КРИМИНОЛОГИЯ

УДК 343.3/.7 DOI: 10.17223/23088451/17/21

А.Ю. Олимпиев, И.А. Стрельникова

КИБЕРБЕЗОПАСНОСТЬ И ЕЕ ОБЕСПЕЧЕНИЕ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Исследуются проблемные вопросы обеспечения кибербезопасности в РФ. На основе анализа юридической литературы и нормативных правовых актов о преступлениях в сфере компьютерной информации высказано несколько суждений: состояние преступности в сфере компьютерной информации определяется уровнем экономического развития; компьютерная информация как общественное отношение охраняется уголовным законодательством РФ; противодействие в сфере компьютерной информации предполагает формирование специальных подразделений в ряде правоохранительных органов.

Ключевые слова: *уголовное законодательство, Уголовный кодекс Российской Федерации, состав преступления, преступление, общественное отношение, компьютерная информация, безопасность, кибербезопасность*

Введение

Предметом данной статьи является безопасность в сфере информационных технологий (кибербезопасность). Актуальность исследования определяется широким распространением данной разновидности преступности в развитых государствах, в том числе и в Российской Федерации. Законодательные органы правовых государств вынуждены реагировать на формирующие общественные отношения, в том числе посредством новых форм уголовно-правовой охраны вновь формирующихся общественных отношений.

Сейчас в Российской Федерации стремительно развиваются информационные технологии и интернет, что стало одним из ключевых факторов, определяющих эти перемены [1. С. 287].

Успешное экономическое и социальное развитие Российской Федерации во многом зависит от эффективности государственного управления.

В настоящее время на территории нашей страны успешно реализуется специальная программа, которая получила название «Цифровая экономика Российской Федерации» (Распоряжение Правительства РФ № 1632-р от 28 июля 2017 г.). Она должна сделать экономику, государственное управление, социальную сферу эффективными и конкурентоспособными и являться основным вектором развития всех сфер социальной жизни.

Независимо от совершаемых действий (снятие наличных денежных средств, использование электронной почты и системы электронного документооборота), уязвимость Российской Федерации в информационном пространстве очевидна. Поэтому информационная безопасность, в особенности в управленческом процессе (в частности в системе МВД РФ), несомненно, актуальна. С возникновением новых киберугроз, появляются ранее не известные процессы, которые от руководителей любого уровня требуют новых компетенций.

Необходимо учитывать, что количество угроз в информационном пространстве Российской Федерации и в мире в целом продолжает расти, нанося национальным экономикам значительный ущерб. В этой связи необходимо обратиться к существующей статистике: так, например, потери мировой экономики за 2016 г. от деятельности киберпреступников, согласно представленным данным World Economic Forum, составляют 445 млрд долл.; в Российской Федерации потери 2017 г. в экономике – около 600 млрд руб. (мнение аналитиков); потери за 2018 г. составляют около 1 трлн руб. Аналитики Всемирного экономического форума считают, что потери мировой экономики составляют в год около триллиона долларов. В Российской Федерации не уделяется должного внимания данной области обеспечения национальной безопасности [2. С. 47].

Актуальным проблемам трансформации в государственных органах и экономике уделено внимание и в послании Президента РФ В.В. Путина; так, он указывал на тот факт, что само по себе эффективное развитие государства в цифровой среде может основываться исключительно на принципах цифровой свободы. Президент подчеркнул, что любые барьеры должны быть устранены, а прогресс нельзя сдерживать. Вместе с тем следует обращать внимание и на существующие и потенциальные риски, вызовы и угрозы, возникающие в цифровой среде, а каждый пользователь должен осознавать свою ответственность. Об этом заявил Президент РФ на Международном конгрессе по киберпреступности в июле 2018 г. [3].

Справочная информация и методология

Первоначально о состоянии теории.

Так, например, В. Буряк закономерно утверждает, что при минимизации межгосударственных конфликтов наиболее действенной мерой становится оптимизация кибербезопасности [4. С. 119].

К схожим идеям пришли и другие авторитетные исследователи, такие как А.А. Корниенко, А.П. Глухов и С.В. Диасамидзе. В своих трудах авторы не только определили требуемое содержание правовой базы в сфере кибербезопасности, но и установили, что в

нашем государстве кибербезопасность напрямую связана с осуществлением надлежащей безопасности автоматизированных систем по управлению технологическими процессами, а также производственными базами на важнейших объектах инфраструктуры Российской Федерации [5. С. 2].

Продолжая исследование, следует также обратиться и к трудам А.А. Евдокимова; так, автор подробно исследовал закономерности, которые напрямую связаны с процессами стандартизации и регулирования информационной безопасности на территории Российской Федерации. На основе проведенного анализа ученый указал, что информационная безопасность в нашей стране и за рубежом развивается весьма динамично, однако в большей своей части непредсказуемо, если говорить о России; в европейских государствах подобные процессы происходят более стабильно, так как все происходящие процессы продиктованы потребностями предпринимателей, а также лояльностью граждан государств, что позволяет полноценно прогнозировать развитие данной отрасли. Проблема же нашего государства связана в первую очередь с тем, что в рамках прошедшего десятилетия были представлены и приняты пакеты разнообразных правовых актов, которые были направлены на защиту информации, чаще всего разнящиеся в деталях. В том числе существенную роль сыграли и принимаемые регуляторы, которые контролируют исполнение подобных правовых актов [6. С. 37].

