденциальности является браузер, так как при поиске какой-либо информации пользователь оставляет цифровые отпечатки. Отпечатки представляют собой индивидуальную информацию о компьютере и включает в себя язык, используемый на данный момент, часовой пояс, расширения в браузере и даже размер дисплея. Большинство людей считают, что если они сменят IP-адрес, то это им поможет избежать цифровых отпечатков, однако это не так. Также, чем больше различных расширений установлено в браузере, чем больше он заполнен, установлена тема и т. п. тем больше вероятность выделиться на фоне остальных пользователей, тем проще идентифицировать того или иного пользователя. Рекомендуется отключить в настройках JavaScript, отключить сохранение cookies и кэша, а также использовать чистый браузер без различных поднастроек. На данный момент есть ряд определенных сайтов, на которых можно проверить, правильно ли он настроен для получения наибольшей защиты.

3) Установление защиты, данному пункту стоит уделять отдельное внимание, именно от этого в большинстве случаев зависит конфиденциальность данных. При регистрации рекомендуется устанавливать уникальный пароль, который никогда не использовался для регистрации другой сети, желательно каждый месяц в целях профилактики менять пароль во всех приложениях, в том числе и социальных сетях. Если существует возможность установить дополнительную защиту в виде аутентификация, желательно ей пользоваться, однако стоит не забывать, что и это помогает не во всех случаях.

4) В последние десятилетие в социальных сетях появилась тенденция выкладывать свои фотографии, рассказывать своей аудитории про различные хобби или привычки, показывать свои татуировки, все это привлекает различных взломщиков и мошенников, которые с определенным багажом информации смогут воспользоваться доверчивостью пользователей в корыстных целях. Для того, чтобы избежать всего этого рекомендуется как можно меньше рассказывать о своих увлечениях, также стараться не оставлять на странички фотки с различными татуировками, пирсингом и т.п., ведь с помощью этих фотографий можно с легкостью идентифицировать того или иного пользователя. Также многие думают, что если создать фейковый аккаунт, то можно оставаться анонимным и полностью защищенным, однако это не так, многие пользователи даже не знают о существовании метаданных, которые существуют во всех файлах в социальной сети, например с помощью фотографии возможно определить дату и время когда эта фотография была сделана, также можно определить место в котором была сделана фотография и с какого устройства она загружена. Рекомендуется перед выставлением фото и различных данных в социальную сеть или отправки друзьям очищать их от метаданных с помощью специальных приложений.

Таким образом можно сделать вывод о том, что социальные сети являются неотъемлемой частью жизни человека, они помогают пользователю поддерживать общение со своими родными и близкими, найти интересующую информацию, быстро обмениваться различными файлами, делиться с друзьями и аудиторией своей личной жизнью, взглядами, увлечениями. Однако не стоит забывать о факторах, которые помогут оставить конфиденциальную информацию в целости и сохранности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Кучерков И.А. О понятии "киберпреступление" в законодательстве и научной доктрине // Юридическая наука. 2019. №10. URL: https://cyberleninka.ru/article/n/o-ponyatii-kiberprestuplenie-v-zakonodatelstve-i-nauchnoy-doktrine (дата обращения: 16.12.2022).

УДК 323.2

Волкова Екатерина Александровна, аспирант, Московский информационно-технологический университет - Московский архитектурно-строительный институт.
Volkova Ekaterina Alexandrovna, graduate student, Moscow Information Technology University - Moscow Institute of Architecture and Civil Engineering.

ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ СОТРУДНИКОВ

THE RIGHT TO THE PRIVACY OF EMPLOYEES

Аннотация. Доклад посвящен актуальной сегодня теме неприкосновенности частной жизни сотрудников. С одной стороны, право на свободу личной жизни, закрепляемое в Конституции РФ, предоставляет возможность человеку самостоятельно управлять и контролировать содержание, объем опубликованной и передаваемой третьим лицам информации о нём. С другой стороны, ряд нормативно-правовых актов позволяют, а в отдельных случаях и обязывают контролировать сотрудников, в том числе с применением технических средств. Доклад раскрывает содержание понятия частной жизни на примере трудовых отношений, неразрывно связанных с личностью работника, а значит, и с информацией, подлежащей охране и защите. Автор стремится проследить, где проходит грань между частной жизнью работника и его рабочими обязанностями. В данном докладе рассмотрены ситуации, когда работодатель может столкнуться с личными данными сотрудников, являющихся элементом его частной жизни, проанализированы основные нормативно-правовые акты, регулирующие работу с персональными данными сотрудников.
Abstract. The report is devoted to the current topic of employee privacy. On the one hand, the right to freedom of personal life, enshrined in the Constitution of the Russian Federation, provides an opportunity for a person to independently manage and control the content, volume of information published and transmitted to third parties about him. On the other hand, a number of regulatory legal acts allow, and in some cases oblige, to monitor employees, including with the use of technical means. The report reveals the content of the concept of private life on the example of labor relations, inextricably linked with the personality of the employee, and therefore with the information subject to protection and protection. The author seeks to trace where the line between the private life of an employee and his work responsibilities lies. This report examines situations when an employer may encounter personal data of employees that are an element of his private life, analyzes the main regulatory legal acts regulating work with personal data of employees.
Ключевые слова: труд, трудовое право, частная жизнь, работодатель, персональные данные сотрудников.
Key words: labor, labor law, private life, employer, personal data of employees.

The right to freedom of personal life, enshrined in Article 23 of Part one of the Constitution of the Russian Federation, is the ability of a person to independently manage and control the content, volume of information published and transmitted to third parties about him.

The European Court of Human Rights in In the Resolution "R.G. and J.N. v. the UnitedKingdom" dated 25.01.2001 (§ 56-59) noted that personal life is a broad concept and does not have an exhaustive definition, and information such as telephone recordings, photographs, the image of a person, his reputation - all this, in accordance with The Convention on the Protection of Human Rights and Fundamental Freedoms, fall under the right to the protection of private life.

According to the Russian legal scholar Georgy Borisovich Romanovsky, as a category of law, private life unites all those spheres of life that are not professional and/or public. Shevchenko I.A. considers private life to be the freedom of a person's legal behavior and his thoughts in the intimate, personal, family and business spheres of his life. Despite the different interpretations of this concept, everyone is united in the fact that this is the sphere of human life that concerns only him and is not subject to external control.

The second article of the Constitution of the Russian Federation proclaims a person, his rights and freedoms as the main value. The rights enshrined in Articles 20-28 of the Constitution of the Russian Federation, including the right to privacy, are inalienable, belong to a person from birth and are fundamental, being the basis for the formation of other rights.

In particular, being one of the types of sectoral law, labor law directly regulates labor, as well as other related social relations. The relationship between the employee and the employer, establishing the rights and obligations for each party, is contractual in nature. Since they are inextricably linked with the identity of the employee, with information related to an individual, they are subject to protection and protection by the state.

In accordance with the Labor Code of the Russian Federation, the employee undertakes to independently perform labor functions for a fee determined by the contract and comply with the rules of internal labor regulations, and the employer undertakes to pay for the work and create the necessary working conditions by providing all the equipment, documentation, and tools necessary to perform labor duties. Obviously, the employee must use the entrusted equipment and technical means exclusively to fulfill his work duties. This, as a rule, establishes not only an employment contract, but also the rules of internal labor regulations or a collective agreement (if any), and any personal use can be interpreted as a violation of labor discipline. However, in practice, it happens that during working hours, employees log in from their work computer, for example, to social networks, online stores for online purchases and other information resources. This is especially often faced by employers whose employees work remotely (remotely).

Of course, in order to avoid this, as well as in order to ensure the technical protection of the confidentiality of information representing a commercial or official secret, the employer resorts to various technical means of controlling employees. The right to use such means is enshrined in part four of Article 10 of the Federal Law "On Trade Secrets".

However, in order for the control to be legal, it is necessary to determine the line between the employee's private life and his work duties. This is where the question of privacy arises.

On the one hand, the right to employer control over employees is enshrined in several articles of the Labor Code of the Russian Federation at once. For example, Part 1 of Article 15 of the Labor Code of the Russian Federation defines labor relations as an agreement based on an agreement between an employee and an employer on the personal performance by an employee for a fee of a labor function in the interests, under the management and control of the employer. A similar wording is contained in the definition of an employment contract in Article 56 of the Labor Code of the Russian Federation. Article 91 of the Labor Code of the Russian Federation defines that an employee is obliged to devote working time to the performance of labor duties, and the employer has the right to control the quantity and quality of work (paragraph one of Article 86 of the Labor Code of the Russian Federation). The place that is directly under the control of the employer, in accordance with Article 209 of the Labor Code of the Russian Federation is a working place, and the specification of the forms and purposes of such control falls within the competence of the employer. In addition, the organization has the right to perform any operations that do not contradict the law with respect to its equipment and other own assets (Article 209 of the Civil Code of the Russian Federation), for example, to introduce technical monitoring and observation systems.

On the other hand, an employee has the right to rely on the guarantees provided by the employer for the protection and protection of information about him, including those transmitted through mail messages, telephone conversations and messengers. You can receive and use this information only with the permission of the employee. This is directly stated in part 1 of Article 24 of the Constitution of the Russian Federation. Therefore, if there is such consent, the actions of the employer do not contradict the law.

As explained by the plenum of the Supreme Court of the Russian Federation in the adopted Resolution "On certain issues of judicial practice in cases of crimes against the constitutional rights and freedoms of man and citizen" No. 46 dated 12/25/2018, when deciding on the presence in the actions of a person of the corpus delicti associated with the violation of privacy, the court must establish whether it was covered by intent.

As judicial practice shows, the condition under which the employer has the right to check the employee's work correspondence, install cameras and control systems is the presence of a local regulatory act at the enterprise and the employee is familiar with it. In this case, if violations are detected, the employer has every reason to dismiss the employee in accordance with paragraph six of Article 81 of the Labor Code of the Russian Federation (Appeal ruling of the Moscow City Court of 28.01.2014 in case No. 33-5570/14).

A similar opinion is held by the European Court of Human Rights, having found no violations in the dismissal of an employee after the seizure of his work computer with documents and photos found in it for third parties. The ECHR noted that the employer lawfully and in order to protect his rights viewed the data on the employee's work computer, since he has the right to demand that employees use the provided technical means and equipment strictly in accordance with their work function and official duties provided for in the employment contract (Resolution "Liburtv. France" dated 22.02.2018).

However, the ECHR notes that in order to establish guarantees of human rights to privacy in the process of labor relations, it is necessary to comprehensively consider and evaluate a number of key factors:

– whether the employee was previously notified about the control systems used by the employer.

– the degree of control and interference of the employer in the personal space of the employee and the presence of legitimate reasons for this;

– the possibility of using a different, less aggressive control system, compared to viewing employee correspondence.

– the consequences of control for the employee and the established guarantees.

Let's consider another situation where an employer may encounter personal data of employees who are an element of his private life. For example, when an employer places employee data on its Internet resource (full name, photo, position, etc.), which is regarded as processing personal data affecting the business reputation of the employer and the employee himself. This is stated in paragraph 12 of the Review of the practice of consideration by courts of cases on disputes on the protection of honor, dignity and business reputation of the Presidium of the Supreme Court of the Russian Federation dated March 16, 2016.

In accordance with the Federal Law "On Amendments to the Federal Law "On Personal Data" dated 12/30/2020 No. 519-FZ, which entered into force on March 1, 2021, personal data allowed for distribution should be understood as the data that an employee of the company allowed the employer to publish on the website and transfer to third parties for processing.

In general, Federal Law No. 152-FZ of 27.07.2006 defines personal data as information directly or indirectly related to an individual and with which he can be identified. These include, for example, full name, education, place of work, family and social status, as well as other information by which you can recognize a person. The amendments introduced

from September 1, 2022 by Federal Law No. 266-FZ of 07/14/2022 establish the obligation for organizations and individual entrepreneurs to inform Roskomnadzor about the collection of personal data of employees. However, it should be borne in mind that the employee's consent to the publication of information about himself on the employer's website and the transfer of such information to third parties is necessarily made out in a separate document from other consents.

It is interesting to see the Resolution of the Constitutional Court of the Russian Federation No. 22-P dated 05/25/2021 "On the case of checking the constitutionality of paragraph 8 of Part 1 of Article 6 of the Federal Law "On Personal Data" at the request of a legal entity that is the editorial office of the mass media. According to the doctor's claim, the courts ordered the editorial office to delete the plaintiff's personal data from the Internet portal and compensate her for moral damage. The editorial board considered that the applied norm was unconstitutional and filed a complaint. However, the Constitutional Court of the Russian Federation recognized the norm as legitimate, indicating that data on a medical worker that had previously become available to an unlimited number of people and had a wide interest for others did not require his consent. However, upon termination of the employment contract, the employer's obligation to update the data posted on third-party websites follows. At the same time, the mass media is obliged to control judgments that are not related to professional activity, delete, modify or publish refutations.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Трудовой Кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 04.11.2022)

2. Федеральный закон «О персональных данных» №152-ФЗ от 27.07.2006.

3. Федеральный закон «О банках и банковской деятельности» №395-1 от 02.12.1990.

4. Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006.

5. Федеральный закон «О коммерческой тайне» №198-ФЗ от 29.07.2004.

6. Федеральный закон "О внесении изменений в Федеральный закон "О персональных данных" № 266-ФЗ от 14 июля 2022.

7. Федеральный закон «О внесении изменений в Федеральный закон «О персональных данных» № 519-ФЗ. от 30.12.2020.

8. Г.Ю. Мордохов. Ограничение права на неприкосновенность частной жизни и личности в ходе расследования уголовного дела. Диссертация. М., 2017.

9. С.С. Занковский. Проблемы развития и перспективы предпринимательского права в современных экономических условиях. Монография. М., 2019.

10. Р.М. Хазиев. Ограничение права на неприкосновенность частной жизни и личности в ходе расследования уголовного дела. Диссертация., Уфа, 2016.

11. Апелляционное определение Московского городского суда от 28.01.2014 по делу №33–5570/14

12. Постановление Конституционного Суда РФ от 25.05.2021 N 22-П "По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона "О персональных данных".

УДК 327

Гукало Екатерина Константиновна, студентка, Комсомольский-на-Амуре государственный университет
Gukalo Ekaterina Konstantinovna, student, Komsomolsk-na-Amure State University
Лопатина Ольга Ивановна, старший преподаватель, Комсомольский-на-Амуре государственный университет
Lopatina Olga Ivanovna, senior lecturer, Komsomolsk-on-Amur State University

ОТРАЖЕНИЕ ПРАВА НА ЧАСТНУЮ ЖИЗНЬ В ЗАКОНОДАТЕЛЬСТВЕ

IMPLEMENTATION OF THE RIGHT TO PRIVACY IN NATIONAL LEGISLATION

Аннотация. В данной статье сделаны попытки обобщить информацию о существовании законов, защищающих право на частную жизнь, отражение этих инструментов регулирования на цифровую среду. Помимо этого, были приведены примеры правомочного сбора личной информации и способы избежать кражи личных данных. Столкнувшись с неравномерным, а иногда и противоречивым правовым ландшафтом, наиболее эффективным ответом является расширение прав и возможностей человека.
Abstract. This article attempts to summarise the existence of laws protecting the right to privacy and the impact of these regulatory tools on the digital environment. In addition, examples of lawful collection of personal information and ways to avoid identity theft have been given. Faced with an uneven and sometimes contradictory legal landscape, the most effective response is human empowerment.
Ключевые слова: законодательство, защита данных, сбор информации, конфиденциальность.
Key words: Legislation, data protection, data collection, privacy.

В наше время, век, где главным ресурсом является информация, неприкосновенность частных лиц, то есть самых обычных граждан, очень важна. Но, к сожалению, сейчас законодательство защищает частных лиц от утечки информации или слежки со стороны правительства гораздо меньше, чем стоило бы. Существует множество ситуаций, когда различные правительства стран нарушали свои права по отношению к гражданам, проживающим на этой территории. Сейчас чрезвычайно важно вносить поправки в законодательство, связанное с неприкосновенностью данных и личной информации человека.

В то время как законодательство о защите данных потенциально может сократить спекулятивный сбор данных компаниями, законы о конфиденциальности данных недостаточно подходят для защиты частных лиц. Права в отношении автоматизированных технологий и неприкосновенности частной жизни слишком часто могут быть нарушены законами других стран.

В настоящее время в качестве реакции на террористические атаки в Европе на национальном уровне были введены расширенные полномочия по наблюдению, при этом большое количество данных передается через границы. Безопасность слишком часто упоминается в качестве причины ограничения использования технологий шифрования, или для создания ‘черных ходов’, которые, вероятно, будут способствовать вторжению в частную жизнь как со стороны правительства, так и со стороны других субъектов.

Уже раздаются голоса против тотальной слежки. Совет Европы призвал государства-члены воздерживаться от неизбирательной массовой цифровой слежки. В 2016 году Европейский суд по правам человека (ЕСПЧ) “вынес решение о тайной слежке по делу Сабо и Висси против Венгрии. Суд установил, что венгерское законодательство 2011 года о тайном наблюдении нарушило статью 8 ЕКПЧ, поскольку оно не для защиты от злоупотреблений” (Доклад об основных правах за 2017 год).

Ссылаясь на “Решение Суда Европейского Союза (CJEU) в цифровом Права Ирландии против Министра связи и других, ЕСПЧ заявил, что там, где национальные правила допускают крупномасштабный или стратегический перехват и где это вмешательство может привести к особо агрессивному вмешательству в частную жизнь”,“гарантии, требуемые существующей прецедентной практикой Конвенции о перехвате, должны быть усилены, чтобы решить проблема такой практики наблюдения” (Отчет об основных правах за 2017 год).

Что касается действующего законодательства, то даже в соответствии с Общим регламентом по защите данных правительства по–прежнему имеют достаточно оснований утверждать, что национальная безопасность – правильно это или неправильно - оправдывает посягательства на частную жизнь. Это не означает, что шаги по обеспечению того, чтобы фирмы и другие лица были более четко осведомлены о том, какую информацию они собирают и как она будет использоваться, не приветствуются, наряду с возможностью для граждан попросить посмотреть, какие данные хранятся, и чтобы они были удалены.

Тем не менее, столкнувшись с неравномерным, а иногда и противоречивым правовым ландшафтом, наиболее эффективным ответом является расширение прав и возможностей человека, предоставление ему знаний и инструментов, необходимых для того, чтобы заботиться о себе.

По моему мнению, каждый человек, работающий в какой-либо компании или дающий согласие на обработку данных, в праве знать и видеть, какую частную информацию о нём хранит правительство и организации во избежание неприятных ситуаций. Особенно каждый человек должен иметь право знать какая личная информация о нём передаётся через те или иные каналы. А всё потому, что любая несогласованная передача личной информации в наше время может выставить человека в плохом свете и разрушить его репутацию. И с нынешней скоростью распространения информации в Сети предотвратить последствия будет просто невозможно, что очень опасно.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Игумнов, Н. А. Толкование права на неприкосновенность частной жизни в условиях цифровизации (на основе практики Конституционного Суда Российской Федерации) / Н. А. Игумнов // Журнал Конституционного правосудия. – 2022. – № 3. – С. 34-38. – DOI 10.18572/2072-4144-2022-3-34-38. – EDN MWPOSO.

2 Ибрагимова, А. Н. г. Понятие персональных данных; информационная безопасность права на неприкосновенность частной жизни согласно анализу статьи 8 Европейской конвенции по правам человека / А. Н. г. Ибрагимова // Северо-Кавказский юридический вестник. – 2021. – № 4. – С. 92-103. – DOI 10.22394/2074-7306-2021-1-4-92-103. – EDN EQMRVA.

УДК 327

Гурский Семен Евгеньевич, студент, Комсомольский-на-Амуре государственный университет
Gursky Semyon Evgenievich, student, Komsomolsk-na-Amure State University
Лопатина Ольга Ивановна, старший преподаватель, Комсомольский-на-Амуре государственный университет
Lopatina Olga Ivanovna, senior lecturer, Komsomolsk-on-Amur State University

НЕПРИКОСНОВЕННОСТЬ ЛИЧНЫХ ДАННЫХ В ВЕК ЦИФРОВЫХ ТЕХНОЛОГИЙ

INVIOLABILITY OF PERSONAL DATA IN THE DIGITAL AGE

Аннотация. Цель статьи рассмотреть развитие современного информационного общества на основе растущей информатизации социальных процессов и систематизировать основные вызовы для приватности и защиты персональных данных пользователей. В связи с этим сделан краткий обзор особенностей цифровой эпохи на основе основных вопросов конфиденциальности и рассмотрены возможные проблемы для персональных данных.
Abstract. The aim of the article is to review the development of the contemporary information society based on growing informatization of social processes and to systematize the main challenges for user's privacy and personal data protection. In this reason a brief overview of features of digital age based on the main privacy issues is made and the possible problems for the personal data are discussed.
Ключевые слова: информационные ресурсы, цифровизация, защита данных, конфиденциальность, безопасность.
Key words: information resources, digitalization, data protection, privacy, security.

Постоянный рост применения информационно-коммуникационных технологий (ИКТ) в современных социальных процессах влияет на развитие информационного общества и определяет необходимость знания их особенностей и возможностей, а также влияния на частную жизнь. Одной из тем для обсуждения в цифровую эпоху является уровень компетентности пользователей цифровых услуг в сетевом пространстве и их цифровая грамотность. Это связано с информатизацией общества, которая создает основу информационного общества и представляет собой непрерывный процесс социально-экономического и научно-технического развития социальной информационной среды. Цель - создание возможностей для удовлетворения информационных потребностей людей в реализации прав граждан, органов власти и организаций. Для этого необходимо обеспечить адекватную защиту персональных данных (ПДн), как для пользователей, использующих ИКТ, например, социальные сети, так и для передачи, хранения или удаленного доступа к распределенным информационным ресурсам в глобальном цифровом пространстве, в том числе в облаке.

Конфиденциальность - это фундаментальное право человека, признанное во многих международных соглашениях и документах, однако важным вопросом является "Что такое конфиденциальность?". Объем и содержание этого понятия могут определяться исходя из национальной культуры и индивидуальных особенностей населения, но есть и общие моменты, такие как неприкосновенность личной информации и ее защита (доступ, использование, распространение, передача и т.д.).

Защита персональных данных (ЗПД) - это право, которое определяется отношениями между человеком и обществом, включая государственные учреждения, компании и другие организации, и напрямую связано с неприкосновенностью частной жизни.

Хартия основных прав Европейского Союза (ХОП), которая стала обязательной к исполнению 1 декабря 2009 года, признает право на неприкосновенность частной жизни в статье 7 и право на защиту персональных данных в статье 8. Кроме того, статья 8 подтверждает принцип, согласно которому персональные данные должны обрабатываться справедливо и для конкретных целей на основе согласия соответствующего лица или для других законных целей, определенных законом.

Реальное начало развития европейской правовой базы по защите данных началось с принятия первого закона о ПДП в земле Гессен в Федеративной Республике Германия (1970), за которым последовали национальные законы Швеции (1973), Германии (1977) и Франции (1978), в 1979 году и в Австрии, Дании, Люксембурге, Норвегии. Испания, Португалия и Австрия включили принципы НДП в свои конституции в качестве основных прав человека. В США принят федеральный закон о неприкосновенности частной жизни, который регулирует "сбор, хранение, использование и распространение информации о частных лицах, которая хранится в системах записей федеральных агентств" и устанавливает конкретные требования к публикации и раскрытию таких данных.

В 1980-х и 1990-х годах нынешняя правовая база НДП для Европы была создана путем разработки рекомендаций по трансграничному потоку доступных данных (1980), учредительной Конвенции 108 Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных, Директивы 95/46/ЕС о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных (1995), Директивы 97/66/ЕС об обработке персональных данных и защите частной жизни в телекоммуникационном секторе (1997).

В XXI веке определяются основные стандарты PDP и законодательная база ЕС, основными документами которой являются Директива 2000/31/ЕС по электронной коммерции, Директива ePrivacy 2002/58/ЕС, Директива 2006/24/ЕС по защите данных трафика при предоставлении общедоступных услуг электронных коммуникаций или сетей связи общего пользования, Директива 2009/136/ЕС по универсальному обслуживанию прав потребителей, относящихся к сетям и услугам электронных коммуникаций.

В современном цифровом мире глобальные коммуникации широко используются для удаленного доступа к информационным ресурсам, веб-сайтам, виртуальным пространствам, дискуссионным и социальным форумам и многому другому. Таким образом, любой пользователь сетевых коммуникаций может свободно "пересекать государственные границы" и получать доступ к удаленным объектам в сетевом пространстве. Основная часть проблем информационной безопасности в сетевом мире может быть связана с нарушением цифровой конфиденциальности (e-privacy), поскольку различные среды в глобальной сети требуют предварительной регистрации пользователей путем предоставления категорий персональных данных, не имеющих прямого отношения к указанной цели. В результате опроса граждан ЕС 74% из них считают, что разглашение персональных данных является существующей проблемой в современном цифровом мире, а еще 84% заявили, что глобальная сеть требует слишком много персональных данных, которые не соответствуют поставленной цели. В то же время 72% пользователей сети опасаются, что они не имеют полного контроля над своими данными. Известно, что некоторые пользователи соглашаются с политикой конфиденциальности, проводимой соответствующим сетевым пространством, не осознавая этого. В некоторых случаях информация об этой политике не предоставляется, или же при регистрации требуется предоставить личную информацию, не имея представления о том, как она будет обрабатываться. В большинстве случаев у пользователей нет другого выбора, кроме как предоставить запрашиваемые личные данные, если они хотят получить доступ к выбранному сетевому пространству.

Вопросы конфиденциальности и ПДП пользователей в глобальной сети широко обсуждаются на различных форумах и институтами на европейском и мировом уровне. Ключевым элементом цифрового пространства является обслуживание веб-сайтов, поскольку важным требованием является то, что опубликованная на них информация должна быть правильной, достоверной и что при общении с пользователями и сборе их персональных данных принимаются необходимые меры защиты. За это отвечает владелец сайта, который должен обеспечить приведение публикуемой информации в соответствие с требованиями нового регламента. Причина этого заключается в том, что данная информация является общедоступной и в определенных случаях может привести к риску для владельцев этих персональных данных (телефон, адрес, фотографии, резюме, финансовые документы и т.д.) с нежелательными финансовыми и психологическими последствиями, а также последствиями для репутации.

Публикуемая информация в сети, в т.ч. в социальных сетях, центрах обработки данных в облаке, а также при построении гетерогенных сред для дистанционного и электронного обучения, должна соответствовать требованиям законной и корректной обработки персональных данных, информация должна быть достаточной и соответствующей цели, иметь четкое согласие лица, являющегося владельцем для своих персональных данных. Одним из обязательных требований GDPR является "право быть забытым / стертым", которое устанавливает право субъекта данных требовать исправления, удаления или блокирования неверных данных, а также требовать удаления ссылок на персональные данные, если информация является неточной, неадекватной, неуместной или чрезмерной для целей обработки данных.

Облачные вычисления (Cloud Computing, CC) - это технология распределенной среды подключенных и виртуальных компьютеров для предоставления компьютерных ресурсов и услуг на договорной основе между клиентом и провайдером. Она основана на многократном найме, что вместе с поддержанием копий данных в разных узлах сети создает возможные риски для конфиденциальности информации. Это устанавливает основное требование к обеспечению надежной информационной безопасности путем предоставления доступа только уполномоченным лицам. Принцип множественного найма может привести к нарушению целостности информации и создать риск нарушения целостности (преднамеренного или непреднамеренного) и доступности поддерживаемых данных, включая персональные данные (удаление, изменение, кража). С другой стороны, так называемые остаточные данные (не удаленные данные в узлах сети) являются явным нарушением "права быть забытым / стертым".

В бизнесе используется подход "единого входа" (SSO) для интеграции производственных каталогов, при этом большинство систем прямой связи также интегрируют аутентификацию с существующими производственными системами, что создает риск для информации, хранящейся при доступе. Другой применяемый подход - "share link", который удобен для обмена данными с различными деловыми партнерами, но не является безопасным, поскольку создает условия для нарушения безопасности системы и утечки данных в неавторизованный домен. Все это требует обеспечения конфиденциальности программного обеспечения, чтобы гарантировать, что каждое приложение или процесс будет обрабатывать и хранить информацию безопасным и надежным образом.

Аналогичные риски существуют и при использовании Интернета вещей (IoT), основанного на наличии множества объектов и устройств, которые подключены к Интернету и могут отправлять и получать данные. Для этого устройства и объекты оснащаются датчиками для измерения параметров и мониторинга их значений с целью управления процессами на уровне дома, города, состояния здоровья людей и т.д. В связи с этим IoT (через подключенные устройства) создает потенциальные возможности для нарушения приватности пользователя, так как относительно независимая связь устройств с Интернетом нарушает конфиденциальность собираемых данных, а без-

опасность в IoT является проблемой, так как зачастую настройка устройств происходит с помощью "слабых" или стандартных паролей.

Нельзя отрицать высокую эффективность цифровизации общества, не только с применением рассмотренных выше технологий, но и в области электронного правительства, электронного обучения, а также с предложением многих электронных услуг (электронный банкинг, электронный бизнес, электронное голосование и т.д.). Однако необходимо также проанализировать возможные проблемы, которые могут привести к нежелательным последствиям для участников цифрового мира, чтобы последние могли знать о них и принять необходимые меры предосторожности для защиты своей частной жизни и личности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Romansky, R. Technological Organization of the Access Management to Information Resources in a Combined e-Learning Environment. International Journal on Information Technologies and Security, ISSN 1313-8251, Vol. 11, No. 4, 2019, pp. 51-62..

2 Romansky, R. Informatization of the Sciety in the Digital Age. Biomedical Journal of Scientific & Technical Research, ISSN 2574-1241, Vol, 33, No.3, 2021, pp.25902-25910. DOI: 10.26717/BJSTR.2021.33.005418

УДК 342.7:004.9

Дель Дарья Станиславовна, студент, Комсомольский-на-Амуре государственный университет
Del Daria Stanislavovna, student of Komsomolsk-on-Amur State University
Казакова Ангелина Игоревна, студент, Комсомольский-на-Амуре государственный университет
Kazakova Angelina Igorevna, student of Komsomolsk-on-Amur State University
Непочатова Валерия Михайловна, старший преподаватель кафедры «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Nepochatova Valeria Mikhailovna, Senior Lecturer at the Department of “Linguistics and Intercultural Communication” of Komsomolsk-on-Amur State University

ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ В ВЕК ЦИФРОВИЗАЦИИ

THE RIGHT TO PRIVACY IN THE DIGITAL AGE

Аннотация. В статье анализируются теоретические и практические аспекты права на неприкосновенность частной жизни в условиях современных цифровизаций. С распространением digital-технологий вопрос о защите персональных данных имеет большое значение в контексте развития и реализации основных прав человека - приватности. Исследование показало, что большинство людей не знают о своих правах на неприкосновенность частной жизни и подвергаются к рассекречиванию своей личной конфиденциальности.

Abstract. The article analyzes the theoretical and practical aspects of the right to privacy in the conditions of modern digitalization. With the spread of digital technologies, the issue of personal data protection is of great importance in the context of the development and implementation of basic human rights - privacy. The study showed that most people are unaware of their privacy rights and are exposed to declassification of their personal privacy.

Ключевые слова: приватность, интернет, цифровые технологии, личные данные, частная жизнь, право на уважение частной жизни.

Key words: privacy, internet, digital technologies, personal data, privacy, privacy rights.

В современном мире цифровых технологий очень важна защита информации в интернете, поскольку каждый человек имеет полное право на неприкосновенность частной жизни и в том числе чувствовать себя защищённым.

Внедрение цифровых технологий в частную жизнь не гарантирует обеспечение безопасности. Таким образом, государство должно обеспечить правовую защиту частной жизни. Статья 23 конституции Российской Федерации гарантирует право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени [3].

В данной статье приводятся реальные примеры из жизни людей, которые сталкивались с посягательством на неприкосновенность их частной жизни.

Рассмотрим первый случай. На электронную почту студенту каждую неделю приходили письма о налоговой задолженности, и он, не проверив, перешел по прикрепленной ссылке и оплатил долг в 986 рублей. Но как выяснилось позднее это оказалась мошенническая схема и задолженность отсутствовала. К тому же он кликнул по нежелательной ссылке, и его почта была взломана. О сложившейся ситуации он рассказал преподавателю по правоведению, и тот осведомил, что все налоговые задолженности можно отследить на портале Госуслуги РФ (Рисунок 1). А на почту посоветовал поставить двухфакторную аутентификацию, чтобы получить доступ к личным данным было сложнее.

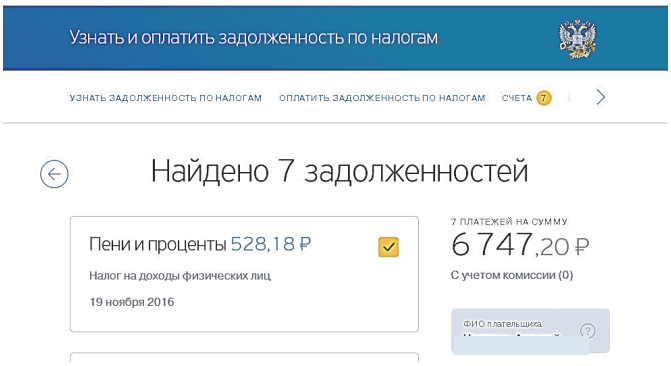

Рисунок 1 – Задолженность на портале Госуслуги РФ

Этот пример наглядно иллюстрирует, что личными данными могут воспользоваться в корыстных целях злоумышленники. Личная информация не всегда может оставаться конфиденциальной. Когда мы соглашаемся на обработку персональных данных, есть риск того, что в будущем они (электронная почта и номер) могут находиться в интернете.

Следующий пример демонстрирует то, как Яндекс компания столкнулась с утечкой личных данных клиентов и не смогла это предотвратить [4]. Популярный сервис по доставке еды и продуктов Яндекс Еда в марте 2022 года столкнулся с утечкой данных о заказах клиентов (Рисунок 2).

Утечка персональных данных - одна из важнейших проблем в области прав граждан в цифровом мире, и они приняли массовый характер [1]. Этот пример показывает, что крупным компаниям стоит вкладывать больше ресурсов в контроль за личными данными клиентов, а органам по надзору в сфере связи, информационных технологий и массовых коммуникаций усилить контрольно-надзорные функции.

А именно:

1. Введение на государственном уровне жестких правил о контроле, и плана, которому компании должны следовать.
2. Проведение систематических проверок с последующими штрафами и наказаниями [2, с. 20].

Рисунок 2 – Утечка данных

Зачастую большинство подростков сталкиваются с тем, когда в сети интернет находят свои личные фотографии, которые были выложены без разрешения, еще хуже, когда снимки блуждают у их знакомых, друзей, одноклассников. Несовершеннолетние дети не знают, как поступать в сложившихся ситуациях, так как они не информированы начёт конфиденциальности частной жизни.

Например, подросток Ю. скинула личную фотографию своей подруге С., ссылаясь на то, чтобы та никому не показывала. Зная, что между Ю. и С. договоренность, школьница даже не подозревала, что ее снимки разлетятся почти по всей школе и каждый старшеклассник при виде героини Ю. будет смеяться над ней и дразнить. После этого инцидента у Ю. появились комплексы насчет своей фигуры, она не любит себя и свое тело, начала его менять, морить себя голодом, пить различные таблетки, впоследствии отправилась на сеанс к психологу, где обрела безуспешный опыт и множество психологических травм. Тогда она не знала, что имеет право на конфиденциальность и неприкосновенность своей частной жизни, поэтому бездействовала.

Этот пример ярко показывает, что любой человек, вне зависимости от возраста, может подвергнуться незаконному посягательству на конфиденциальность личной жизни, а также, что не информированность о правах граждан приводит к отрицательным последствиям.

На сегодняшний день существуют множество исследований в данной области, однако не все направлены на меры пресечения, которые будут призывать стимулировать знания своих прав, а также за рассекречивание конфиденциальности.

Нужно внедрять следующие меры, чтобы таких ситуаций было меньше:

1. Необходимо ввести дополнительный предмет в школе для того, чтобы дети владели информацией, например, как в современном digital мире защитить свои данные и какой закон руководствуется защитой персональных данных.
2. Для компаний усилить контрольно-надзорные функции, то есть систематично проводить проверки с последующими штрафами и ввести план, которому должны будут следовать компании.
3. Для того, чтобы никто не смог узнать вашу электронную почту и номер, стоит внимательно разузнать информацию о компании, которая запрашивает обработку ваших персональных данных и, соответственно, прочитать положение, которое прикрепляют компании, необходимо ознакомиться с журналом посещений вашего почтового сервиса, установите двухфакторную аутентификацию, чтобы в будущем не пришлось долгое время восстанавливать взломанный электронный почтовый ящик, необходимо следовать всем рекомендациям в области кибербезопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ
1. Зорькин, В. Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума // Российская газета. 2018. № 7578 (115). URL: https://rg.ru/2018/05/29/zorkin-zadacha-gosudarstva-priznavat-i-zashchishchat-cifrovye-prava-grazhdan.html (дата обращения: 11.11.2022).
2. Карцхия А.А. Цифровой императив: новые технологии создают новую реальность // ИС. Авторское право и смежные права. 2017. № 8. С. 17-25.
3. Права и свободы человека и гражданина // Пенсионный фонд Российской Федерации. URL: https://pfr.gov.ru/order/konstituciya/~4846 (дата обращения 11.11.2022).
4. «Яндекс» сообщил об утечке данных пользователей «Яндекс.Еды» // Forbes. URL: https://www.forbes.ru/tekhnologii/457605-andeks-soobsil-ob-utecke-dannyh-polzovatelej-andeks-edy (дата обращения: 11.11.2022).

УДК 327

Дуденко Богдан Сергеевич, студент, Комсомольский-на-Амуре государственный университет
Dudenko Bogdan Sergeyevich, student, Komsomolsk-na-Amure State University
Лопатина Ольга Ивановна, старший преподаватель, Комсомольский-на-Амуре государственный университет
Lopatina Olga Ivanovna, senior lecturer, Komsomolsk-on-Amur State University

ИСТОРИЧЕСКИЕ ПРЕДПОСЫЛКИ КРАЖИ ЛИЧНОЙ ИНФОРМАЦИИ

HISTORICAL BACKGROUND TO IDENTITY THEFT

Аннотация. В данном докладе сделаны попытки проследить хронологию возникновения кражи личной информации. Такие действия имели место еще до нашей эры, хоть и носили отличный от современного характер. С возникновением виртуального пространства эти действия были перенесены человечеством в него. В статье перечислены основные формы регулирования личной информации и меры наказания за ее кражу.
Abstract. This report attempts to trace the chronology of identity theft. Such activities took place before our era, albeit of a different nature than today. With the emergence of virtual space, these actions have been carried over into virtual space. The article lists the main forms of regulating personal information and the penalties for stealing it.
Ключевые слова: право на частную жизнь, кража личности, цифровизация, контроль над распространением информации.
Key words: right to privacy, identity theft, digitalisation, information dissemination controls.

