Научная статья
УДК 343.9
DOI: 10.47475/2311-696X-2023-39-4-155-161

С. 155–161

НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ: ЗАЩИЩЕНЫ ЛИ МЫ?

Ольга Сергеевна Кайгородова
Тюменский институт повышения квалификации сотрудников МВД России, Тюмень, Россия
kaigorodoff@mail.ru

Аннотация. В статье рассматриваются тенденции развития современного общества, трансформация которого все глубже уходит в цифровую сферу. Безусловное удобство имеющихся электронных ресурсов, призванных решить большинство насущных проблем человечества — от оплаты товаров, услуг до решения вопросов, связанных с реализацией прав и свобод человека и гражданина, ставит, в том числе, и вопрос, связанный с безопасностью хранения данных на электронных носителях, защите их от компрометации или атак. Решение вопроса о защите информации, в том числе представленной в цифровом виде, возможно только на уровне государства путем принятия достаточной нормативной правовой базы. В статье проанализированы отдельные нормативные акты, регламентирующие вопросы обеспечения кибербезопасности, которые автором разделены на две группы: нормативные правовые акты, определяющие виды информации, подлежащей государственной защите; нормативные правовые акты, регламентирующие основные термины, определения, порядок и механизм обеспечения безопасности информации, в том числе, содержащейся на электронных носителях информации. Исследование данного вопроса побудило автора поставить вопрос о том, насколько мы все же защищены в киберпространстве, и дать на него ответ.

Ключевые слова: кибербезопасность, информационная безопасность, угрозы и вред информационной безопасности, защита информации, содержащейся на электронных носителях, открытые источники информации

Для цитирования: Кайгородова О. С. Нормативно-правовое обеспечение кибербезопасности: защищены ли мы? // Правопорядок: история, теория, практика. 2023. № 4 (39). С. 155–161. DOI: 10.47475/2311-696X-2023-39-4-155-161

Research article

REGULATORY AND LEGAL SUPPORT OF CYBERSECURITY: ARE WE PROTECTED?

Olga S. Kaigorodova
Tyumen Institute of Advanced Training of Employees of the Ministry of Internal Affairs of Russia, Tyumen, Russia
kaigorodoff@mail.ru

Abstract. The article examines the trends in the development of modern society, the transformation of which is going deeper into the digital sphere. The absolute convenience of the available electronic resources designed to solve most of the pressing problems of mankind — from paying for goods, services to solving issues related to the realization of human and civil rights and freedoms, raises, among other things, the issue related to the security of storing data on electronic media, protecting them from compromise or attacks. The decision on the protection of information, including information presented in digital form, is possible only at the state level by adopting a sufficient regulatory framework. The article analyzes individual regulations regulating cybersecurity

issues, which are divided into two groups by the author: regulatory legal acts defining the types of information subject to state protection; regulatory legal acts regulating the basic terms, definitions, procedure and mechanism for ensuring the security of information, including information contained on electronic media. The study of this question prompted the author to raise the question of how we are still protected in cyberspace and give an answer to it.

Keywords: cybersecurity, information security, threats and harm to information security, protection of information contained on electronic media, open sources of information

For citation: Kaigorodova OS. Regulatory and legal support of cybersecurity: are we protected? *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2023;(4):155-161. DOI: 10.47475/2311-696X-2023-39-4-155-161 (In Russ.)

Введение

В современном обществе все сложнее представить себя вне цифрового формата жизни. Безусловное удобство, призванное решить большинство насущных задач, как то: оплата услуг, запись на прием к врачу, подача различного рода заявлений в государственные органы, удовлетворение потребности общения на расстоянии, сопряжено с опасностью утери информации, хранящейся на электронных носителях. В связи с этим остро стоит вопрос защиты подобного рода информации, а соответственно, информационной безопасности, которая, стала предметом изучения и дискуссий многих ученых уже на протяжении нескольких лет [1; 2; 3; 12]. Угрозы и вред информационной безопасности, несмотря на кажущуюся эфемерность, на самом деле нельзя недооценивать. Паника, озлобленность, ненависть отдельных этнических групп, нарушение работы серверов и сайтов, влекущие, в том числе, утрату конфиденциальных данных — вот только немногие негативные последствия. Пандемия COVID-19 стала еще одним фактором, способствующим нарастанию паники. Ученые верно отмечают, что «карантин» и «великий» локдаун спровоцировали в обществе экспоненциальный рост страха за здоровье свое и своих близких, сформировали предчувствие катастрофического развития событий. В совокупности с социальным десантированием и масштабным распространением фейковых новостей, такой общественный настрой стал объектом пристального интереса со стороны как преступных сообществ, действующих в цифровой среде, так и отдельных киберпреступников [4, с. 186]. Пандемия способствовала росту кибератак и фишинговых рассылок с вредоносным программным обеспечением [5, с. 9].