Введение. Две трети утечек информации происходят не в силу злого умысла. В остальных случаях это намеренные действия киберпреступников, сотрудников организации или ее подрядчиков. Однако краж личной информации появилась не только в современное время. Так в одной из притч сказано: «Когда Исаак, второй из патриархов Израиля, стал стар и немощен, он подозвал к себе своего старшего сына, Исава, и сказал: «Пойди на охоту, налови мне дичи, приготовь мое любимое блюдо, и перед самой смертью я благословлю тебя, и все, что было моим, станет твоим».

Об этом узнала его жена, Ревекка, и сказала своему младшему сыну, Иакову, самому наловить дичи и, выдав себя за брата, получить благословение и наследство самому. Так он и сделал.

Пока Исав был на охоте, Иаков взял из ближайшего загона двух козлят, приготовил их и подал отцу. Воспользовавшись плохим зрением отца, он выдал себя за старшего брата, обманом присвоил себе его первородство и стал третьим патриархом Израиля.

И пусть за тысячу лет до нашей эры Иакову и удалось обойти систему, в XXI веке ему пришлось бы сильно постараться, чтобы повторить подобное».

Кража личности

Схема, которую Иаков ловко провернул в Ветхом завете, в наше время называют кражей личности.

Впервые этот термин появился в 1964 году в США, в связи с взлетом популярности услуг, предоставляемых удаленно, без личного присутствия. Злоумышленники крали персональные данные жертв, включая SSN (Social Security number) широко распространенный способ идентификации личности. В частности, выпуска кредитных карт и получения кредитов.

Для подтверждения личности по телефону организациям достаточно было знать имя, адрес и номер SSN, которые можно было найти либо на выброшенных чеках, либо получить на черном рынке за 30 долларов.

С тех пор, прошло полвека, мошенники из рытья в мусорных баках перешли на рытьё данных в интернете, что сильно упростило им задачу по хищению персональных данных.

Однако и технологии по защите этих самых персональных данных не стояли на месте.

Персональные данные и Роскомнадзор

Согласно Федеральному закону Российской федерации 152-ФЗ "О персональных данных", Персональные данные - любая информация, позволяющая как точно идентифицировать физическое лицо, так и составить о нём чёткий образ или предположить, что в конкретном случае речь идёт именно об определенном человеке, а не о каком-либо абстрактном.

К персональным данным относят:

- ФИО;
- Дата и место рождения;
- адрес проживания и регистрации;
- образование, доход, профессия;
- паспортные данные, ИНН, СНИЛС;
- семейное, социальное или имущественное положение.
- номер телефона
- адрес электронной почты.

Важно понимать, что перечисленные данные являются едва ли не общедоступными, но это не значит, что к их распространению можно относиться халатно.

Каждый раз, покупая что-либо в интернет-магазинах или заказывая еду на дом, вы подвергаете себя риску, пусть и незначительному.

Публикация персональных данных в общем доступе осуществляется только с письменного согласия их владельца (субъекта персональных данных). В любое время субъект может отозвать свое согласие на публикацию и требовать их немедленного удаления из общего доступа.

Гражданин сам несет ответственность за публикацию своих данных, будь то запись на прием к врачу или заказ еды на дом. Однако надзор за любыми операциями с персональными данными граждан осуществляет Роскомнадзор.

В современном инфополе, о Росомнадзоре [1] сложилось не самое лучшее мнение. У молодежи деятельность организации вызывает смех и сочувствие, с их беско-

нечными попытками блокировать то, что нельзя заблокировать. Но их настоящую пользу отрицать невозможно.

Роскомнадзор контролирует деятельность организаций по вопросам работы юридических и физических лиц с персональными данными граждан, проводит проверки, как по жалобам заявителей или по собственной инициативе и, если находит нарушения, привлекает представителей организаций к административной или вовсе прекращает деятельность компании.

И если публикация личных данных произошла без согласия их владельца, то он вправе обратиться в судебные и правоохранительные органы с целью привлечения виновных лиц к предусмотренной законом ответственности.

И поэтому, наиболее уязвимым аспектом общественной жизни гражданина Российской Федерации является как раз тот, в работе которого сотрудники Роскомнадзора разбираются меньше всего - интернет.

Вторжение в частную жизнь и чем это грозит

Статья 23 конституции Российской федерации гласит, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Так же, каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (только если этого не требует суд.)

Статья предполагает запрет любых форм произвольного вмешательства в частную жизнь со стороны государства и гарантирует защиту от такого вмешательства третьих лиц. путем установления уголовной ответственности за нарушение этих прав в нормах, описанной в статье 137 Уголовного кодекса Российской Федерации [2].

За сбор или распространение каким-либо способом сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия, то вас ждет уголовная ответственность в виде штрафа в размере до трехсот пятидесяти тысяч рублей, лишение права занимать определенные должности или заниматься определенной деятельностью на срок до шести лет, лишение свободы на срок до пяти лет.

Вернее, могла бы ждать, если бы вы сами не содействовали раскрытию своих тайн.

Невидимая рука рынка

В мире цифровых технологий и глобализации, человек рассматривается как потребитель. Поэтому, сохранность тайн и персональных данных интересует невидимую руку рынка меньше всего.

Ни для кого не будет откровением, что крупные корпорации используют данные своих пользователей, и даже не скрывают это. Например, популярная социальная сеть Тик ток постоянно считывает данные о местоположении и истории поиска пользователей и отправляет их в Китай. Условия использования персональных данных написаны в пользовательских соглашениях, которое все равно никто не читает.

Эти данные используются для продвижения рекламы и составления рекомендаций, но точно неизвестно, для чего ещё.

Причин для паники и паранойи нет, но всегда важно знать, что теперь человек всегда у всех на виду и соблюдать осторожность.

Иаков прожил под чужим первородством более ста лет, и в наше время преступники так же часто остаются безнаказанными.

Заключение. Кража данных может привести не только к серьезным убыткам и потере репутации, но и к многомиллионным штрафам, как это было в случаях с известными корпароциями.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Дорожкин, М. А. Деятельность Роскомнадзора в современном обществе / М. А. Дорожкин, Ю. М. Коплович // Инновационные решения социальных, экономических и технологических проблем современного общества : Сборник научных статей по итогам круг-

лого стола со всероссийским и международным участием, Москва, 15-16 мая 2021 года. – Москва: Общество с ограниченной ответственностью "КОНВЕРТ", 2021. – С. 199-200.

2 Колобов, А. Н. Система интернет-регулирования в Российской Федерации / А. Н. Колобов // Форум молодых ученых. – 2018. – № 6-2(22). – С. 228-230. – EDN YLPZCX.

УДК 327

Захаров Данил Александрович, студент, Комсомольский-на-Амуре государственный университет
Zakharov Danil Alexandrovich, student of Komsomolsk-na-Amure State University
Мусалитина Евгения Александровна, кандидат культурологии, доцент кафедры «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Musalitina Evgenia Aleksandrovna, PhD in Culture Studies, Assistant Professor, «Linguistics and Cross-Culture Communication Department», Komsomolsk-na-Amure State University

ВЛИЯНИЕ КИБЕРШПИОНАЖА НА ЧАСТНУЮ ЖИЗНЬ

IMPACT OF CYBERSPIONAGE ON PRIVATE LIFE

Аннотация. В современном обществе в условиях повсеместной компьютеризации стремительно развиваются информационные технологии, затрагивающие практически все сферы жизни. Особую актуальность эти технологии приобрели в сфере бизнеса, в сфере услуг и продаж товаров широкого потребления. Для развития предприятия необходима реклама, которая стала массовой в сети Интернет. В настоящее время реклама часто сопровождается «коммерческой прослушкой», что нарушает права на неприкосновенность частной жизни. В статье рассматривается проблема кибершпионажа в процессе развития информационных технологий.
Abstract. In modern society, in the context of widespread digitalization information technologies are rapidly developing, affecting almost all spheres of life. These technologies have gained particular relevance in the business sector, in the service sector and in the sale of consumer goods. For the development of the enterprise, advertising is necessary, which has become massive on the Internet. Nowadays, advertising is often accompanied by "commercial wiretapping" which violates the right to privacy. The article deals with the problem of cyber espionage with the help of information technology. The article deals with the problem of surveillance of users using information technologies.
Ключевые слова: контекстная реклама, кибершпионаж, информационные технологии, неприкосновенность частной жизни.
Key words: contextual advertising, cyber espionage, information technology, privacy.

Пользователи мобильных устройств отмечают, что информация, которую они запрашивают с помощью поисковых систем или в устной беседе в скором времени появляется во всплывающей рекламе. Также, занимаясь самостоятельным изучением иностранного языка, можно обнаружить, что появляется реклама услуг репетиторов. В следствие этого, возникает предположение, что мобильный телефон или планшет может выполнять функцию слежения. В век информационных технологий цифровые устройства незаменимыми устройствами для выполнения многих задач, но, одновременно, они передают личную информацию о пользователе третьим заинтересованным лицам. Несмотря на та, что такая функция смартфонов могла показаться нереальной еще несколько лет назад, в настоящее время она прочно вошла в жизнь абонентов [4].

Помимо внедрения рекламы, отобранной с помощью прослушивания гаджетов, появилась реклама, основанная на активном использовании сети Интернет. Одним из видов такой рекламы является контекстная реклама. Она включает два вида – поисковая контекстная реклама и тематические объявления.

Обратимся к рассмотрению контекстной рекламы. Поисковая контекстная реклама включает текстовую рекламу, баннеры, видеорекламу или короткие ролики (длительностью до 10 секунд), появляющуюся в верхних строчках результатов поискового запроса. Такой вид контекстной рекламы существует в виде гиперссылки, предназначенной для направления пользователя на рекламируемый сайт или коммерческое сообщество той или иной социальной сети. Реклама наиболее актуальных для пользователя услуг или товаров (на основе степени частотности соответствующих запросов) занимает первую строчку в результатах поиска.

Тематические контекстные объявления появляются при открытии любого сайта если его тематика соответствует анализируемым системой интересам пользователя. Это выявляется по поисковым запросам или посещениям иных сайтов и определяется специальными файлами, остающимися на устройстве пользователя при работе в сети Интернет [5].

Другой способ для системы получить конфиденциальную информацию о пользователе заключается в предоставлении такого рода информации самим пользователем. Например, многие приложения или социальные сети запрашивают доступ к хранилищу фотографий для их публикации, или доступ к геолокации при использовании интерактивной карты, а голосовые помощники просят предоставить доступ к микрофону. При этом, работа этих приложений может осуществляться и без доступа к подобного рода данным [2].

В настоящее время специалисты по информационной безопасности выделяют следующие технологии слежки за пользователями:

1. «Суперкуки» (SuperCookies). В браузерах существует уязвимость, с помощью которой владельцы сайтов получают возможность шпионить за посетителями. Такой уязвимостью являются «суперкуки» – это небольшие файлы, остающиеся на устройстве после посещения того или иного сайта. При возвращении на электронный ресурс, «суперкуки» распознают ваш гаджет, что позволяют загружать страницу быстрее. Также через такие файлы можно увидеть документы и изображения, просмотренные пользователем. При этом, защититься от такой слежки практически невозможно, поскольку «суперкуки» не хранятся на вашем компьютере или смартфоне и самостоятельно их удалить не представляется возможным. Как правило, пользователи не придают значения этому факту до тех пор, пока не происходит утечки их персональных данных внимания, до тех пор, пока данные не попадают в руки злоумышленников.

2. Технология «Фингерпринтинг» (Fingerprinting) известная также как цифровой отпечаток браузера и представляющая собой еще один способ слежки. Принцип ее работы заключается в том, что при посещении сайта каждому пользователю присваивается уникальный идентификатор. В нем содержатся все данные о настройках браузера конкретного пользователя. Например, владелец ресурса может распознать операционную систему, используемый язык, часовой пояс и даже историю браузера. Принцип действия схож с работой правоохранительных органов по снятию отпечатков пальцев. Полная защита от такой слежки также невозможна, но при использовании браузеров с повышенной конфиденциальностью передается намного меньше сведений.

3. Технология «Кликстрим» (Clickstream). Такая технология следит за действиями человека на сайтах и анализирует его маршрут в Интернете [6].

Очевидно, что подобная слежка в рекламных целях может оказать весьма негативное влияние на конфиденциальность персональных данных. При этом современные технологии не позволяют с уверенностью утверждать, что персональные данные защи-

щены. Утечки происходят регулярно у провайдеров разных компаний. В связи с этим, пользователем стоит ограничить доступную личную информацию в сети [3].

Рассматривая проблему защиты прав человека на неприкосновенность личных данных в условиях стремительного развития цифровизации всех сфер жизни общества, необходимо упомянуть так называемый «общественный договор». Этот документ регламентирует то, как правовое государство обязано обеспечивать граждан правами и свободами, в том числе и в киберпространстве. Этот «договор» закреплен в основном законе страны – Конституции [1]. Таким образом, в условиях роста утечки персональной информации, отслеживания действий и общения пользователей в сети, государство постоянно совершенствует методы регулирования сохранности персональной информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Байрамбекова А. Н. Правовые аспекты информационной безопасности в РФ / А. Н. Байрамбекова // Cognitio Rerum. – 2020. – № 12. – С. 18-23.

2. Жабин Д. Р. Практические аспекты реализации цифровых прав и их защиты / Д. Р. Жабин // Вопросы устойчивого развития общества. – 2022. – № 8. – С. 435-442.

3. Колосова И. А. Контекстная реклама как один из эффективных современных каналов рекламы / И. А. Колосова // Актуальные проблемы и перспективы развития экономики: российский и зарубежный опыт. – 2019. – № 20. – С. 79-83.

4. Лапин Р. Д. Массовая коммерческая прослушка телефонов / Р. Д. Лапин // Молодой ученый. – 2020. – № 9(299). – С. 17-19.

5. Лужнова Н. В. Процесс разработки контекстной рекламы как инструмент продвижения цифрового маркетинга / Н. В. Лужнова, О. М. Калиева // Вестник Самарского муниципального института управления. – 2022. – № 1. – С. 26-35.

6. Попова Л. Ю. Современные технологии интернет-продвижения (SEO-оптимизация, контекстная и баннерная реклама, контент- и видеомаркетинг, таргетинг в социальных сетях и др.) / Л. Ю. Попова // Аспирант. – 2022. – № 3(71). – С. 16-20.

УДК 004.048

Ильченко Валерий Юрьевич, студент Комсомольский-на-Амуре государственный университет
Ilchenko Valery Yuryevich, student of Komsomolsk-na-Amure State University
Климова Екатерина Викторовна, старший преподаватель, Комсомольский-на-Амуре государственный университет
Klimova Ekaterina Viktorovna, senior lecturer of Komsomolsk-na-Amure State University

КОНФИДЕНЦИАЛЬНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ

PRIVACY IN SOCIAL NETWORKS

Аннотация. В настоящее время обмен информацией через социальные сети стал повседневным элементом в жизни каждого человека. Во время обмена, к сожалению, мы сами не задумываясь, передаем сведения о нас через социальные сети. В данной статье мы рассмотрим пути воздействия социальных сетей на жизнь, и их конфиденциальности.
Abstract. Currently, the exchange of information through social networks has become an everyday element in everyone's life. During the exchange, unfortunately, we ourselves do not hesitate to transmit information about us through social networks. In this article, we will look at the ways social networks affect life, and their privacy.

Ключевые слова: социальная сеть, корпорация, личные данные, шифрование, конфиденциальность.
Key words: social network, corporation, personal data, encryption, privacy.

A social network is an interactive multi–user website, the information of which is filled in by the network participants themselves. The site is an automated social environment that allows people united by common interests to communicate. Communication between the subjects takes place through a web service of internal mail.

Social networks play a huge role in a person's life due to the fact that a person not only communicates in them, but also solves various household and business tasks, but unfortunately, no matter how many social networks try to carefully protect users' personal data, their ownership remains under question. It is true that social networks retain information, but they can also easily publish and distribute it at their discretion [2].

There are two concepts, such as security and confidentiality. Usually, a security breach occurs when someone gets to secure encryption and uses it for their own purposes. Violation of confidentiality consists in illegal access to information about a person's private life.

For example, someone posted a photo and his or her data on their page and as a result, another company uses them for research or commercialization.

So, many smartphones and laptops with a camera that can be physically closed are becoming popular. Either such cameras are hidden under the lid, or they are pushed out if necessary.

Following the example of the popularity of such models, many developers have already released updates in which you can also find out when your camera is working. For example, the indicator will light up in the phone every time the application uses the camera, even if it does not display the frame. The first smartphone with a pop-up camera was VivoNex, released in 2018. Retractable cameras delight both aesthetes who wanted frameless smartphones without any cutouts for the camera, and those who are worried about their privacy. Smartphones with similar cameras solve both problems [1].

Many skeptics still believe that the hidden use of cameras is not displayed in any way if it is not the main function in the application. As an example, we are often given advertising that corresponds to our desires. Users tell how they say something out loud, they also see an advertisement for this product, which undoubtedly arouses suspicion and disapproval. In their defense, we can say that most often the desire for the product appears after viewing [5].

The algorithm of the process is following: we firstly see the product somewhere, pay attention, put a like or go to the site, then the algorithms of the system give us advertising more often, and we often switch to the product to compare or just view it again. It does not mean that phones «eavesdrop» on us [4].

In any case, despite different opinions, our safety and security of personal data does not depend on ourselves. We can seal the cameras up, no matter how unreasonable it sounds, but the option itself is reliable. We can expose a minimum amount of information about the person in order to prevent us from calculating our data.

Personal data protection is an important issue for people of all ages. There are several simple rules for protecting your personal data online, they help a person to maintain confidentiality:

1. Each social network is an invaluable source of information for attackers who collect personal data, which they then use for deception and fraud. That's why it's so important to properly configure the privacy of your Facebook profile, VKontakte, Odnoklassniki and any other social network.

2. Your mail stores the «keys» to most of your accounts, since the password recovery procedure is most often carried out using email messages. Therefore, it is vital to secure your main mailing address, to which the Internet bank and the most important sites for you (for ex-

ample, social networks) are linked. If you want to register on a dating site or in some dubious service, it's better to create a second (or even a third or even a fourth) mailbox.

4. Do not publish online photos of your documents, tickets and payment receipts.

5. Do not use open Wi-Fi networks. They may look like a completely reliable Internet source provided by a local cafe or even a library, but it will be difficult for you to distinguish "respectable" Wi-Fi from «malicious». To create such a network, the criminal will need only a laptop and a Wi-Fi adapter. In addition, scammers really use this method to intercept usernames and passwords of users trying to connect to the Internet using their Wi-Fi networks.

6. Avoid unreliable passwords. Weak combinations practically do not protect against anything.

7. Remember that the issue of privacy is as relevant for children as it is for adults. Cyber bullying is not a myth, many teenagers around the world suffer from it. Therefore, it is important not to publish posts, photos and videos that may offend your child now or in the future.

8. Many people do not read the labels when installing the program, but simply click "Next". In this case, along with the necessary utility, a whole package of useless add-ons is installed that can change the settings that are familiar to you to unfamiliar ones: for example, put a new home page and your search service.

Unfortunately, some attempts to protect your data may be unsuccessful, because there is nothing more flexible than the human brain, which can build chains of logical connections and then it will not be difficult to find everything you need.

A person will find a way to find out about others all that he needs. Such a global thing as the Internet can lose data only in one case: when the main server and communication are lost. Otherwise, our information will always be somewhere on the network on the server as remote material [3].

It is important to use social media carefully:

1. Get into the habit of starting and ending the day not from the Internet - this is the main and mandatory condition.

2. Make an acceptable timing of social media visits per day, identify sites that are not needed.

3. Do not go to the sites that take up the most time.

4. Delete unnecessary apps on your phone. Without seeing regular notifications, it will be easier for you to dive into real world.

5. Use closed social groups.

6. Remove the ability to check social networks.

7. Spend more time with friend’s offline.

8. Remove social media apps from devices, it is a radical but working way to protect yourself and your data.

All of the above methods will help not only to protect yourself online, but also to make life better offline.

In conclusion, we want to say a simple, but important thing - we are usual people who are not interested in huge corporations individually. Moreover, the information about us is valuable only in one case if we hide it.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Алёшин О.В. Технологические основы построения автоматических систем управления связью высокодинамичных систем управления специального назначения // I-methods. 2019. Т. 11. № 1. С. 52-65.

2. Ильюшин Ю.В. Исследование запаса устойчивости систем автоматического управления // Альманах современной науки и образования. 2012. № 1. С. 26-37.

3. Петаг А. Нечеткое моделирование и управление. Москва : БИНОМ. Лаборатория знаний, 2012. – 798 с.
4. Соловьев В.А. Искусственный интеллект в задачах управления. Интеллектуальные системы управления технологическими процессами. Владивосток : Дальнаука. 2010. – 267 с.
5. Трофимов Ю.В. Способ разработки и испытания системы автоматического управления и мобильный стенд для тестирования электронной системы управления. Патент на изобретение 2755027 C1, 10.09.2021. Заявка № 2020140673 от 08.12.2020.

УДК 323

Калмыкова Любовь Константиновна, студент, Комсомольский-на-Амуре государственный университет
Kalmykova Liubov Konstantinovna, student of Komsomolsk-na-Amure State University
Шушарина Галина Алексеевна, кандидат филологических наук, доцент, заведующий кафедрой «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Shusharina Galina Alekseevna, Candidate of Philological Sciences, Associate Professor, Head of the Department “Linguistics and Intercultural Communication”, Komsomolsk-na-Amure State University

ПОЛИТИКА КНР В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

CHINA'S POLICY IN THE INTERNET SPACE

Аннотация. Данная статья посвящена рассмотрению новых направлений в политике КНР. Актуальность данного исследования заключается в том, что в связи с растущим научным интересом к опыту крупнейших стран мира по вопросам организация Китая является одной из сильнейших в данной области научно-технического прогресса и активно использует их во внутренней и внешней политике. В данной статье также описываются угрозы информационной безопасности КНР и делаются выводы по результатам данного исследования.
Abstract. This article is devoted to the consideration of new directions in the policy of the People's Republic of China. The relevance of this study lies in the fact that due to the growing scientific interest in the experience of the largest countries in the world on the organization of China is one of the strongest in this field of scientific and technological progress and actively uses them in domestic and foreign policy. This article also describes the threats to the information security of the People's Republic of China and draws conclusions from the results of this study.
Ключевые слова: Китайская Народная Республика, информационная безопасность, кибербезопасность, информационная политика, киберпространство, интернет, информационные технологии.
Key words: People's Republic of China, information security, cybersecurity, information policy, cyberspace, Internet, information technologies.

«Сильное сетевое государство» - термин, характеризующий Китай. Обладая всеми условиями и ресурсами, страна ведет активную деятельность в сфере подготовки государственных институтов. На данный момент более чем 854 миллиона интернет-пользователей Китая проводят свое время в Интернете, что сильно превышает общее

число пользователей в ЕС и США. Немаловажен факт наличия своей абстрагированной от всех Интернет-зоны, которая управляется только государственными предприятиями. Это обуславливается тем, что в стране существуют жесткие меры в отношении цензуры, поэтому большинство популярных европейских интернет-ресурсов не могут вести свою деятельность на территории Китая. [1]

Базовые положения интернет-политики Китая были изложены в статье «Белая книга», выпущенная Государственным информационным советом КНР в 2019 году. Стоит выделить несколько ключевых моментов, затронутых в книге: проникновение и популяризация Интернета в обществе, доступность Интернета, изучение прав и свобод человека в Интернет-пространстве, регулирование Интернет-зоны и кибербезопасность.

Хотелось мы отметить, что правительство Китая ввело такое понятие, как «интернет-правительство», которое обеспечило исключительное право на возможность обособления китайской паутины и кибербезопасности от любых внешних вторжений. Такое Интернет-доминирование позволило сконцентрироваться на развитии материального и экономического благополучия населения. [1]

Налаживание определенной технологической базы для обеспечения населению информации сподвигло правительство КНР принять программу «Национальная стратегия информатизации и развития» в 2016 году. Главная цель программы – достичь мирового признания и стать конкурентноспособными на рынке к 2020 году. Кроме этого, одной из задач является создание международной сети связи с самыми современными технологиями и программным обеспечением к 2025 году. Таким образом, Китай повысит процент соперничества на рынке и сможет более ясно регулировать проблемы кибербезопасности. Существует теория, которая гласит, что в XXI веке Китай будет способен иметь всемирное влияние на процессы информатизации ввиду их специфичной концепции социализма вместе с программами, направленными на развитие информационных баз. Поэтому перед государством стоят задачи не только стать лидерами в производстве высокотехнологичных баз, но и разработка нового программного обеспечения. Эта программа также близка к идеям, сформулированным в стратегических инициативах Internet Plus и China 2025.

Такие компании, как Alibaba, Tencent и Baidu формируют монопольную политику государства и цензуру на внутреннем рынке в отношении всемирной паутины. Эти цифровые гиганты выпускают настолько огромное количество приложений, что захватывают большую часть рынка цифровых технологий и не оставляют возможности войти в их зону своим конкурентам. [3] Такая ситуация на интернет-рынке Китая называется «Троецарствие». Alibaba работает в сфере электронной коммерции и занимается развитием операционных систем, а Tencent является лидером в продвижении социальных сетей и владеет крупнейшей социальной сетью Китая WeChat и разными развлекательными и игровыми платформами. В таких условиях иностранные компании не успевают адаптироваться к условиям и правилам ведения бизнеса и не способны конкурировать. Такая монопольная политика и четкое разделение труда только доказывает эффективность управления государством крупными компаниями, которые нацелены на развитие информационных процессов в сети. А крупные компании, как Google, Facebook и Amazon лишены права легально работать на территории Китая, поэтому они ищут различные способы наладить связь, создавая разные приложения и сервисы. Однако, полиция активно принимает меры против использования таких приложений. [4]

Информационная безопасность является главной составляющей при реализации информационной политики Китая. Поэтому национальная стратегия кибербезопасности формирует основы информационной безопасности и национальной стабильности, так как государство должно быть уверенно в политической, социальной и культурной защищенности от любых вмешательств. [2]

Руководство информационной политики осуществляется Центральным военным советом, Бюро расследований общественной информации и сетевой безопасности Китайской Народной Республики, Министерством общественной безопасности и Министерством науки и технологий. Как можно подметить, контроль за исполнением информационной безопасности ведется строго государственными органами. Преимущество, которое есть у Китая, в том, что у КПК достаточный объем полномочий для управления и контроля разведывательной полицией. И организующую роль в этом играет Центральная комиссия по киберпространству, членами которой являются председатель КНР Си Цзиньпин, верховный советник КНР Ли Кэцян, а также руководители соответствующих ведомств и комиссий. [5]

Помимо государственной поддержки в этой сфере Китай также активно сотрудничает с некоторыми негосударственными субъектами такими, как Huawei, Venustech, Qihu 360, Leadsec и Westone.

Проведенные исследования приводят нас к некоторым выводам касательно современной Интернет-политики Китая. Главная цель – создать «сильную сетевую нацию». Стремясь достичь этого, китайского правительство будет всячески развитию национальной экономики, ведя успешную систему контроля отечественного Интернета и защищая его от иностранного вмешательства. Государство уже предприняло серьезные шаги в этом направлении: создало специализированное агентство, приняло национальную стратегию развития и безопасности киберпространства и определило четкую позицию в международной организации киберпространства. Также правительство наладило сотрудничество с основными отечественными технологически-развитыми компаниями.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Антипов К.В. Киберконфликт в китайско-американских отношениях и поиски диалога // Проблемы Дальнего Востока. 2013. № 6. С. 39-54. Булавин А.В. О подходах США и Китая к обеспечению кибербезопасности // Общество: политика, экономика, право. 2014. № 1. С. 27-31.

2. Ватрушкин А.А. Правовые основы обеспечения кибербезопасности критической инфраструктуры Российской Федерации // Евразийская адвокатура. 2017. Т. 31. № 6. С. 78-84.

3. Ибрагимова Г.Р. Стратегия КНР в киберпространстве: вопросы управления интернетом и обеспечения информационной безопасности // Индекс безопасности. 2013. Т. 6. № 19. С. 169-184.

4. Кошурникова Н.А. Особенности информационной политики современного Китая // Китай: история и современность: материалы IX международной научно-практической конференции «Китай: история и современность» 22-23 октября 2015. Екатеринбург: Уральский федеральный университет имени первого Президента России Б.Н. Ельцина, 2016. С. 279-284.

5. Разумов Е.А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. 2017. Т. 98. № 4. С. 156-170.

УДК 004.056.53

Калугин Михаил Игоревич, студент, Комсомольский-на-Амуре государственный университет
Kalugin Mikhail Igorevich, student of Komsomolsk-na-Amure State University
Хритов Антон Евгеньевич, студент, Комсомольский-на-Амуре государственный университет
Khritov Anton Evgenievich, student of Komsomolsk-na-Amure State University
Малышева Наталья Васильевна, кандидат филологических наук, доцент, Комсомольский-на-Амуре государственный университет
Malysheva Natalia Vasilievna, PhD in Philology, Associate Professor, Komsomolsk-na-Amure State University

ТРАНСФОРМАЦИЯ ГРАНИЦ ПУБЛИЧНОГО И ЧАСТНОГО

TRANSFORMATION OF THE BOUNDARIES OF PUBLIC AND PRIVATE

Аннотация. В данной статье рассматривается развитие современного информационного общества, основанного на растущей информатизации социальных процессов, и систематизация основных проблем конфиденциальности пользователей и защиты персональных данных. Представлен краткий обзор особенностей цифровой эпохи, основанный на основных вопросах конфиденциальности, в котором описываются возможные проблемы с персональными данными.
Abstract. In this article, the development of the modern information society based on the growing informatization of social processes and the systematization of the main problems of user privacy and personal data protection has been considered. The research gives a brief overview of the digital age features in the aspect of main privacy issues; it describes possible problems with personal data.
Ключевые слова: информатизация, информационные ресурсы, цифровизация, защита данных, конфиденциальность, безопасность.
Key words: informatization, information resources, digitalization, data protection, privacy, security.

Постоянный рост применения информационно-коммуникационных технологий в современных социальных процессах влияет на развитие информационного общества и определяет необходимость знать их особенности и возможности, а также влияние на частную жизнь. Одной из тем для обсуждения в цифровую эпоху является уровень компетентности пользователей цифровых сервисов в сетевом пространстве и их цифровая грамотность. Это связано с информатизацией общества, которая закладывает основу информационного общества и представляет собой непрерывный процесс социального, экономического и научно-технического развития социальной информационной среды. Цель состоит в том, чтобы создать возможности для удовлетворения информационных потребностей людей в реализации прав граждан, органов власти и организаций. Это требует обеспечения надлежащей защиты персональных данных, как для людей, использующих ИКТ, такие как социальные сети, так и для передачи, хранения или удаленного доступа к распределенным информационным ресурсам в глобальном цифровом пространстве, в том числе в облаке.

Неприкосновенность частной жизни является фундаментальным правом человека, признанным во многих международных соглашениях и документах, но важный вопрос заключается в том: "Что такое неприкосновенность частной жизни?" Объем и содержание концепции могут быть определены исходя из национальной культуры и ин-

дивидуальных особенностей населения, но есть и общие вещи, такие как неприкосновенность личной информации и ее защита (доступ, использование, распространение, передача и т.д.). По этой причине каждый имеет право на защиту персональных данных. Таким образом, определяются две формы защиты, которые отражают предмет – “право на неприкосновенность частной жизни” и “право на защиту данных”.

Существует не так много попыток определить "право на неприкосновенность частной жизни", и некоторые комментарии заключаются в следующем:

1 Этот термин не следует определять как отдельное юридическое право, и существующих законов, касающихся неприкосновенности частной жизни, должно быть достаточно.

2 Для того, чтобы определить личную неприкосновенность (неприкосновенность частной жизни), необходимо найти общую связь между различными сущностями судебного дела по данной теме.

3 В других источниках конфиденциальность трактуется как "цифровая конфиденциальность" и предлагается рассматривать право на неприкосновенность частной жизни как независимое право, заслуживающее регулирования.

Краткое изложение комментариев в литературе заключается в том, что право на неприкосновенность частной жизни — это право защищать все, что непосредственно связано с человеком (тело, дом, собственность, мысли, чувства, секреты, личность, переписку и т.д.). Это право позволяет индивиду самому выбирать, какую часть личного пространства сделать доступной для других, а также определяет способ и время использования [1].

В современном цифровом мире глобальные коммуникации широко используются для удаленного доступа к информационным ресурсам, веб-сайтам, виртуальным пространствам, дискуссионным и социальным форумам и многому другому. Таким образом, любой пользователь сетевых коммуникаций может свободно "пересекать национальные границы" и получать доступ к удаленным сайтам в сетевом пространстве.

Основная часть проблем информационной безопасности в сетевом мире может быть связана с нарушением цифровой конфиденциальности (e-privacy), поскольку различные среды в глобальной сети требуют предварительной регистрации пользователей путем предоставления категорий персональных данных, которые напрямую не связаны с указанной целью. Опрос граждан ЕС выявил, что 74% из них считают, что раскрытие персональных данных является существующей проблемой в современном цифровом мире, в то время как еще 84% заявили, что глобальная сеть требует слишком много персональных данных, что не соответствует поставленной цели. В то же время 72% пользователя сети опасаются, что у них нет полного контроля над своими данными. Известно, что некоторые пользователи соглашаются с политикой конфиденциальности, поддерживаемой соответствующим сетевым пространством, не осознавая этого. В некоторых случаях информация об этой политике не предоставляется, или личная информация требуется при регистрации без представления лица о том, как она будет обрабатываться. В большинстве случаев у пользователей нет иного выбора, кроме как предоставить запрошенные персональные данные, если они хотят получить доступ к выбранному сетевому пространству [2].

Конфиденциальность пользователей и PDP (Политика обработки персональных данных) в глобальной сети широко обсуждаются на различных форумах и институтами европейского и мирового уровней. Ключевым элементом цифрового пространства является обслуживание веб-сайтов, поскольку важным требованием является то, что опубликованная на нем информация должна быть правильной, надежной и что при общении с пользователями и сборе их персональных данных принимаются необходимые меры защиты. Это ответственность владельца сайта, который должен обеспечить приведение опубликованной информации в соответствие с требованиями нового регламен-

та. Причина этого заключается в том, что данная информация является общедоступной и в определенных случаях может привести к риску для владельцев этих персональных данных (телефон, адрес, фотографии, резюме, финансовые документы и т.д.) с нежелательными финансовыми и психологическими последствиями, а также последствиями для репутации.

Опубликованная информация в сети, в том числе в социальных сетях, центрах обработки данных в облаке, а также при построении гетерогенных сред для дистанционного и электронного обучения, должна соответствовать требованиям к законной и корректной обработке персональных данных. Такая информация должна быть достаточной и соответствующей цели, иметь четкое согласие пользователя - лица, которое является владельцем персональных данных. Одним из обязательных требований GDPR (Общий регламент по защите данных) является “право быть забытым /удаленным”, которое устанавливает право субъекта данных запрашивать исправление, удаление или блокировку неверных данных, а также требовать удаления ссылок на персональные данные, когда информация является неточной, неадекватной, неуместной или чрезмерной для целей обработки данных [3].

Основные требования к интернет-провайдерам для различных типов сетевых коммуникаций четко определены в различных документах по защите данных [4]. Одним из таких документов является следующее:

1) обеспечение конфиденциальной связи путем запрета прослушивания, подслушивания или хранения сообщений без согласия субъекта данных;

2) обеспечение безопасности услуг с помощью соответствующих мер, введенных поставщиками электронной почты;

3) уведомления об утечках данных, когда поставщик выявляет проблемы безопасности, приводящие к потере или краже персональных данных;

4) данные о трафике и местоположении должны быть удалены или анонимны, когда они больше не требуются для целей связи или в других юридических ситуациях;

5) предварительное согласие перед отправкой нежелательных коммерческих сообщений (известных как "спам"), которые включают текстовые сообщения SMS и другие электронные сообщения;

6) требование предварительного согласия на включение общедоступных каталогов (номер телефона, электронная почта / почтовый адрес) в общедоступный каталог.

"Cookie" (небольшой текстовый файл с пользовательской информацией, хранящийся на веб-сайте для повышения производительности за счет сохранения пользовательских предпочтений) широко распространен в Интернете. Согласно новым правилам, пользователь должен быть проинформирован об использовании файлов cookie. Следует запрашивать его согласие, предоставив возможность деактивировать или не принимать файлы cookie на своем собственном устройстве. Это также право пользователя знать, как будет использоваться информация из файлов cookie.

Другая область - социальные коммуникации, объединенные в общее направление социальных вычислений, которые являются инструментом для взаимоотношений с друзьями, семьей и коллегами. Следует иметь в виду, что предоставление личной информации, фотографий и комментариев может быть замечено более широким кругом людей, чем считалось ранее, и это приводит к возможному риску для конфиденциальности. В некоторых случаях настройки на сайтах, которые работают по умолчанию, позволяют одним щелчком мыши принимать условия пользователя, фактически не зная, что они разрешают в своих учетных записях. Даже при однократном посещении сайта персональные данные пользователя сохраняются и автоматически отправляются в центральный офис.

Нельзя отрицать высокую эффективность цифровизации общества не только с применением технологий, рассмотренных выше, но и в области электронного прави-

тельства, электронного обучения, а также с предложением многих электронных услуг (электронный банкинг, электронный бизнес, электронное голосование и т.д.). Однако также необходимо проанализировать возможные проблемы, которые могут привести к нежелательным последствиям для участников цифрового мира, чтобы последние могли знать о них и принимать необходимые меры предосторожности для защиты своей конфиденциальности и личности. Это основная причина для изложения данного материала, который представляет собой краткий обзор исследований, проведенных авторами в области защиты персональных данных и конфиденциальности, политик безопасности и технологий организации систем управления доступом к информационным ресурсам, включая массивы (профили) с персональными данными.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Бауман З. Индивидуализированное общество. - М.: Логос, 2005. 390 с.

2 Луман Н. Медиа коммуникации (Общество общества. Ч. II). - М.: Логос, 2005. 280 с.

3 Кучерков И.А. О понятии "киберпреступление" в законодательстве и научной доктрине // Юридическая наука. 2019. №10. URL: https://cyberleninka.ru/article/n/o-ponyatii-kiberprestuplenie-v-zakonodatelstve-i-nauchnoy-doktrine (дата обращения: 16.12.2022).

4 Политика конфиденциальности и защита персональной информации // Krona URL: https://krona.ru/policy/ (дата обращения: 12.11.2022).