Фактически человек сегодня «живет» в сети, отмечает В. Д. Ипатов, «общается, развивается, совершает покупки, получает информацию, выражает свою гражданскую позицию. Вместе с тем такой образ жизни имеет негативные стороны: посредством информационных технологий совершаются правонарушения, формируются экстремистские движения, развязываются информационные войны» [6, с. 30].

Преступления в сфере кибербезопасности направлены на получение масштабных результатов при нарушении большого количества прав и законных интересов. В связи с этим, информационная безопасность каждого отдельно взятого человека зависит, в том числе, от информационной безопасности государства, призванного защищать законные права и свободы своего народа в информационной среде.

Ученые определяют следующие основные направления обеспечения информационной безопасности: правовая защита; организационная защита; инженерно-техническая защита, призванные разрабатывать механизмы защиты информации на уровне государства, организации, отдельной личности [7, с. 197]. Такая совокупность направлений обеспечения информационной безопасности в их взаимосвязи, при условии постоянного развития, соответствующего современным реалиям, позволит обеспечить безопасность в информационной среде.

Описание исследования

Информационная среда — это сфера деятельности, связанная с созданием, распространением, преобразованием и потреблением информации. Как сфера правового регулирования информационная сфера представляет собой совокупность субъектов права, осуществляющих такую деятельность, объектов права, по отношению к которым, или в связи с которыми эта деятельность осуществляется, и социальных отношений, регулируемых правом или подлежащих правовому регулированию [8, с. 215].

Информационная безопасность заключается в защите всех данных юридических и физических лиц, независимо от вида информации и места и способа ее хранения. Кибербезопасность, в свою очередь, направлена на защиту цифровых данных. В настоящее время больший

массив информации представлен в электронном виде, включая государственные сервисы услуг, такие как Портал государственных услуг Российской Федерации, Личный кабинет налогоплательщика и т. д. 22 декабря 2022 года принят Федеральный закон № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации»[1], то есть биометрические персональные данные физического лица также будут размещены в единой биометрической системе в электронной форме. Информация о данных пациентов все чаще также хранится в электронном формате — это облегчает доступ к данным пациента любым врачом и из любого кабинета, но возникает вопрос о безопасности хранения данной информации. Большим массивом электронной информации оперируют многофункциональные центры, банки, магазины, в том числе, интернет-магазины, страховые компании, социальные сети — таких примеров много. Даже та информация, которая должна быть представлена на бумажном носителе, зачастую исполняется сначала в электронном виде и только затем распечатывается. Например, протоколы процессуальных действий при расследовании уголовных дел. То есть, такие данные, в части хранения их на электронном носителе, также не защищены от компрометации или атак. В связи с этим, нормативные правовые акты, регламентирующие защиту информации, направлены, в том числе, и на защиту данных в цифровом (электронном) виде.

Решение задачи защиты информации возможно только на уровне государства. В первую очередь задачу информационной безопасности призваны решить положения Конституции РФ[2]. К таким положениям относятся следующие нормы:

— каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения (ч. 2 ст. 23 Конституции РФ);

— каждому гарантируется свобода мысли и слова (ч. 1 ст. 29 Конституции РФ);

— никто не может быть принужден к выражению своих мнений и убеждений или отказу от них (ч. 3 ст. 29 Конституции РФ);

— каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом (ч. 4 ст. 29 Конституции РФ);

— гарантируется свобода массовой информации. Цензура запрещается (ч. 4 ст. 29 Конституции РФ).