УДК 316.733

Коваленко Софья Александровна, студент, Комсомольский-на-Амуре государственный университет
Kovalenko Sofia Alexandrovna, student of Komsomolsk-na-Amure State University
Шушарина Галина Алексеевна, кандидат филологических наук, доцент, заведующий кафедрой «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Shusharina Galina Alekseevna, Candidate of Philological Sciences, Associate Professor, Head of Department of Linguistics and Intercultural Communication, Komsomolsk-na-Amure State University

КУЛЬТУРА ОТМЕНЫ КАК НОВЫЙ ИНСТРУМЕНТ МАНИПУЛЯЦИИ

CANCEL CULTURE AS A NEW WAY OF MANIPULATION

Аннотация. Культура отмены (cancel culture), представляет собой современный вид народного голосования, который стал ведущей силой в контроле общества в последние годы. идея культуры отмены в данного феномена заключается в игнорировании определенных людей или брендов в связи с их поступками, непринятыми в обществе. Данный феномен является сложным социально значимым движением. В статье рассматриваются как история культуры отмены, так и влияние на сферы жизни через социальные сети, а также изучаются прецедентные масштабные случаи отмены.
Abstract. The culture of cancellation (cancel culture) is a modern kind of popular vote, which has become a leading force in the control of society in recent years. the idea of the cancellation culture in this phenomenon is to ignore certain people or brands in connection with their actions that are not accepted in society. this phenomenon is a complex socially significant movement. The article examines both the history of culture and the impact on spheres of life through social networks. and precedent-setting large-scale cases of cancellation are also being studied.

Ключевые слова: культура отмены, феномен Баадера-Майнхоф, социальные сети, спираль молчания, нетерпимость.
Key words: cancel culture, Baader-Meinhof phenomenon, social networks, spiral of silence, intolerance.

Как мы можем видеть, в последнее время социальные сети стали влиять не только на общение в обществе, но и на политическую, спортивную и даже личную сферы. В самом начале развития социальные сети были ресурсом для различного взаимодействия людей. Сегодня это стал силой общества, которая направлена на продвижение социально значимых культурных установок. Социальные сети развились в площадки, где люди обмениваются информацией и могут влиять на жизнь других. Сегодня в большей степени под влияние социальных сетей попадают медийные личности или компании, которые нарушают социально приемлемые нормы или высказываются вразрез с общепринятыми взглядами. Так из-за наличия разнообразных идеологий и взглядов на жизнь люди формируют группы по интересам что в скором времени приводит к столкновениям этих групп и интересов. В случае, когда большинство людей по всей сети против высказывания или действия, появляется такой феномен как отмена. За последние года акт отмены личности или бренда стал ведущей коллективной практикой.

На данный момент культура отмены изучена не так глубоко, и многие связывают это с опасением исследователей попасть под влияние отмены. Стоит отметить, что мнения общества о каких-либо недопустимых действиях или высказываниях меняются быстрее чем мы можем представить. Это затрудняет анализ и прогнозирование дальнейшего влияния поступков на одобрение общества или осуждение. нельзя не заметить, что при просмотре какого-либо контента люди чаще обращают внимание на, то, что отражает их мировоззрению, поэтому так часто можно встретить людей с аналогичным мышлением на страницах, которые интересны. За счет инстинктов человека, мы разделяем все окружение на «Я», «Мы», «Наше» и «Они», «Чужие», «Их». Из-за такого разделения, которое в древние века помогало выжить, в наше время человек только само идентифицируется и находить поддержку общества. А для собственной безопасности отгораживает феномен отмены мнимой или реальной угрозы. Под влиянием двух когнитивных искажений, а именно селективного внимания и склонности подтверждать свое мнение люди видят и слышат чаще то, что в какой-то степени подтвердит их взгляд и игнорируют факты, которые могут разрушить привычную картину мира. Данный феномен называется Феномен Баадера — Майнхоф, что переросло в феномен культуры отмены, а именно отмены того, что не соответствует мнению.

Все чаще отмена приобретает форму крайней нетерпимости, может приводить к разрыву всех взаимодействий с представителями осуждаемого. Нередко доходило до массовой травли знаменитостей, порицания целого бренда за высказывание работника. Сегодня мы можем наблюдать как общество отменяет не просто мировую компанию, а целую страну. На момент публикации данной статьи главной жертвой отмены мирового сообщества является Россия, которую уже «отменили» порядка 400 компаний. Данные решения направлены на призыв России изменить внешнеполитические действия. Можно отметить, что феномен превратился в политический инструмент давления, посредством которого экономического и политического игнорирования стало возможным манипулировать странами в угоду ведущих лидеров [2]. Сегодня мы можем наблюдать как традиционно аполитичные сферы так же подвержены данному феномену. Так, российские спортивные клубы были исключены из международных федераций волейбола баскетбола и хоккея [3]. А международные чемпионаты FIFA и UEFA [4] отказали России в участии. с Россией разорвала контракты и NHL [5,6]. Были отменены соревнования по зимним видам спорта [3] и этапы Формулы-1.

Поднимая тему культуры отмены, не стоит исключать и предложенную немецким политологом Э. Ноэль-Нойман концепцию спирали молчания. Согласно данной концепции люди опасаются быть осужденными и не высказывают свое мнение, будучи уверенными, что окажутся в меньшинстве. Все чаще крупные медийные представители не могут свободно высказывать мнение без учета всех установок публики. Вероятность оказаться изгоем общества приводит к тому, что люди боятся высказать свое личное мнение больше, чем хотят быть услышанными. Мы можем видеть, как общество через социальные сети буквально диктует как правильно думать и делать. Как на личность, так и на общественное мнение оказывается значимое влияние и, следовательно, меняется восприятие картины мира и индивидуальная, и социальная. При этом данное влияние часто искажает реальную ситуацию в угоду обществу и обществу и является действенным средством манипуляции, так как через запугивание и моральное давление общество требует изменить мнение или свое видение.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Ноэль-Нойман Э. Общественное мнение// Открытие спирали молчания / Перевод с нем.; общ. ред. и предисл. Н.С. Мансурова. М., 1996. 352 с.
2. Культура и природа политической власти: теория и практика.
3. Какие спортивные соревнования перенесли из России // ТАСС. URL: https://clck.ru/sJtED (дата обращения: 21.10.2022).
4. «Решение носит дискриминационный характер»: ФИФА иУЕФА отстранили российские клубы и сборные от участия в турнирах // RT на русском. URL: https://clck.ru/sJtCv (дата обращения: 06.11.2022).
5. EA Sports удалила все российские клубы и сборные из игр FIFA и NHL // РИА Новости Спорт. URL: https://clck.ru/sJtGM (дата обращения: 21.10.2022).
6. НХЛ разорвала связь с Россией // Сибнет. URL: https://clck. ru/sJtDW (дата обращения: 21.03.2022).

УДК 323.2

Костецкая Екатерина Сергеевна, студент Комсомольского-на-Амуре государственного университета.
Kostetskaya Ekaterina Sergeevna, student of Komsomolsk-on-Amur State University.
Подкич Светлана Александровна, старший преподаватель Комсомольского-на-Амуре государственного университета.
Podkich Svetlana Alexandrovna, senior lecturer, Komsomolsk-on-Amur State University.

ОПАСНОСТЬ ЦИФРОВИЗАЦИИ. ЦИФРОВОЙ «КОНЦЛАГЕРЬ»

THE DANGER OF DIGITALIZATION. DIGITAL «CONCENTRATION CAMP»

Аннотация. Цифровая трансформация постепенно приходит во все сферы жизни каждого человека, и со временем она будет становиться все более явной и заметной. Мы живем в информационном веке. Каждый год объемы доступной и необходимой человеку информации возрастают, требуется все больше ресурсов на их анализ. Для обработки огромных массивов данных стали все чаще использовать ИИ, которые могут самостоятельно принимать решение, на основе заданных алгоритмов. Искусственный интеллект на службе государства обеспечивает безопасность и соблюдает интересы страны. Однако он сам по себе несет опасность для личных свобод и прав человека.
Abstract. Digital transformation is already gradually coming into all spheres of every person’s life, and over time it will become more apparent and noticeable. We live in the information

age. Every year, the amount of information available and necessary by man increases, requires more resources to analyze them. Large data sets are increasingly being processed using AI, which can make their own decisions based on given logic. Artificial intelligence in the service of the state provides security and respects the interests of the country. However, it itself poses a danger to individual freedoms and human rights.
Ключевые слова: искусственный интеллект, цифровизация, цифровая личность, цифровые данные.
Key words: artificial intelligence, digitalization, digital personality, digital data.

Уже с конца 90-х годов в мире начали говорить о технологиях цифровизации. С тех пор прошло более 20 лет, и интернет вещей стал для нас привычным явлением. Практически у каждого дома есть умные устройства, начиная от смартфона и заканчивая цифровыми помощниками.

Цифровизация, инфраструктур изначально предназначалась для создания комфортной среды. Так в сфере здравоохранения введение цифровых технологий и основанных на инновационных программных решениях алгоритмов диагностирования болезней позволяет дистанционно отслеживать состояние здоровья человека. Кроме того, с внедрением систем ИИ в медицине происходит трансформация отношений врача и пациента. Массивы данных обрабатываются техническими средствами, что высвобождает время для общения с больным. [4]

Цифровизация экономики позволила нам через обработку данных получать быстрый доступ к всевозможным услугам: электронные платежи, электронный документооборот, онлайн-услуги и т.д. Была изменена система управления бизнесом: как частные, так и государственные компании обязывают переходить на электронные платформы и вести отчетность и работу там.

Система образования также претерпела значительные изменения с развитием и внедрением информационных технологий. Многие учебные заведения всех уровней образования не только оптимизируют свое документооборот посредством цифровизации внутренних бизнес-процессов, но и активно применяют новые технологии в самом образовательном процессе: от работы на ЭВМ во время очных занятий, до организации дистанционных образовательных форматов с помощью технологи онлайн-обучения. Подобные технологии обучения имеют немало преимуществ: образование становится общедоступным, сокращается объем бумажной работы. Кроме того, планшеты и ноутбуки повсеместно заменяют бумажные носители, позволяя хранить больше информации и обеспечивая постоянный доступ к ней.

Цифровизация города (т.н. «smart city») и дома (т.н. «internet of things») позволяют собирать и анализировать большие объемы данных о функционировании городской среды и ее жителей. Обработка массивов данных, собранных камерами видеонаблюдения и иными устройствами производится с помощью искусственного интеллекта, что позволяет как предотвратить нештатные ситуации, так и обеспечить своевременное реагирование на уже произошедшие инциденты.

Повсеместное внедрение информационных технологий открывается все новыми преимуществами в самых разных отраслях. Цифровизация документооборота сделала намного проще работу с электронными документами. Система автозаполнения позволяет исключить человеческий фактор с его ошибками. Искусственный интеллект в виде голосовых помощников уже может оперировать информацией и улучшать жизнь человека. [2]

Перечисленные выше плюсы и возможности цифровизации выстраивают утопический мир. К сожалению, у каждой медали есть две стороны.

Одним из наиболее спорных с этической точки зрения последствий масштабного сбора данных является рейтинговая система в том ее виде, который применяется к человеку в целом. Примером такого может служить социальный рейтинг Китая, одной из

наиболее подверженных глобальной экспансии информационных технологий стран. При внедрении такой системы, искусственный интеллект на службе государства собирает и обрабатывает данные от государственных учреждений и коммерческих организаций по каждому человеку. На этом основании система может создать «алгоритм судьбы», начиная со сбора биометрических данных, ДНК, медицинских данных с самого рождения до смерти. [1]

В эту систему стекаются всевозможные сведения, собранные о человеке. Предпочтения в еде, о чем ваши разговоры, ваши запросы в поисковиках, какая одежда для вас предпочтительнее, ваши просмотры (данные на смартфонах записанные или «подслушанные», видео с камер), как пример контекстная реклама, которая предлагает товары и услуги, которые недавно обсуждались человеком.

Базы биометрических данных помогут найти кого угодно за считанные минуты по городским камерам и камерам в помещениях, а так же геолокации устройств. С примером использования сбора данных о вашем передвижении (маршрут, вид транспорта). Например, по некоторым данным вооружённые силы США покупают данные о местоположении, а приложение для мусульманских молитв передаёт пользовательские данные о местоположении подрядчикам в сфере обороны.

При краже медицинских данных ущерб включает заниженные кредитные рейтинги и отказ в обслуживании. Если воры установят пороговые значения для максимальных выгод по полису, держатели полиса могут оказаться не в состоянии получить своевременное покрытие для срочного лечения. Они могут увидеть увеличение годовой стоимости своей страховки или вообще отказать в покрытии.

Уже сейчас система может оценить ваши поведенческие характеристики. С помощью биометрического распознавания, считывать реакции (анализ изменения зрачка, пульс, давление) фитнес браслеты могут оценить уровень стресса в режиме реального времени. Аккумулированные отзывы о личности человека (любое упоминание о вас в просторах интернета), в совокупности с биометрическими показателями позволяют создания "слепка личности".

Система на службе государства, уже сейчас имея доступ к вашей цифровой личности, может карать неугодных. Заморозка счета, или ограничение передвижение на общественном транспорте. Во многих странах принят закон о режиме чрезвычайной ситуации, при введении которой все финансовые потоки переходят под контроль государства. Пример это мы можем наблюдать в Канаде. Банки начали замораживать счета участников и спонсоров протестов против коронавирусных ограничений в Оттаве. Также существует возможность запрета посещения определенных мест (как пример, запрет на посещение общественных мест без Green Pass.) или отказа в медицинской помощи.

Кроме рассмотренной выше системы «социального рейтинга» существует ряд других спорных с морально-этической точки зрения вопросов, которые появляются с развитием информационных технологий.

Цифровая личность может легко стать объектом неправомерных действий. Несмотря на постоянное улучшение и развитие систем кибербезопасности, данные пользователей могут оказаться в свободном доступе как по ошибке, так и в результате целенаправленного взлома или продажи. Последствия подобных т.н. «сливов» могут быть самыми разными, начиная с безобидных комментариев в социальных сетях, до шантажа и использования в мошеннических схема. Примеры утечек только за 2022 год в России:

- в Сеть попали базы данных клиентов сервиса для заказов товаров из-за границы CDEK.Shopping и маркетплейса «СДЭК.Маркет», всего почти 120 тыс. строк;
- злоумышленники смогли получить доступ к базе данных Start за 2021;
- 29 июля была выложена часть базы данных «Почты России» В интернет утекли имена и телефоны отправителей и получателей;

- в начале мая в даркнете выставили на продажу базу данных клиентов лаборатории «Гемотест»;

- «Яндекс.Еда» в следствии утечки, персональные данные курьеров сервиса оказались в открытом доступе.

- В марте в интернете появился ресурс, на котором персональные данные пользователей были опубликованы в виде карты. Сайт позволял узнать адрес доставок, телефон, электронную почту, сумму заказов за шесть месяцев.

Модель технического типа в медицине может привести к обезличиванию больного. Врачи могут быть заменены ИИ и роботами, которые выбирают алгоритм автоматизации процессов, а не заботу о пациенте. В качестве примера можно привести ситуацию, когда обследование пациента проходит дистанционно, в формате опроса на сайте. Тут может встать вопрос об этических нормах (стоит ли бороться за жизнь человека, целесообразен ли уход за пожилыми, и должны ли иметь шансы на жизнь дети, которым еще в утробе выявили какие-либо отклонения). [4]

Не только взрослых, но и детей всячески вовлекают в цифровую среду, собирая данные о них. Сейчас на каждого ребенка создается цифровой профиль. Операторами и владельцами этих платформ выступают как государственные, так и частные структуры. Сбор данных (участие в олимпиадах, электронный журнал, посещение кружков и секций), несет за собой тотальный контроль за людьми. Так цифровая платформа может взращивать и трансформировать индивидуума по заданным лекалам государства или крупных корпораций. Человек в новой системе образования уж не будет принадлежать самому себе, произойдёт упразднение личности.

Безусловно, на данном этапе развития технологий ИИ, вычислительные мощности ещё недостаточно велики для сбора, обработки, и хранения подробнейшей информации на каждого человека, но темпы развития технологий заставляют задуматься о возможных вариантах будущего. Например, личность человека и реальность вокруг него можно будет формировать и корректировать. Имея данные о предпочтениях и вкусах, можно незаметно направлять выбранный объект (человека) к принятию нужных для кого-либо решений. Можно будет более продуктивно управлять индивидом в реальности, задавая ему программу жизни (где поселиться, куда лучше идти работать и какие действия лучше совершать). Так же существует возможность отмены «любви», как не целесообразного процесса, а для поддержания популяции задать алгоритм: одобрение второй половинки, сколько и когда иметь детей. Одним из таких рычагов воздействия может стать «метавселенная», где будет происходить анализ и тесты над личностью. [3]

Таким образом, государство может получить тотальный контроль над жизнью граждан. Это является прямой угрозой демократических начал в управлении, препятствует созданию гражданского общества и способствует усилению контроля над гражданами. [5]

Конечно, в данной статье рассмотрены не все проблемы цифрового «концлагеря» и опасности искусственного интеллекта. И пока цифровизацию мы воспринимаем как удобство, остается открытым вопрос: «Кто мы в будущем, личности или алгоритмы?»

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Асмоловский, М. Д., Колпакова Т. В Система Социального рейтинга как механизм социального управления в КНР // Забайкальский государственный университет, 2020. – 24 с.

2 Бакутина, Н. С. Гражданское общество и новые информационно-коммуникационные технологии // Вестник Нижегородского университета им. Н. И. Лобачеваского, 2015. - №2. 90 с.

3 Бочарников И. В. Информационно-коммуникативные противоречия и проблемы современных процессов глобализации // Экология внешней и внутренней среды социальной системы (ЭкоМир-9): матер. конф. (Мытищи–Москва, 29–30 марта 2018 г.). М.: Издательство МГТУ им. Н. Э. Баумана, 2019. С. 190-192.

4 Введенская Е. В. Цифровизация и роботизация в медицине: этические аспекты / Е. В. Введенская // Философские науки, 2022. – 122 с.

5 Маниковская М.А., Цифровизация образования: вызовы традиционным нормам и принципам морали // Власть и управление на Востоке России. 2019. № 2 (87). С. 100–106.

УДК 349.23/24

Курочкина Анастасия Николаевна, преподаватель, Северо-Западный институт (филиал) Университета им. О.Е. Кутафина (МГЮА)
Kurochkina Anastasia, lecturer, North-Western Institute (branch) of Kutafin Moscow State Law University (MSAL)

ВИДЕОНАБЛЮДЕНИЕ ЗА РАБОТНИКОМ

VIDEO SURVEILLANCE OF AN EMPLOYEE

Аннотация. Рассмотрены вопросы, возникающие при осуществлении дистанционного наблюдения за работником: законность, обоснования, требования. Непременные условия, необходимые для легитимного осуществления видеонаблюдения за работником. Неприкосновенность частной жизни работника. Недопустимость чрезмерного контроля за работником.
Abstract. The issues arising in the implementation of remote monitoring of an employee are considered: legality, justifications, requirements. Indispensable conditions necessary for the legitimate implementation of video surveillance of an employee. Employee's privacy. The inadmissibility of excessive control over the employee.
Ключевые слова: работник, трудовой договор, частная жизнь, работодатель, видеонаблюдение.
Key words: employee, employment contract, private life, employer, video surveillance.

Современные технологии неустанно входят в нашу жизнь, проникая во все сферы деятельности. С развитием передовых средств и способов информационной константы взаимодействия работника и работодателя, последний всё чаще прибегает к различным способам проверки и наблюдения за работой сотрудников. Это делается по разным причинам: с целью выявления корпоративного шпионажа, предотвращения хищения денежных средств, контроля общения работника с непосредственными клиентами, в целях безопасности, анализа и оптимизации рабочего процесса и просто для того, чтобы работник работал честно и добросовестно, согласно должностной инструкции, не отвлекаясь на посторонние, не относящиеся к работе дела и вещи. Поскольку это явление нового времени, возникает резонный вопрос – насколько это законно? Является ли это вторжением в частную жизнь работника? В какой мере допустимо вторжение в личное пространство работника?

Конституция Российской Федерации защищает неприкосновенность частной жизни, личную и семейную тайну, а также гарантирует каждому право на тайну переписки, телефонных переговоров, почтовых и иных сообщений. Ограничение этого права возможно только по решению суда [1, ст. 23].

Заключая трудовой договор, работник берет на себя обязанность соблюдать трудовую дисциплину и исполнять в течение дня исключительно поручения работодателя. Использование технических средств связи, принадлежащих работодателю, должно осуществляться только для исполнения трудовых функций. Соблюдение данного требования вполне законно и обоснованно: работодатель преследует цель повышения качества работы, своевременного выполнения поставленных перед сотрудником задач, увеличения количества продаж или выпускаемой продукции. Использование современных средств наблюдения и контроля за работником также способствует этой цели.

До недавнего времени трудовое законодательство ни в какой мере не содержало норм относительно каких-либо средств дистанционного контроля. Лишь в 2022 году в Трудовой кодекс РФ была введена статья 214.2, дающая право работодателю использовать в целях контроля за безопасностью производства работ приборов, устройств, оборудования и (или) их комплексы (системы), обеспечивающих дистанционную видео-, аудио- или иную фиксацию процессов производства работ, обеспечивать хранение полученной информации [2]. Иных норм, которые регулировали бы отношения работника и работодателя при установлении последним средств информационного слежения, кодекс на данный момент не содержит.

Одним из самых распространенных способов контроля, используемых работодателем, является видеонаблюдение за работником на рабочих местах. Установление в офисе видеонаблюдения довольно сложная процедура, поскольку часто встречает сопротивление работников, считающих это вторжением в личную жизнь [8].

Изображение сотрудника с записи видеокамер представляется биометрическими персональными данными [3, ст. 11]. По внешности изображенного на видео, можно идентифицировать и установить его личность. Поэтому видеонаблюдение за сотрудником должно происходить только с его согласия. Работодателю необходимо соблюдать требования ФЗ «О персональных данных» и получить такое согласие в письменном виде [3].

Важно учесть, что видеокамеры не должны нарушать гарантированную Конституцией РФ неприкосновенность частной жизни, а поэтому должны быть установлены, например, в коридорах, при входах в здание, в рабочих кабинетах, лифтах, но ни в коем случае не в туалетах, раздевалках и душевых. Видеонаблюдение должно производиться открыто, а не тайно, иначе это будет уже слежка за сотрудниками, запрещенная законодательством, и работодатель в данном случае может быть привлечен к ответственности [6]. Скрытое видеонаблюдение возможно только в рамках оперативно-розыскных мероприятий уполномоченными на то лицами [4]. Видеонаблюдение за работником должно производиться исключительно в рабочее время [7].

Работник имеет право на полную достоверную информацию об условиях труда [2, ст. 21], поэтому работодателю либо следует разработать положение относительно установки камер видеослежения и целесообразности видеонаблюдения за работниками [5], либо внести необходимые сведения в правила внутреннего трудового распорядка [6].

При этом суды расходятся во мнениях, является ли установка видеокамер существенным изменением трудового договора, которое фиксируется, согласно Трудовому кодексу РФ, за 2 месяца (ст. 74), или не является таковым.

Так, Нагайбакский районный суд Челябинской области в своем решении от 20.09.2018 г. установил, что для фиксации изменений условий труда, а именно – установки камер видеонаблюдения, работодатель обязан уведомить работника не позднее чем за два месяца о предстоящих изменениях (ст. 74 ТК РФ) [10].

Решением Ленинградского районного суда г. Калининграда напротив, установлено, что согласно положениям ст. 57 ТК РФ наличие или отсутствие камер видеонаблюдения на рабочем месте не отнесено к существенным условиям труда, и, следовательно, не требуется соблюдения требований ст. 74 ТК РФ при введении видеонаблюдения. Увольнение по п. 7 ч. 1 ст. 77 ТК – отказ работника от продолжения работы в

связи с изменением определенных сторонами условий трудового договора – суд признал незаконным [11].

Такой же позиции придерживается и Мичуринский городской суд Тамбовской области, который в своём решении от 15 июля 2016 г. по делу № 2-947/2016 указал, что исходя из смысла ст. 57 Трудового кодекса РФ наличие или отсутствие видеонаблюдения не относится к существенным условиям трудового договора [12].

В условиях нахождения на рабочем месте понятие частной жизни и тайны переписки имеет тонкую грань: работник по неосмотрительности может совершить действия, раскрывающие моменты его частной жизни. Постоянное наблюдение за работником в течение дня (смены) может привести к тому, что работодателю может стать известна какая-либо информация относительно частной жизни работника. Непрерывный контроль за работником принимает агрессивный характер и становится похожим на слежку [9]. Применение дистанционного способа наблюдения за работниками должно отвечать следующим принципам: работодателю следует оценивать только те действия или бездействие, которые относятся непосредственно к трудовой функции работника и только в рабочее время, во время отдыха работник не должен находиться под наблюдением; избегать непрерывного наблюдения за работником в течение всего рабочего дня без должной необходимости.

Внедрение такого вида контроля за работником как видеонаблюдение, с одной стороны, приносит пользу, поскольку во многом является гарантом безопасности предприятия, сохранности ценностей, повышения уровня эффективности деятельности работника. С другой – велик шанс необоснованного вторжения в личное пространство работника при непрерывном наблюдении в течение всего рабочего дня (смены), поскольку в условиях многочасовой работы и выполнения прямых трудовых обязанностей сотрудник совершает и некоторые действия частного характера: звонки по телефону родным, прием лекарств и пр. Отношения в этой области требуют дальнейшего уточнения и регулирования со стороны законодателя.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 14.03.2020 № 1-ФКЗ) // Собрание законодательства РФ, 01.07.2020, № 31, ст. 4398.

2. Трудовой кодекс РФ № 197-ФЗ от 30.12.2002 (в ред. от 07.10.2022, с изм. от 15.07.2022) // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru

3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ред. от 14.07.2022) // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru

4. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» (ред. 28.06.2022) // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru

5. Дячук М. «Большой брат» на работе. Регламентируем использование техсредств контроля за сотрудниками // Кадровая служба и управление персоналом предприятия. 2021. № 12. С. 36 – 45.

6. Егорова Е.С. Видеонаблюдение на рабочем месте // В сборнике: Правовые и гуманитарные исследования. Сборник научных статей студентов и аспирантов. Санкт-Петербург, 2016. С. 37-40.

7. Корнеюк А.Л. Видеонаблюдение в организации: вопросы законности и целесообразности // Вестник № 3 / 2018. С. 58-63.

8. Материалы сайта SuperJob https://www.superjob.ru/research/articles/113484/3-iz-4-sotrudnikov-ne-protiv-sistem-ofisnogo-videonablyudeniya/ Дата обращения: 17.11.2022 г.
9. Офман Е.М. Наблюдение и контроль в трудовых отношениях: баланс прав и интересов работников и работодателей //Журнал российского права. 2021. Т. 25. № 11. С. 73-87.
10. Решение Нагайбакского районного суда Челябинской области № 2-246/2018 2-246/2018~М-238/2018 М-238/2018 от 20 сентября 2018 г. по делу № 2-246/2018 // https://sudact.ru/ (дата обращения: 18.11.2022).
11. Решение Ленинградского районного суда г. Калининграда № 2-2243/2017 2-2243/2017~М-1140/2017 М-1140/2017 от 25 мая 2017 г. по делу № 2-2243/2017 // https://sudact.ru/ (дата обращения: 18.11.2022).
12. Решение Мичуринского городского суда Тамбовской области № 2-947/2016 2-947/2016~М-598/2016 М-598/2016 от 15 июля 2016 г. по делу № 2-947/2016 // https://sudact.ru/ (дата обращения: 18.11.2022).

УДК 004.6

Малышев Василий Михайлович, студент, Комсомольский-на-Амуре государственный университет
Malyshev Vasily Mikhailovich, student of Komsomolsk-na-Amure State University
Малышева Наталья Васильевна, кандидат филологических наук, доцент,
Комсомольский-на-Амуре государственный университет
Malysheva Natalia Vasilievna, PhD in Philology, Associate Professor, Komsomolsk-na-Amure State University

КОНФИДЕНЦИАЛЬНОСТЬ ЛИЧНОЙ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

CONFIDENTIALITY OF PERSONAL INFORMATION IN SOCIAL NETWORKS

Аннотация. Защита конфиденциальности личной информации в интернете стала одной из насущных проблем как среди пользователей, так и компаний, предоставляющих социальные сети. Большинство компаний разработали несколько методов для снижения угроз и рисков для конфиденциальности пользователей. Эти риски включают в себя незаконное использование личной информации, которое может привести к таким действиям как кража личных данных. Поскольку большинство пользователей используют свои мобильные телефоны для получения доступа в Интернет, необходимо создать настройки конфиденциальности, совместимые с мобильными телефонами. Метод выбора настроек конфиденциальности также должен быть упрощен, чтобы дать пользователям четкое представление о данных, которые будут переданы другим.
Abstact. Protecting personal information privacy has become a controversial issue among both users and online social network providers. Most providers have developed several techniques to decrease threats and risks to the users' privacy. These risks include the illegal use of personal information which may lead to such acts as identity theft. As most users use their mobile phones for Internet services, privacy settings that are compatible with mobile phones need to be developed. The method of privacy setting selection should also be simplified to provide users with a clear picture of the data that will be shared with others.
Ключевые слова: безопасность, персональные данные, информация, данные, социальная сеть, конфиденциальность, защита, технологии.
Key words: security, personal data, information, data, social network, privacy, protection, technology.

Информационно-коммуникационные технологии (ИКТ) играют важную роль в современном сетевом обществе. Они повлияли на онлайн-взаимодействие между пользователями, которые понимают, что такое средства безопасности и их значение для частной жизни. Существует необходимость в разработке бóльшего количества механизмов безопасности для различных коммуникационных технологий, особенно для онлайновых социальных сетей.

Конфиденциальность имеет большое значение для разработки систем безопасности. Большинство компаний, предоставляющих социальные сети, предлагают настройки конфиденциальности, позволяющие разрешить или запретить другим пользователям доступ к личной информации. Например, на сайте MySpace есть настройки конфиденциальности для людей младше 18 лет, чтобы содержание их профиля было доступно только для их друзей и других людей младше 18 лет. В дополнение к расширению использования мобильных интернет-устройств некоторые сайты социальных сетей предоставили пользователям мобильные версии для поддержки различных типов дисплеев мобильных телефонов.

Итак, целью данной статьи является описание взаимосвязи между настройками конфиденциальности личной информации в онлайн-социальных сетях и их применимостью для мобильных интернет-устройств.

В соответствии с поставленной целью, определим круг задач:

1 Определить понятие «конфиденциальность» в ИКТ.

2 Уточнить понятие «конфиденциальность» применительно к социальным сетям.

3 Привести примеры нарушения конфиденциальности в социальных сетях.

Расширение использования информационно-коммуникационных технологий в современном мире оказало значительное влияние на взаимодействие между пользователями. Это особенно актуально для людей, которые используют мобильные устройства для общения друг с другом или для доступа в Интернет. Пользователям мобильного интернета сложно понять, где и как хранится их информация и кто уполномочен ее использовать. Поэтому защита данных пользователей мобильного интернета и повышение их уверенности в конфиденциальности данных стали настоящей проблемой.

Cavoukian (2009) ввел термин «конфиденциальность при проектировании», который означает необходимость решения проблем конфиденциальности с самого начала. Автор определил его как философию для улучшения проектирования путем включения вопросов конфиденциальности в качестве требований в такие области проектирования, как технологическое проектирование, бизнес-практика и физическое проектирование [1].

Проблема «конфиденциальности при проектировании» стала основной при разработке онлайн-приложений. Различные провайдеры социальных сетей, например, Facebook, Google и Twitter, соревнуются в обеспечении такого уровня приватности в своих приложениях, который вызывал бы доверие у пользователей.

Использование концепции «приватности по замыслу» в качестве стандарта для разработки приложений даст пользователям больше полномочий решать, какой информацией они хотят делиться с кем-либо.

Представим определение термина «конфиденциальность».

В контексте ИКТ существуют различные определения конфиденциальности. Bünnig и Cap описали конфиденциальность как защиту личной информации от неправомерного использования злоумышленниками и разрешение определенным уполномоченным лицам доступа к этой личной информации, делая ее видимой для них [2]. Ni. и другие соавторы в статье [3] определили конфиденциальность как набор политик конфиденциальности, которые заставляют систему защищать частную информацию. Taheri утверждает, что конфиденциальность особенно важна в широком спектре приложений, которые стремятся защитить информацию о местоположении пользователя и скрыть некоторые детали от других. Поскольку понятие приватности многогранно, ни одно

определение приватности не охватывает все аспекты этого термина [4]. Поэтому, основываясь на определении приватности, данном Bünnig, в данном исследовании рассматривается в первую очередь информационная приватность [2].

3 Конфиденциальность социальных сетей.

Пользователи социальных сетей могут делиться различными аспектами личной информации с другими людьми; однако эти детали могут быть использованы «друзьями» не по назначению. Исследование Gross R и Acquisti A. [5], посвященное вопросам конфиденциальности пользователей Facebook, показало, что 91 процент пользователей загрузили свои фотографии, 88 процентов поделились датой своего рождения, 40 процентов показали свой номер телефона, а 51 процент написали свой текущий адрес. Подобный обмен личной информацией может привести к злоупотреблению данными, намеренному или нет. Например, некоторые люди делятся со своими друзьями такими данными профиля, как полное имя, пол и номер телефона. Если аккаунт в социальной сети одного из друзей пользователя будет взломан, спаммер или хакер может использовать личные данные для шантажа пользователя. Другой пример – неправомерное использование данных о статусе отношений. Если пользователь X помолвлен с пользователем Y, и пользователь X скрывает статус отношений в своем профиле, а пользователь Y - нет, то другие пользователи, которые могут видеть данные его профиля, могут узнать статус отношений пользователя X через профиль пользователя Y.

Также, известно, что пожилые пользователи на своих аккаунтах в социальных сетях, более осторожно относятся к размещению личной информации, такой как дата рождения, список друзей и информация о школе, чем более молодые пользователи. Следовательно, пожилые пользователи Интернета более обеспокоены конфиденциальностью личной информации, чем молодые пользователи. Некоторые из молодых пользователей публикуют собственную информацию, не зная о рисках, которые могут возникнуть в результате неправильного использования этих данных. Интернет-среда может быть опасной для пользователей, независимо от возраста, из-за возможной утечки личных данных.

Gross [5] приводит случай с американскими спортсменами, чьи фотографии, размещенные в Интернете, были неправомерно использованы сайтом, публиковавшим истории о скандалах в спорте.

Campisi P., Maiorana E. И Neri A. [6] провели исследование на выборке из 4000 студентов Университета Карнеги-Меллон, пользующихся аккаунтами в социальных сетях. Они обнаружили, что значительная часть студентов не заботится о рисках конфиденциальности, которые могут увеличить вероятность неправомерного использования личной информации студента третьими лицами. Другое исследование тех же авторов утверждает, что более 77 процентов респондентов не читают политики конфиденциальности.

Возможность контролировать параметры конфиденциальности очень важна для повышения доверия пользователей к провайдерам социальных сетей. Поскольку пользователи Интернета представляют различные культуры и возрасты, опции конфиденциальности должны быть понятными, простыми и удобными в использовании. Пользователи должны иметь возможность в любое время контролировать свои опции конфиденциальности. Эти параметры конфиденциальности позволяют пользователям принимать или отклонять. Например, некоторые пользователи не хотят публиковать конфиденциальную информацию, такую как информацию о здоровье или медицинскую информацию. Эти пользователи знают, что люди с менее благородными намерениями могут причинить вред взрослым или детям, злоупотребляя их личной информацией.

Исследование, проведенное Casarosa [7], показало, что несовершеннолетние интересуются новыми технологиями и Интернетом, и к ним могут обращаться незнакомые люди в Интернете с просьбой завязать дружбу. Когда веб-сайт публикует личную

информацию несовершеннолетнего без предоставления родителям (или опекуну ребенка) права выбора параметров конфиденциальности, потенциальные хищники могут использовать некоторые личные данные несовершеннолетнего.

Итак, обзор зарубежных источников по проблеме конфиденциальности личной информации в социальных сетях позволил выявить два направления работы: 1) повышение осведомленности пользователей о потенциальных угрозах размещения личной информации различного уровня в социальных сетях, 2) разработка протоколов и алгоритмов защиты персональных данных со стороны провайдеров социальных сетей и приложений.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Cavoukian, A. Privacy by design…Take the Challenge. Information and Privacy Commissioner of Ontario. – Canada, 2009, pp. 3-6.

2 Bunnig, C., Cap, C. H. Ad Hoc Privacy Management in Ubiquitous Computing Environments // Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services. CENTRIC '09. Second International Conference. 2009. pp.85-90.

3 Ni, Q., etc. Privacy-aware role-based access control // ACM Transactions on Information and System Security (TISSEC). 2010. 13, 24.

4 Taheri, S.; Hartung, S.; Hogrefe, D. Achieving Receiver Location Privacy in Mobile Ad Hoc Networks // Social Computing (SocialCom), IEEE Second International Conference. 2010. pp.800-807.

5 Acquisti, A. & Gross, R. Imagined communities: Awareness, information sharing, and privacy on the Facebook, Lecture Notes in Computer Science. – Michigan, 2006, pp. 36-58.

6 Campisi, P., Maiorana, E.; Neri, A. Privacy protection in social media networks a dream that can come true? // Digital Signal Processing (16th International Conference), 2009, pp.1-5.

7 Casarosa, F. Child Privacy Protection Online: How to Improve It through Code and Self-Regulatory Tools, 2010. - URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1561570 (дата обращения: 06.11.2022).

УДК 004.6

Малюта Артем Павлович, студент, Комсомольский-на-Амуре государственный университет
Malyuta Artem Pavlovich, student, Komsomolsk-na-Amure State University
Лопатина Ольга Ивановна, старший преподаватель, Комсомольский-на-Амуре государственный университет
Lopatina Olga Ivanovna, senior lecturer, Komsomolsk-on-Amur State University

ХАКЕРСТВО КАК УГРОЗА СОХРАННОСТИ ЛИЧНОЙ ИНФОРМАЦИИ В КИБЕРПРОСТРАНСТВЕ

HACKING AS A THREAT TO THE SECURITY OF PERSONAL INFORMATION IN CYBERSPACE

Аннотация. Целью данной работы было изучение угроз информационной безопасности, информационной угрозы и источника угроз безопасности с помощью агентов угроз. Она была посвящена значению понятия "хакеры" и восприятию общественностью слова "хакеры" с особым акцентом на различные типы хакеров в организациях и в обществе. Эмпирическая литература предлагает лучший способ предотвращения проблем взлома в обществе и показывает, что стратегии мотивации белых шляп, черных шляп и хакеров-шпионов в значительной степени задействованы и эффективны для проверки работы организаций.

Abstract. The purpose of this paper was to examine threats to information security, information threat and the source of security threats through threat agents. It focused on the meaning of 'hackers' and the public perception of the word 'hackers' with a particular focus on the different types of hackers in organisations and in society. The empirical literature offers the best way to prevent hacking problems in society and shows that white hat, black hat and spy hacker motivation strategies are heavily leveraged and effective for auditing organisations.
Ключевые слова: угрозы информационной безопасности, информационная угроза, источник угроз безопасности и хакеры.
Key words: information security threats, information threat, security threats source and hackers.