Вместе с тем, необходимо понимать, что мы живем в социуме, и права одного человека заканчиваются там, где начинаются права другого человека. Это правило нашло свое отражение в нормативных правовых актах различного уровня, в первую очередь, в Конституции РФ, а именно:

— не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства (ч. 2 ст. 29 Конституции РФ);

— установлено право государства определять перечень сведений, составляющих государственную тайну (ч. 4 ст. 29 Конституции РФ).

Очерчивая круг запрещенных деяний, право тем самым признает все остальные деяния дозволенными. Свобода человека в этом случае ограничивается минимальным образом — за ее границами остается лишь то, что явно вредно для общества [9, с. 37].

Указом Президента РФ от 05.12.2016 года № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[3] (далее — Доктрина) утверждена Доктрина, являющаяся документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, в котором развиваются положения Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ

[1] Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации : Федеральный закон от 29.12.2022 № 572-ФЗ // Официальный интернет-портал правовой информации/ URL: http://publication.pravo.gov.ru/Document/View/0001202212290024 (дата обращения: 02.09.2023).

[2] Конституция Российской Федерации : принята всенародным голосованием 12.12.1993 г. с изм., одобр. в ходе общероссийского голосования 01.07.2020 // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/constitution/ (дата обращения: 02.09.2023).

[3] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 05.12.2016 № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

от 2 июля 2021 г. № 400[1] (далее — Стратегии), а также других документов стратегического планирования в указанной сфере.

Как верно отметил А. К. Дубень, национальная безопасность представляет собой безопасность как населения, проживающего на территории страны, так и власти, и окружающей среды в целом. Все это свидетельствует о многоаспектном характере национальной безопасности [10].

Правовую основу Стратегии составляют Конституция РФ, Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»[2] , Федеральный закон от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации»[3], другие федеральные законы, нормативные правовые акты Президента Российской Федерации (ч. 4 ст. 1 Стратегии).

Кроме того, вопросы обеспечения кибербезопасности регламентированы и другими нормативными правовыми актами, которые можно разделить на две группы. Нормативные правовые акты первой группы определяют виды информации, подлежащей государственной защите. Это, например, закон РФ «О государственной тайне»; федеральные законы «Об информации, информационных технологиях и о защите информации», «О персональных данных», «О средствах массовой информации», «О государственной дактилоскопической регистрации в Российской Федерации», «О банках и банковской деятельности», «О связи», «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»; Уголовный кодекс РФ, Кодекс РФ об административных правонарушениях, Уголовно-процессуальный кодекс РФ; Указ Президента РФ «Об утверждении Перечня сведений, отнесенных к государственной тайне». Это, безусловно, далеко не полный перечень нормативных правовых актов, регламентирующих перечень охраняемых законом данных, содержащихся, в том числе, в цифровом виде.

При оперировании различными данными целесообразно уточнить, относится ли интересующая информация к сведениям, охраняемым законом[4].

Ко второй группе относятся нормативные правовые акты, регламентирующие основные термины, определения, порядок и механизм обеспечения безопасности информации, в том числе, содержащейся на электронных носителях информации: федеральные законы «Об информации, информационных технологиях и о защите информации», «Об организации предоставления государственных и муниципальных услуг», «Об электронной подписи», указы Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации», «О Стратегии национальной безопасности Российской Федерации», «Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг.»; постановления Правительства Российской Федерации «О единой системе межведомственного электронного взаимодействия», «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)», приказы МВД России «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года», «Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации», «Об утверждении структуры и системы адресации интегрированной мультисервисной телекоммуникационной сети Министерства внутренних дел Российской Федерации», «Об утверждении планаграфика перехода Министерства внутренних дел Российской Федерации на использование отечественного офисного программного обеспечения на 2018 год и на плановый период до 2020 года», «Об утверждении Требований к информационному взаимодействию уполномоченной субъектом Российской Федерации организации и территориального органа МВД России, включая правила передачи данных по каналам связи с использованием информационных систем»; ГОСТ Р 50922-96. Защита информации. Основные термины и определения; ГОСТ Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации; ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология (ИТ). Методы и средства

[1] Стратегия национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 02.07.2021 № 400 // Собрание законодательства РФ. 2021. № 27 (часть II). Ст. 5351.