Мир превратился во всемирный город благодаря повсеместному использованию Интернета, где с помощью одного щелчка мыши мысль одного человека может достичь миллиардов людей по всему миру. Преимущества информации для корпораций просто непостижимы. Информация на сегодняшний день является основным направлением деятельности организаций и экономик в связи с глобализацией продуктов и рынков. Препятствие, создаваемое территорией, начинает сходить на нет, поскольку виртуальные организации работают круглосуточно. Возросшая зависимость организаций от информации, соответственно, привела к увеличению зависимости cia (конфиденциальность, целостность и доступность) - это три основные характеристики информационной безопасности. Конфиденциальность гарантирует, что к данным имеют доступ только те, кто имеет на это право, целостность информации служит состоянием полноты и отсутствия повреждений, а доступность позволяет пользователям или другим системам получить доступ к информации.

Информационная безопасность - это защита данных и их основных компонентов. Ferrari и Thuraisingham представили информационную безопасность как защиту информации и структур от опасностей, например, несанкционированного доступа, незаконного использования, воздействия, прерывания, изменения или уничтожения. Согласно данным института Ponemon, Уолтерс и Уолтерс выяснили, что разрывы в информационной безопасности происходят, когда информация не защищена должным образом, и несанкционированные люди могут получить к ней доступ. Для организаций разрыв регулярно включает в себя настоящие бюджетные проблемы, дорогостоящие иски, репутационный ущерб и в возмутительных случаях потерю бизнеса. Оптовое мошенничество, несчастья, связанные с деньгами, и шокирующая оценка - вот лишь часть результатов взлома информации для людей. Восстановление информации занимает много лет, а ущерб, связанный с деньгами, является жестоким.

Информационная безопасность имеет широкое распространение и включает в себя специализированные, поведенческие, административные, философские и иерархические методологии, которые рассматривают страхование и сдерживание опасностей для информационных ресурсов. Несмотря на то, что часть вопросов об информационных системах в области инфобезопасности рассматривает социально-философские проблемы или социально-авторитетные проблемы, в основном они сосредоточены вокруг специализированных вопросов, касающихся разработки и использования подсистем безопасности. Например, передовые технические подходы для решения проблемы предотвращения вторжения в авторитетные структуры, обнаружения атак типа "отказ в обслуживании" и более продвинутые решения для защиты брандмауэров.

Хотя эти технические, внешне ориентированные усилия важны, одна зона, которая является подавляющим недостатком в законной защите информационных ресурсов, - это индивидуальный клиент внутри организации. Это особенно важная проблема, поскольку, по оценкам исследователей, около половины вторжений и нарушений безопасности происходят изнутри организации авторитетными инсайдерами. До недавнего времени исследований, изучающих операционный аспект информационной безопасности, не хватало.

Однако с совершенствованием информационно-коммуникационных технологий и расширением доступа к интернету организации оказываются беззащитными перед различными видами угроз. Действительно, их информация подвергается цифровым атакам и последующему ущербу. Опасности исходят из различных источников, например, из учения представителей или нападения программистов. Несчастья, связанные с финансовыми потерями, вызванными нарушениями безопасности, по большей части не могут быть определенно выделены, поскольку критическое число несчастий происходит от менее масштабных эпизодов безопасности, что создает недооценку шансов безопасности информационной системы. Следовательно, менеджеры должны знать об опасностях, которые влияют на их преимущества, и осознавать их влияние, чтобы понять, что они должны делать, чтобы противостоять нападениям, выбирая подходящие контрмеры.

По мере того, как современность киберхакеров продолжает расширяться, их методы и цели также совершенствуются. Вместо того чтобы создавать обширные интернет-черви, которые стали так хорошо известны, эти преступники в настоящее время тратят больше энергии на нарушения, связанные со сбором богатства, включая введение в заблуждение и кражу информации. Cyber-media india online ltd, рекомендует, что поскольку домашние куэсты регулярно предпринимают наименьшие усилия по созданию системы безопасности, они стали наиболее широко ориентированы на сбор. Кибермедиа сообщает, что 86% всех хакерских атак приходится на домашних пользователей. По мере роста числа атак на домашних клиентов появляются новые системы, включая использование вредоносного кода для атак на веб-программы и настольные приложения.

Дамико утверждает, что эффективные и действенные методы исследования могут ограничить вероятность взлома. Хотя пользователи персональных систем могут не чувствовать, что они связаны с системой, любое действие в Интернете может считаться "организованным действием". Поэтому меры безопасности, используемые системами, могут быть полезны и домашним пользователям. Коммутаторы и брандмауэры могут регулировать доступ к домашнему компьютеру, но могут использоваться и более специфические меры.

Безопасность верхнего уровня рассматривала различия в системах предотвращения сетевых вторжений и обнаружения сетей. Согласно его выводам, системы предотвращения "автоматически обнаруживают и блокируют вредоносный сетевой трафик и трафик приложений, позволяя при этом легитимному трафику продолжать движение к месту назначения". Далее говорится, что обнаруженная система может заметить необоснованную активность, но где защита от быстро действующих атак? Полностью защищенная система может остановить и предотвратить проникновение вредоносных сайтов в компьютерную систему или получение доступа к ней. "Система предотвращения должна постоянно работать с задержкой, подобной задержке коммутатора". В связи с развитием технологий старые пользователи технологий не могут быть защищены на основе предыдущих технологий, они должны быть современными, чтобы победить вредоносное программное обеспечение.

Система защиты от вирусов и вредоносных программ не должна блокировать сайты, не представляющие опасности для системы, даже если система находится под угрозой атаки. Она должна иметь степень защиты от вредоносных программ и регулярно обновляться.

По сути, персональные пользователи системы должны знать различные техники, которые используются для взлома и проникновения в компьютерную систему. При взломе человек может использовать различные инструменты для доступа к информации через всемирную паутину. Следует помнить, что система не всегда крадет полезные данные, она также может быть использована для сохранения контента (например,

пиратских фильмов) или система может быть завербована в онлайновую "армию ботов". Для того чтобы повысить безопасность частного владельца от хакеров, можно предпринять некоторые шаги, например, убедиться, что антивирусная система его компьютера обновляется. Пользователи компьютеров всегда подвергались атакам вредоносных программ из-за небрежного отношения к обновлению программного обеспечения, за которое они заплатили. Вирусная база данных должна постоянно обновляться, потому что вредоносные угрозы всегда продолжают трансформироваться, поэтому обновления программного обеспечения всегда доступны, в ситуации, когда оно не обновляется, система пользователя может быть заражена вредоносным программным обеспечением.

Hackingalert предложил способ, с помощью которого пользователи могут получить решение проблемы, установив соответствующий брандмауэр. Брандмауэр действует как щит, предотвращающий несанкционированный доступ к компьютерной системе. Однако брандмауэр не стирает данные, которые хранятся в системе. Для обеспечения большей безопасности необходима подписка на антивирусную программу, так как в случае, если вирусу удалось обойти брандмауэр, он не сможет пройти через эффективный антивирус. На рынке существует множество троянских и вирусных программ, и использование различных типов поможет устранить угрозы для сети или системы.

Хакеры - это мудрые люди, которые, возможно, изначально не испытывают страсти к своему таланту, но делают это ради денег. Основной мотив хакеров - сделать информацию доступной для всех, и они считают правильным использовать для достижения своей цели программы, созданные кем-то другим. Прежде чем мы продолжим, необходимо понять, что такое хакер.

В первую очередь, хакер не может считаться преступником, потому что он не нарушает закон и не запускает вирус в систему. Точно так же хакер не может рассматриваться как ребенок, который просто сидит, ест и наблюдает за своим окружением.

Тот, кто занимается взломом, обычно не является компьютерным гуру, потому что не может ввести коды безопасности всех веб-сайтов или программных приложений. Точно так же он не тот, кто просто сидит и занимается плотницкой работой, например, собирает и соединяет дерево, чтобы сделать стул или мебель. Аналогично выводам Санглахи хакер обладает некоторыми чертами и характеризуется как человек с интересными чертами, он использует свой мозг для нестандартного мышления и обычно пытается сделать то, во что другие люди не верят или даже не думают делать. Сабахи считает, что тот, кто исследует и создает новые вещи, новые эпизоды, а также делает вещи так, как никто не представлял и не думал, является хакером.

В 2013 году все эти определения превратились в значительно более негативные значения. Согласно словарю Merriam-webster, "хакер" описывается как "человек, который незаконно получает доступ к информации в компьютерной системе и иногда вмешивается в нее". "Это определение заставило многих людей бояться компьютерных хакеров, но не все хакеры - плохие люди. Хакеров можно разделить на различные категории, которые рассмотрены ниже.

По словам эксперта по онлайн безопасности intel security, компьютерные хакеры обычно делятся на различные типы: белые шляпы, черные шляпы, серые шляпы, скрипткидди, хактивисты, кибертеррористы, хакеры-шпионы, фрикеры, и последний хакер мотивирован правительством, известным как спонсируемые государством хакеры.

Белые шляпы пытаются помочь предотвратить взлом слабых систем и пытаются сделать Интернет более безопасным местом для людей. Черные шляпы делают все наоборот; они создают проблемы и иногда могут навредить людям и компаниям, крадя их личные данные, деньги и другие вещи. Хакер в серой шляпе - это человек, который находится между хакером в белой шляпе и хакером в черной шляпе. Обычно "серая шляпа" осуществляет взлом без разрешения администраторов сети, которую он взла-

мывает. Но он будет раскрывать уязвимости сети администраторам и предлагать исправление уязвимости за деньги. script kiddies — это уничижительный термин для хакеров "черной шляпы", которые используют заимствованные программы для атак на сети и порчи веб-сайтов в попытке сделать себе имя. Хактивист - хакер с политическими намерениями. Хактивист обладает теми же навыками, что и хакер, и использует те же инструменты, что и хакер.

Основная причина взлома - привлечение внимания. Киберхакеры обычно имеют политический или религиозный мотив, соответствующий их убеждениям, и пытаются создать хаос и напряженность, дестабилизируя работу критически важных объектов. Хакеры обычно планируют похитить секреты и получить доступ к самым важным файлам безопасности. Хакеры могут действовать в пределах юрисдикции организации, где они действуют как шпионы, или они могут действовать извне. Основная причина хакерства - выполнение работы, за которую им платят. Тот, кто взламывает карту предоплаты без оплаты, также является хакером. Хакеров может использовать государство или правительство для получения секретов своих врагов. Они используют всемирную паутину для сбора информации о конкретном правительстве. Девять из этих групп используют различные стратегии взлома, которые они применяют для выполнения своих задач. Многие хакеры, как "черные шляпы", так и "белые шляпы", работают в организациях.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Кузяев, Н. С. Методы взлома и защиты учетных записей в социальных сетях / Н. С. Кузяев // Лучшая студенческая статья 2016 : сборник статей Международного научно-практического конкурса. – Пенза : ИП Гуляев Герман Юрьевич, 2016. – С. 34-42. – EDN VXWNYL.

2 Магеррамов, З. Т. Применение модели рисков информационной безопасности / З. Т. Магеррамов, Х. В. Амирасланов, М. С. Алишов // Современная наука, общество и образование: актуальные вопросы, достижения и инновации : монография. – Пенза : Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. – С. 188-201. – EDN XXMUVL.

УДК 347.77(510)

Минкина Екатерина Сергеевна, студент, Комсомольский-на-Амуре государственный университет
Minkina Ekaterina Sergeevna, student of Komsomolsk-na-Amure State University
Когай Сергей Геннадьевич, старший преподаватель, Комсомольский-на-Амуре государственный университет
Kogai Sergei Gennadevich, Senior Lecturer, Komsomolsk-on-Amur State University

КРАТКИЙ АНАЛИЗ НАРУШЕНИЙ ПРАВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В СЕТЕВОЙ КОММУНИКАЦИИ КНР

A BRIEF ANALYSIS OF INTELLECTUAL PROPERTY INFRINGEMENTS IN CHINA ONLINE COMMUNICATIONS

Аннотация. С развитием науки и техники и диверсификацией средств связи нарушения в сетевом общении приобрели взрывной характер, диверсификация субъектов общения, неурегулированность коммуникационных площадок, неконтролируемая скорость коммуникации сделали сетевую коммуникацию прав интеллектуальной собственности затруднённой. С 2006 года Госсовет КНР обнародовал «Положение о защите права на информационное сетевое общение», в котором впервые с законодательной точки зре-

ния были разделены обязанности различных субъектов сетевого общения, сбалансированы интересы различных правозащитников, и стала одной из базовых систем правовой защиты прав интеллектуальной собственности. Однако слабая правовая осведомленность правонарушителей, отсутствие регулирующих полномочий и отсутствие отраслевой самодисциплины – все это проблемы, которые необходимо срочно решить в сфере правовой защиты от нарушений и прав интеллектуальной собственности в текущей сетевой коммуникации.

Abstract. With the development of science and technology and the diversification of means of communication, violations in network communication have become explosive, the diversification of communication subjects, the unsettled communication platforms, and the uncontrolled speed of communication have made network communication of intellectual property rights difficult. Since 2006, the State Council of the People's Republic of China promulgated the "Regulations on the Protection of the Right to Information Network Communication", which for the first time, from a legislative point of view, divided the responsibilities of various subjects of network communication, balanced the interests of various human rights defenders, and became one of the basic systems of legal protection of intellectual property rights. However, poor legal awareness of offenders, lack of regulatory authority, and lack of industry self-discipline are all issues that urgently need to be addressed in the field of legal protection against infringement and intellectual property rights in current online communications.

Ключевые слова: сетевая связь, деликтная ответственность, права интеллектуальной собственности, правовая защита.
Key words: network communication, tort liability, intellectual property rights, legal protection.

В условиях развития торгового взаимодействия между странами, а так же ориентации на поощрение высокотехнологического экспорта, особенно актуальным становится вопрос регулирования прав интелектуальной собственности на территории Китая.

О характеристиках нарушения сетевых коммуникаций в Китайской Народной Республике.

Анонимность интернет-среды часто способствует быстрому доступу людей к информации и распространению речи, но в то же время позволяет ущемлению права сетевого общения продолжать размножаться в смеси сознательного и бессознательного. Пользователи онлайн-платформ часто предстают в виртуальном мире как «ложные» личности. Правила платформы не очень обязывают к поведению, а надзор за нарушением также сложно осуществить. В сетевой коммуникации наиболее часто встречаются нарушения авторских прав, патентных прав и прав на товарные знаки. В авторском праве случайная перепечатка без указания источника. После экспоненциального распространения сложно определить ответственность за нарушение промежуточного распространителя. Что касается патентных прав и прав на товарные знаки, то для того, чтобы обслуживать трафик интернет-коммуникаций, подделка и искажение связанных продуктов часто делаются привлекательным образом, и происходят нарушения. В виртуальной сетевой среде, где преобладает трафик, распространение сетевой информации претерпело огромные изменения по сравнению с традиционным поведением при распространении. В этом случае закон должен дать более полную защиту правообладателям. Технические меры защиты стали важной частью защиты права на сетевое общение. Столкнувшись с явлением, когда преступники пользуются техническими лазейками, активно уничтожают оригинальную технологию по субъективной воле, а также распространяют и загружают аудиовизуальные произведения без разрешения правообладателя, следует определить как нарушение.

Сложное управление деликтной ответственностью отстает.

Сетевое общение изменило традиционный режим общения сверху вниз и предоставило пользователям равные права на общение с организациями через сетевые плат-

формы. Установление равного статуса не только стимулирует идею общественности активно выражать свое мнение, но и позволяет им участвовать в распространении онлайн-информации посредством репостов, лайков и комментариев. Из-за участия общественности и отсутствия строгих проверок со стороны «привратников» произведения, нарушающие авторские права, часто получают непредсказуемое распространение. Например, во время трансляции китайского телевизионного сериала «Во имя народа - 人民的名义» пиратские ресурсы в Интернете разлетались по всему миру, а стремительное распространение онлайн-площадок часто становилось резервуаром для пиратства. Разгул пиратства — типичный представитель нарушения авторских прав в сетевой коммуникации, но определить ответственность очень сложно. В соответствии с принципом деликтной ответственности в действующей правовой системе КНР субъективная воля становится основным условием определения ответственности. Однако сложно иметь единый стандарт «субъективного намерения» на интернет-платформе, существует множество причин для «случайно нажал на скачивание», «подумал, что интересно поделиться с друзьями», «я также видел это у других». ", что делает субъективным желание определить ответственность за нарушение стало сложной проблемой в настоящее время.

Трудности, с которыми сталкивается правовая защита прав интеллектуальной собственности в сети Интернет Китая.

Законодательство об интеллектуальной собственности отстает, а правоприменительные нормы несовершенны.

С появлением в 2006 году первого законодательного акта об охране интеллектуальной собственности законы и положения КНР в области интеллектуальной собственности постепенно совершенствовались, в основном включая «Закон об авторском праве», «Закон о патентах» и «Закон о товарных знаках». По сравнению с зарубежными странами, в КНР относительно немного законодательства об интеллектуальной собственности и относительно мягкие меры наказания. Сдерживание нарушений прав интеллектуальной собственности является недостаточным, и охват защиты интеллектуальной собственности нуждается в дальнейшем расширении [2]. Три традиционных закона могут быть основой для решения большинства проблем сетевого общения, но в реальном общении все еще существует множество других проблем, связанных с нарушением прав. Например, при регистрации почтовых ящиков крупных порталов при согласии с условиями обслуживания в начале регистрации по умолчанию предоставляется право собственности на все аудиовизуальные материалы и текстовую информацию. Это не только нарушение неприкосновенности частной жизни, но и нарушение прав интеллектуальной собственности, но трудно найти основание для осуждения в законе.

Прорывной путь правовой защиты прав интеллектуальной собственности в сетевой связи

Усовершенствовать законодательство об интеллектуальной собственности и усилить функции государственного надзора.

Столкнувшись с относительным отставанием действующего законодательства о правах интеллектуальной собственности на сетевое распространение, необходимо не только совершенствовать соответствующее законодательство, но и в полной мере использовать действующую правовую защиту для осуществления средств правовой защиты. Во-первых, усилить определение предмета ответственности за нарушение при совершенствовании законодательства, особенно определение поставщиков сетевых услуг, включая права и обязанности основных веб-порталов и платформ социальных сетей, а также разумность и законность соглашений о конфиденциальности пользователей. Это важная правовая основа для того, чтобы «сетевые посредники» действовали в качестве «привратников». Каждая платформа также может сформировать соглашение о платформе в соответствии со своей ситуацией для дальнейшей очистки сетевой среды. Во-

вторых, улучшить справочный стандарт для установленной законом компенсации. Разблокируйте канал жалоб правообладателя, поймите фактический ущерб правообладателя, объедините фактический незаконный доход нарушителя, а также объедините профессиональные мнения, чтобы сформировать обязательный законный стандарт размера ущерба с оговоркой о покрытии. В-третьих, в полной мере использовать действующие соответствующие законы и постановления. В судебной практике использовать принципиальное и рациональное использование традиционных законов и постановлений об интеллектуальной собственности для решения онлайн-сценариев, искать различные виды средств правовой защиты от различных нарушений и реагировать на чрезвычайные нарушения и крупномасштабные нарушения.

Поэтому с учетом особенностей уголовных дел и особенностей разных регионов необходимо проводить правовое воспитание в индивидуализированном порядке. В первую очередь необходимо усилить пропаганду и внедрение интернет-морали. Такого рода популяризация права должна начинаться с юных лет, особенно молодежи, и повышать интернет-юридическую грамотность.

В целях дальнейшего усиления защиты прав интеллектуальной собственности в онлайн-общении необходимо сформировать модель, основанную на национальном законодательстве, отраслевой самодисциплине, юридических талантах в качестве связующего звена и участии общественности в качестве основы. Хорошая сетевая среда может быть создана только совместными усилиями нескольких сторон. С точки зрения повышения отраслевой самодисциплины сетевым платформам и поставщикам услуг необходимо совместно сформировать «систему привратника». От просмотра информации до графического редактирования и функционального управления веб-сайтами все должны выполнять свои обязанности по «охране сетевых прав интеллектуальной собственности людей». Сегодня, с ускорением интернет-общения, правовая система КНР в области интеллектуальной собственности начала формироваться. Однако перед лицом сложной и переплетенной сетевой коммуникационной среды, таких проблем, как неясность субъектов правонарушений, трудности с определением ответственности и слабая правовая осведомленность граждан часто появляются в сети. Необходимо ускорить научное законодательство, укрепить отраслевую самодисциплину и постоянно улучшать и совершенствовать с разумными мерами. Только так можно в полной мере гарантировать законные права и интересы субъектов интеллектуальной собственности в сетевом общении, вернуть обществу чистое сетевое пространство.

Несмотря на достигнутый прогресс, определенные трудности в области зашиты прав интелектуальной собственности в КНР по ряду вопросов еще не были разрешены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Фэн Сяоцин. Закон об интеллектуальной собственности [M]. Пекин: Китайский университет политических наук и права, 2008: 176.

2. Лю Сянго. Опыт американской системы авторского права и экономики авторского права для справки［J］. Правовая система и общество, 2019 (33): 90-93.

3. Нарушение прав интеллектуальной собственности в сетевой коммуникации КНР https://www.66law.cn/topic2012/qfglzscq/

4. Непочатова В.М. Роль средств массовой информации в процессе конструирования имиджа страны // Ученые записки Комсомольского-на-Амуре государственного технического университета. 2022. № 6 (62). С. 36-40.

5. Petrunina Z.V., Shusharina G.A. Potential for implementation of Asia-Pacific region experience in developing business-incubators in the Russian Far East // В сборнике: Proceedings of the International Scientific Conference "FarEastCon" (ISCFEC 2020). Серия: Advances in Economics, Business and Management Research. Vladivostok, 2020.

УДК 342.7:004.9

Михалёва Виолетта Сергеевна, студент, Комсомольский-на-Амуре государственный университет
Mikhaleva Violetta Sergeevna, student of Komsomolsk-on-Amur State University
Непочатова Валерия Михайловна, старший преподаватель кафедры «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Nepochatova Valeria Mikhailovna, Senior Lecturer at the Department of "Linguistics and Intercultural Communication" of Komsomolsk-on-Amur State University

ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ В ВЕК ЦИФРОВИЗАЦИИ

THE RIGHT TO PRIVACY IN THE DIGITAL AGE

Аннотация. В данной статье анализируются некоторые аспекты, (практические и теоретические) права на охрану частной жизни в условиях цифровизации общества. Когда мы говорим о персональных данных, на первое место выходит конфиденциальность – это и есть безопасность информации. По сути, конфиденциальность – это право человека остаться неприкосновенным, спокойным и не переживающим из-за угроз, шантажа и банальных рекламных звонков и спамерских писем. Это базис права на неприкосновенность частной жизни, гарантированного верховными законами всех цивилизованных стран мира. Идея прав и свобод человека номинально остается основной базовой идеей, лежащей в основе существования современного государства.
Abstract. This article analyzes some aspects (practical and theoretical) of the right to privacy protection in the conditions of digitalization of society. When we talk about personal data, privacy comes first – it is the security of information. In fact, privacy is a person's right to remain inviolable, calm and not worry about threats, blackmail and banal advertising calls and spam emails. This is the basis of the right to privacy, guaranteed by the highest laws of all civilized countries of the world. The idea of human rights and freedoms nominally remains the main idea underlying the existence of the modern state.
Ключевые слова: цифровизация, конфиденциальность, цифровые технологии, личные данные, права человека, охрана частной жизни.
Key words: digitalization, privacy, digital technologies, personal data, human rights, privacy protection.

The 21st century is approaching the expected digital technologies. Digital technologies can help in acquiring new needs, facilitating social interaction, spreading independent and independent living, and improving governance and various services in our lives.

Digital technologies are the outstanding achievements of mankind and allow you to create unprecedented opportunities, but there is also the risk of losing your data from the collection. Article 23 of the Constitution of the Russian Federation guarantees the right to privacy, personal and family secrets, protection of one's honor and good name.

Indeed, privacy is truly personal data.

The constitutional right of everyone to privacy has received a fairly detailed study in the documents of the Constitutional Court. For example, an explanation of the key concept of "private life". The Constitutional Court calls private life that area of a person's life that relates to an individual, concerns only him and is not subject to control by society and the state, if it is not illegal.

This article provides real examples from the lives of people who have faced infringement on their privacy.

Let's consider the first case. The data of 533 million Facebook users from 106 countries, including 10 million users from Russia, was made public in April 2021.

The data included phone number, Facebook ID, full name, geolocation, geolocation history, date of birth, email address, relationship status, and biography.

This may be a critical threat to the millions of crypto traders and investors who could be vulnerable to SIM swapping and other identity-based attacks.

Among the leaked data of Facebook users, Mark Zuckerberg's data was even found, including a phone number. (Picture 1).

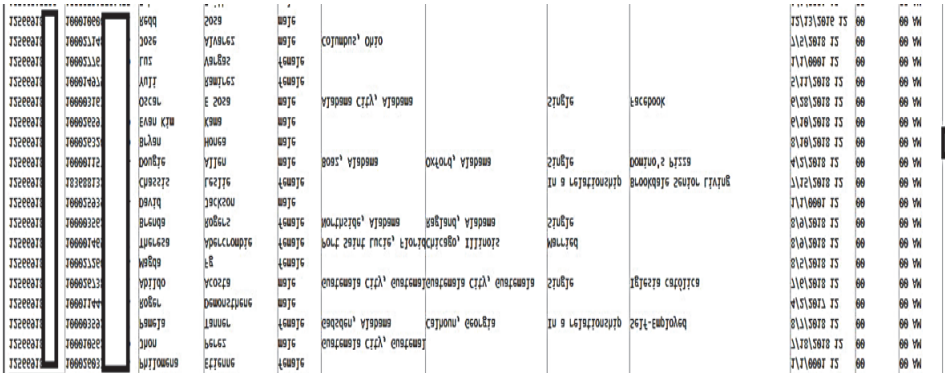

Figure 1 - Data of 533 million Facebook users who leaked to the Web

This example clearly illustrates that attackers can use personal data for their own purposes. Personal information may not always remain confidential. When we consent to the processing of personal data, there is a risk that in the future they (email, number, name) may be located on the Internet.

Leakage of personal data is one of the most important problems in the field of citizens' rights in the digital world, and they have become widespread. This example shows that large companies should invest more resources in monitoring the personal data of customers, and the supervisory authorities in the field of communications, information technology and mass communications should strengthen their control and supervisory functions, and the customers themselves who use the services of sites should be more careful.

Websites, mobile applications and online services regularly collect information about visitors. On the one hand, this is practical - sites remember logins, passwords and automatically enter them to enter your personal account, store links that you previously opened. On the other hand, scammers can hack into your account and gain access to your mail or bank card.

To protect yourself, remember a few rules. That is:

1. Create long passwords, use uppercase and lowercase letters, various characters, numbers. Create your own password for each service and program. Or remember 5 typical passwords, while they should not be the same as the most common passwords.

2. Create long passwords, use uppercase and lowercase letters, various characters, numbers. Create your own password for each service and program. Or remember 5 typical passwords, while they should not be the same as the most common passwords.

3. Do not share too personal information on social networks so that scammers cannot use this information.

4. Keep track of your digital footprint as apps and websites collect your location. It will not be possible to completely hide geolocation, but you can turn it off in those programs in which it is not needed for work. Back up your data, recently there have been more cases of blocking devices for the purpose of ransom.

The right to privacy, being complex and covering many aspects of human life, is becoming increasingly important in the 21st century. It is in the era of informatization that this right, more than ever, needs detailed regulation and protection.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ
1. Baranov V.M. On the legislative definition of "private life" // Citizen's right to information and protection of privacy: Collection of scientific papers, part 1. Nizhny Novgorod, 1999. P. 34-37.
2. Lopatin V.N. Protection of the right to privacy. // Journal of Russian law. 1999. No. 1. P. 85-97.
3. Sokolova I.V. Social Informatics and Sociology: Problems and Perspectives of Interrelation. Moscow: Soyuz, 1999. 228p.
4. Maleina M.N. Personal non-property rights of citizens: concept, implementation, protection. Moscow: MZ-Press, 2001. 244 p.

УДК 347.23

Наливайко Наталья Сергеевна, студент; Комсомольский-на-Амуре государственный университет
Nalivayko Natalia Sergeyevna, student of Komsomolsk-on-Amure State University
Шибико Ольга Сергеевна, кандидат культурологии, доцент, Комсомольский-на-Амуре государственный университет
Sibiko Olga Sergeyevna, PhD in Culture Studies, associate professor, Komsomolsk-on-Amure State University

ПОСЛЕДСТВИЯ КРАЖИ ЛИЧНЫХ ДАННЫХ И МЕТОДЫ БОРЬБЫ В СЛУЧАЕ ИХ УТЕЧКИ

CONSEQUENCES OF IDENTITY THEFT AND METHODS OF COMBATING IN CASE OF ITS LEAKAGE

Аннотация. В докладе приводятся разные виды последствий утечки персональных данных, а также того, каким образом эти последствия оказывают влияние на человека и компании. Авторами рассматриваются различные способы кражи информации. Исследуется как психологический, так и материальный ущерб утечки данных, из чего приводится последующий алгоритм действий для минимизации ущерба компаниям и простым гражданам.
Abstract. The paper presents different types of consequences of personal data leakage, how these consequences affect a person or a company, as well as various ways of information theft by intruders. Both psychological and material damage to the individual or to a company is investigated, and the subsequent algorithm of actions for minimizing damage to companies and ordinary citizens is presented.
Ключевые слова: кража личных данных, раскрытие персональных данных, утечка информации.
Key word: identity theft, disclosure of personal data, leakage of information.

Нынешняя эпоха цифровизации принесла человечеству большие возможности во всех сферах жизни от повседневности до промышленности, от образования до транспорта, от медицины до экономики и т. д. Вместе с тем появились и новые вызовы, которые требуют пристального рассмотрения для их лучшего понимания и нахождения путей решения появляющихся проблем.

Кража личных данных и киберпреступность – сравнительно недавние явления в современном обществе. Эти явления неразрывно связаны с развитием информационных технологий и так называемой цифровизацией многих сфер жизни общества. Различные

аспекты этой проблемы привлекают внимание чиновников, общественных деятелей и, конечно, ученых. Проблемы информационной безопасности изучаются инженерами, социологами, юристами, культурологами, психологами, а также учеными, работающими на стыке этих направлений [1; 2; 5]. В данном докладе, используя междисциплинарный подход, мы рассмотрим такой аспект информационной безопасности, как кража личных данных, ее последствия, а также возможные методы борьбы с этим явлением.

Киберпреступность является одним из самых быстрорастущих видов преступной деятельности в современном обществе. Распространенность этого преступления превосходит преступления, связанные с мошенничеством с кредитными картами и чеками. Кража личных данных происходит, когда человек использует личность другого человека с намерением незаконно получить выгоду. Жертва кражи личных данных может понести не только финансовые потери, но и другие неблагоприятные последствия, например, репутационный ущерб. Что касается юридических лиц, доступ к чужой информации дает компаниям преимущество в конкурентной борьбе, утечка важных данных приводит к финансовым потерям и даже к ликвидации компаний. Поэтому секретная корпоративная информация должна быть защищена на всех этапах использования: при создании, перемещении и хранении.

Развитие информационных технологий увеличивает риск потери данных. Любое вмешательство в системы предприятий или бизнеса, не говоря уже о простых пользователях сети, рискует нанести вред компании, поэтому при использовании электронных носителей и передаче информации может быть полезным ужесточить контроль над каналами передачи информации. Особенно важна защита коммерческой тайны, изобретений, новых разработок, баз данных и служебной переписки.

Основными негативными последствиями утечки конфиденциальной информации являются прямой материальный ущерб, ухудшение репутации компании, потеря клиентов, партнеров, поставщиков, товарных рынков и т.д. Размер ущерба от утечки информации зависит от многих факторов, среди которых принято выделять упущенную выгоду из-за испорченного имиджа; штрафы; компенсационные выплаты по искам; снижение стоимости акций компании применительно к акционерным обществам (если данные попали на рынок инсайдерской информации); прямой ущерб (стоимость разработки конструкторских и технологических решений, проигранные тендеры, незаключенные контракты и другие обстоятельства) [4]. Объем убытков в полной мере оценить сложно, тем более что в России такой статистики нет, а бизнес ориентируется на опыт зарубежных компаний, пострадавших от утечки конфиденциальной информации. Например, согласно исследованию Cost of Data Breach [8], в США потеря клиентов обходится средней компании в 4,35 млн. долларов, и как минимум еще 1,5 млн. долларов тратится на расследование, реабилитацию и судебные издержки.

Похитители личных данных могут использовать любое количество низко- или высокотехнологичных способов, чтобы получить доступ к личной идентификационной информации. Злоумышленники, которым удаётся получить персональные данные, в полной мере могут воспользоваться ими, чтобы нанести максимальный ущерб. И в этом случае речь идёт не только о материальном ущербе, но и серьёзной психологической нагрузке [6; 7].

Как только похитители личных данных получат личную информацию, они могут продолжать тратить деньги, используя номера счетов кредитных и дебетовых карт, чтобы покупать дорогостоящие товары, такие как компьютеры, которые они могут затем легко продать. Кроме того, они могут открывать новые счета кредитной карты, используя имя, дату рождения и SSN. Есть возможность изменить почтовый адрес в учетной записи чужой кредитной карты. Затем самозванец увеличивает расходы на счете. Поскольку счета отправляются на новый адрес, может пройти некоторое время, прежде чем пострадавший осознает, что возникла проблема.

Среди возможных последствий утечки или кражи персональных данных называют оформление автокредитов на украденное имя, установку телефонной или беспроводной связи на имя владельца, подделку чеков или дебетовых карт с последующим обнулением банковского счета, подачу заявлений о банкротстве на чужое имя и т. д. [2; 4]. Все эти последствия негативно влияют на доброе имя, репутацию и психическое состояние людей.

Что касается сферы бизнеса, то значительная часть утечек происходит из-за проблем внутри самой компании, а не только из-за внешних взломов или хакерских атак. Конфиденциальная информация может покидать компанию и по вине сотрудников. К утечке информации могут привести такие действия, как случайное или преднамеренное разглашение конфиденциальных данных, подкуп, шантаж и другие противоправные действия конкурентов или преступников, склоняющих персонал компании к сотрудничеству, отсутствие ненадлежащего контроля и несоблюдение условий обеспечения информационной безопасности, обмен производственным опытом, отсутствие контроля над тем, как сотрудники используют корпоративные информационные системы, а также конфликты между сотрудниками, которые могут быть спровоцированы случайным подбором персонала, отсутствием шагов по построению команды и некоторыми другими кадровыми проблемами [2].

Для борьбы с последствиями утечки личных данных можно применить алгоритм из нескольких шагов: найти и защитить источник утечки; выявить лиц, заинтересованных в утечке кадров с доступом к конфиденциальной информации; определить информацию, которая могла быть затронута утечкой; предупредить об инциденте людей, которым может быть причинен вред украденной информацией; при необходимости обратиться в правоохранительные органы [5].

Если речь идёт о предприятии, то имеет смысл провести анализ активности пользователей в корпоративной сети с тем, чтобы выяснить, кто причастен к утечке информации. Для этого используются системы мониторинга, анализирующие информационные потоки внутри предприятия, или DLP-системы, которые предназначены для защиты от утечек информации из корпоративной сети и от действий инсайдеров. В случае серьезной утечки, действительно, лучше обратиться в правоохранительные органы. Благодаря современным техническим разработкам, для борьбы с последствиями киберпреступлений могут использоваться DLP-системы [3], которые помогают собирать улики, контролируют каналы передачи, формируют отчеты и автоматически оповещают о потенциальных угрозах.

В целом, на основании вышеизложенного можно сделать вывод, что кража персональной информации имеет целый спектр последствий и значительно влияет на жизнь как физических, так и юридических лиц, а самый лучший способ избежать последствий утечки – предотвратить саму утечку. Однако даже если это произошло, стоит не забывать, что такие вещи могут произойти с любым человеком и любой компанией, поэтому необходимо вовремя принимать меры по минимизации ущерба.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Герасимова А. В., Смирнов В. М. Обеспечение сохранности персональных данных в информационном пространстве // Международный журнал гуманитарных и естественных наук. № 5-1, 2021. [Электронный ресурс] URL: URL: https://cyberleninka.ru/article/n/obespechenie-sohrannosti-personalnyh-dannyh-v-informatsionnom-prostranstve (дата обращения: 21.11.2022)

2. Кузьмин А. Ю. Кража персональных данных (криминологический аспект) // Oeconomia et Jus. № 3. 2020. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/krazha-personalnyh-dannyh-kriminologicheskiy-aspekt (дата обращения: 21.11.2022).

3. Мавринская Т. В, Лошкарёв А. В., Чуракова Е. Н. DLP-системы и тайна личных переписок // Интерактивная наука. 2017. №14. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/dlp-sistemy-i-tayna-lichnyh-perepisok (дата обращения: 21.11.2022).
4. Утечка персональных данных: последствия // [Электронный ресурс] URL: https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/utechki-personalnyh-dannyh/posledstviya/ (дата обращения 20.11.2022)
5. Albrecht C. How to protect and minimize consumer risk to identity theft // Journal of Financial Crime. 2011. Vol. 18 (4). Pp. 405-414.
6. Betz-Hamilton A. A Comparison of the Financial, Emotional, and Physical Consequences of Identity Theft Victimization Among Familial and Non-Familial Victims // Journal of Financial Counseling and Planning. 2022. Vol. 33 (2), Pp. 217-227.
7. Exploring the psychological and somatic impact of identity theft // [Электронный ресурс] URL: https://pubmed.ncbi.nlm.nih.gov/14979359/ (дата обращения 20.11.2022)
8. What is the Cost of a Data Breach in 2022? // [Электронный ресурс] URL: https:// www.upguard.com/blog/cost-of-data-breach (дата обращения 20.11.2022)

УДК 82-1/-9

Носаченко Родион Алексеевич, студент; Комсомольский-на-Амуре государственный университет
Nosachenko Rodion Alexeyevich, student, Komsomolsk-na-Amure State University
Шушарин Никита Станиславович, студент; Комсомольский-на-Амуре государственный университет
Shusharin Nikita Stanislavovich, student, Komsomolsk-na-Amure State University
Шушарина Галина Алексеевна, кандидат филологических наук, доцент, Комсомольский-на-Амуре государственный университет
Shusharina Galina Alexeyevna, PhD in Philology, Associate Professor, Komsomolsk-on-Amur State University

НОВЫЕ ЦЕННОСТИ В ЭПОХУ ЦИФРОВИЗАЦИИ

NEW VALUES IN THE DIGITAL AGE

Аннотация. Исследование посвящено выделению физической и экономической безопасности как ценности постиндустриального общества. Прозрачность мира становится ведущей характеристикой современного цифрового общества, с каждым днем становится все сложнее сохранять свою частную жизнь и свои персональные данные. С одной стороны, изменения в обществе требуют прозрачности для рационализации различных процессов в жизнедеятельности социума. С другой стороны человек по собственному желанию рассказывает о своей жизни в Интернет-пространстве.
Abstract. The study is devoted to highlighting physical and economic security as a value of post-industrial society. Transparency of the world is becoming a leading characteristic of modern digital society, each day it becomes more and more difficult to preserve one's privacy and personal data. On the one hand, changes in society require transparency to rationalize various processes in the life of society. On the other hand, a person, of his or her own volition, talks about his or her life in the Internet space.
Ключевые слова: ценность, частная жизнь, цифровизация, постиндустриальное общество.
Key words: value, privacy, digitalization, post-industrial society.

Категория ценности интересовала мыслителей различных времен. Среди философов, которые внесли заметный вклад в понимание ценности можно выделить Г. Лотце, Т. Гоббса, И. Канта, Э. Гуссерля и других. Каждый из названных ученых формировал свою трактовку смыла ценности, тем самым, придавая категории ценности многомерный, междисциплинарный характер.

Философский словарь определяет ценность как философскую категорию, обозначающую социально обусловленные значения материальных и духовных явлений, определяющих смыслы бытия человека и общества в целом [4].

Стремительное развитие информационных технологий является основным признаком постиндустриального общества. Массовая цифровизация приводит к тому, что люди ищут способы адаптироваться к ней через формирование новых ценностей, отличных от традиционных ценностей. Если традиционные ценности подчеркивают важность религии, связи между родителями и детьми, почтительного уважения к старшим и традиционным семейным ценностям, то в современном постиндустриальном обществе ценностью признается индивидуализм, стремление к самовыражению: «В современных постиндустриальных обществах традиционным ценностям противопоставлены светско-рациональные ценности» [3]. Одной из таких ценностей можно назвать – физическая и экономическая индивидуальная безопасность. Современные граждане добровольно отказываются от сохранения своих личных данных в тайне в обмен на тот комфорт, который предоставляет человеку информационное общество. Так, передвижение любого жителя современного города ежедневно фиксируется видеокамерами, разговоры в различных службах по оказанию услуг (скорая помощь, полиция, жилищно-коммунальные службы и т.п.) записываются для обеспечения безопасности. Совсем не так давно, мы могли сделать запрос в справочную службу города и выяснить персональные данные любого человека, проживающего в этом городе. Телефонные справочники с фамилиями и адресами свободно лежали на столах в почтовых пунктах. Сегодня это воспринимается как нарушение права человеку на частную жизнь. Законы в любой стране мира тщательно оберегают сохранение персональных данных.

Стремительное развитие цифровых технологий несет с собой ряд угроз, в частности, персональные данные попадают в руки мошенников, в результате чего происходят кражи денежных средств с банковских карт. Обладание чужими персональными данными представляет ценность для навязываемой рекламы, политического манипулирования.

Особую значимость для человека среди большого массива его персональных данных можно назвать реквизиты банковских карт, информацию о состоянии здоровья. Люди не стремятся разглашать информацию о перенесенных заболеваниях, медицинских обследованиях, посещениях врача, поскольку такая информация может повредить репутации человека, нанести ущерб его профессиональной карьере и т.д. Особую ценность для современного человека представляет его аккаунт в социальных сетях. Аккаунт - обозначение страницы в социальной сети, совокупность личных данных пользователя, индивидуализирующих его [1]. «Сетевой аккаунт сам по себе представляет ценность, и его утрата может быть очень болезненна психологически, а иногда и финансово» [2]. Для простого обывателя опасность представляет взлом личной странички мошенниками и использование ее в корыстных целях, например, с целью объявления сбора материальной помощи, размещения нежелательного и компрометирующего контента и пр. Известно, что аккаунты можно монетизировать за счет предоставления собственной страницы в рекламных целях, чем могут воспользоваться мошенники.

Исследователи с уверенностью говорят, что прозрачность становится ведущей характеристикой современного цифрового общества, с каждым днем становится все сложнее сохранять свою частную жизнь и свои персональные данные. С одной стороны, изменения в обществе требуют прозрачности для рационализации различных про-

цессов в жизнедеятельности социума, например, создание баз данных доноров, суррогатных матерей и пр. С другой стороны человек по собственному желанию рассказывает о своей жизни в Интернет-пространстве, делится с читателями новостями, размещает фотографии своих близких и друзей и т.д.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Босык, О. И. Страница в социальной сети как объект гражданских прав // Наука и инновации XXI века: Сборник статей по материалам VI Всероссийской конференции молодых ученых, Сургут, 27 сентября 2019 года. – Сургут: Сургутский государственный университет, 2020. С. 90-94
2. Макаров, С. Прекрасный, опасный, кибербезопасный мир. Всё, что важно знать детям и взрослым о безопасности в интернете – М., 2022. 568 с.
3. Фактор, А.М. Камолов, С.Г. Никандрова, А.А. Человеческие ценности в цифровую эпоху // Моделирование, оптимизация и информационные технологии. Научный журнал №2(21). 2018. С.86-103.
4. Философская энциклопедия. URL: https:// https://terme.ru/termin/cennost.html

УДК 364.01

Олефиренко Евгения Евгеньевна, студент, Комсомольский-на-Амуре государственный университет
Olefirenko Evgenia Evgenievna, student, Komsomolsk-on-Amur State University
Шинкорук Марина Владимировна, кандидат педагогических наук, доцент, Комсомольский-на-Амуре государственный университет
Shinkaruk Marina, Candidate of Pedagogical Sciences, Associate Professor, Komsomolsk-on-Amur State University

ПРИНЦИП КОНФИДЕНЦИАЛЬНОСТИ В СОЦИАЛЬНОЙ РАБОТЕ КАК ФАКТОР ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛУЧАТЕЛЯ СОЦИАЛЬНЫХ УСЛУГ

THE PRINCIPLE OF CONFIDENTIALITY IN SOCIAL WORK AS A FACTOR TO PROTECT THE PERSONAL DATA OF THE BENEFICIARY OF SOCIAL SERVICES

Аннотация. В статье раскрывается понятие «персональные данные»; рассмотрены проблемы безопасности личности в виртуальном мире; раскрыта важность защиты персональных данных гражданина; охарактеризован принцип конфиденциальности в социальной работе как фактор безопасности получателя социальных услуг в практике учреждения социальной защиты.
Abstract. The article reveals the concept of "personal data"; the problems of personal security in the virtual world are considered; the importance of protecting personal data of a citizen is revealed; the principle of confidentiality in social work is characterized as a security factor for the recipient of social services in the practice of a social protection institution.
Ключевые слова: данные, информация, принцип конфиденциальности, социальная работа, получатель социальных услуг, клиент.
Key words: data, information, confidentiality principle, client.

В сегодняшних реалиях, в век компьютеризации, цифровизации существует угроза незаконного распространения персональных данных гражданина, ведущая к нарушению прав личности и неприкосновенности частной жизни. Это обстоятельство актуализирует поиск путей, направленных на защиту персональных данных личности.

Пользователи смартфонов, компьютеров и других современных электронных устройств оставляют всё больше личной информации в глобальной сети: отправляют копии документов, удостоверяющих личность по незащищенной электронной почте, оставляют данные банковских карт в интернет-магазинах. Этим активно пользуются преступники. По данным министерства внутренних дел Российской Федерации за «январь-сентябрь 2022 года на территории России было совершено 378 510 преступлений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, из них с использованием расчетных (пластиковых) карт – 94 727, фиктивных электронных платежей – 1 042, сети «Интернет» 276 146, средств мобильной связи – 150 099»[5].

Защита персональных данных гражданина закреплена на законодательном уровне. Согласно Федерального закона № 152-ФЗ от 27.07.2006 года «О персональных данных», персональные данные – «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)» [3,7].

Социальная работа – это сфера деятельности, в которой предполагается востребование, доступ, обработка и хранение персональных данных получателей социальных услуг, в связи с чем необходимо особое внимание в работе с информацией, получаемой от клиентов как в письменной, так и в устной форме.

Результаты развития области электронной обработки данных позволили государственным учреждениям создавать большие банки данных для повышения эффективности и облегчения сбора и обработки персональных данных. В органах государственной власти, подведомственных министерству труда и социальной защиты, безопасность персональных данных клиента обеспечивается при помощи принципа конфиденциальности – одного из основополагающих принципов, регулирующих как делопроизводство, так и этическую систему, лежащую в основе взаимодействия социального работника и получателя услуг. Принцип конфиденциальности в социальной работе регулирует обращение с информацией, получаемой от клиента, и обязывает специалиста не допускать утечку информации и всячески предотвращать её разглашение [4].

Принцип конфиденциальности связан с тем, что в процессе своей профессиональной деятельности специалист по социальной работе получает доступ к информации о получателе социальных услуг, в случае разглашения которой может причинить вред ему или его близким. Конфиденциальная информация о клиенте – это любая информация, доступ к которой ограничен. Прежде всего это информация и данные, которые известны определенному кругу лиц и представляющие для них особую ценность. Так к конфиденциальной информации можно отнести сведения о болезнях, психических заболеваниях клиента, негативных привычках, криминальном прошлом или настоящем, семейных конфликтах и т.п. Лишь в особых случаях специалист по социальной работе (социальный работник) обязан раскрыть определенным органам власти некоторые данные о клиенте, не получая его согласие (в случае совершения преступления, либо угрозы его совершить). Также социальный работник, в некоторых случаях, может передать информацию о клиенте третьим лицам, если это в его интересах, и исключительно с его согласия. Сохранение конфиденциальности о клиенте – это залог дальнейшей продуктивной работы и фактор выстраивания конструктивного взаимодействия, доверительных отношений, от которых зависит удовлетворенность качеством социальных услуг[1,2].

Защита персональных данных граждан закреплена на законодательном уровне. В соответствии Федеральным законом от 28.12.2013 №442-ФЗ (ред. от 11.06.2021) «Об основах социального обслуживания граждан в Российской Федерации», предоставлять информацию о клиенте социальных служб минуя его или его представителя согласие возможно лишь при работе с персональными данными в рамках межведомственного взаимодействия [8].

Реализация принципа конфиденциальности предполагает следующие долженствования в отношении социального работника:

- неразглашение информации, которую он получает от клиента или его родных, в том числе и после прекращения оказания социальных услуг;
- сохранение в тайне личности клиента и источников информации о клиенте, если только его не обязывает к этому закон;
- информирование получателя социальных услуг о возможных случаях разглашения информации о нём;
- оглашение с письменного согласия клиента информации о нем лишь в случае необходимости планирования действий по преодолению трудной ситуации;
- отказ делиться информацией о клиенте с его родными и близкими;
- возможность делиться информацией о клиенте с его близкими лишь в случае существования реальной угрозы жизни и здоровью клиента;
- возможность разглашения информации о клиенте по решению суда или административной комиссии (в случае дисциплинарных разбирательств по поводу самого специалиста);
- предоставление получателю социальных услуг разъяснений и получение подтверждения о том, что ему понятно, о чем, почему и для чего его спрашивают;
- разъяснение получателю социальную услуг того, как будет осуществляться защита его персональных данных;
- избегание разговоров о получателях услуг вне профессионального контекста и с лицами, не участвующими в оказании социальной услуги[6].

В краевом государственном бюджетном учреждении «Комсомольский-на-Амуре дом-интернат для престарелых и инвалидов» действует регламент об обработке личных данных клиентов учреждения на основе принципа конфиденциальности. Этот документ устанавливает порядок обработки персональных данных в учреждении; обеспечивает защиту прав и свобод гражданина при обработке его персональных данных, в том числе защиту прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, уполномоченных на обработку персональных данных, за невыполнение норм, регулирующих обработку и защиту персональных данных. В учреждении обрабатываются и хранятся следующие документы и сведения, содержащие данные получателей социальных услуг, обязательные для оказания социальных услуг: путевка министерства социальной защиты населения Хабаровского края; заявление гражданина или его законного представителя; документ, удостоверяющий личность получателя социальных услуг; документ законного представителя клиента учреждения; индивидуальная программа предоставления социальных услуг; копия индивидуальной программы реабилитации инвалида; документ о составе семьи получателя социальных услуг; справка, выданная медицинской организацией, содержащая заключение врачей и состоянии здоровья получателя социальных услуг; справка МСЭ (для инвалидов); копия решения суда о признании гражданина недееспособным; документы о доходах; документы о принадлежащем имуществе (при наличии такового). При поступлении гражданина в учреждение, специалист по социальной работе формирует личное дело получателя социальных услуг, в которое помещаются вышеуказанные документы.

Получатель социальных услуг (законный представитель) лично дают специалисту по социальной работе письменное разрешение на обработку своих персональных данных, которое впоследствии хранится в бумажном виде. К обработке персональных данных получателя социальных услуг допускаются только работники учреждения, подписавшие обязательство о соблюдении конфиденциальности. Документы, содержащие личные данные клиента учреждения, хранятся в металлических несгораемых шкафах, доступ к которым имеет определенный круг лиц. Копирование и извлечение персональных данных допускается только в служебных целях с разрешения руководителя учреждения. Все сотрудники, связанные с обработкой и защитой персональных данных, обязаны подписать обязательство о соблюдении конфиденциальности. С согласия получателя социальных услуг (законного представителя), данного в письменной форме, допускается передача информации третьим лицам, в интересах получателя социальных услуг. Персональные данные получателей социальных услуг подлежат обработке и хранению в электронном виде и на бумажном носителе. В электронном виде персональные данные могут быть отправлены в другие органы государственной власти (ПФР, миграционная служба и т.п.) через электронный социальный регистр населения (ЭСРН), информационный ресурс, который обеспечивает регистрацию граждан, которые имеют право на получение социальных услуг, либо уже ее получают. Договор на получение социальных услуг клиента учреждения, содержащий его персональные данные, хранится 75 лет с даты истечения срока действия договора.

Работники учреждения несут персональную ответственность за нарушение правил обработки и защиты персональных данных клиента.

Таким образом, принцип конфиденциальности выступает фактором защиты персональных данных получателя социальных услуг, обеспечивая построение конструктивного взаимодействия доверительных отношений между социальным работником и клиентом, от которых зависит эффективность дальнейшей работы специалиста и удовлетворенность клиента качеством социальных услуг.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Арсеньева, Ж.В. К вопросу о соблюдении профессиональной тайны в социальной работе (на примере законодательства Франции) / Ж.В. Арсеньева // Вестник ТОГИРРО, 2014. - №3(30). – С.442-443

2 Гаврилюк, Н.Э Философские ценности социальной работы в практической деятельности территориального центра социального обслуживания / Н.Э. Гаврилюк // Отечественный журнал социальной работы. – 2015. -№1(60). – С. 157-161

3 «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» (Заключена в г. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ N 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) // Консультант плюс.- URL.: http://www.consultant.ru/document/cons_doc_LAW_121499. – Режим доступа: для зарегистр. пользователей

4 Конфиденциальность // Википедия-свободная энциклопедия.-URL.: u.wikipedia.org/wiki/Конфиденциальность. - Режим доступа: свободный

5 Краткая характеристика состояния преступности в Российской Федерации за январь-сентябрь 2022 года (статистический бюллетень) / Министерство внутренних дел Российской Федерации. – Москва, 2022. - URL.: https://xn--b1aew.xn--p1ai/reports/item/33388812/. - Режим доступа: свободный

6 Тимченко, Е.А. Особенности конфиденциальности персональной информации в социальной сфере / Е.А. Тимченко, В.Д. Кленюшина //Синергия Наук,2019. - №31. – С.1566-1570

7 Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ (последняя редакция) // Консультант плюс. - URL.: http://www.consultant.ru/document/cons_doc_LAW_61801. – Режим доступа: для зарегистр. пользователей

8 Федеральный закон от 28.12.2013 N 442-ФЗ (ред. от 11.06.2021) "Об основах социального обслуживания граждан в Российской Федерации"// Консультант плюс. - URL.: http://www.consultant.ru/document/cons_doc_LAW_156558.- Режим доступа: для зарегистр. пользователей

УДК 342.7:004.9

Потютенко Андрей Владимирович, студент, Комсомольский-на-Амуре государственный университет
Potyutenko Andrey Vladimirovich, student of Komsomolsk-on-Amur State University
Непочатова Валерия Михайловна, старший преподаватель кафедры «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Nepochatova Valeria Mikhailovna, Senior Lecturer at the Department of “Linguistics and Intercultural Communication” of Komsomolsk-on-Amur State University

ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ В ВЕК ЦИФРОВИЗАЦИИ

THE RIGHT TO PRIVACY IN THE DIGITAL AGE

Аннотация. В данной статье будут проанализированы аспекты права на неприкосновенность частной жизни в условиях нашего века цифровизации, а именно теоретический аспект и практический аспект. Из-за того, что цифровые технологии стали распространяться по всему, у людей возник вопрос о защите своих персональных данных от чужих лиц, следуя из реализации одного из основных прав человека-приватность. Если же мы просмотрим различные исследования и их результаты, то мы увидим интересную картину. Так как оказывается, что большинство людей либо не знают, либо не сильно заботятся об своих правах на неприкосновенность частной жизни, и из-за этого подвергают опасности свои личные данные.

Abstract. This article analyzes aspects of the right to privacy in assessing our age of digitalization, namely the theoretical aspects and the practical aspect. Due to the fact that digital-technologies began to spread around the world, people have a question about protecting their personal data from strangers, which follows from the implementation of one of the fundamental human law-privacy. If we look at various studies and the results, we will see an interesting picture. Because it turns out that most people either don’t know or don’t care much about their privacy rights, and because of this, they personal data is at risk.

Ключевые слова: приватность, интернет, цифровые технологии, личные данные, частная жизнь.

Key words: privacy, internet, digital technologies, personal data, privacy, privacy.

В нашем современном мире различных технологий, включая цифровые технологии, очень важным аспектом является личная безопасность, которая включает в себя защиту информации в интернете, ведь этот аспект позволяет человеку чувствовать себя хотя и не в полной, но в безопасности.

Казалось бы, цифровые технологии в нашей с вами частной жизни уже позволяют лучше защитить нас, но на самом деле они не дают нам гарантированную безопас-

ность. Согласно резолюциям Генеральной Ассамблеи и Совета по правам человека Управление Верховного комиссара ООН по правам человека (Рисунок 1) (далее УВКПЧ) проводит экспертные консультации и публикует доклады, посвященные проблемам, связанными с соблюдением права на неприкосновенность частной жизни и других прав человека в цифровом мире. Например, доклад от 3 августа 2018 года на тему «Право на неприкосновенность частной жизни в цифровой среде».

В этом докладе приводятся рекомендации по решению некоторых из наиболее острых проблем, которые были связаны с правом на неприкосновенность частной жизни в эпоху цифровых технологий. А также в нем содержался краткий обзор правок международного уровня. Затем рассматривались обязательства стран, государств и ответственность предприятий на эту тему, в том числе обсуждались надлежащие гарантии и вопросы надзора над этим.

Рисунок 1 - УВКПЧ

Несмотря на то, что большинство стран смогли реализовать все эти рекомендации, все равно происходят ситуации, когда частная жизнь становится известна посторонним нам людям. Яркий тому пример, случай, который произошел с компанией Facebook (является частью Meta признана в Российской Федерации экстремистской организацией). В 2021 году данные более 1,5 млрд пользователей были выложены в сеть и продаются на различных хакерских сайтах. Сама же Facebook отрицала эту информацию. При этом все данные что были украдены оказались реальными. А именно настоящие имена пользователей, телефонные номера, адреса электронных почт, а также места их геолокации. Телеграмм канал Mash назвал это самым большим сливом данных за всю историю Facebook. И также было сообщено что утечка произошла из-за уязвимости, которая была устранена в августе 2019.

Данный случай хорошо демонстрирует, что даже самые большие и известные компании иногда могут пренебречь защитой частных данных собственных пользователей, которые платят за некоторые услуги, предоставляемые компанией, и данным компаниям нужно более ответственно относиться к защите данных. Не говоря уже и о некоторых более мелких компаниях. И этими данными могут воспользоваться различные злоумышленники. Ведь когда мы соглашаемся на обработку персональных данных в различных компаниях мы сами создаем дополнительные риски для себя.

Также стоит отметить, что в некоторых странах не существует так такого права на неприкосновенность частной жизни в общем, включая и цифровой аспект. Например, в Китае. Для них это является нормой, что родители могут спокойно зайти в комнату ребенка, когда тот занимается какими-либо делами, включая личные дела.

В целом, в наш цифровой век защите персональных, хоть и уделяется внимание, но этого все равно недостаточно для того, чтобы обезопасить пользователей и их данные.

Поэтому необходимо, чтобы были либо применены, либо внедрены следующие меры:

1. Необходимо чтобы за компаниями проводились различные контрольные и надзорные работы, а именно, чтобы проводились различные проверки систем безопасности. Также необходимо ввести систему штрафов.
2. Необходимо предоставить пользователям возможность ознакомиться с условиями предоставления личных данных, и возможность отказаться от их предоставления.

3. Необходимо, чтобы информация об организациях, в которые пользователь предоставляет свои личные данные, была в открытом доступе. А также достоверность данных организаций.

4. Необходимо увеличить количество часов информатики, и предоставить дополнительные материалы об персональной безопасности.

5. Необходимо создать бесплатные курсы для людей преклонного возраста, которые в современных технологиях не способны сами разобраться, о персональной защите данных и навыками владения цифровыми технологиями.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1.Сайт Ведомости. Ru URL: https://www.vedomosti.ru/technology/news/2021/10/04/889649-v-seti-poyavilas-informatsiya-o-prodazhe-dannih-15-mlrd-polzovatelei-facebook (дата обращения 16.11.2022).

2.Сайт ООН. URL: https://www.ohchr.org/ru/privacy-in-the-digital-age (дата обращения 16.11.2022).

3.Ромашов, П. А. К вопросу о праве на неприкосновенность частной жизни в цифровой век. URL: https://cyberleninka.ru/article/n/k-voprosu-o-prave-na-neprikosnovennost-chastnoy-zhizni-v-tsifrovoy-vek/viewer (дата обращения: 16.11.2022).

УДК 336

Просвирина Дана Владимировна, студентка; Комсомольский-на-Амуре государственный университет
Prosvirina Dana Vladimirovna, student of Komsomolsk-na-Amure State University
Мусалитина Евгения Александровна, кандидат культурологии, доцент кафедры «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Musalitina Evgenia Aleksandrovna, PhD in Culture Studies, Assistant Professor, «Linguistics and Cross-Culture Communication Department», Komsomolsk-na-Amure State University

КИБЕРМОШЕННИЧЕСТВО И СПОСОБЫ ЗАЩИТЫ ОТ НЕГО

CYBER FRAUD AND WAYS TO PROTECT AGAINST IT

Аннотация. Достижения в сфере развития информационных технологий нередко используются злоумышленниками в корыстных целях. Мишенью преступников становятся банковские счета, дебетовые и кредитные карты, персональные данные и даже информация о состоянии здоровья. В России феномен интернет-мошенничества за последние 10 лет приобрел новые формы и способы реализации. В стране с каждым годом увеличивается число онлайн-преступлений, в условиях текущей социально-экономической ситуации появляются новые схемы обмана пользователей. В статье рассматривается явление кибермошенничества, причины успеха преступников в этой сфере и способы защиты от подобного рода преступлений.

Abstract. Achievements in the field of information technology development are often used by attackers for personal gain. Criminals target bank accounts, debit and credit cards, personal data and even health information. In Russia, the phenomenon of Internet fraud over the past 10 years has acquired new forms and methods of implementation. The number of online crimes increases every year in the country, and attackers come up with more and more sophisticated schemes to deceive users, adjusting to the specifics of the current socio-economic situation. The article discusses the phenomenon of cyber fraud, the reasons for the success of criminals in this area and ways to protect against this kind of crime.

Ключевые слова: кибермошенничество, онлайн преступление, интернет, интернет безопасность, персональные данные.
Key words: cyber fraud, online crime, internet, internet security, personal data.

Кибермошенничество относится к актам хищения и/или обмана пользователей сети интернет, как правило, с целью материального обогащения [2]. Преступниками разработано много схем онлайн преступлений, при этом, методы обмана постоянно совершенствуются. Тем не менее, можно выделить наиболее частые схемы и способы, используемые в кибермошенничестве:

В первую очередь, интернет преступники стремятся завладеть финансами пользователей, поэтому наиболее популярным методом совершения преступлений в сфере информационных технологий является кража имущества в виде денежных средств с банковского счета жертвы.

Так как данный вид хищения является наиболее популярным, обратимся к рассмотрению схемы и способов, которыми пользуются интернет-мошенники:

1. Создание вредоносных программ. Основная идея данной схемы заключается в том, что *«…мошенник создает компьютерную программу, зараженную вирусом, схема такого мошенничества действует так: программа имеет способность блокировать файлы, находящиеся на жестком диске компьютера. Следующим действием является то, что программа запрашивает перевести некую сумму денежных средств для получения кода разблокировки файлов компьютера*» [6]. Таким образом, злоумышленник может получить данные логина и пароля с помощью онлайн банка, не предпринимая лично никаких дополнительных действий.

2. Фишинг. Не менее распространенный и действенный способ завладеть личной информацией о пользователе заключается в следующем: злоумышленник создаёт мошеннический сайт, который находится в свободном доступе сети Интернет. При посещении сайта пользователю предлагается перейти по другой закреплённой ссылке, где необходимо пройти краткую регистрацию по номеру телефона или почте, после чего жертва получает сообщение с код-паролем. Далее мошенник сам связывается с жертвой и, представляясь сотрудником банка, просит назвать полученный ранее код. Тем самым, человек собственноручно открывает похитителям доступ к банковскому счету [6].

Однако, вышерассмотренные схемы онлайн мошенничества имеют множество аналогов и модификаций, и могут касаться не только информации о финансовом состоянии пользователя, но и его здоровья.

Злоумышленники трансформируют мошенническую деятельность, учитывая те или иные неблагоприятные события, происходящие в стране или отдельных регионах. Так, например, возникновение пандемии COVID-19 привело к появлению новых видов киберпреступлений [5]. Феномен онлайн преступлений, связанных с ковид, стал особенно актуальным в последние два года и стал предметом исследования многих специалистов разных сфер гуманитарного знания. Так, например, российский правовед Батюкова В. Е в своих трудах раскрыл проблему предупреждения интернет-мошенничества в кризисные для общества периоды [2]. Ещё одно явление, которое возникло совсем недавно – преступления, связанные с информационными продуктами, которые продаются блогерами в интернет пространстве. Мошенники умеют выявить актуальные для многих людей проблемы и используя психологические приемы, убедить потенциальную жертву купить информационный курс или «чудо-продукт», которые станут панацеей от всех трудностей. Данный способ можно назвать самым «деликатным» по способу получения преступниками денежных средств, поскольку пользователь отдаёт их сам. Одновременно, он является одним из самых серьезных правонарушений, поскольку пользователь является обманутым и не получает обещанную услугу или товар после произведенной им оплаты [1].

В последние несколько лет проблема кибермошенничества стала актуальной для исследования с точки зрения разных социальных сфер. Необходимо отметить, что борьба с этим видом преступлений осложняется лакунами в законодательстве. Аспект правового регулирования проблемы нашел свое отражение в работах российских исследователей А.О. Галаховой, Е.А. Горбуновой и др. [3].

Распространение в интернет пространстве кибермошенничества требует разработки эффективных средств борьбы с ними. Исследователи М. Х. Ордоков, Э. Т. Шафиева выделяют следующие меры противодействия интернет-мошенничеству: 1) при установке приложения на компьютер или смартфон необходимо проверять в настройках, к каким данным оно запрашивает доступ и с какой целью; 2) нельзя переходить по подозрительным ссылкам, где предлагается указать личные данные, не связанные с содержанием этого сайта; 3) нельзя передавать третьим лицам свои логины и пароли, а также не сообщать код-пароли, поскольку именно они являются «ключом» для доступа к личным данным; 4) перед тем, как воспользоваться услугами или купить какой-либо товар, необходимо проверить продавца, ознакомиться с отзывами других пользователей об этом блогере или магазине. Следует перепроверять информацию о продукте, который планируете приобрести [4].

Подводя итог, необходимо отметить, что с развитием информационных технологий и изменением текущей социально-экономической ситуации кибермошенники разрабатывают новые схемы и способы обмана интернет пользователей. В силу этого необходимо помнить о защите персональной информации и соблюдать основные меры безопасности при совершении финансовых операций в сети.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Байжумаева М. А. Кибермошенничество / М. А. Байжумаева // Новый юридический вестник. – 2022. – № 3(36). – С. 67-69.

2. Батюкова В. Е. Предупреждение кибермошенничества в период COVID-19 / В. Е. Батюкова // Образование и право. – 2020. – № 11. – С. 347-349. – DOI 10.24411/2076-1503-2020-11154.

3. Галахова А. О. Инфопродукты блогеров как сфера, не урегулированная законодателем / А. О. Галахова, Е. А. Горбунова // Актуальные вопросы современной науки и технологий : Сборник статей II Международной научно-практической конференции, Петрозаводск, 31 марта 2022 года. – г. Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская И.И.), 2022. – С. 13-18.

4. Ордоков М. Х. Основные тенденции борьбы с кибермошенничеством / М. Х. Ордоков, Э. Т. Шафиева // Пробелы в российском законодательстве. – 2021. – Т. 14. – № 4. – С. 108-111.

5. Путиенко Н. А. Проблема кибермошенничества / Н. А. Путиенко // Актуальные проблемы борьбы с преступностью на современном этапе, Волгоград, 28–29 мая 2020 года. – Волгоград: Волгоградская академия Министерства внутренних дел Российской Федерации, 2020. – С. 352-355.

6. Смирнов В. М. Наиболее популярные схемы кибермошенничества в сети Интернет / В. М. Смирнов, А. В. Кузина // Тенденции развития науки и образования. – 2022. – № 86-1. – С. 110-113. – DOI 10.18411/trnio-06-2022-32.

УДК 008

Пустовит Никита Евгеньевич, студент, Комсомольский-на-Амуре государственный университет
Pustovit Nikita Eugenevich, student of Komsomolsk-na-Amure State University
Иванов Антон Анатольевич, кандидат культурологии, доцент, Комсомольский-на-Амуре государственный университет
Ivanov Anton Anatolyevich, Candidate of Cultural Sciences, Associate Professor, Komsomolsk-on-Amur State University

ДЕГЛОБАЛИЗАЦИЯ В КИБЕРПРОСТРАНСТВЕ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ НА ПОСЯГАТЕЛЬСТВА ИЗВНЕ

DEGLOBALISATION IN CYBERSPACE AS A MEANS OF ENSURING SECURITY AGAINST EXTERNAL ENCROACHMENT

Аннотация. В данной статье рассмотрены варианты влияния на информацию и формирования общемирового мнения посредством изоляции отдельных стран, что в свою очередь приводит в деглобализации киберпространства. Это может иметь противоречивые последствия: с одной стороны, обеспечить безопасность личных данных, с другой – усугубить конфронтацию стран.
Abstract. This article examines options for influencing information and shaping global opinion by isolating individual countries, which in turn leads to the deglobalisation of cyberspace. This can have contradictory consequences: on the one hand, it can ensure the security of personal data, and on the other, it can exacerbate the confrontation of countries.
Ключевые слова: личные сведения, деглобализация, киберпространство.
Key words: personal information, de-globalisation, cyberspace.

Информация - один из самых желанных ресурсов нашей планеты, призывающий нас изучить, как она служит объектом власти и доминирования в национальных и международных политических процессах. Напряженность вокруг этого ресурса возникает не только на территориях, непосредственно контролируемых государствами, но и на спорных территориях, включая нематериальное принятие их, как это происходит в киберпространстве.

Российско-украинская война олицетворяет это. "Отключив" Россию и, наоборот, сохранив сервис в Украине, отношение GAFAMs (Google, Apple, Facebook, Amazon и Microsoft), фактически стали заинтересованными сторонами в конфликте и проецируют новое видение своей власти, что в свою очередь имеет глубокий геополитический вес. Такие события усиливают чувство недоверия к киберпространству и усиливают дебаты вокруг управления Интернетом и киберсуверенитета - областей, в которых крупные державы пытаются подтвердить свою стратегическую власть.

Хорошо известна роль, которую цифровые социальные сети сыграли в военизации и активизме во время "арабской весны" 2011 года, протестов в Гонконге в 2019-2020 годах и первой "домбасской войны" в Украине в 2014 году. Совсем недавно, во время Covid-19, эта роль продолжала расширяться, поскольку проблема американских гигатехов вышла на передний план на фоне взаимодействия инфодемических ставок и на фоне подавляющего доминирования GAFAMs в информационной экосистеме.

В силу самоуспокоенности или боязни поставить под угрозу перспективы развития изначально перспективных технологий, государственные органы многих стран не смогли адекватно оценить масштабы этих преобразований. Многие сегодня беспомощно наблюдают за волнением, которое бросает вызов их собственным желаниям, о чем

свидетельствуют возможности цензуры главы государства (как в случае с Дональдом Трампом, лишенным аккаунта в Twitter в 2021 году), проведения или срыва выборов (как в случае со скандалом Cambridge Analytica и подозрениями Facebook в манипулировании персональными данными), а также подключения или отключения страны, сознательно заняв позицию в конфликте, например, между Россией и Украиной.

В свете этой беспрецедентной глобальной конфигурации можно предположить, что она будет иметь три последствия. Во-первых, ускорение процесса детерриториализации киберпространства. Этот новый театр международной напряженности фактически усугубил негативные внешние эффекты, способствующие риску деглобализации. Эта проблема возникла, по крайней мере, после кризиса 2008 года на временной шкале открытости мировой торговли, а сегодня она конкретно сфокусирована на телекоммуникациях. Хорошо известно, что стратегии разводных мостов оседлали волны популизма и национализма. Это может показаться нелогичным в наш век гиперконнективности, но сегодня это находит благодатную почву в запрете Москвой Facebook, Twitter, Instagram и Youtube, и наоборот, в исключении ЕС главного банка России, Сбербанка, из системы Swift, основного протокола связи в киберпространстве.

Следствием вышеизложенного является вероятная переоценка двух других вопросов - управления Интернетом и киберсуверенитета. Первый вопрос стоит на дипломатической повестке дня с момента проведения Всемирного саммита по информационному обществу в Женеве в 2003 году и в Тунисе в 2005 году. Переполненное обещаниями цифровых технологий, управление Интернетом долгое время оставалось слабым звеном в конституционализме, руководствуясь исключительно рыночными соображениями.

Поскольку США обычно выступают за саморегулирование как предпочтительный механизм Интернета, их подход подтвердил этот статус-кво. Сложность заключается в отсутствии консенсуса относительно идеальной правовой архитектуры. С самого начала государственная политика США была сдержанной, с надеждой на саморегулирование, которая в итоге так и не реализовалась.

Прославленному принципу глобального Интернета, не зависящего от политической власти, Россия и Китай на протяжении многих лет выступали против "суверенного Интернета", где государства имеют право голоса через механизмы, которые должны быть разработаны под руководством Организации Объединенных Наций и/или Международного союза электросвязи (МСЭ). В 2008 году дебаты возобновились после избрания Обамы, чья победа была приписана, в частности, массовому обращению к социальным сетям и использованию возможностей, предоставляемых Веб 2.0.

Начиная с 2010 года, растущее значение социальных медиа переместило дебаты по управлению Интернетом с периферии в центр, хотя и не в том направлении, которого добивалась администрация США, ослабленная в 2013 году разоблачениями Эдварда Сноудена о системах слежки АНБ (Агентства национальной безопасности). Эти разоблачения стали сенсацией и поставили проблемы защиты частной жизни и персональных данных в центр матрицы, которую мы называем "геополитикой Интернета".

Второй вопрос, киберсуверенитет, не отвязан от первого. Борьба идет за контроль над прибыльным рынком данных, который сегодня является основной областью противостояния сверхдержав и многочисленных приложений искусственного интеллекта. Тот факт, что гигатехи сильно жаждут подводной кабельной инфраструктуры (три четверти которой принадлежит GAFAM), подтверждает эту точку зрения. В гонке за поставками Китай и США враждовали из-за полупроводниковой промышленности, и совсем недавно "Закон о чипах", план, представленный Европейской комиссией в феврале 2022 года, аналогично отражает это соперничество. До сих пор превосходство США казалось неприступным. Но надолго ли? Стремление Китая превзойти США очевидно по целому ряду направлений. Пекин стремится занять центральное место в мировой экономике к 2049 году, к 100-летию коммунистического Китая, и для этого дела-

ет ставку на эти технологии в качестве основной стратегии развития. Что касается конкретно социальных сетей, в первую очередь следует отметить стремительный взлет китайской социальной сети TikTok, которая в 2020 году стала самым скачиваемым приложением в мире, опередив Facebook. Этот успех не прошел даром в США, где Вашингтон рассматривает возможность запрета TikTok в основных магазинах, Appstore и Playstore, официально на том основании, что Пекин может использовать его в целях шпионажа. Эти нападки не отличаются от нападок на другую китайскую компанию, Huawei.

За последнее десятилетие кибербезопасность стала одним из главных вопросов для Китая, причем Пекин стремится не только стать кибердержавой, но и вступить в гонку за нормотворчество в киберпространстве. И здесь, как и в случае с управлением Интернетом, Китай выступает за равные условия игры, когда каждое государство имеет право голоса в определении правил и норм, регулирующих киберпространство во всем мире. Такова же позиция России, которая неоднократно пыталась возглавить международное движение, предоставляющее национальным правительствам приоритет в формировании стандартов киберпространства.

Переговоры вокруг корневых DNS-серверов, важнейшего оборудования, позволяющего перенаправлять данные через доменные имена (в настоящее время в мире существует тринадцать корневых DNS-серверов), наглядно иллюстрируют масштаб ставок. Пекин выступает за многосторонние, а не многопартийные переговоры, чтобы свести к минимуму любую возможность сохранения контроля Соединенными Штатами.

Другие области стратегического соперничества включают борьбу за 5G и Интернет вещей, где и Китай, и США стремятся навязать свои стандарты. Старый континент также стремится привнести свой ритм через инициативы по модернизации существующего корпуса цифровых ресурсов, включая Закон о цифровых услугах и Закон о цифровом рынке.

Темой, связанной с обсуждением киберсуверенитета, является степень ответственности государств в случае киберинцидента с трансграничными последствиями, а также степень контроля, который они должны осуществлять над инфраструктурой, расположенной на их территории.

Один из разделов западной доктрины предполагает, что на этом уровне правила, применимые к физическому миру, действуют и в киберпространстве, поэтому их достаточно перенести. Такой подход соответствует рекомендациям Таллиннского руководства - руководства, опубликованного в 2013 году рабочей группой по мандату Организации Североатлантического договора (НАТО), которая приняла расширительное толкование обычного международного права о суверенитете.