[2] О безопасности : Федеральный закон от 28.12.2010 № 390-ФЗ // Российская газета. 2010. 29 дек. (№ 295).

[3] О стратегическом планировании в Российской Федерации : Федеральный закон от 28.06.2014 № 172-ФЗ // Российская газета. 2014. 03 июл. (№ 146).

[4] См., например: Перечень нормативных актов, относящих сведения к категории ограниченного доступа (материал подготовлен специалистами КонсультантПлюс) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_93980/ (дата обращения: 02.09.2023).

обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель; ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности; ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности и др.

Отметим, что нормативные правовые акты, регламентирующие сферу информационной безопасности, не декларативны. За нарушения предусмотренных законом норм права в данной сфере предусмотрена различного рода ответственность. Так, например, в соответствии со ст. 12 федерального закона от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации», информация, составляющая коммерческую, служебную или иную охраняемую законом тайну и полученная должностными лицами контрольного (надзорного) органа при осуществлении государственного контроля (надзора), муниципального контроля, не подлежит разглашению, за исключением случаев, установленных федеральными законами. За разглашение информации, составляющей коммерческую, служебную или иную охраняемую законом тайну, должностные лица контрольного (надзорного) органа несут ответственность, предусмотренную федеральными законами. Вред (ущерб), причиненный контролируемому или иному лицу в результате разглашения должностными лицами контрольного (надзорного) органа информации, составляющей коммерческую, служебную или иную охраняемую законом тайну, подлежит возмещению[1]. Статья 13.11 Кодекса об административных правонарушениях РФ предусматривает ответственность за нарушения законодательства РФ в области персональных данных; статья 137 Уголовного кодекса РФ — за нарушение неприкосновенности частной жизни. Либо имеет место ситуация, когда человек специально фотографируется или снимается на видео с целью последующего опубликования этого изображения без его согласия в сети Интернет. В данном случае будет иметь место нарушение ст. 152.1 Гражданского кодекса РФ — обнародование и использование изображения гражданина допускается только с согласия этого гражданина, либо, если его нет в живых, с согласия детей и пережившего супруга, а при их отсутствии — с согласия родителей[2]. В данных случаях речь, конечно же, идет об умышленном нарушении действующего законодательства.

Стоит сказать о тех ситуациях, в которых лицо, не имея на то никакого умысла, преследуя абсолютно другие цели — например, поделиться эмоциями от поездки, выставив свои фото в социальных сетях, может стать источником распространения в сети Интернет различной информации, касающейся третьих лиц. В том числе той, которой третьи лица, случайно оказавшиеся на фото, видео, делиться не хотели. Так, например, в сети Интернет размещены истории путешественников, на фото которых — только природа и архитектура[3]. В этом случае, думается, авторы озаботились морально-этическим аспектом своих действий, так как, действительно, далеко не все люди желают публичности. На других сайтах — новостных, блогеров (например, путешественников), — помимо объекта интереса в кадр могут попасть люди, которые в этом не заинтересованы, а иногда и категорически против. Просто автор фото не уведомил их о своих намерениях, относясь к этому легкомысленно. Но именно цели разгласить какие-либо персональные данные, порочащие других людей сведения, другую информацию о них, не желал[4]. Закономерен вопрос, а много ли информации можно получить по таким данным из открытых источников, пользуясь легальными программами поиска в сети Интернет. Отметим, что таких программ — великое множество и технический прогресс не стоит на месте. Поэтому отметим только некоторые из них.

[1] О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации : Федеральный закон от 31.07.2020 № 248-ФЗ // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=0&nd=102801479&intelsearch=&firstDoc=1 (дата обращения: 29.09.2023).

[2] Гражданский кодекс РФ. Часть 1 : от 30.11.1994 № 51-ФЗ // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=0&nd=102033239&intelsearch=&firstDoc=1 (дата обращения: 29.09.2023).