В связи с этим вопрос о суверенитете в киберпространстве затрагивает все еще зияющую рану - отсталость развивающихся стран, которым уготован статус простого пользователя/потребителя, но которые все еще не теряют надежды на возможность включить свой голос в многосторонние переговоры при условии, что изменения в контексте международной политики и безопасности не будут диктовать иное. Они предполагают, что киберпространство будет рассматриваться как международное общее благо и, следовательно, будет свободно от какого-либо исключительного суверенного контроля.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Пастухова, Н. Б. Суверенитет: от глобализации до деглобализации / Н. Б. Пастухова, А. Л. Барциц // Евразийский юридический журнал. – 2019. – № 11(138). – С. 75-77. – EDN SDHOAL.

2 Спиридонова Валерия Игоревна Глобализация в XXI В. : инновация или новые перспективы? // Век глобализации. 2018. №3 (27). URL: https://cyberleninka.ru/article/n/globalizatsiya-v-xxi-v-innovatsiya-ili-novye-perspektivy (дата обращения: 23.11.2022).

УДК 342.7:004.9

Смирнов Артем Андреевич, студент, Комсомольский-на-Амуре государственный университет
Smirnov Artyom Andreevich, student of Komsomolsk-on-Amur State University
Непочатова Валерия Михайловна, старший преподаватель кафедры «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Nepochatova Valeria Mikhailovna, Senior Lecturer at the Department of "Linguistics and Intercultural Communication" of Komsomolsk-on-Amur State University

ПРАВО НА КОНФИДЕНЦИАЛЬНОСТЬ В ЭПОХУ ЦИФРОВЫХ ТЕХНОЛОГИЙ

THE RIGHT TO PRIVACY IN THE DIGITAL AGE

Аннотация. В этом докладе мы рассмотрим проблему конфиденциальности в эпоху цифровизации во всемирной сети Интернет, о том, как она изменила концепцию личной конфиденциальности и как изменились правовые стандарты, которые мы используем сегодня. Также рассмотрим потребность в последовательных, тщательно проработанных законах о цифровой неприкосновенности частной жизни и анализируется влияние этих законов на практику связей с общественностью в цифровом мире. Разные исследования показали, что большинство людей не знают о своих правах на конфиденциальность частной жизни и подвергаются к рассекречиванию различной личной информации.
Abstract. In this report, we will look at the problem of privacy in the era of digitalization on the world Wide Web, how it has changed the concept of personal confidentiality and how the legal standards that we use today have changed. We will also consider the need for consistent, carefully elaborated laws on digital privacy and analyze the impact of these laws on the practice of public relations in the digital world. Various studies have shown that most people are unaware of their privacy rights and are exposed to declassification of various personal information.
Ключевые слова: конфиденциальность, интернет, приватность, личные данные, частная жизнь, социальные сети, законы и право.
Key words: privacy, internet, privacy, personal data, privacy, social networks, laws and law.

Что такое современная конфиденциальность? Предотвращение утечки какой-либо личной информации. В нынешнюю эпоху постоянной цифровой трансформации сказать однозначно что это такое невозможно. Суровая правда заключается в том, что нет никакого способа гарантировать конфиденциальность в современном цифровом мире. В этом году сообщалось, что голосовой ассистент Алиса и Google прослушивает и записывает ваши разговоры. Утечки данных продолжают происходить. И хотя Яндекс и Google проповедует, что будущее связано с конфиденциальностью, можем ли мы действительно доверять мировым интернет-корпорациям? Можно рассуждать со стороны права ссылаясь на статью 23 Конституции РФ, но вся неоднозначность не дает полной защиты от утечек.

Несмотря на то, что мы свободно используем термины о неприкосновенности личных данных, существует большая разница между безопасностью / защитой и конфиденциальностью. Конфиденциальность – это уполномоченный договор установления границ, который позволяет нам пользователям определять, кто может получить доступ к каким данным о нас, где, когда и с какой целью. Простыми словами конфиденциальность — это договор определения того, когда мы хотим закрыть жалюзи во время своего интернет-серфинга: информацию о наших интернет-покупках, музыкальных предпочтениях или выборе студенческого клуба. Договор решает и связывает нас с кем-то, кто получает финансовую выгоду от вашей личной информации, а когда нет.

К сожалению, единственный способ, которым пользователь может быть уполномочен устанавливать границы конфиденциальности – это прозрачность со стороны самих компаний. Например, пользователи должны знать, какие типы информации собираются у них, чтобы иметь возможность принимать обоснованные решения о том, какой информацией они хотят поделиться. К сожалению, большинство компаний хоронят эту информацию за терминами и услугами. Кто-нибудь когда-нибудь читал пользовательское соглашение полностью, прежде чем нажать «Я согласен»?

Например, мы получаем рекламу вещей, о которых у нас только что был частный разговор с другом по телефону, или мы получаем таргетированную рекламу какого-либо продукта или услуги после прослушивания определенного подкаста или прочитав статью. Очевидно, что некоторые компании переступают границы конфиденциальности. Но многих из нас это устраивает.

Согласно недавнему исследованию среди российских интернет-пользователей, 51% россиян знают, что компании преследуют свои коммерческие интересы, но все равно пользователи предоставят свои данные, если получат какую-то выгоду взамен. Потребители хотят персонализированного контента. Они хотят, чтобы к ним относились как к человеку, а не как к некому числу. Именно для этого необходимо собрать данные. Это компромисс, и компании должны лучше работать над укреплением доверия, когда речь заходит о конфиденциальности и безопасности.

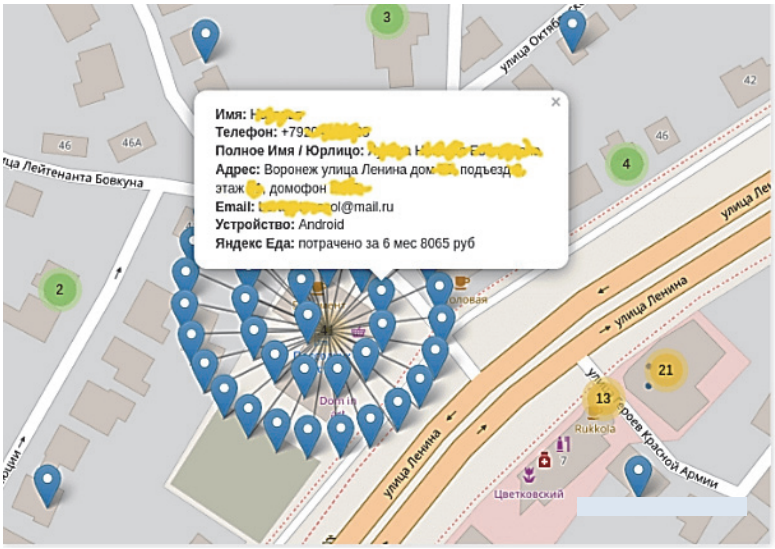

Рисунок 1 – Пример утечки данных сервиса Яндекс Еда в марте 2022 года

Можно увидеть на данном примере, что довольно подробный список личных данных, которыми могут воспользоваться в корыстных целях злоумышленники. Личная информация не всегда может оставаться конфиденциальной.

Компании, которым мы доверяем свои личные данные должны быть прозрачными при сборе эти самых данных, также они должны сообщать пользователю, если утечка всё же произойдет. Многие компании ради собственной выгоды пытаются скрыть информацию об утечке данных от пользователя, но скрыть это невозможно, следствием этого спустя месяц компания приносит свои извинения, но личные данные носятся по интернету уже долгое время. Надо быть предельно внимательным, и понимать какую информацию доверять интернет-компаниям. Мы отказываемся от нашей конфиденциальности, становимся постоянными пользователями, и хотим, чтобы к нам относились с уважением и чтобы наши данные были в безопасности.

О неадекватных правовых стандартах в цифровую эпоху. Нынешние правовые стандарты для борьбы с нарушениями конфиденциальности неадекватны для цифровой

среды. «Право на неприкосновенность частной жизни» в своем юридическом понимании распространяется на личные вещи и имущество. Как же тогда можно определить нарушения конфиденциальности в мире, управляемом Интернетом, если право на неприкосновенность частной жизни связано только с физической собственностью?

Правовые стандарты для определения нарушений конфиденциальности не могут интерпретировать нарушения цифровой конфиденциальности, потому что их очень мало. Законы о конфиденциальности, такие как “Закон об информации, информационных технологиях и о защите информации”, считается удручающе устаревшими. Например, электронная почта старше 180 дней не получает никакой защиты конфиденциальности, и «в соответствии с действующим законодательством можно получить доступ к этим материалам без разрешения судьи и просто с помощью административной повестки, что многие эксперты по конфиденциальности считают неправильным. Законы о цифровой конфиденциальности имеют жизненно важное значение и должны быть последовательными по всей стране, поскольку Интернет не знает географических границ. Обжаловать законом в современной России, нарушения, направленные на использование личной информации в злостных или же корыстных целях очень сложно.

Необходимо подготовить правовую базу для подобных случаев и проинформировать пользователей и компании, использующих личную информацию.

Выводом послужит перечень необходимых советов и предложений как можно обезопасить себя от утечек и сохранить конфиденциальность в нашем информационном мире.

1. Будьте бдительны, когда вводите свои личные данные на различных сайтах.
2. Обязательно читайте пользовательское соглашение об обработке персональных данных. Большинство людей принимает данное соглашение, не читая. Именно так, мы даем разработчикам и компаниям разрешение на передачу персональных данных третьим лицам, которые используют их в разных целях.
3. Не стоит загружать какой-либо контент из непроверенных источников. Вы рискует установить шпионское ПО, которое может долгое время скрываться в устройстве, ничем себя не выдавая. Программа-шпион коллекционирует данные о пользователе, записывает все нажатия клавиш и делает снимки с экрана. После этого информация отправляется владельцу вредоносной программы.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Зорькин, В. Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума // Российская газета. 2018. № 7578 (115). URL: https://rg.ru/2018/05/29/zorkin-zadacha-gosudarstva-priznavat-i-zashchishchat-cifrovye-prava-grazhdan.html (дата обращения: 11.11.2022).
2. Карцхия А.А. Цифровой императив: новые технологии создают новую реальность // ИС. Авторское право и смежные права. 2017. № 8. С. 17-25.
3. Права и свободы человека и гражданина // Пенсионный фонд Российской Федерации. URL: https://pfr.gov.ru/order/konstituciya/~4846 (дата обращения 11.11.2022).
4. «Яндекс» сообщил об утечке данных пользователей «Яндекс.Еды» // Forbes. URL: https://www.forbes.ru/tekhnologii/457605-andeks-soobsil-ob-utecke-dannyh-polzovatelej-andeks-edy (дата обращения: 11.11.2022).

УДК 004

Турешова Асель Талаповна, студент, ПИУ им. П. А. Столыпина филиал РАНХиГС
Tureshova Asel Talapovna, student of Povolzhsky Institute of Management named after P.A. Stolypin
Хачатурян Анна Робертовна, студент, ПИУ им. П. А. Столыпина филиал РАНХиГС
Khachaturyan Anna Robertovna, student of Povolzhsky Institute of Management named after P.A. Stolypin
Затонская Ольга Викторовна, старший преподаватель, ПИУ им. П. А. Столыпина филиал РАНХиГС
Zatonskaya Olga Viktorovna, senior lecturer, Povolzhsky Institute of Management named after P.A. Stolypin

ФИШИНГ КАК УГРОЗА КОНФИДЕНЦИАЛЬНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

PHISHING AS A PRIVACY THREAT IN SOCIAL NETWORKS

Аннотация. С развитием информационных технологий происходит распространение киберпреступлений. Фишинг является одним из самых распространенных видов интернет мошенничества. В данной статье мы рассматриваем влияние фишинга на конфиденциальность данных пользователей в социальных сетях. Эта тема очень актуальна и важна в силу того, что современный человек постоянно пользуется социальными сетями, а следовательно, вероятность стать жертвой мошенничества остается крайне высокой. Объектом исследования является сам фишинг, как разновидность мошенничества в сети Интернет, предметом – его воздействие на конфиденциальность личных данных людей в сети. Целью работы мы ставим изучение самого явления фишинга, его методы, а также конкретное влияние на личные данные, размещенные людьми в социальных сетях. Результатом работы является получение знаний о фишинговых атаках в социальных сетях и о способах защиты от них.
Abstract. With the development of information technology, cybercrime is spreading. Many users face fraud via the Internet. Phishing is one of the most common types of fraud. In this article we consider the influence of phishing on privacy of users' data in social networks. This topic is very relevant and important, because the modern man constantly uses social networks, and therefore, the probability of falling victim to fraud remains extremely high. The object of the study is phishing itself, as a kind of fraud on the Internet, the subject - its impact on the confidentiality of personal data of people in the network. The aim of the work is to study the phishing phenomenon itself, its methods, as well as the specific impact on personal data posted by people in social networks. The result of the work is gaining knowledge about phishing attacks in social networks and about ways of protection from them.
Ключевые слова: фишинг, социальная сеть, конфиденциальность, мошенничество, фишинг-атаки.
Key words: phishing, social networks, privacy, fraud, phishing attack.

Введение. Информационные технологии в наше время развиваются с необыкновенной скоростью, и, бесспорно, они упрощают нашу жизнь, превращая сложные задачи в легко осуществимые. Тем не менее, данные новшества также несут в себе и некоторую опасность, ведь данные, содержащиеся в социальных сетях или интернет-сайтах, всегда находятся под угрозой. Киберпреступления происходят все чаще, наиболее распространенными среди них являются преступления, связанные с мошенничеством. Фишинг является одним из видов интернет-мошенничества. В данной статье мы рассмотрим то, как происходило развитие фишинга, какие методы и техники используют злоумышленники и как фишинг влияет приватность данных в социальных сетях

Основная часть.

Фишинг – вид интернет-мошенничества, при котором злоумышленники стремятся заполучить идентификационную информацию о пользователях. Сюда можно отнести кражу паролей, номеров карт, банковские счета и других конфиденциальных данных.

Атаки фишеров с каждым днем совершенствуются, все чаще и чаще применяются методы социальной инженерии. Пользователя всегда пытаются запугать, придумав вескую причину, почему он должен передать свои личные данные.

Историческая справка

Первое упоминание термина «фишинг» было зафиксировано в 1996 году, когда от лица компании «America Online» мошенники получили данные к аккаунтам клиентов.

Дальнейшим значимым периодом был 2001 год, в котором фишинговой атаке подверглись платежные системы. Следующим направлением, на которое обратили внимание злоумышленники, стали популярные социальные сети. Так, фишинговые действия распространились на известную зарубежную сеть MySpace в 2006 году, а уже в 2008 году с подобным столкнулась российская социальная сеть ВКонтакте.

В 2012-2013 годах фишинг распространил свое действие на 102,1 тысячу пользователей во всем мире. Согласно статистике, лидирующими странами оказались Германия, США, Индия и Вьетнам. К 2019 году число атакованных пользователей выросло на 72%.

Методы фишинговых атак.

Атаки могут осуществляться при помощи различных методов. Как и говорилось ранее фишинг-атака может содержать в себе социальную инженерию, а еще она может включать в себя и другие методы, приведенные ниже.

Email/Spam – в данном случае применяется подход «spray and pray», т. е. одно и то же электронное письмо отправляется злоумышленниками миллионам пользователей, после этого они просто ожидают, что кто-нибудь поддастся фишинговой атаке.

Content Injection – метод, осуществляемый с помощью замены фишером части контента внутри надежного веб-сайта или социальной сети.

Session Hijacking – метод, при котором мошенник захватывает сеанс, используя особый механизм управления веб-сеансом для кражи данных.

Link Manipulations – метод, при котором мошенник отправляет ссылку на вредоносный сайт.

Также реализуется такой метод манипулирования ссылками, как покупка домена с различными написаниями популярного домена, например: googlle.com и т.д. Website Forgery – метод, в рамках которого вредоносный веб-сайт выдается за подлинный, с помощью межсайтового скриптингга или подмены сайта.

Однако методов распространения фишинга существует гораздо больше, нами были перечислены лишь самые основные.

Проявление фишинга в социальных сетях

Фишинг имеет свое место в различных сферах, он может быть связан как и с платежной системой, так и с данными социальных сетей. То в каких областях распространены фишинговые атаки, можно также узнать из квартальных отчетов рабочей группы по вопросам антифишинга APWG Phishing Activity Trends Report за 2 квартал 2022 года.

На основе данной диаграммы, мы можем сделать вывод, что фишинговые атаки в социальных сетях крайне распространены, то есть данные, содержащиеся в аккаунтах пользователей различных социальных сетей, постоянно находятся под угрозой. То как именно фишинговые атаки реализуются мошенниками и какой вред конфиденциальности данных они наносят мы и рассмотрим далее в этой статье.

В современном мире социальные сети представляют собой прекрасную платформу для осуществления фишинговых атак, так как они являются неотъемлемой ча-

стью жизни любого среднестатистического человека. Кроме того, различные компании пользуются социальными сетями для поддержания связи с клиентами. Рассмотрим детально различные виды фишинга в социальных сетях.

Фишинг в Instagram (запрещен на территории РФ. Meta Platforms Inc. признана экстремистской организацией)

Известная социальная платформа пользуется большим спросом у людей по всему миру, так как с помощью его использования у людей есть возможность узнать подробности жизни других людей посредством выкладывания постов с фотографиями, историй. Instagram (запрещен на территории РФ. Meta Platforms Inc. признана экстремистской организацией) вызывает интерес и у фишеров. Для осуществления своих вредоносных действий они начинают с создания поддельной страницы для входа в сеть, которая схожа с оригинальной версией. Убеждая пользователя в угрозе его аккаунта, фишеры аргументировано вынуждают человека ввести свои ID и пароль на поддельной странице, после введения которых пользователя направляют на настоящий сайт. Но при этом данные уже оказываются в руках мошенников, и они имеют полный доступ к Instagram-аккаунту (запрещен на территории РФ. Meta Platforms Inc. признана экстремистской организацией), благодаря которым в последствии смогут осуществлять слежку за пользователем, запрашивать у подписчиков личную информацию о нем, при этом удаляя факты своего присутствия.

Следующей современной социальной сетью, заслуживающей внимания, является Facebook (запрещен на территории РФ. Meta Platforms Inc. признана экстремистской организацией). На данной платформе фишеры начинают свою атаку с сообщения о возникновении проблемы с учетной записью, для решения которой необходимо войти в систему и ввести персональные данные. Переходя по ссылке, пользователя направляет на поддельный сайт, и после ввода логина и пароля злоумышленник получает доступ к аккаунту. Трудность заключается в том, что сообщение отправляется через почту Facebook (запрещен на территории РФ. Meta Platforms Inc. признана экстремистской организацией), что усложняет задачу отличить настоящие ссылки от поддельных.

По аналогичным мошенническим схемам фишеры овладевают данными пользователей и в других социальных сетях, как Linkedln, Twitter, ВКонтакте, а также мессенджерах, например, WhatsApp, Viber, Telegram

Методы защиты от фишинга в социальных сетях

Ключевым правилом, которого необходимо придерживаться на постоянной основе, чтобы не стать жертвой фишинга является то, что свои данные следует вводить только на проверенных и официальных сайтах.

Для того, чтобы распознать мошеннический сайт и избежать утечки личных данных в социальных сетях, можно придерживаться следующих требований:

1) Проводить анализ сайта, на который переходите. Как правило, они должны иметь домены .ru .com , например, vk.com. Также стоит обратить внимание на искаженные адреса, например, s-google.com. Наличие таких недочетов указывает на опасный сайт и должно заставить пользователя насторожиться.

2) Стоит обращать внимание на дизайн сайта. Устаревший дизайн, чаще всего, указывает на мошеннический сайт.

3) В строке с адресом важным условием является то, что должен быть указан протокол HTTPS, т.е. стоит заострять внимание на соединение с сайтом.

Рассматривая фишинг в глобальном масштабе, для защиты от него как в социальных сетях, так и на иных сайтах, пользователям рекомендуется установить антивирус, который будет блокировать вредоносные сайты.

Заключение

В результате проделанной работы можно сделать следующие выводы. Изучение фишинга является важным аспектом, который должен затрагивать каждого современ-

ного и продвинутого человека. Полностью исключить использование социальных сетей является нерациональным решением, так как на них базируются многие процессы. Именно поэтому людям следует максимально обезопасить себя различными способами, обеспечивающими предотвращению утечки личных данных пользователей и обеспечивающими их конфеденциальность в социальных сетях

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Гуськова А. М. Фишинг как основной метод социальной инженерии в схемах финансового мошенничества // 3 международная научная конференция Исследования молодых ученых, 2019. – 10 с.

2. Все о фишинге [Электронный ресурс] // информационный ресурс компании Malwarebytes URL: https://ru.malwarebytes.com/phishing/ (дата обращения: 20.11.2022)

3. Кузнецов А. Что такое фишинг и как от него защититься [Электронный ресурс] URL: https://rb.ru/story/what-is-fishing/ (дата обращения: 18.11.2022)

4. Что такое фишинг через социальные сети? [Электронный ресурс] // информационный ресурс платформы кибербезопасности Trend Micro One URL: https://www.trendmicro.com/ru_ru/what-is/phishing/social-media-phishing.html (дата обращения: 20.11.2022)

5. Квартальный отчет APWG Phishing Activity Trends Report за 2 квартал 2022 года [Электронный ресурс] // информационный ресурс рабочей группы по вопросам антифишинга APWG URL: https://docs.apwg.org/reports/apwg_trends_report_q2_2022.pdf (дата обращения: 18.11.2022)

УДК 004

Турмачева Анастасия Эдуардовна, студентка; Комсомольский-на-Амуре государственный университет
Turmacheva Anastasia Eduardovna, student of Komsomolsk-na-Amure State University
Мусалитина Евгения Александровна, кандидат культурологии, доцент кафедры «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Musalitina Evgenia Aleksandrovna, PhD in Culture Studies, Assistant Professor, «Linguistics and Cross-Culture Communication Department», Komsomolsk-na-Amure State University

КОНЦЕПЦИЯ «НУЛЕВОГО ДОВЕРИЯ» КАК ЭФФЕКТИВНЫЙ СПОСОБ ЗАЩИТЫ МЕДИЦИНСКИХ БАЗ ДАННЫХ

THE CONCEPT OF «ZERO TRUST» AS AN EFFECTIVE WAY TO PROTECT MEDICAL DATABASES

Аннотация. Медицинские учреждения в России и за рубежом активно переходят на цифровую систему документооборота и создания единых баз данных. В связи с участившимися случаями утечки медицинской информации, особую актуальность приобрела проблема обеспечения безопасности такого рода информационных баз. В статье рассматривается архитектура безопасности с «нулевым доверием» как эффективный способ защиты электронных баз данных. Анализируется принцип ее работы, возможности и ожидаемые результаты.

Abstract. Medical institutions in Russia and abroad are actively switching to a digital document management system and creating unified databases. In connection with the increasing cases of leakage of medical information, the problem of ensuring the security of such infor-

mation bases has acquired particular relevance. The article discusses the security architecture with «zero trust» as an effective way to protect electronic databases. The principle of its work, possibilities and expected results are analyzed.
Ключевые слова: медицинские базы данных, концепция нулевого доверия, личные данные, медицина, утечка.
Key words: medical databases, zero trust concept, personal data, medicine, leak.

Последние два десятилетия медицинские учреждения в России и за рубежом активно переходят на цифровую систему документооборота и создания единых баз данных. При этом, развитие медицинской информатизации не только обеспечивает удобство для пациентов в области медицины, но также создает проблему безопасности данных в сфере здравоохранения. В связи с участившимися случаями утечки медицинской информации, особую актуальность приобрела проблема обеспечения безопасности такого рода информационных баз. В эпоху развития онлайн технологий персональные данные стали «дорогим товаром», который имеет конкретную стоимость для кибер преступников. В электронных базах имеется много конфиденциальной информации, такой как протоколы приемов специалистов, диагнозы, рецепты и статус лекарств. При этом, медицинские данные, установленные как секретные, могут быть распространены злоумышленниками за материальное вознаграждение. Из-за специфики медицинской отрасли реальная ценность ее данных очень высока. Медицинская промышленность и сфера медицинских услуг стали наиболее пострадавшей областью утечки данных, а участившиеся крупномасштабные инциденты с нелегальным распространением персональных данных влекут серьезные социально-экономические последствия. Из-за некоторых пробелов системы защиты данных в самой информационной базе здравоохранения утечка данных может произойти в любое время и в любом месте. Поэтому можно говорить об особой уязвимости персональной медицинской информации.

В настоящий момент зафиксировано несколько случаев утечек данных особо крупного масштаба в сфере здравоохранения. Так, в 2021 г. в частной компании «Kaiser Medical Group» (США) были похищены данные 70 тыс. медицинских карт [2]. Злоумышленники получили доступ к электронной почте сотрудника корпорации в Вашингтоне, где они находились в течение нескольких часов без разрешения, содержащей большое количество защищенной медицинской информации.

В 2020 г. произошел взлом базы данных американского медицинского центра «Broward Health», в результате чего пострадало более 1,3 млн пациентов. «Broward Health» - это один из крупнейших центров здравоохранения во Флориде (США), предоставляющий широкий спектр медицинских услуг и ежегодно принимающий более 60 тыс. госпитализаций [1]. Расследование показало, что хакеры, взломавшие веб-сайт, получили личную информацию о пациентах, включая дату рождения, домашний адрес, номер телефона и банковскую информацию.

Вышеупомянутые инциденты кибербезопасности имеют некоторые общие черты. Во-первых, это вопрос полномочий. После того, как злоумышленник получит учетную запись, он может использовать полномочия по управлению учетной записью для совершения кибератаки. Кроме того, отсутствует всесторонний и глубокий мониторинг безопасности и возможности реагирования, что приводит к невозможности быстрого обнаружения и предотвращения атак. Наряду с внешними хакерскими атаками внутренние угрозы не меньшую опасность для нелегального распространения персональных данных. Согласно ежегодному отчету об утечке данных, опубликованному американским телекоммуникационным концерном «Verizon», медицинская отрасль является единственной среди всех отраслей, в которых внутренние угрозы превышают внешние. Так, внутренние угрозы составляют 57%, а внешние угрозы 43% [3].

С развитием приложений в области интернет-медицинского обслуживания и интеллектуального медицинского обслуживания выдвигаются более высокие требования к сотрудничеству и обмену информацией между медицинскими учреждениями, однако большинство из них уделяют недостаточное внимание проблеме безопасности данных. Специализированные информационные системы больницы многочисленны и сложны, а сами веб-сайт имеют лакуны в системе безопасности. Например, возможно возникновение ситуации, когда защита дает сбой, и процесс обнаружения потенциальных рисков становится невозможным. В таких условиях персональные данные становятся максимально уязвимыми.

Для решения данной проблемы медицинские учреждения вводят систему архитектуры безопасности с «нулевым доверием». Эта система основана на принципе обязательной проверки любых информационных источников. Медицинское учреждение используя электронные приложения во внутренней сети больницы, не подключается напрямую к Интернету. Пользователи получают доступ к авторизованным бизнес-приложениям через «клиент входа» [5]. Таким образом зашифрованные каналы позволяют обеспечить безопасный доступ и избежать риска прямых кибер атак. Хакеры не могут производить какие-либо манипуляции в такой сети, что существенно повышает безопасность медицинских баз данных.

Следующий принцип «нулевого доверия» заключается в предоставлении доступа к системе только для авторизованных пользователей. Аутентификация и авторизация осуществляются на основе строгой проверки личности пользователей по нескольким параметрам, таким как пароль/IP-адрес/MAC-адрес/местоположение для входа, для предотвращения несанкционированного доступа, незаконного доступа, фишинга, потери и взлома пароля и других угроз безопасности [4].

Благодаря внедрению концепции «нулевого доверия» медицинские учреждения получили возможность эффективного управления безопасностью данных; предоставления целевой технической поддержки различным проблемным аспектам в работе организации; обеспечения поддержки в онлайн режиме; оценки рисков; снижения нагрузки на защиту данных и уравновешивания конфликта между развитием бизнеса медицинских учреждений и безопасности персональных данных.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Баишев Н. П. К вопросу о государственно-правовом регулировании защиты персональных данных в медицине / Н. П. Баишев // Ростовский научный вестник. – 2021. – № 2. – С. 9-11.

2. Крылов А. П. Медицинские базы данных. Что важно знать врачу? / А. П. Крылов // Терапевт. – 2021. – № 10. – С. 58-61. – DOI 10.33920/MED-12-2110-07.

3. Окишев Б. А. Реализация охраны персональных данных в сфере медицины / Б. А. Окишев // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2022. – № 4(92). – С. 120-126. – DOI 10.17803/2311-5998.2022.92.4.120-126.

4. Пельтихина О. В. Законы о хранении и использовании персональных данных в медицине / О. В. Пельтихина, А. М. Морозов, Ю. Д. Белякова // Современный ученый. – 2020. – № 1. – С. 260-264.

5. Пономарева О. Н. Особенности защиты персональных данных в медицине / О. Н. Пономарева // Вестник Уральского государственного медицинского университета. – 2020. – № 4. – С. 53-54.

УДК 343.34: 004

Цзян Суя, студентка Комсомольского-на-Амуре государственного университета
Jiang Suya, student, Komsomolsk-na-Amure State University
Шушарина Галина Алексеевна, кандидат филологических наук, доцент, Комсомольский-на-Амуре государственный университет
Shusharina Galina Alexeyevna, PhD in Philology, Associate Professor, Komsomolsk-on-Amur State University

ЗАЩИТА ДЕТЕЙ В ИНТЕРНЕТЕ

PROTECTING CHILDREN ON THE INTERNET

Аннотация. В статье освещается проблема защиты частной жизни детей в Интернете. Формулируются меры по противодействию онлайн-угрозам с точки зрения основных участников политики защиты приватности в виртуальном пространстве.
Abstract**.** The article highlights the problem of protecting the privacy of children on the Internet. Measures to counter online threats are formulated from the standpoint of the main actors in the policy of protecting privacy in the virtual space.
Ключевые слова: интернет, дети, частная жизнь, кибербуллинг.
Key words**:** internet, children, privacy, cyberbullying.

The rapid development of information technology brings with it not only various conveniences for a person, but also various problems associated with the violation of human rights in the digital space, for example, privacy. Of particular danger is the violation of the right to inviolability of children's privacy. The well-known IT company Kaspersky Lab conducted a study to find out the digital habits of children. The data obtained shows that “Most often they need the Internet for playing games (in 76% of cases), watching videos (in 70% of cases), chatting with friends (in 67% of cases) and preparing for lessons (in 53% of cases).” Modern children most often visit sites in the Audio and Video category (43.6%): first of all, they watch bloggers on YouTube, listen to music on streaming platforms, and spend time watching Netflix series [1]. From Mediascope data, the share of Internet users aged 12 to 24 in Russia approached 100% and amounted to 97.1% [3] 26). Wherein, when visiting various Internet sites, children easily indicate their personal data and do not notify their parents about which sites they visit: 58% of children report that they hide something from their parents from what they do on the Internet - they go to the sites they need through anonymizers, tor browsers, but most often they simply go online when their parents are not at home [2].

The danger of uncontrolled visits to websites by children may be, firstly, the theft of money, secondly, the formation of dependence on virtual games, thirdly, the content of unwanted information on websites (photos and videos of murders and other serious crimes against a person, calls for violence, etc.). In addition, children, due to their age, do not have the life experience to stop communicating with people on the Internet, they cannot determine the degree of adequacy of those strangers who impose friendship on them on the Web. As a result of such communication, children can become members of various sects, criminal groups associated with drug trafficking, and be subjected to cyberbullying.

Realizing the degree of danger, civil society is developing various measures to protect children in the Internet space. Here we can distinguish several areas of child protection policy on the Web, depending on the main actors of such a policy. We include the state, IT companies, parents and teachers as the main actors.

To protect the rights of the child, the state develops and adopts federal laws. So, in the Russian Federation, the Federal Law of December 29, 2010 No. 436-FZ “On the Protection of Children from Information Harmful to Their Health Development” regulates relations that develop regarding the protection and protection of health, normal development, physical, in-

tellectual, moral, mental the safety of children, the rights and legitimate interests of children in the circulation of information that is harmful to their social, spiritual and moral well-being.

IT companies are developing technological projects that can protect children from online threats. For example, Kaspersky Lab has developed the Kaspersky Safe Kids solution, which restricts children's access to unwanted websites and applications. As a result, parents can be aware of what the child is looking for on the Internet, regulate the time of using programs. Kaspersky Safe Kids also allows you to determine the current location of the child in real time.

Parents or teachers, for their part, can also take a number of measures to ensure the safety of children. It is necessary to constantly explain to children which sites are harmful to visit, about the need to limit the time of their stay on the Internet, and not to disclose personal information to strangers on the network. Some websites of the same IT companies contain advice for parents and children on how to use the Internet safely [4].

Thus, the problem of protecting the frequency life of children on the Internet has many aspects and requires the interaction of various actors, such as governments, IT companies and parents.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

5. Безопасность в интернете: возрастные рекомендации для детей и подростков // https://www.kaspersky.ru/resource-center/preemptive-safety/kids-guidelines

6. Дети в интернете: 4 главных опасности и как от них защититься // https://www.pravmir.ru/deti-v-internete-4-glavnyih-opasnosti-i-kak-ot-nih-zashhititsya/

7. Доля пользователей интернета в России среди молодежи приблизилась к 100% // https://www.rbc.ru/technology_and_media/12/01/2021/5ffde01e9a79478eb5230426

4. Цифровые привычки: каждый четвёртый ребёнок проводит в гаджетах всё свободное время // https://www.kaspersky.ru/about/press-releases/2021_cifrovye-privychki-kazhdyj-chetvyortyj-rebyonok-provodit-v-gadzhetah-vsyo-svobodnoe-vremya

5. Petrunina Z.V., Shusharina G.A. Potential for implementation of Asia-Pacific region experience in developing business-incubators in the Russian Far East // В сборнике: Proceedings of the International Scientific Conference "FarEastCon" (ISCFEC 2020). Серия: Advances in Economics, Business and Management Research. Vladivostok, 2020.

УДК 004

Цирукина Дарья Кирилловна, студентка; Комсомольский-на-Амуре государственный университет
Tsirukina Daria Kirillovna, student of Komsomolsk-na-Amure State University
Мусалитина Евгения Александровна, кандидат культурологии, доцент кафедры «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Musalitina Evgenia Aleksandrovna, PhD in Culture Studies, Assistant Professor, «Linguistics and Cross-Culture Communication Department», Komsomolsk-na-Amure State University

КОНФИДЕНЦИАЛЬНОСТЬ ЛИЧНОЙ ПЕРЕПИСКИ В ИНТЕРНЕТ-ЧАТАХ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ОБЩЕСТВА

PRIVACY OF PERSONAL CORRESPONDENCE IN INTERNET CHATS IN THE INFORMATION SOCIETY

Аннотация. С развитием информационных технологий появляется все больше возможностей для передачи информации, а процесс обмена данными упрощается. Однако, с развитием Интернет коммуникации особую актуальность приобрела проблема приват-

ности общения в Интернет чатах. Частная жизнь людей с технологическим прогрессом становится менее защищенной от постороннего наблюдения. В статье рассматриваются условия соблюдения конфиденциальности личной переписки в чатах сети Интернет.
Abstract. With the development of information technology, there are more and more opportunities for the exchange of information between people, the process of data exchange is simplified. However, with the development of Internet communication the problem of the privacy of communication in Internet chats has become particularly relevant. The privacy of people with technological progress is becoming less protected from outside surveillance. The article discusses the conditions for maintaining the confidentiality of personal correspondence in chats on the Internet.
Ключевые слова: интернет, конфиденциальность, частная жизнь, чат, информационное общество, личная переписка.
Key words: internet, privacy, privacy, chat, information society, personal correspondence.

Возможности коммуникации активно расширяются благодаря развитию информационных технологий. При этом, с одной стороны, люди приобретают новые права, а с другой стороны, все чаще сталкиваются с их нарушением. Права гражданина, связанные с частной жизнью, в настоящее время распространяются еще и на цифровую среду. Однако интернет и социальные сети упрощают возможность наблюдения за пользователями. Появились возможности прослушивания разговоров, чтения чужих переписок, слежки за перемещением через сопровождающие нас устройства.

Вторжение в цифровую сферу жизни происходит ежедневно без согласия на то самих пользователей. В таких условиях право на частную жизнь становится трудно реализуемым. В силу этого, многие люди принимают наблюдение за ними как факт, не защищая свои права. Между тем, право на неприкосновенность частной жизни прописано в Конституции РФ в ст. 23: «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения» и является личным субъективным правом в жизни каждого [3].

Переписка в Интернет чатах и социальных сетях постепенно заменяет реальное общение, в ходе которого в свободный доступ попадают скриншоты переписки из личного аккаунта [5]. Тем не менее, уголовную ответственность за нарушение тайны переписки и иных сообщений устанавливает ст. 137 и 138 Уголовного Кодекса РФ [6].

Обратимся к рассмотрению понятия приватности в интернете. Прежде всего, это право на хранение, передачу, предоставление данных третьим лицам и отображение личной информации. Конфиденциальность в сети является частью приватности данных [2]. Исследователь Л. О. Красавчикова в работе, посвященной правовой защите личной жизни, указывала на то, что тайна представляет информацию о действиях или состоянии определенного лица, не подлежащая разглашению [4]. Охраняемая законом тайна – это установленное законом конфиденциальное состояние информации об особо важных сторонах жизни и деятельности личности, общества государства [2].

По статистике около 70 % информационных преступлений совершается с помощью кражи персональной информации, которая является основой информационных отношений [1]. Получение злоумышленниками доступа к конфиденциальным данным может иметь серьезные последствия. Так, например, в 2021 г. базы данных клиентов и сотрудников, финансовые документы утекали в сеть из 91 % российских компаний. Около 60 % таких утечек произошло из-за действий самих сотрудников [3]. Они разглашают конфиденциальную информацию в социальных сетях, чатах, не придавая значения потенциальной слежке за перепиской. Многие веб-сайты и соцсети используют файлы «cookies» для упрощения работы пользователями. Одновременно эти файлы применяются для нежелательного отслеживания информации. Помимо этого, пользова-

тели используют ненадежные пароли, переходят по опасным ссылкам, допускают проникновение на устройства сетевых вирусов.

Невнимательность пользователей и низкий уровень цифровой грамотности способствует росту экономических убытков и даже совершению терактов. Согласно официальным заявлениям государственных органов, именно из-за угрозы террористических атак, уполномоченные структуры следят за переписками. Необходимость этого объясняется тем, что в мессенджерах могут обсуждать планы террористические группировки. По этой причине на протяжении двух лет в России действовала блокировка мессенджера «Telegram». Мессенджер отказался сообщать ключи шифрования переписок и не предоставил доступ к перепискам, однако стал сотрудничать с властями в противодействии терроризму.

Государство отслеживает переписки пользователей не только с целью предотвращения террористических атак. Потенциально пользователи в личных сообщениях могут нарушать законы. Не менее важным фактором в данном вопросе являются мошеннические схемы, разглашающие переписки и частные данные. Они получают необходимую информацию из личных сообщений и предают ее огласке. Привлечь к ответственности таких преступников чрезвычайно проблематично, поскольку цифровые технологии обеспечивают возможность скрывать свою личность и избегать уголовного преследования.