[3] См., например, Автопробег из Санкт-Петербурга на запад и обратно. Ч. I Псков // ОТЗЫВ.RU. URL: https://otzyv.ru/review/223277/ (дата обращения: 29.09.2023) и др. Таких, кстати, не мало.

[4] См., например: Стоит ли ехать в Абхазию. Отзывы туристов о жилье, еде, пляжах и экскурсиях с фото // Дзен. URL: https://dzen.ru/a/ZIHHW88nY3oNOaiA/ (дата обращения: 29.09.2023). На данной странице представлены фотографии пляжа в Новой Гагре, на которых также изображены отдыхающие, одетые соответственно. Думается, не все из них захотели бы оказаться на этом фото.

Наиболее простой и доступной представляется поисковая строка в Google, Yandex, в которой по изображению человека или местности можно их найти.

При помощи поисковой системы «Search-4faces» можно осуществить поиск лица по фотографиям в социальных сетях[1].

При помощи онлайн-просмотрщика данных EXIF с поддержкой GPS «Pic2Map» осуществляется поиск геолокации по фото[2]. Затем при помощи калькулятора положения солнца «SunCalc»[3] можно установить время съемки (для этого должны быть известны место и дата съемки).

Анализ полученных данных позволяет получить достаточно большой информации о лице, изображение которого могло случайно оказаться на чужом фото.

Доступный поиск позволяет найти не только изображение. Так, для поиска различной информации (документов, сайтов) используется поисковая система «Мамонт»[4].

Сервис Whois[5] позволяет установить домен, IP-адрес, их широту и долготу и другие данные, касающиеся объекта поиска.

К комплексному методу сбора информации относится OSINT (*open source intelligence*) — разведывательная дисциплина и комплекс мероприятий, инструментов и методов для получения и анализа информации из открытых источников. Он применяется в отношении конкретных людей, организаций, а также событий, явлений и целей[6]. Данный инструментарий предлагает методы сбора информации при помощи различных программ и сайтов из новостных материалов, публикаций, постов и комментариев в социальных сетях, данных с камер видеонаблюдения — то есть, только из открытых источников. Инструменты OSINT позволят раскрыть такие данные как IP-адрес, email, домены, обнаружить подключённые устройства и сети, выявить уязвимости и потенциальные угрозы безопасности, проанализировать данные социальных сетей и многое другое.

К поисковым системам также можно отнести различные боты в мессенджерах, например, в Telegram — poisk_5bot.

Сеть Интернет может быть использована не только в целях нарушения прав конкретного человека, но и обезличенной группы людей, например, при использовании кибертехнологий террористическими группами в целях воздействия на объекты жизненно-важной инфраструктуры, обеспечения финансирования преступной деятельности [10].

Заключение

Таким образом, на сегодня сеть Интернет — это огромный массив информации, в том числе той, которые отдельные лица делиться не желали. Какого-либо реально работающего инструментария, доступного любому лицу, по удалению его данных из сети Интернет на сегодня не имеется. В ряде случаев, можно обратиться к специалистам, при помощи которых можно удалить из сети Интернет определенного рода информацию. Но для этого, безусловно, требуются определенные специальные знания.

Думается, требуется достаточно четкая и ясная регламентация действий по размещению информации в сети Интернет, касающейся третьих лиц. Данная норма не должна быть декларативна — требуется предусмотреть ответственность за ее нарушение. Введенная норма потребует создание методики по ее применению. В целом, такие действия на законодательном уровне также будут способствовать обеспечению кибербезопасности нашего государства в целом и отдельного человека — в частности.

Вышеизложенное позволило прийти к следующим выводам:

1. Интеграция различных сфер жизнедеятельности общества в цифровое пространство неизбежна. Она будет только нарастать.

2. Вопрос защиты информации всегда стоял остро. Сейчас уместно и своевременно говорить о защите информации, находящейся в цифровом формате на электронных носителях.

3. Вопрос защиты информации, в том числе, находящейся в цифровом формате на электронных носителях, возможен только на уровне государства, в том числе,путем принятия достаточной нормативной правовой базы.

4. Нормативные акты, регламентирующие вопросы обеспечения кибербезопасности, автором разделены на две группы: нормативные правовые акты, определяющие виды информации, подлежащей государственной защите; нормативные правовые акты,

[1] URL: https://search4faces.com (дата обращения: 29.09.2023).

[2] URL: https://www.pic2map.com/ (дата обращения: 29.09.2023).

[3] URL: https://www.suncalc.org/#/40.1789,-3.5156,3/2023.09.24/18:50/1/3 (дата обращения: 29.09.2023).

[4] URL: https://www.mmnt.ru/help?open=1156240947_0 (дата обращения: 29.09.2023).

[5] URL: https://www.reg.ru/whois/ (дата обращения: 29.09.2023).

[6] URL: https://blog.skillfactory.ru/glossary/osint/ (дата обращения: 29.09.2023).

регламентирующие основные термины, определения, порядок и механизм обеспечения безопасности информации, в том числе, содержащейся на электронных носителях информации.

5. На сегодня нет достаточной нормативной правой базы, позволяющей в полном объеме соблюсти законные права и свободы человека в интернет-пространстве. В связи с этим назрела необходимость в создании норм права с предусмотренной за их нарушение ответственностью, позволяющих оградить конкретного человека от несогласованного распространения о нем информации в сети Интернет. Гарантии отдельно взятого человека будут являться основой кибербезопасности и всего государства.

Список источников

1. Метелев И. С., Устинов А. Ю. Информационная безопасность // Сибирский торгово-экономический журнала. 2016. № 4 (25). С. 76–79. EDN: WMGNKV.

2. Турдумамбетова Б. Н. Субанбекова С. С. Информационная безопасность // Международный журнал гуманитарных и естественных наук. 2018. № 6-1. С. 190–195. EDN: UUDNLT.

3. Кряжевских К. А. Влияние информационной культуры на уровень информационной безопасности // Вопросы российской юстиции. 2023. № 24. С. 568–573.

4. Хисамова З. И., Бегишев И. Р. Цифровая преступность в условиях пандемии: основные тренды // Всероссийский криминологический журнал. 2022. Т. 16, № 2. С. 185–198. DOI: 10.17150/2500-4255.2022.16(2).185-198

5. Королькова Е. Залог цифровой гигиены // Полиция России. 2021. № 5. С. 9.

6. Ипатов В. Д. Современные информационные вызовы, проблемы и перспективы // Состояние и основные направления развития информационной безопасности Союзного государства в условиях современных вызовов и угроз : материалы постоянно действующего семинара при Парламентском Собрании Союза Беларуси и России (Минск, 27–28 апреля 2022 г.) / под ред. С. Г. Стрельченко. Минск : Секретариат Парламентского Собрания Союза Беларуси и России, 2022. С. 30–34.

7. Чернова Э. Р. Правовое обеспечение информационной безопасности в Российской Федерации // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2021. № 21-2. С. 197–198. EDN: FAWMES.

8. Информационные технологии в юридической деятельности : учебник / С. Я. Казанцев, Н. Р. Шевко. Москва : ЮСТИЦИЯ, 2020. 318 с.

9. Степанов О. А. Противодействие кибертерроризму в цифровую эпоху : монография. Москва : Юрайт, 2022. 103 с.

10. Дубень А. К. Информационная безопасность в системе национальной безопасности: актуальные проблемы информационного права // Вопросы безопасности. 2023. № 1. С. 51–57. DOI: 10.25136/2409-7543.2023.1.40078 EDN: AOZZYF.

11. Пучков Д. В. Кибертерроризм как новая угроза // Виктимология. 2021. Т. 8, № 4. С. 382–391. EDN: PZEHVT.

12. Бегишев И. Р. Культура информационной безопасности: психолого-правовой аспект // Психология и право. 2021. Т. 11, № 4. С. 207–220. DOI: 10.17759/psylaw.2021110415

КОНФЛИКТ ИНТЕРЕСОВ
Конфликт интересов отсутствует

CONFLICT OF INTEREST
There is no conflict of interest

Дата поступления статьи / Received: 07.10.2023.
Дата рецензирования статьи / Revised: 15.11.2023.
Дата принятия статьи к публикации / Accepted: 05.12.2023.