Таким образом, роль цифровой информации в современном мире постоянно растет, а ее утечка может привести к серьезным последствиям: экономическим убыткам, актам терроризма, ограничению свободы граждан, унижению чести и достоинства личности. В связи с этим, очевидна необходимость совершенствования законодательства касательно защиты прав пользователей в сфере цифровых технологий, совершенствования систем электронных продуктов, социальных сетей и мессенджеров для обеспечения конфиденциальности в сети.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Бегишев И. Р. Преступления в сфере обращения цифровой информации / И. Р. Бегишев, И. И. Бикеев. – Казань : Издательство "Познание", 2020. – 300 с. – (Цифровая безопасность). – ISBN 978-5-8399-0726-3.

2. Бланк В. А. Тайна связи в условиях информационного общества / В. А. Бланк // Актуальные вопросы публичного права : Материалы XIX Всероссийской научной конференции Студентов и молодых ученых, Екатеринбург, 12–13 ноября 2020 года. – Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования "Уральский государственный юридический университет", 2020. – С. 18-25.

3. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) (с поправками от 30 декабря 2008 г., 5 февраля, 21 июля 2014 г., 14 марта 2020 г.)/ [Электронный ресурс] // URL: http://base.garant.ru/10103000/#ixzz6ccbxOVJy/ (дата обращения: 19.10.2022).

4. Красавчикова Л. О. Личная жизнь под охраной закона. М., 1983. С. 119 Кузнецов, П. У. Информационное право: учебник / Москва: ЮСТИЦИЯ, 2019. С. 315-327.

5. Пирожкова Е. С. К вопросу о защите авторских прав в социальных сетях / Е. С. Пирожкова // Актуальные проблемы гражданского права и процесса: взгляд молодого ученого : Сборник Всероссийской студенческой научно-практической конференции, Пермь, 30 ноября 2018 года / Ответственный составитель И.А. Сыкалов. – Пермь: Пермский институт Федеральной службы исполнения наказаний, 2019. – С. 242-247.

6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 27.12.2018) // Собрание законодательства РФ. 17.06.1996, № 25, ст. 2954.

УДК 82-1/-9

Чжан Фань, студент; Комсомольский-на-Амуре государственный университет
Zhang Fan, student, Komsomolsk-on-Amur State University
Шушарина Галина Алексеевна, кандидат филологических наук, доцент, Комсомольский-на-Амуре государственный университет
Shusharina Galina Alexeyevna, PhD in Philology, Associate Professor, Komsomolsk-on-Amur State University

ОХРАНА ЧАСТНОЙ ЖИЗНИ В КИТАЕ

PRIVACY IN CHINA

Аннотация. Работа посвящена рассмотрению вопроса охраны частной жизни в Китайской Народной Республике. Рассматривается система социального кредитования, перечислены законы, охраняющую частную жизнь и личную информацию. С учетом правоохранительной практики Китая и опыта, накопленного другими странами, представлены два подхода к обеспечению неприкосновенности личной информации в сетях.
Abstract. The work is devoted to the issue of privacy protection in the People's Republic of China. The system of social credit is considered, the laws protecting private life and personal information are listed. Taking into account China's law enforcement practices and the experiences of other countries, two approaches to ensuring the privacy of personal information on networks are presented.
Ключевые слова: цифровизация, частная жизнь, личная информация, коллективистская культура.
Key words: digitalization, privacy, personal information, collectivist culture.

В настоящее время цифровизация общества происходит стремительными темпами. Человек оценил все преимущества, которая дает цифровая среда, а именно, оформление различных документов, общение в социальных сетях, совершение покупок, доступ к различным развлечениям, получение образования. Все эти удобства доступны из дома. Не желая покидать виртуальную реальность, человек самостоятельно и добровольно сообщает подробности своей частной жизни в Интернет пространстве. Однако, помимо очевидных положительных последствий для создания комфортной среды обитания, чрезмерная де-анонимность может нести риски и угрозы для человека.

В различных странах общество реагирует по-разному на возможные негативные последствия персональной открытости в сети. Особенно ярко это проявляется в западных и восточных странах, которые согласно классификации культур, предложенной социологом Гертом Ховстеде в 1970-е годы на основе проведенного им тестирования сотрудников крупной транснациональной корпорации [7], различаются по параметру индивидуализм - коллективизм. Согласно этому признаку выделяются индивидуалистские общества, где интересы человека / индивида ставятся выше общественных. Такой тип культуры преобладает в западных странах (европейские страны, США). Коллективистские общества, напротив, культивируют принадлежность к определённой группе и верность ее идеям, мировоззрению, что представляется высшей ценностью (страны Азии, Африки, Латинской Америки).

Различия между индивидуалистскими и коллективистскими обществами проявляется и в вопросах отношения к охране частной жизни. Жители западноевропейских стран и США уделяют большое внимание концепту прайвеси (privacy). «Прайвеси – (англ. privacy-тайна, уединение, частная жизнь) - особая правовая категория в англо-американской правовой системе, означающая тайну и неприкосновенность частной

жизни, интимную сферу человека» [1]. Данный концепт пронизывает всю картину мира англосаксонских стран. Западные культуры ценят индивидуализм и рассматривают неприкосновенность частной жизни, как механизм взаимодействия с другими людьми или внешним миром.

В коллективистских культурах к вопросам приватности и ее охраны относятся менее щепетильно, что дает возможность западным средствам массовой информации называть такие страны полицейскими государствами или миром Оруэлла. Написанный в 1948 году роман Джорджа Оруэлла “1984” рассказывает о выдуманной стране, в которой власти контролируют каждого жителя. Одной из причин появления подобных аналогий в отношении Китая можно назвать разрабатываемую властями КНР «систему социального кредитования», т.е. «экосистему цифровых баз, в которой будет хранится актуальная информация о поведении граждан, компаний и государственных структур» [6]. В зависимости от соблюдения государственных стандартов в своем поведении тот или иной житель Китая получает индивидуальный рейтинг, открывающий или ограничивающий доступ гражданина к существенным социальным льготам и преимуществам, например, возможность лечь в больницу без залога. На первый взгляд, складывается впечатление о нарушении неприкосновенности частной жизни, что особенно актуально и остро в эпоху повсеместной цифровизации. Однако, это не соответствует действительности. Так, например, в КНР в гражданском кодексе понятию *частная жизнь* и ее неприкосновенности удаляется большое внимание. Согласно статье 1032 Гражданского кодекса, который был принят на 3-й сессии Всекитайского собрания народных представителей тринадцатого созыва 28 мая 2020 года, неприкосновенность частной жизни – это мир частной жизни физического лица, а также личное пространство, частная деятельность и личная информация, которую они не хотят раскрывать другим лицам. В статье 1033 перечислены типичные действия, которые трактуются как нарушение неприкосновенности частной жизни. Кроме того, в Китае действует Закон о защите личной информации Китайской Народной Республики, который был принят на 30-м заседании Постоянного комитета Всекитайского собрания народных представителей 20-го созыва 2021 августа 2021 г. в целях защиты прав и интересов на персональные данные, регулирования деятельности по обработке персональных данных и содействия разумному использованию персональных данных [4]. Дополнительно можно указать на действие следующих законов: Закон о безопасности данных, Закон о криптографии [3]. Инновация КНР в виде создания системы социального кредитования имеет ряд положительных аспектов, о которых подробно написано в различных исследованиях [2]. Сами китайцы адекватно относятся к введению такой системы, поскольку, в истории этого государства существовали организации «пятидворки» и «десятидворки», внутри которых все друг за другом следили и помогали [6].

Таким образом, вопросам отношения к вопросам частной жизни уделяется большое внимание во всех странах мира.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Большой юридический словарь. URL: https://law-enc.net/word/p/prajvesi.html

2. Галиуллина С.Д., Бреслер М.Г., Сулейманов А.Р. и др. Система социального кредитования в Китае как элемент цифрового будущего // Вестник УГНТУ. Наука, образование, экономика. Серия экономика. № 4 (26), 2018. С. 114-121.

3. О современной политике Китая в киберпространстве. URL: http: //d-russia.ru/o-sovremennoj-politike-kitaja-v-kiberprostranstve.html

4. Портал законов Китая – CJO. URL: http: //ru.chinajusticeobserver.com/law/x/personal-information-protection-law20210820

5. Право на неприкосновенность частной жизни в Гражданском кодексе Китая. URL: https://prc.today/pravo-na-neprikosnovennost-chastnoj-zhizni-v-grazhdanskom-kodekse-kitaya/
6. Цифровая карма: как будет работать система социального кредита в Китае. URL: http: // trends.rbc.ru/trends/social/60e5ca569a7947a00440ba11
7. Exploring Culture: Exercises, Stories and Synthetic Cultures. Gert Jan Hofstede, Paul Pedersen & Geert Hofstede. URL: http://www.geerthofstede.nl

УДК 004

Чувеева Александра Анатольевна, студентка; Комсомольский-на-Амуре государственный университет
Chuveeva Aleksandra Anatolievna, student of Komsomolsk-na-Amure State University
Мусалитина Евгения Александровна, кандидат культурологии, доцент кафедры «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Musalitina Evgenia Aleksandrovna, PhD in Culture Studies, Assistant Professor, «Linguistics and Cross-Culture Communication Department», Komsomolsk-na-Amure State University

ПРОБЛЕМА УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СОЦИАЛЬНЫХ СЕТЯХ

PERSONAL ANONYMITY IN SOCIAL NETWORKS, WAYS AND PROBLEMS OF ITS REALIZATION

Аннотация. Цифровые технологии онлайн-коммуникации прочно и надолго вошли в жизнь людей. С появлением сети Интернет и социальных сетей проблема утечки персональных данных и конфиденциальности информации стала особенно актуальной. Сохранение персональных данных означает неразглашение и сохранение в тайне сведений разного плана о конкретной личности, получения информации о его местоположении, невозможность идентифицировать личность без добровольного на то согласие. В статье рассматривается проблема утечки персональной информации в социальных сетях и методы борьбы с ней.
Abstract. Digital technologies of online communication have firmly and permanently entered people's lives. With the advent of the Internet and social networks, the problem of leakage of personal data and confidentiality of information has become particularly relevant. The preservation of personal data means the non-disclosure and secrecy of information of a different plan about a particular person, obtaining information about his location, the inability to identify a person without voluntary consent. The article deals with the problem of leakage of personal information in social networks and methods of dealing with it.
Ключевые слова: утечка персональных данных, социальные сети, конфиденциальность информации, частная жизнь, защита данных в интернете.
Key words: leakage of personal data, social networks, confidentiality of information, privacy, data protection on the Internet.

Цифровые технологии онлайн-коммуникации прочно вошли в жизнь людей разных возрастов и стали частью реальности, причем не виртуальной, а материальной. С появлением сети Интернет и социальных сетей проблема конфиденциальности информации стала особенно актуальной. Поэтому сейчас особенно важно следить за тем, какая информация попадает в свободный доступ сети.

В связи с актуальностью данной темы, в настоящее время появилось большое количество научно-исследовательских работ, изучающих феномен утечки персональ-

ных данных пользователей в сети. Среди них можно выделить труды, описывающие процесс защиты пользовательской информации в социальных сетях (Ш. Донг) [3], занимающиеся изучением нарушения информационной приватности в сетях (Л. В. Чеснокова) [5], а также исследующие вопрос влияния анонимности в Интернете на личностное поведение (А. Ю. Афонькин) [1].

Обратимся к рассмотрению понятия сохранения персональных данных. Под ним подразумевается: а) отсутствие личных данных пользователя в открытом доступе; б) требование, согласно которому респондент не идентифицируется во избежание неправомерного использования его данных против его личных интересов.

Одной из основных причин стремления пользователей социальных сетей скрыть личные данные является желание защититься от возможных противоправных действий со стороны третьих лиц [4].

Можно выделить два основных способа сохранения персональных данных в Интернете:

1) технический способ;

2) социальный способ.

Технический способ защиты от утечки персональных данных заключается в удалении пользователем информации о своей локации в Сети.

Социальный способ подразумевает, что личность не использует настоящую информацию о себе в Интернете.

Существует другая классификация способов защиты персональной информации, в рамках которой выделяют визуальную и дискурсивную защиту. Визуальный вид анонимности подразумевает под собой скрытие визуальной, а также звуковой информации личности (фотографии, видео). Дискурсивная анонимность – это когда пользователь скрывает имя, возраст, местонахождение, а также место учебы или работы.

Согласно американскому исследованию по выявлению степени самораскрытия студентов в социальных сетях, проводимому в 2020 г., представители женского пола детальней раскрывают персональную информацию в Сети, чем мужчины [4].

В 2021 г. в США было проведено исследование среди подростков по выявлению уровня раскрытия персональной информации в Интернете. В исследовании приняли участие 802 человека в возрасте от 12 до 17 лет. В результате были получены данные, отражающие популярность разных видов выкладываемой информации:

- фотографии (91%);
- информация о хобби, фильмах, книгах, музыке и т.д. (84%);
- дата рождения/ возраст (82%);
- местоположение/ город проживания (71%);
- информация о семейном положении (62%);
- адрес электронной почты (53%) [2].

Наименее популярными по результатам опроса оказались видеоролики (24%) и указание номера телефона (20%) [5].

По данным, полученным в результате исследования, можно сделать вывод о том, что самым популярным типом размещаемой информации среди пользователей социальных сетей и Сети Интернет является фотография, а самым редким – контактные данные [2].

Поскольку персонализированная информация пользователей тесно связана с конфиденциальностью, Интернет-провайдер обычно анонимизирует пользовательские данные, прежде чем предоставлять их для свободного доступа. Размещенная в социальных сетях информация позволяет узнать многое о пользователе. В современном мире, такие важные данные, как электронная почта, банковские счета, медицинская информация, а также записи звонков подвержены просмотру и многократной передаче, что делает их «прозрачными». Поэтому проблема анонимности в сети стала наиболее обсуждаемой в виртуальном обществе.

В настоящее время ситуация с конфиденциальностью информации улучшается. С каждым годом появляются новые способы защиты данных. Примером этому может послужить популярная в России и странах СНГ социальная сеть «ВКонтакте». Разработчики разработали эффективные меры по защите пользовательской информации. Так, данная социальная сеть предлагает систему двухфакторной аутентификации, что подразумевает обычный ввод логина и пароля, а затем код, который отправляется на личным номер телефона пользователя. Данная сеть также предоставляет возможность скрыть информацию от нежелательных пользователей, и позволяет сделать профиль закрытым. В этом случае общедоступной становится только информация, размещенная в шапке профиля.

Информационные технологии стремительно развиваются, и вместе с тем улучшается качество защиты персональных данных от утечки в Сети. Об этом свидетельствует появление в браузерах так называемой функции «инкогнито», которая позволяет пользователю быть относительно «невидимым». С помощью этого можно посещать сайты, совершать поиск информации и просматривать ленту в социальных сетях без отслеживания и сохранения в истории этих действий. Благодаря этому люди более свободно стали высказывать свое мнение и делится им в социальных сетях, заводить новые знакомства.

Однако у этого явления есть и существенные минусы. Так, можно отметить отсутствие авторского права на фотографии или цитаты; появление большей ответственности за информацию, размещаемую в сетях. Кроме того, все эти функции не дают гарантий, что сайты не будут получать персональную информацию, считывая IP-адрес пользователя, нарушая право на частную жизнь.

Таким образом, можно сделать вывод о том, что система сохранения персональных данных от утечки в сети еще несовершенна и требует большого внимания. Несмотря на то, что существуют различные функции, призванные обеспечить защиту данных, проблема незаконного использования личной информации в социальных сетях остается нерешенной и требует дальнейшего изучения.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Афонькин А. Ю. К вопросу о влиянии анонимности в Интернете на поведение пользователей / А. Ю. Афонькин, Н. А. Ноздрина // Современный опыт внедрения инноваций в науку и образование : Сборник статей по материалам международной научно-практической конференции, Уфа, 16 марта 2018 года. – Уфа: Общество с ограниченной ответственностью "Научное партнерство "Апекс", 2018. – С. 3-5.

2. Быльева Д. С. Анонимность в социальных сетях / Д. С. Быльева, С. Д. Михайленко, А. В. Рагозина // Неделя науки СПбПУ : Материалы научной конференции с международным участием, Санкт-Петербург, 19–24 ноября 2018 года. – Санкт-Петербург: Федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого", 2019. – С. 287-290.

3. Донг Ш. Защита личной пользовательской информации в социальных сетях: дилеммы правоохранительной практики Китая / Ш. Донг, К. Ли // Юридическая наука и правоохранительная практика. – 2015. – № 4(34). – С. 170-179.

4. Карпов Д. С. Способы и средства обеспечения анонимности в глобальной сети интернет / Д. С. Карпов, З. А. Ибрагимова // Правовая информатика. – 2021. – № 3. – С. 60-67. – DOI 10.21681/1994-1404-2021-3-60-67.

5. Чеснокова Л. В. Утрата информационной приватности в социальных сетях и проблема коллапса контекста / Л. В. Чеснокова // Научный результат. Социальные и гуманитарные исследования. – 2022. Т. 8. № 2. С. 94-105. – DOI 10.18413/2408-932X-2022-8-2-0-7.

УДК 316.472.43

Шахова Олеся Александровна, студентка, Комсомольский-на-Амуре государственный университет
Shakhova Olesya Aleksandrovna, student of Komsomolsk-na-Amure State University
Малышева Наталья Васильевна, кандидат филологических наук, доцент, Комсомольский-на-Амуре государственный университет
Malysheva Natalia Vasilyevna, PhD in Philology, Associate Professor of Komsomolsk-na-Amure State University

ПРОБЛЕМЫ КОНФИДЕНЦИАЛЬНОСТИ ПРИ ВЕДЕНИИ АККАУНТОВ ЗНАМЕНИТОСТЕЙ В СОЦИАЛЬНЫХ СЕТЯХ

PRIVACY ISSUES OF CELEBRITIES MAINTAINING SOCIAL MEDIA ACCOUNTS

Аннотация. Данная работа освещает ряд проблем, с которыми могут столкнуться знаменитости в социальных сетях, посредством их ведения или же простого наличия аккаунта. В статье также затрагиваются причины, по которым звезды могут как прекратить виртуальное общение с поклонниками, так и продолжить его несмотря на потенциальные негативные последствия.
Abstract. This work highlights the list of problems that celebrities may face on social networks, by means of their managing or by simply having an account. The article also touches upon the reasons why stars can both stop virtual communication with fans and continue it no matter negative consequences may be.
Ключевые слова: знаменитости, личная жизнь, социальные сети, давление, конфиденциальность.
Key words: celebrities, personal life, social networks, pressure, privacy.

Многие согласятся с тем, что в эпоху рассвета Интернета и создания социальных сетей структура современной жизни изменилась навсегда, преобразовав способы, по средством которых мы общаемся, развлекаемся, дискутируем и многое другое. Меняющий социальные установки Интернет представляет собой новую реальность, связанную совершенно новым набором стандартов, в которых часто трудно ориентироваться.

Играя роль симулятора реальной жизни, наполненной большой дозой сенсаций и эмоциональных всплесков, социальные сети вызывают у многих людей трудности, связанные с проявлением тревоги, страха и прочих негативных эмоций посредством различных факторов. Создавая бурлящую массу проблем, вызывающих депрессию, беспокойство, чувство изоляции и ненависть к себе, социальные сети оказывают значительное воздействие на психическое здоровье.

Это подтверждает нескольких крупных исследований, одно из которых, проведенное в 2018 году, показало, что использование социальных сетей напрямую связано с нарушением сна, что может повлечь за собой возникновение депрессивного состояния и потерю памяти. В случае знаменитостей, которым приходится предоставлять контент миллионам подписчиков, такие вышеупомянутые проблемы могут проявляться более выражено.

Ситуация усугубляется различными видами интернет-травли, при которой люди по всему миру начинают преследовать крупных звезд в социальных сетях за какое-либо действие или мнение. Для кого-то простые слова незнакомцев всего лишь пустой звук, но нередко именно обычные слова могут ранить до глубины души. “Иногда невозможно избежать чтения обидных замечаний. Ты зацикливаешься на негативных моментах.

Тебе говорят: "Ты уродина". Как будто хотят проникнуть в твою душу. Представьте, какую неуверенность испытываешь после этого," – заявила американская певица и актриса Селена Гомес [3]. В последние годы подобные сообщения вынудили Келли Мари Тран, Милли Бобби Браун, Лорд и многих других отказаться от социальных сетей.

Возможность влиять на подписчиков путем публикации определенной информации оказывает беспрецедентное давление на звезд, которым приходится бороться со стрессом повседневной реальности и интенсивным давлением в Интернете, пребывая в постоянном ощущении отсутствия возможности скрыться от глаз средств массовой информации. Любой может отпустить шутку, которая зашла "слишком далеко", совершить, казалось бы, незначительную оплошность в Facebook или непреднамеренно "лайкнуть" неправильный пост, но для знаменитостей действия подобного рода могут подорвать карьеру и репутацию.

Также стоит учесть, что для многих знаменитостей трудно просто выйти из дома, не столкнувшись с поклонниками, которые часто не уважают понятие "личного пространства". Весь этот перечень факторов во времена популярности социальных сетей приводит к усилению беспокойства. Это объясняет, почему многие известные люди берут перерывы от социальных сетей; некоторые говорят, что они делают это для поддержания своего психического здоровья.

"Я не пользуюсь социальными сетями, и мне кажется, что именно так у людей появляется возможность брать под контроль свою репутацию", - сообщила американская актриса Элизабет Олсен во время одного из своих интервью. "Мне кажется, что ты позволяешь людям прикасаться к тебе, когда у тебя есть Instagram или Twitter, а я не хочу, чтобы меня все время трогали" [3].

К перечню недостатков использования социальных сетей знаменитостями добавляется и тот факт, что у некоторых фанатов могут развиться парасоциальные отношения – односторонние отношения, при которых человек ощущает со звездой близкое знакомство, которое основано только на постах в социальных сетях. В связи с этим могут возникать ситуации, при которых известный человек или же его менее известный избранник сталкиваются с прямыми угрозами и преследованиями, направленными на расставание пары.

По этой причине в контрактах многих звезд присутствует пункт о запрете на романтические отношения, остерегающие от необоснованной ненависти. Также известны случаи, при которых знаменитости, не живущие в обособленных элитных районах, были вынуждены переезжать из-за избытка встречающихся на их пороге поклонников. С подобной ситуацией столкнулся американский актер и комик Пит Дэвидсон [2].

В 2018 году, после расставания с Арианой Гранде, Дэвидсон удалил свой аккаунт в Instagram, перед удалением сославшись на то, что больше не мог справляться с постоянными негативными комментариями от разгневанных фанатов. "Нет, все в порядке", - писал он в Instagram. "Нет, ничего не случилось. Я просто больше не хочу быть в Instagram. Или в любой другой социальной сети. Интернет - это злое место, которое не помогает мне чувствовать себя лучше".

Другая история связана с британским певцом Эдом Ширaном, который в декабре 2015 года объявил, что берет перерыв от социальных сетей. В своем Instagram он написал, что последние пять лет были насыщенными на события, и ему удалось побывать во многих местах, но он осознал, что видел не через призму собственных глаз, а через телефон. Он воспользовался отдыхом от социальных сетей как возможностью путешествовать по миру и увидеть все то, что он пропустил.

Несмотря на все негативные стороны социальных сетей, для большинства звезд ведение аккаунта необходимо. Социальные сети могут стать мощным инструментом для знаменитостей, которые желают повысить свою популярность или которые хотят отреагировать на какие-либо негативные комментарии в свою сторону, а также нередко опровергнуть слухи. Кроме того, социальные сети представляют собой мост коммуни-

кации между звездой и фанатами, которые могут узнать новости из первых уст, не ссылаясь на традиционные средства массовой информации.

Знаменитости продвигают многие проекты и бренды непосредственно через свой аккаунт в социальных сетях, чем зарабатывают немалые деньги. Крупные бренды тратят более 40 миллионов долларов в год на рекламные кампании, проводимые звездами, что, в свою очередь, приносит еще большую прибыль.

Статистика показывает, что потенциальный зритель не обратит внимание на рекламируемый новый фильм, если его трейлер будет вставлен в эфирное время между двумя другими непривлекательными рекламами. Но если знаменитость, пользуясь своим авторитетом и популярностью, расскажет про этот же фильм в социальных сетях, связываясь с фанатами напрямую, рекламная кампания будет в десятки раз успешнее.

Подводя итог вышесказанному, можно сделать вывод, что никто не защищен от негативного влияния социальных сетей. И чем большей популярностью обладает человек, тем труднее ему проживать собственную жизнь, наполненную теми редкими моментами, о которых никто не будет знать. Нескончаемое внимание со стороны сотен тысяч людей вынуждает забыть о личных желаниях в угоду постоянным публикациям ради поклонников. Жизнь известных людей никогда не была легкой, но с активным развитием и популяризацией социальных сетей, она становится все больше похоже на банальное существование без права на ошибку.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Celebrities Increasingly Ditching Social Media - Do Fame Seekers Need To Be On Twitter? / Peter Suciu. URL : https://www.forbes.com/sites/petersuciu/2022/08/24/celebrities-increasing-ditching-social-mediado-fame-seekers-need-to-be-on-twitter/?sh=306cfbe037b9 (Дата обращения 12.11.2022).

2. The human cost of celebrity social media / Calum Russell. URL : https://faroutmagazine.co.uk/human-cost-celebrity-social-media/ (Дата обращения 12.11.2022).

3. 23 Celebrities Talk About Social Media Anxiety and Why They Quit the Internet / Ashani Jodha. URL https://www.slice.ca/20-celebrities-talk-about-social-media-anxiety-and-why-they-quit-the-internet/ (Дата обращения 12.11.2022).

УДК 1234.56

Шевчук Кристина Александровна, студент, Комсомольский-на-Амуре государственный университет
Shevchuk Kristina Aleksandrovna, student of Komsomolsk-na-Amure State University
Шушарина Галина Алексеевна, кандидат филологических наук, доцент, заведующий кафедрой «Лингвистика и межкультурная коммуникация», Комсомольский-на-Амуре государственный университет
Shusharina Galina Alekseevna, Candidate of Philological Sciences, Associate Professor, Head of Department “Linguistics and intercultural communication”, Komsomolsk-na-Amure State University

РЕГУЛИРОВАНИЕ ИНТЕРНЕТА В СТРАНАХ ЕВРОСОЮЗА

INTERNET REGULATION IN THE EUROPEAN UNION COUNTRIES

Аннотация. Данная работа посвящена исследованию основных технологий регулирования интернета в странах Евросоюза за последние три года. В работе освещены основные законодательные базы Европарламента. Динамика развития правового регулирования информационных отношений в сети Интернет в Европейском Союзе контролирует-

ся Кодексом поведения по противодействию незаконным и ненавистническим высказываниям. В странах ЕС существует целый ряд законов, охраняющих персональные данные человека в Интернете.

Abstract. This work is devoted to the study of the main Internet regulation technologies in the EU countries over the past three years. The paper highlights the main legislative bases of the European Parliament. The dynamics of the development of the legal regulation of information relations on the Internet in the European Union is controlled by the Code of Conduct on Combating Unlawful and Hate Speech. In the EU countries, there are a number of laws that protect the personal data of a person on the Internet.

Ключевые слова: информационные отношения, Интернет, Евросоюз, Кодекс, информационный обмен, персональные данные, незаконный контент.

Key words: information relations, Internet, European Union, Code, information exchange, personal data, illegal content.

Интернет сделал свой первый шаг в 1969 году, став первой децентрализованной системой взаимосвязанных компьютеров. В то время прообраз Интернета имел другое название – ARPANET (Advanced Research Projects Agency Network).

ARPANET очень долго не была засекречена, вскоре после своего изобретения она была передана общественности для огласки. В процессе этой трансформации в Интернете не появилось понятие страны или региона. Глобальное использование Интернета началось в 1994 году, как раз в это время шла прокладка кабелей по дну океана для установления связи между континентами. С этого момента началось всемирное развитие Интернета.

Что с этим делают страны ЕС и как они пытаются регулировать интернет?

Основной целью европейского регулирования Интернета является обнаружение и удаление контента, который классифицируется как террористический, радикальный, пиратский или иным образом незаконный. Система доменных имен (DNS) используется для блокировки такого контента между обнаружением и удалением. В целом задача, которая стоит перед правоохранительными органами, заключается в выявлении и устранении первопричины.

В 2020 году Еврокомиссия завершила работу по созданию правил для интернет-компаний. Услуги технологических компаний, не соответствующие требованиям законодательства Европейского Союза, не будут допущены на европейский рынок. Законы жестко регулируют действия ведущих компаний. Чтобы регулировать эти законы, у интернет-компаний нет другого выбора, кроме как предоставлять конкурентам свои данные, чтобы их товары и услуги проходили строго легальным путем.

9 ноября 2020 года Совет министров ЕС решил принять решение и обязать операторов социальных сетей, таких как WhatsApp, Twitter, создать мастер-ключи для мониторинга чатов и сообщений со сквозным шифрованием.

Другими словами, принятие этого закона приводит к тому, что правительства государств получат доступ к сообщениям и чатам, зашифрованным этими мессенджерами.

10 августа 2021 года Европарламент одобрил массовую слежку за личными сообщениями. Известно, что Европарламент поддержал и принял резолюцию Chatcontrol – нарушение конфиденциальности, которое позволяет операторам мессенджеров отслеживать электронную почту и сообщения и автоматически, по заданным критериям, искать общественно опасные материалы во всех личных сообщениях каждого пользователя, и сообщать о таких случаях в правоохранительные органы.

Также 9 июля 2021 года Европарламент одобрил законопроект, позволяющий контролировать пользователей в целях защиты детей, позволяющий операторам мессенджеров сканировать входящую информацию на своих платформах, не опасаясь нарушения европейских законов о конфиденциальности, в том числе общего регламен-

та по защите данных (General Регламент о защите данных, GDPR), когда речь идет о насилии в отношении детей.

В конце апреля 2021 года Европейский парламент принял закон, требующий от провайдеров «удалить или отключить доступ к контенту, помеченному как террористический» в течение одного часа после уведомления соответствующих органов. Такие уведомления действительны на всей территории ЕС без предварительного судебного разбирательства.

Например, на территории РФ такие действия возможны только после решения суда, который выносит решение и обязывает Ростехнадзор удалить данный контент.

В 2022 году Германия одобрила введение биометрического распознавания возраста для авторизации в социальных сетях. 31 мая 2022 года Комиссия по защите прав несовершеннолетних одобрила три системы, которые проверяют возраст людей с помощью технологий искусственного интеллекта, чтобы предотвратить воздействие вредного контента на несовершеннолетних.

Следует отметить, что 27 апреля 2022 года Евросоюз достиг договоренности о законе о цифровых услугах. Стало известно, что власти ЕС согласовали закон о цифровых услугах, регулирующий деятельность крупных интернет-сервисов. Помимо прочего, он обязывает сервисы объяснять пользователям, как работают рекомендательные алгоритмы, и предоставлять исследователям доступ к данным для оценки работы. В случае доработки закон вступит в силу в 2024 году.

Google и Facebook запретили в Европе использование персональных данных пользователей для рекламы образа жизни, предпочтений, интересов, потребительских интересов и всего, что с этим связано (так называемая таргетированная реклама).

В январе 2022 года Европарламент рассмотрел предложение о введении закона, направленного на ограничение использования персональных данных для таргетированной рекламы в Евросоюзе. Ожидается, что новые правила вступят в силу в начале 2023 года.

Подводя итог, хотелось бы отметить, что регламенты в Европе – это свод правил. Еврокомиссия разрабатывает пакет возможных мер: штрафы, возможность принимать решения при слиянии или разделении компаний, если они хотят сохранить доступ к Единому рынку. Также, в дополнение, в странах ЕС действует огромное количество законов, которые направлены на хранение персональных данных в сети Интернет.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Рассолова, И. М. Информационные правоотношения. Теоретические аспекты / И. М. Расолова, - М.: Проспект, 2017. - 208 с.

2 Irene Kostaki Commission targets operating system, apps// New Europe. 2022. https://www.neweurope.eu/article/eu-vs-google/

3 Миятович, Д. А. Свобода выражения мнения в Интернете. Отчет организации по безопасности и сотрудничеству в Европе. / Д. А. Миятович, -Брюссель, 2021.

4 TADVISER: Германия одобрила внедрение ИИ-систем - URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1% (дата обращения: 08.11.2022).

5 TADVISER: Европейский союз достиг соглашения - URL: https://www.tadviser.ru/index.php%D1%8F:%D0%A0%D0%B5%D0%B3%D1% (дата обращения: 08.11.2022).

6 TADVISER: ЕС блокирует ИТ-компании - URL: https://www.tadviser.ru/index.php%B5%D1%82%D0%B0_%D0%B2_%D1%81 (дата обращения: 09.11.2022).

7 The Proposed EU General Data Protection Regulation. A guide for inhouse lawyers, Hunton & Williams LLP, June 2015, p. 14

УДК 364.14

Шинкорук Милена Денисовна, студент, Комсомольский-на-Амуре государственный университет
Shinkoruk Milena Denisovna, student, Komsomolsk-on-Amur State University
Шинкорук Марина Владимировна, кандидат педагогических наук, доцент, доцент кафедры «Педагогика, психология и социальная работа», Комсомольский-на-Амуре государственный университет
Shinkoruk Marina Vladimirovna, Candidate of Pedagogical Sciences, Associate Professor, Associate Professor of Pedagogy, Psychology and Social Work Department, Komsomolsk-on-Amur State University

ОТНОШЕНИЕ К ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ КАК ПРОЯВЛЕНИЕ ЛИЧНОСТНЫХ ГРАНИЦ СУБЪЕКТА

ATTITUDE TO PERSONAL INFORMATION AS A MANIFESTATION OF THE SUBJECT'S PERSONAL BORDERS

Аннотация. В статье рассмотрена значимость исследования проблемы защиты персональных данных и возможности, раскрывающиеся при раскрытии психологического ракурса этой проблемы через характеристику связи отношения к персональной информации и личностных границ субъекта. Представлено соотношение феноменов: личностные границы, локус контроля, самооценка; дано описание вариантов отношения к персональной информации относительно характеристики личностных границ субъекта.
Abstract. The article discusses the discovery of data protection problems and the opportunities that are revealed when a psychological perspective of this problem is discovered through a characterization of the relationship between relationships to personal information and personal boundaries. The ratio of phenomena is presented: personal boundaries, locus of control, self-esteem; the description of variants of relations to particular informational characteristics in relation to the personal boundaries of the sphere is given.
Ключевые слова: персональная информация, отношение к персональным данным, личностные границы, локус контроля, самооценка, субъект.
Key words: personal information, attitude to personal data, personal boundaries, locus of control, self-esteem, subject.

Вопрос о связи отношения к персональной информации и состояния границ субъекта обретает свою актуальность в контексте развития практики цифровизации – с одной стороны и устойчивости национального менталитета [2; 5], построенного на «Мы-концепции» - с другой. Широкомасштабная цифровизация бросает вызовы соблюдению прав человека на неприкосновенность частной жизни, личную и семейную тайны, защиту своей чести и достоинства, поиск, сбор, хранение и использование информации [6]. Этот процесс разворачивается на фоне сохранения коллективистских основ менталитета, построенного на расширенной интимно-личностной сфере общения, на Мы-концепции [1].

В последнее время отмечается повышенное внимание как теоретиков так и практиков из различных сфер знания о человеке и обществе (психологии, педагогики, права, медицины, информатики, экономики и др.) к содержанию понятия «личностные границы», которое в целом можно рассматривать как теоретический конструкт, отражающий место дифференциации своего и чужого, место разделения ответственности. Часто в работах по психологии подчеркивается связь личностных границ, локуса контроля и самооценки.

Локус контроля, как способ приписывания ответственности за результаты своей и чужой деятельности [3, с. 241], связан с личностными границами как следствие и результат. Несформированность личностных границ не позволяет субъекту ощутить ответственность за себя и отказаться (признать невозможность) отвечать за чувства и мысли других людей, формируя внешний локус контроля [4]. Самооценка, отражающая уровень самоуважения и принятия себя [3, с. 437] так же зависит от простроенности границ: чем пунктирнее, расшатанее границы личности, тем зависимей и неустойчивей самооценка, тем меньше самоуважение и ниже принятие себя.

На наш взгляд, понятие «личностные границы» связано и с таким междисциплинарным понятием как «персональная информация». Эта связь может быть выражена через психологическую категорию «отношение», в значении «чувства», то есть как устойчивая эмоциональная связь[3, с.544]. Для отражения этой эмоциональной связи можно.

Для выражения отношения можно использовать понятие «уважение». Если субъект уважительно относится к персональной информации о себе и других, то это свидетельствует о простроенности его личных границ. При распознавании личностной границы важно понимать, что входит в круг границ. Его составляют то, что принадлежит субъекту, то, на что он может влиять и чем может единолично распоряжаться, это - тело, мысли, убеждения, ценности, отношение к себе и к другим.

Границы могут быть сильными (четкими, ясными, простроенными) и слабыми (пунктирными). Слабость/сильность личностных границ определяется дифференциацией своего и чужого, т.е способностью человека различать, где он (его тело, мысли, чувства, потребности, вещи, пространство), а где другой

Люди с сильными границами представляются уверенными в себе, способными захватывать и удерживать внимание, удовлетворять свои потребности. Это люди, имеющие контакт с собственной агрессией, признающие её и умеющие ею пользоваться. Это, однако, не означает, что такой тип людей предпочитает нападающую стратегию, покушается на чужое и стремиться завладеть им. Напротив, люди с хорошими границами четко дифференцируют своё и чужое, с уважением относятся к чувствам, мыслям и вещам Другого, не посягают на неприкосновестность чужих границ. Это в полной мере относится и к персональной информации, которая для человека с хорошими личностными границами является безусловной ценностью, что определяет приоритет субъекта в обращении с личной информацией и безусловное право в принятии решения обращения с персональными данными. Это обстоятельство выступает для личности с простроенными границами регулятором жизнедеятельности, лежа в основе этической системы субъекта.

Люди со слабыми границами, напротив, выглядят неувернными, сомневающимися, мечущимися, путающими своё и чужое. При этом собственная отдельность может не осознаваться, и человек считает своё чужим и наоборот. Часто такой вариант отношения к себе маркируется чувствами обиды, долга и вины. Человек не считает себя вправе отказать, полагает, что любой запрос из вне должен быть им удовлетворён, игнорируя при этом собственные потребности и ресурсы. При этом, подобное отношение (игнорирование) распространяется и на желания, готовность и ресурсность другого – человек с плохими границами ждет, что любой его запрос будет удовлетворён, то есть его вложения гарантированно будут ему возвращены. Сталкиваясь с отказом, человек с плохими границами испытывает разочарование, обиду. Видно, что в центре этической системы такого человека лежит не уважение к себе и другим, а слитность и должествование, регулирующие, в том числе, и отношение к персональной информации. Человек с плохими границами не рассматривает персональные данные как ценность, определяя из своих субъективных представлений о хорошем и плохом, добре и зле, правильном и неправильном, что можно говорить о другом, оставаясь в границах, а что будет являться выходом из границ. Не чувствуя границ и не придавая ценности чужому, такая личность

представляет возможным делиться информацией о другом, включая персональные данные. Этот же подход человек с плохими границами применяет и в отношении себя, полагая, что информация о нем по умолчанию интересна собеседнику (и, игнорируя обратную связь, навязывает её) или что он не имеет права распоряжаться ей, включая запрет на предъявление и распространение (и при любом запросе полностью её раскрывает).

Таким образом, представляется возможным рассматривать отношение к персональной информации как проявление личностных границ субъекта и применять описание этого отношения в характеристике качества личностных границ субъекта.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Кузнецова Е.Н., Хилько (Швецова) О.В. Соблюдение личных границ субъектов образовательного процесса как условие личной безопасности // В сборнике: Психологическое сопровождение образования: теория и практика. Сборник научных статей по материалам XI международной научно-практической конференции. В 2-х частях. Под редакцией И.А. Загайнова, О.Г. Купцовой. Йошкар-Ола, 2021. С. 118-123.

2. Мартыненко Е.А. Психологическая суверенность личности как состояние границ субъекта // Азимут научных исследований: педагогика и психология. 2019. Т. 8. № 3 (28). С. 349-352.

3. Мещеряков Б.Г., Зинченко В.П. Большой психологический словарь // URL: https://spbguga.ru/files/03-5-01-005.pdf. (дата обращения 20.10.2022). – Режим доступа: свободный.

4. Мозговая Н.Н., Манвелян Н.Г., Костенко С.А. Функция границы личности, жизнестойкости у студентов с разным локусом-контроля // Проблемы современного педагогического образования. 2020. № 68-4. С. 297-301.

5. Парамонов А.В., Терехов А.В. Правовые аспекты защиты персональных данных // В сборнике: Тамбовские правовые чтения имени Ф. Н. Плевако. Материалы V международной научно-практической конференции: В 2 Т.. Тамбов, 2021. С. 274-277.

6. Рукавишникова И.В. Неприкосновенность частной жизни и защита персональных данных в интернет-пространстве // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2021. № 12 (139). С. 65-69.

УДК 327

Шульга Ангелина Николаевна, студентка, Комсомольский-на-Амуре государственный университет
Shulga Angelina Nikolaevna, student, Komsomolsk-na-Amure State University
Лопатина Ольга Ивановна, старший преподаватель, Комсомольский-на-Амуре государственный университет
Lopatina Olga Ivanovna, senior lecturer, Komsomolsk-on-Amur State University

МОНОПОЛИЗАЦИЯ КИБЕРПРОСТРАНСТВА

MONOPOLISATION OF CYBERSPACE

Аннотация. Сегодня киберпространство управляется в среде, где решения принимаются множеством субъектов, включая правительства, бизнес, гражданское общество и отдельных лиц или кратко "заинтересованные стороны". Такое формирование политики "снизу вверх" направлено на то, чтобы поставить все заинтересованные стороны на равный уровень для децентрализованного управления; однако оно не может остановить правительство США и американские компании от того, чтобы стать более равными,

чем другие, и эта проблема беспокоит примерно более половины правительств мира. Эти правительства, возглавляемые Россией и Китаем, требуют перестроить управление интернетом на многосторонней основе под эгидой ООН, чтобы получить авторитетную роль и зоны суверенитета в так называемом безграничном и открытом для всех интернете.

Abstract. Today, cyberspace is managed in an environment where decisions are made by multiple actors, including governments, businesses, civil society and individuals or briefly 'stakeholders'. This bottom-up policymaking seeks to put all stakeholders on an equal footing for decentralised governance; however, it cannot stop the US government and US companies from becoming more equal than others, an issue that worries about more than half of the world's governments. These governments, led by Russia and China, are demanding that Internet governance be restructured on a multilateral basis under the auspices of the UN to gain an authoritative role and zones of sovereignty in a so-called borderless and open Internet for all

Ключевые слова: киберпространство, гегемония, монополизация, управление Интернетом.
Key words: cyberspace, hegemony, monopolisation, Internet governance.

Изобретение Интернета во многом изменило наше мировоззрение. Используя понятия, взятые из истории экономики, некоторые экономисты называют его "Третьей промышленной революцией". Для исследований в области безопасности это пространство уже стало "пятым доменом" в дополнение к наземному, морскому, воздушному и космическому. Некоторые люди даже осмеливаются утверждать, что в "недалеком" будущем киберпространство станет "Параллельной Вселенной". Почти каждая компания, учреждение и правительство были вынуждены перестроиться, чтобы соответствовать физическим и виртуальным требованиям Интернета. С наступлением нового тысячелетия эти технологии начали влиять на все сферы жизни.

Использование Интернета стало настолько распространенным, что его сравнивают с самой большой страной, по словам Михр: "Если бы киберпространство было страной, оно было бы самым большим и самым населенным в мире, хотя и без какой-либо конституции или правительства". Здесь возникает вопрос многих: "Есть ли проблемы со структурой?".

Ответ на этот вопрос зависит от того, как мы на него посмотрим. С технической точки зрения киберпространство управляется практически безупречно. Нелегко увидеть жалобы на плохое управление Интернетом.

Многостороннее управление - это среда, где решения принимаются правительствами, бизнесом, гражданским обществом и отдельными лицами в координации, ставя все эти органы на равный уровень для децентрализованной модели управления и основанной на формировании политики "снизу вверх". Следует сказать, что рамки для такого рода транснационального управления уже существуют в таких секторах, как финансовое регулирование, экологическая политика и глобальное здравоохранение, все из которых не могут управляться на национальной основе. В киберпространстве этот метод управления также направлен на имитацию "безграничного и открытого для всех" характера интернета. Полномочия по отдельным функциям распределены между различными субъектами, и в целом отсутствует авторитетная роль государств. Многостороннее управление подчеркивает предполагаемые усилия по привлечению всех заинтересованных сторон за стол переговоров, оно развивалось параллельно с интернетом и стало отличительной чертой его управления как "модель интернета".

Один из авторитетных институтов киберуправления, Корпорация по присвоению имен и номеров в Интернете (ICANN), всегда была горячо обсуждаемым институтом этой модели управления, и это лучший пример для разъяснения управления с участием множества участников как "гетерогенной полиархии". ICANN была создана в 1998 году как некоммерческая общественно-полезная организация для управления "Системой доменных имен" Интернета, выделения (или координации выделения) и присвоения про-

токольных адресов Интернета, что в целом означает, что ICANN отвечает за координацию процедур кибермира и обеспечение стабильной и безопасной работы сети. В настоящее время эта организация частного сектора, расположенная в Калифорнии, управляет и контролирует наиболее важные основы Интернета, имея юридический статус в соответствии с законодательством США. Этот вопрос заставляет национальные правительства проявлять повышенный интерес к политическим решениям ICANN, поскольку интернет-политика пересекается с национальным законодательством в различных вопросах, таких как интеллектуальная собственность, неприкосновенность частной жизни, правоприменение и кибербезопасность. ICANN, как прототип многостороннего управления, также подвергается критике за такие особенности, как недостаточное участие правительства, слишком большой надзор со стороны американского правительства, отсутствие легитимности и договорные отношения с правительством США.

Многосторонность - это институциональная форма, созданная для координации отношений между тремя или более государствами в соответствии с заранее определенными и обобщенными принципами поведения. Использование этого термина после второй мировой войны было направлено в основном на противодействие односторонним действиям или двусторонним договоренностям, заключенным с целью усиления влияния сильных на слабых. Изначально многосторонний подход был направлен на снижение уровня международных конфликтов путем использования глобального управления "многих". В то время, когда он был представлен, государства всего мира собирались за разными столами в качестве единственных правовых субъектов на основе Вестфальского порядка. Сегодня сторонники многостороннего подхода требуют того же самого: сделать государства единственными действующими лицами и создать управление для более многостороннего и нисходящего администрирования интернета во имя общественного порядка, национального суверенитета и более жесткого контроля над информационными потоками. Ключевое слово здесь - "суверенитет". Суверенные государства требуют контроля над "сетями и данными" интернета в глобальном контексте. Они требуют создания "многонационального, демократического и прозрачного" управления киберпространством через агентство, созданное под эгидой ООН, оставляя транснациональным корпорациям, НПО, ученым или экспертам в области права лишь консультативную роль [1].

С другой стороны, хотя европейцы больше настаивают на роли государства как защитника интересов граждан, США пользуются поддержкой группы, которая сопротивляется чисто межправительственному подходу к управлению. В этом контексте сторонникам статус-кво необходимо сохранить текущую ситуацию децентрализованного/распределенного, глобального/транснационального управления интернетом и управление мировой интернет-архитектурой в том виде, в котором она находится в руках всемирного кластера промышленных, академических и неправительственных субъектов. Ревизионисты пытаются изменить управление в более централизованную форму, которая должна функционировать на межправительственных платформах, основанных на национальном суверенитете. Ревизионисты пытаются улучшить не только управление, но и сам "интернет", поскольку предлагаемое ими изменение - это попытка положить конец самой природе интернета как открытой для всех, безграничной, всемирной среды.

Истоки этих увлекательных и противоречивых дебатов восходят к ревизионистским требованиям, которые появились первыми в виде соображений безопасности.

Первое известное злоупотребление доменным именем ".iq" произошло в 2002 году. Большое жюри США предъявило обвинения частной компании "Infocom" в том, что она экспортировала компьютерное оборудование в Ливию и Сирию. ICANN возложила на эту компанию ответственность за регистрацию веб-адресов для Ирака, и она обеспечивала правильную маршрутизацию интернет-трафика под иракским доменным именем. iq. Суд присяжных законсервировал домен ". iq" и положил конец существова-

нию всех серверов в киберпространстве. В 2005 году в официальном докладе, подготовленном рабочей группой ООН по управлению интернетом, отмечалось, что файлы и системы корневой зоны Системы доменных имен находятся под "односторонним контролем правительства Соединенных Штатов".

Вторым заметным и более (не)известным событием стал скандал PRISM, когда Агентство национальной безопасности США было поймано с поличным в 2015 году за кибершпионажем по всему миру. Бывший сотрудник Центрального разведывательного управления (ЦРУ) Эдвард Сноуден раскрыл действия АНБ по мониторингу сетей на основании национальной безопасности через программу PRISM. Эти два события доказали, что США могут сохранить суверенный контроль над регулирующим органом ICANN и сделать сетевые объекты других суверенных государств законными целями, управляя интернет-гигантами, такими как Google, Facebook, Microsoft и др. Это означает двойные стандарты, когда речь идет о концепции суверенитета Интернета.

Реалисты указывают на различные аспекты безопасности неуправляемого (управляемого многосторонним подходом) интернета. Для авторитарных государств речь идет в основном об обеспечении безопасности режима, и это вопрос внутренней безопасности, связанный с отношениями между государством и обществом. Интернет в его нынешней безграничной форме рассматривается как инструмент "вторжения" западных либеральных идей, таких как демократия, что ставит под сомнение легитимность авторитарных правительств. Социально-политические движения, кибератаки, хактивизм, киберпреступность, кибершпионаж и неправомерное использование персональных данных постоянно бросают вызов правительствам в социальной, экономической и культурной сферах. Решением проблемы является объединенное управление киберпространством в рамках межправительственного института [2].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Комиссаров, Е. А. Проблемы монополизации в it-сфере / Е. А. Комиссаров // Образование и наука без границ: социально-гуманитарные науки. – 2018. – № 9. – С. 14-17.

2 Токошов, Р. И. Регулирование интернет-отношений: правовые основы, проблемы, рекомендации / Р. И. Токошов // Вестник Ошского государственного университета. – 2020. – № 1-3. – С. 254-260.

УДК 81-1/-9

Шушарин Никита Станиславович, студент, Комсомольский-на-Амуре государственный университет
Shusharin Nikita Stanislavovich, student, Komsomolsk-on-Amur State University
Шушарина Галина Алексеевна, кандидат филологических наук, доцент, Комсомольский-на-Амуре государственный университет
Shusharina Galina Alexeyevna, PhD in Philology, Associate Professor, Komsomolsk-on-Amur State University

ЦИФРОВАЯ ИДЕНТИЧНОСТЬ: К ОПРЕДЕЛЕНИЮ ПОНЯТИЯ

DIGITAL IDENTITY: TO THE DEFINITION OF THE CONCEPT

Аннотация. Работа посвящена рассмотрению понятия «цифровая идентичность». Рассматриваются составляющие элементы цифровой идентичности. Делается вывод о возрастающем влиянии цифровой идентичности в современном мире, формулируются угрозы и риски, связанные с ролью цифровой идентичности в обществе. Помимо этого представлено понятие «цифровой профиль» как элемент включения человека в виртуальную реальность.

Abstract. The work is devoted to the concept of "digital identity". The constituent elements of digital identity are considered. The conclusion is made about the growing influence of digital identity in the modern world, the threats and risks associated with the role of digital identity in society are formulated. In addition, the concept of 'digital profile' as an element of human inclusion in virtual reality is presented.
Ключевые слова: идентичность, цифровая идентичность, персональные данные, безопасность.
Key words: identity, digital identity, personal information, security.

В настоящее время в науке представлено значительно количество работ, посвящённых вопросам идентичности [8]. Сам термин «идентичность» получил и продолжает получать значительное количество интерпретаций, а именно, термин *идентичность* употребляется в значении самости, уникальности, самоопределения личности, принадлежности к определённой общности людей и т.д. В настоящем исследовании под идентичностью мы понимаем «осознание человеком самого себя через набор устойчивых характеристик, ответ на вопрос «Кто я?»» [2].

Повышенное внимание к проблеме идентичности объясняется несколькими основаниями, среди которых потребность человека к объединению в коллективы на основе общих интересов, качеств личности, идей, мировоззрения и пр. «Каждый индивид подсознательно стремится к обретению единства с окружающим миром, и нет более надежных оснований такого единства, чем интеграция в культурно-символическое пространство той или иной культурной общности» [6, с. 219]. Кроме того, постоянные изменения в структуре общества, смена парадигм, изменения в трактовке традиционных ценностей заставляют человека вновь и вновь переосмысливать свое место в мире и искать единомышленников.

Различные интерпретации понятия идентичности позволяют говорить о различных типах идентичности. Так, исследователи выделяют национальную идентичность [4], региональную идентичность [5], культурную идентичность [7], профессиональную идентичность [9] и т.д.

В настоящее время мировое общество переживает очередной кризис, который можно назвать глобальным, поскольку он влияет на все регионы мира, а также на социальное бытие [1]. Данный кризис определен повсеместным развитием и внедрением информационных технологий, порождая вторичную реальность, которую принято называть виртуальной реальностью. «Виртуальная реальность, развивающаяся по своим собственным законам, изначально охватывала все большее количество людей, в то время как на данном этапе она развивается путем углубления участия в жизни каждого индивида и, как следствие, общества в целом» [1, с. 11].

Формирование виртуальной реальности позволило исследователям поставить вопрос о существовании цифровой идентичности, под которой понимается «процесс создания индивидом своей цифровой проекции (следа) в сети, который включает в себя весь комплекс данных о человеке в Интернете» [3, с. 209]. Цифровой профиль / цифровая идентичность включает несколько составляющих, а именно, персональную информацию, которую человек самостоятельно размещает на различных Интернет-платформах и социальных сетях (имя, статус, фотографии и видеоматериалы, обозначение принадлежности к определённому Интернет-сообществу). Перечисленная персональная информация может соответствовать действительности, но может значительно отличаться от реальной. Человек стремится создать свое лучшее «Я» в виртуальном пространстве, используя технические способы (фотошоп, фильтры и прочие редакторы), придумывая себе новую биографию, новое имя, новую окружающую его физическую реальность (дом, машину, семью, друзей и прочее). Такой интересный и яркий профиль особенно важен при поиске партнера.

Цифровой профиль включает также информацию об активности человека в сети Интернет (местоположение человека в реальном топологическом пространстве, которое возможно отслеживать через различные мобильные приложения, список веб сайтов, которые человек регулярно или время от времени посещает для поиска информации, развлечений, совершения покупок).

Если блок персональной информации человек может контролировать и не публиковать нежелательный для себя контент, то блок неконтролируемой информации «анализируется различными алгоритмами и сравнивается с данными других пользователей для выявления значимых статистических корреляций» [3]. Информация, которой человек не всегда готов делиться с другими пользователями Интернета, может стать причиной различных негативных последствий, в частности, кибермошенничества, шпионажа, кибершантажа и других преступных деяний. Такую информацию стремятся получить рекламодатели и маркетологи для формулирования способов воздействия и поиска своих потенциальных покупателей. Не случайно все острее становится запрос общества на охрану своих персональных данных в виртуальной среде не только со стороны государственных структур, но и со стороны самих социальных сетей.

В современном мире можно с уверенностью говорить о том, что цифровая идентичность становится неотъемлемым элементом личной идентичности, оказывая влияние на жизнь каждого человека и общества в целом, вызывая риски и угрозы, связанные с повсеместной цифровизацией, сбором и анализом больших данных. Поэтому формирование цифровой идентичности становится вопросом личной и общественной безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Багрова Е. В. Типологизация кризисов современного социального бытия // Гуманитарные исследования. 2019. № 1 (22). С. 9-12.

2. Большая российская энциклопедия. URL: https:// https://bigenc.ru/philosophy/text/2000174

3. Кондаков А.М., Костылева А.А. Цифровая идентичность, цифровая самоидентификация, цифровой профиль: постановка проблемы // Вестник РУДН. Серия: Информатизация образования. 2019. Т. 16. № 3. С. 207–218.

4. Кочетков В.В. Национальная и этническая идентичность в современном мире // Вестн. Моск. Ун-та. Сер. 18. Социология и политология. 2012. № 2. С. 144-162.

5. Крылов М.П. Теоретические проблемы региональной идентичности // Гуманитарная география. М.: Институт наследия, 2006. Вып. 3. С. 157.

6. Малыгина И. В. Методологические дискурсы этнокультурной идентичности: ресурс взаимодополнительности // Ярославский педагогический вестник. 2015. № 5. С. 219-224.

7. Матузкова Е.П. Культурная идентичность: к определению понятия // Вестник Балтийского федерального университета им. И. Канта. 2014. Вып. 2. С. 62—68.

8. Фадеичева М.А. Национальная и этническая идентичность: гражданин между холизмом и робинзонадой // Альманах «Дискурс-ПИ» (электронный журнал). − Вып. 2. [Электронный ресурс]. − Режим доступа: http://discourse-pm.ur.ru/avtor/fadeicheva.php

9. Шнейдер Л.Б. Профессиональная идентичность и память: опыт генетической реконструкции // Мир психологии. 2001. № 1.

10. Шушарина Г.А. Ценностные номинации региональной идентичности // Вестник Челябинского государственного педагогического университета. 2017. № 7. С. 179-184.

УДК 343.34 : 004

Юй Цюци, студентка Комсомольского-на-Амуре государственного университета
Yu Qiuqi, student, Komsomolsk-na-Amure State University
Шушарина Галина Алексеевна, кандидат филологических наук, доцент, Комсомольский-на-Амуре государственный университет
Shusharina Galina Alexeyevna, PhD in Philology, Associate Professor, Komsomolsk-on-Amur State University

КИБЕРПРЕСТУПНОСТЬ: К ОПРЕДЕЛЕНИЮ ПОНЯТИЯ

CYBERCRIME: TO THE DEFINITION OF THE CONCEPT

Аннотация. Исследование посвящено определению понятия "киберпреступность". Выявлены виды киберпреступлений. Приведена статистика совершенных киберпреступлений в России и Китае, приведены примеры явлений, связанных с киберпреступностью.
Abstract. The study is devoted to the definition of the concept of "cybercrime". The types of cybercrime are identified. The statistics of committed cybercrimes in Russia and China, examples of cybercrime phenomena are given.
Ключевые слова: киберпреступность, цифровизация, компьютер, Интернет.
Key words: cybercrime, digitalization, computer, Internet.

The rapid development of information technology, the widespread digitalization of various spheres of social life has not only positive consequences for a person in the form of comfort, but also negative consequences. One such negative aspect of digitalization is the emergence of cybercrime.

The first mention of the use of a computer for criminal purposes dates back to the 1960s. The public danger of the problem under consideration is recognized at the national and international level. The United Nations defines cybercrime as follows: “cybercrime” is any crime that can be committed by a computer system or network, within a computer system or network, or against a computer system or network [5]. Analyzing this definition, it is possible to divide cybercrimes into two major types, namely, cybercrimes, computer crimes and crimes committed in cyberspace [2]. The first type includes 1) illegal access; 2) illegal interception; 3) interference with data; the second type of crimes is interference in the system [2]. Some experts also single out a group of cybercrimes related to copyright infringement.

According to information presented at a meeting of the State Duma of the Russian Federation, out of 1.2 million crimes committed in Russia in 2021, about 27% are cybercrime. Of the total number of cybercrimes, 212.8 thousand were committed using the Internet, 126.7 thousand - mobile communications, 103.7 thousand - bank cards, 21.8 thousand - computer equipment, 6.6 thousand - software tools, 922 - fictitious electronic payments [four]. In China, the police investigated and processed 62,000 cybercrime cases in 2021 [3].

Most often, attacks by intruders were aimed at obtaining confidential information. In addition, due to the actions of criminals, there were interruptions in the work of organizations, disruption of the main activity [1].

There are several ways in which criminals commit cybercrime, including the use of malware, DDOS attacks, a combination of social engineering and malicious code, and illegal activities in the form of distribution of illegal content.

The Criminal Code of the Russian Federation contains a number of articles providing for criminal liability for relevant socially dangerous acts: chapter 21, chapter 28. In China, the Cyber Security Law came into force on June 1, 2017. According to the document, the Chinese authorities will seek a safe, open, legalized cyberspace, which should also be, first of all,

peaceful. It is emphasized that the security and sovereignty of cyberspace must be protected as resolutely as the physical borders of the state.

The rapid development of digital technologies brings with it a number of threats, in particular, personal data falls into the hands of fraudsters, as a result of which money is stolen from bank cards. Possession of other people's personal data is valuable for imposed advertising, and political manipulation.

Thus, we can conclude that despite the growth of cybercrime in the world, countries are pursuing an active policy to combat cybercrime.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Актуальные киберугрозы: I квартал 2022 года // https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/#id2

2. Буз С.И. Киберпреступления: понятие, сущность и общая характеристика // Юристъ-Правоведъ, 2019, № 4 (91). С. 78-82.

3. Китай рассмотрел 62 000 дел о киберпреступлениях в 2021 году // https://regnum.ru/news/society/3469745.html

4. Комитет Госдумы привёл данные статистики о киберпреступлениях. URL: https://d-russia.ru/komitet-gosdumy-privjol-dannye-statistiki-o-kiberprestuplenijah.html

5. Хусяинов Т. М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве // Уголовный закон Российской Федерации: Проблемы правоприменения и перспективы совершенствования материалы всероссийского круглого стола. 2015.

УДК 343.34 : 004

Ющук Екатерина Сергеевна, студентка, Комсомольский-на-Амуре государственный университет;
Yushuk Ekaterina Sergeevna, student of Komsomolsk-na-Amure State University
Васильева Анна Алексеевна, старший преподаватель, Комсомольский-на-Амуре государственный университет
Vasileva Anna Alexeevna, Associate Professor, Komsomolsk-na-Amure State University

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ВЕЛИКОБРИТАНИИ

PERSONAL DATA PROTECTION IN THE UNITED KINGDOM

Аннотация. Данная работа посвящена исследованию политики безопасности персональных данных, предпосылок возникновения и развития мер по ее обеспечению в Великобритании, а также анализу применения средств информационного контроля в различных сферах деятельности на основании экспертных оценок, опубликованных в средствах массовой информации.
Abstract. This work is devoted to the study of personal data protection policy of the United Kingdom, preconditions and development of its enforcement measures, as well as analysis of information control tools implementations in various fields of activity based on expert assessments published in mass media.
Ключевые слова: персональные данные, Великобритания, кибербезопасность.
Key words: personal data, the United Kingdom, cybersecurity.

Персональные данные и несанкционированный доступ к ним – это зачастую пренебрегаемый аспект информационной безопасности. Утечки баз данных пользователей сегодня являются обыденностью и, за редкими исключениями, практически не вызывают резонанс. Однако, полученная таким образом информация способна нанести

куда больший вред, чем опустошенная кредитная карта или спам, размещенный на личной странице ничего не подозревающего гражданина. Личная информация может использоваться злоумышленниками в социальной инженерии для получения доступа к информации, имеющей политическую, научную или военную значимость, последующее разглашение которой влечет неконтролируемые последствия.

Одним из примеров описанной ситуации служит инцидент с Лиз Трасс. Согласно отчету, опубликованному на сайте издания Daily Mail чуть больше чем через неделю после отставки Лиз Трасс с поста премьер-министра Великобритании, хакерами были получены данные, составляющие государственную тайну. Данные удалось заполучить из-за пренебрежения Трасс, занимавшей на тот момент пост министра иностранных дел, мерами информационной безопасности, так как для обмена информацией, предназначенной для ограниченного круга лиц, Трасс использовала личный телефон и незащищенные каналы связи. Предполагается, что для взлома была использована шпионская программа Pegasus [1], однако, даже в случае наличия активных действий по внедрению со стороны взломщиков, факт нарушения правил информационной безопасности, брифинги по которым, согласно утверждениям британского правительства, регулярно проводятся среди министров и персонала, неоспорим. Несоблюдение базовых правил обмена сведениями, составляющими государственную тайну, на таком высоком уровне на данный момент привело к тому, что Лейбористская партия Великобритании потребовала от британского правительства провести детальное независимое расследование, а также ужесточения мер безопасности. Член Лейбористской партии Иветт Купер в своем комментарии для новостного сервиса Sky News заявила, что «в текущей ситуации возникает ряд вопросов к кибербезопасности» [2]. Британское правительство, в свою очередь, отказалось комментировать детали системы безопасности, но отметили ее «надежность при защите от киберугроз» [3]. Также было заявлено о проведении нового обучения сотрудников служб безопасности. В нем будет уделено особое внимание запрету на использование министрами личных телефонов в рабочих целях, согласно рекомендациям руководителей спецслужб Великобритании.[4] Помимо этого, усугубляет ситуацию сокрытие факта утечки Борисом Джонсоном, на тот момент премьер-министром Великобритании, и секретарем кабинета министров Сайомоном Кейсом во избежание ее влияния на эффективность летней предвыборной кампании консерваторов, в которой Трасс победила [5]. Помимо этого, контекст сообщений, связанный с ситуацией в Украине, привлек внимание официальных представителей Великобритании к Российской Федерации как возможному организатору взлома. Руководитель парламентского комитета по обороне Соединенного Королевства Тобиас Эллвуд заявил, что это «постоянная угроза со стороны России» [6]. Однако, поиск виновных во взломе не является продуктивным, а служит цели переключить внимание наблюдателей с проблем обеспечения кибербезопасности на внешние факторы.

В данной ситуации явно наблюдается тенденции к реактивному решению возникших проблем. Однако, проактивное поведение и адекватные меры профилактики позволили бы избежать подобных утечек. В случае с Лиз Трасс необходимы более строгие меры, направленные на соблюдение министрами правил информационной безопасности. Текущие меры, если судить по усиленному вниманию спецслужб Великобритании и проведению дополнительных брифингов, подвергнутся ужесточению. В целом, несмотря на освещение в СМИ, ситуации с утечками персональных данных быстро исчезают с заголовков газет, что позволяет виноватым в утечке значительно смягчить, а в некоторых случаях и вовсе избежать последствий. Это, в свою очередь, влечет дальнейшее пренебрежение правилами информационной безопасности, что порождает дальнейшие утечки. В отсутствие механизмов, эффективно регулирующих подобные ситуации, персональные данные всех участников информационного обмена будут находиться под постоянной и значительной угрозой несанкционированного доступа.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Liz Truss is on her FOURTH new mobile phone number since July after she was allegedly hacked by Russian agents / Mail Online – website of the Daily Mail, a newspaper in the United Kingdom. URL: https://www.dailymail.co.uk/news/article-11394445/Liz-Truss-FOURTH-new-mobile-phone-number-July-alleged-Russian-hacking.html (дата обращения 25.11.2022). - Режим доступа: свободный.

2. UK politicians demand probe into Liz Truss phone hack claim / KSLTV – Utah News URL: https://ksltv.com/510325/uk-politicians-demand-probe-into-liz-truss-phone-hack-claim (дата обращения 25.11.2022). - Режим доступа: свободный.

3. U.K. politicians call for "urgent independent investigation" into Liz Truss phone hack claim / CBS News – Breaking news, 24/7 live streaming news and top stories. URL: https://www.cbsnews.com/news/liz-truss-phone-hack-claim-uk-cybersecurity (дата обращения 25.11.2022). - Режим доступа: свободный.

4. Spy chiefs tell ministers ‘stop using your phones’ after Liz Truss hack / Metro.co.uk – News, Sport, Showbiz, Celebrities from Metro. URL: https://metro.co.uk/2022/10/31/spy-chiefs-tell-mps-to-stop-using-your-phones-after-liz-truss-hack-17671671 (дата обращения 25.11.2022). - Режим доступа: свободный.

5. Во взломе телефона Лиз Трасс обвинили «российских агентов» / Московский Комсомолец – Новости России и мира. URL: https://www.mk.ru/politics/2022/10/30/vo-vzlome-telefona-liz-trass-obvinili-rossiyskikh-agentov.html (дата обращения 25.11.2022). - Режим доступа: свободный.

6. Liz Truss's Phone was Hacked, the Information about it – Withheld / Novinite.com - Sofia News Agency, Bulgarian news in English, EU, world. URL: https://www.novinite.com/articles/217299/Liz+Truss%27s+Phone+was+Hacked%2C+the+Information+about+it+%E2%80%93+Withheld (дата обращения 25.11.2022). - Режим доступа: свободный.

УДК 343.34 : 004

Яковлева Ирина Михайловна, студентка, Комсомольский-на-Амуре государственный университет;
Yakovleva Irina Mikhailovna, student of Komsomolsk-na-Amure State University
Васильева Анна Алексеевна, старший преподаватель кафедры Лингвистики и межкультурной коммуникации, Комсомольский-на-Амуре государственный университет
Vasileva Anna Alekseevna, senior lecturer of the Linguistic and Cross-cultural communication department, Komsomolsk-na-Amure State University

COOKIE-ФАЙЛЫ КАК СРЕДСТВО ПОЛУЧЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ И МЕТОД НАРУШЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ

COOKIE-DATA AS A MEANS OF OBTAINING PERSONAL DATA AND A METHOD OF VIOLATING CONFIDENTIALITY

Аннотация. Данная статья посвящена системе сбора и хранения персональных данных cookie-файлы. Рассматривается концепция и использование таких файлов, а также возможности получения информации третьими лицами в корыстных целях, свободном обмене данной информации на просторах Интернета и способах защиты своих данных.
Abstract. This article is devoted to the such system for collecting and storing personal data as cookies. The concept and use of such files are considered, as well as the possibility of obtaining information by third parties for selfish goals, the free exchange of this information on the Internet and ways to protect their data.

Ключевые слова: безопасность, персональные данные, цифровизация, хранение данных, пользователи.
Key words: safety, personal data, digitalization, data storage, users.

Сегодня каждый человек использует Интернет в различных целях и сталкивается с различными сообщениями о сборе информации персональных данных и передвижениях по тем или иным сайтам. Так, очень часто мы встречаемся с сообщениями cookie, благодаря которым можно составить портрет человека, его увлечения и другую информацию. Поэтому очень важно, чтобы люди знали о таких файлах, на что они дают свое согласие, принимая соглашение cookie-файлов, кто и как с ними взаимодействует, и какие операции с ними проводит, а имели доступ к сведениям о том, как защитить, удалить или вовсе не формировать свои данные.

Cookies – это текстовые файлы небольшого объема со служебной информацией для браузера. Обычно такие файлы содержат в себе информацию о посещениях тех или иных сайтов, логин и пароль и другие данные.

Основная задача cookies состоит в том, чтобы сделать поиск в Интернете более комфортным. Так, сайты, на которых вы бывали ранее и вводили какие-либо данные сохраняются и второй раз их вводить уже не нужно.

Cookie-файлы содержат в себе следующую информацию: 1) личные данные для авторизации (логин, E-mail, пароль и т.д.); 2) тип устройства и его комплектация, с которого вы зашли на сайт [1].

Самый яркий пример использования cookie-файлов - это таргетированная реклама, основанная на личных предпочтениях и посещениях сайтов пользователя. Часто люди замечают, что спустя несколько дней после поиска какой-либо вещи или явления при последующем использовании Интернета появляется реклама всего, что связано с тем или иным поиском ранее. Такая же ситуация бывает в том случае, когда рядом с телефоном вы обсуждаете, к примеру, покупку какой-то вещи и вам даже не нужно ничего вводить, рекламные объявления также с большой вероятностью покажут вам тот объект, который обсуждался.

В большинстве случаев основные cookies помогают упростить работу. Тем не менее, вы должны понимать, что в любой системе есть и плюсы и минусы. Так, данные файлы могут нанести ущерб конфиденциальности ваших данных. Они могут собирать личные данные, что потребовало ужесточения правил защиты – например, многие сайты должны выполнять рекомендации, указанные в Общем регламенте по защите данных (GDPR).

Для того, чтобы лично познакомиться с тем, что же такое таргетированная реклама и файлы cookie, можно провести эксперимент. Для начала стоит удалить прежний кэш с устройства и попробовать ввести в поиске некую лексему и перейти по нескольким ссылкам. Позже, переходя уже по другим запросам, мы можем видеть рекламу, где нам предлагаются различные статьи и продукты по данной теме. При подготовки данного исследования в поисковые сервисы неоднократно были введены запросы, связанные с темой безопасности в сети Интернет. В результате работы cookie-файлов можно увидеть таргетированную рекламу, демонстрируемую на посторонних сайтах, не относящихся к теме исследования. В рисунке 1 показана реклама, появившаяся в ходе данного эксперимента на юмористическом портале. Данная реклама предлагает перейти на сайт, чтобы узнать информацию по следующим темам: как распознать звонок мошенника, что такое «фишинг», как обезопасить детей в интернете; а также предлагает «активировать кибербезопасность».

При переходе по ссылке данной рекламы мы видим информационный портал «Госуслуги», на страницах которого нам предложено ознакомиться с методами обеспечения кибербезопасности и «кибергигиены». На Рисунке 2 можно заметить, что есть отметка о городе, из которого был проведен запрос. Следовательно, cookie-сервисы на данном компьютере собирают информацию не только о запросах, но и о геолокации.

Рисунок 1 – Таргетированная реклама

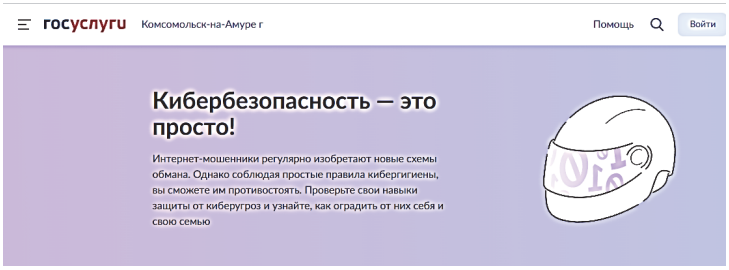

Рисунок 2 – Сайт, на который ведет таргетированная реклама

Проанализировав содержание страницы, на которую ведет таргетированная реклама, можно сделать вывод о том, что ключевыми словами для подбора рекламы являлись «кибербезопасность», «хакер», «cookie-файлы».

Конечно, людей беспокоит большое количество вылезающей уже неактуальной для поиска рекламы, которая мешает спокойно посещать сайты. Всегда стоит внимательно прочитать соглашение прежде, чем принять его, ведь когда вы раскроете свои данные тому или иному сайту, третьи лица могут даже неосознанно передавать информацию о вашей активности мошенникам. Также, сторона, собирающая данные, может не быть причастна к злоумышленному их использованию, но она может продавать ваши данные другим лицам, которые могут использовать их в мошеннических целях.

Согласно Регламенту GDPR, такие файлы должны иметь ряд принципов: 1) принцип прозрачности, который обеспечивает открытость, честность и правдивость информации. Сайт должен предоставлять пользователям информацию о том, как она обрабатывает данные и куда их передает. 2) принцип доступности, который обеспечивает четкость информативного сообщения, а также то, что данное сообщение вы сможете найти без труда.

Также, определяется ряд прав для субъекта, самыми важными из которых являются: право на прекращение обработки данных, право быть забытым на том или ином сайте и право на рассмотрение ситуации, если пользователь считает, что сбор и хранение его данных незаконна [2].

Сегодня большое количество сайтов знают о нас довольно много фактов. Все эти компании, социальные сети и сайты анализируют эту информацию и делятся ею друг с другом, предугадывают наши действия и желания, подкидывая нужную рекламу. И это лишь малая часть возможных действий персональных данных третьими лицами. Поэтому в наше время каждый человек должен знать о таких методах сбора информации о себе, способах их заполучения мошенниками и как можно защитить себя и свои данных [3].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Cookies / Calltouch blog. URL: https://www.calltouch.ru/blog/glossary/cookies/ (Дата обращения 15.11.2022). – Режим доступа: свободный.

2. Регулирование Интернета развивается, файлы cookie остаются / Information security. Информационная безопасность. URL: https://lib.itsec.ru/articles2/pravo/regylirovanie-interneta-razvivaetsya,-faili-cookie-ostautsya (Дата обращения 15.11.2022). – Режим доступа: свободный.

3. Что такое cookies? / Binance academy. URL: https://academy.binance.com/ru/articles/what-are-cookies (Дата обращения 15.11.2022). – Режим доступа: свободный.

СОДЕРЖАНИЕ

Научное издание

ГЛОБАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОСТИ:
ПОИСКИ И ПУТИ РЕШЕНИЯ

Материалы общественного онлайн-обсуждения
«Threats to international peace and security caused by terrorist acts (Угрозы международной безопасности, вызванные терроризмом)», 27 октября 2022 г. и круглого стола со всероссийским участием «The Right to Privacy in the Digital Age (Право на неприкосновенность частной жизни в век цифровизации)», 29 ноября 2022 г.

Ответственный редактор Г. А. Шушарина

Статьи публикуются в авторской редакции

Подписано в печать 27.12.2022.
Формат 60×84 1/16. Бумага 65 г/м^2. Ризограф RISO EZ 570E.
Усл. печ. л. 15,80. Уч.-изд. л. 14,00. Тираж 21 экз. Заказ 30761.

Полиграфическая лаборатория
Федерального государственного бюджетного
образовательного учреждения высшего образования
«Комсомольский-на-Амуре государственный университет»
681013, Комсомольск-на-Амуре, пр. Ленина, 27.