В.Н. Лопатин, подготовивший статью на основе доклада в рамках VI Международной научно-практической конференции «Информационные технологии и право (Правовая информатизация – 2018)» (Республика Беларусь, г. Минск, 17 мая 2018 г.), высказал обобщающее суждение о том, что, если исходить из закономерности информационного развития, можно прийти к выводу, что повышение уровня организованности социальных систем напрямую влияет на возрастание роли саморегулирования, поэтому в государствах ЕАЭС и БРИКС, чтобы обеспечить единообразие в подходах при сближении национальных правовых систем, выделяют три подобных уровня: высокий уровень саморегулирования, к которому относятся, например, профессиональные кодексы поведения; средний уровень саморегулирования, где преобладают стандарты регулирования в виде мягкой силы и возможности использования потенциалов национального, а также межгосударственного технического комитета по стандартизации, получившего название «Интеллектуальная собственность»; низкий уровень саморегулирования, в рамках которого преобладает регулирование нормативной и правовой базы [7. С. 16].

Е.Г. Багоян в своих трудах анализировал особенности законодательного регулирования информационной безопасности через призму блокчейн-технологий; он затрагивал не только финансовую сферу воздействия, но и сферу защиты авторских прав, а также заключения смарт-контрактов. В частности, он утверждал, что на технологию блокчейн действует правовой режим информационных систем. Кроме этого, структура платформы подразумевает, что изменения состояния записываются в блокчейн. Все узлы, которые в сети, должны поддерживать копию блокчейна и при этом ограничивать общий размер блокчейнов техническими возможностями оборудования. Скорость обработки транзакций ограничивается протоколом распространения записи и выбора лидера блокчейна и привязана к скорости, с которой новые блоки объявляются ведущими узлами. Новые транзакции могут занять по времени от нескольких минут до нескольких часов. На блок общее количество транзакций ограничивается размером этого блока любого блокчейна. Чтобы дать возможность всем узлам стать лидером в следующем раунде, они должны получить новый объявленный блок примерно в одно и то же время. В связи с этим размер блока обычно ограничен пропускной способностью восходящего канала узлов. От способности любого человека, который может выполнить аудит исходного блока, зависит целостность блокчейна [8. С. 43].

Р.Р. Мазитов отмечает, что информационная безопасность в России, а также существующие проблемы по ее обеспечению в некоторой мере отражаются не только в рамках теоретических исследований российских и иностранных авторов, но и в официальных актах. В качестве примера он приводит такие понятия, как национальная и информационная безопасность, информационная организация государства и многие другие, которые по своей сути являются основами разнообразных программ, доктрин и концепций не только государства, но и большей части политических и общественных организаций. Ключом же автор считает тот факт, что они начали привлекать существенное внимание СМИ. Вместе с тем в процессе развития научного и технического прогресса возрастает и общая роль информационной безопасности не только личности, но и общества, а также государства. Все чаще можно наблюдать ситуации, когда информация приводит к крупным авариям, конфликтам, в том числе и военным, а также способствует дезорганизации органов государственного управления. Влияние информации отчетливо прослеживается и в сфере финансовой системы, а также в научной среде. Основываясь на этих факторах, следует заключить, что с повышением уровня цифровизации общества возрастают опасности, а значит, и информационная безопасность должна становиться более надежной [9. С. 6].

К.М. Керценбаум рассмотрел процесс нарастания сложностей обеспечения информационной безопасности, в связи с развитием и сменой интересов киберпреступников [10. С. 32].

А.В. Тонконоговым была разработана дефиниция понятия «кибернетическая безопасность». В своей работе он не только определил структурные угрозы рассматриваемому институту, но и выявил ключевые направления развития отечественной государственной политики в сфере обеспечения информационной безопасности. Автор также отмечал, что реализация кибербезопасности не может обеспечиваться исключительно минимизацией несанкционированного доступа, в некоторых случаях подобный доступ следует полностью исключить. Должна отсутствовать сама возмож-

ность несанкционированного доступа к информационным ресурсам, а препятствование нормальной деятельности информационных механизмов государственного и общественного управления сведено к незначительному минимуму. Основываясь на данных обстоятельствах, под кибернетической безопасностью следует понимать особое состояние защищенности информационных механизмов управления общества и государства, а также устойчивость подобных механизмов к деятельности деструктивных факторов не только внешнего, но и внутреннего проявления. В данной связи кибернетическая безопасность представляется в качестве разновидности национальной безопасности как состояния защищенности не только от внешних, но и от внутренних угроз в условиях повсеместной цифровизации общества и наличия кибернетического пространства. Развитие же подобного пространства возможно только при условии полного и объемного научного осмысления, а также надлежащего уровня правового закрепления, в том числе создания особых структур, которые и занимались бы обеспечением национальной безопасности Российской Федерации [11. С. 40].

А.А. Чеботарева исследовала подходы ученых разных специальностей к определению сущности понятия «информационная безопасность». Проблемы информационной безопасности возможно решить только за счет скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер [12. С. 3].

А.А. Паненков приводит ряд аргументов в пользу того, что кибертерроризм представляет реальную угрозу национальной безопасности Российской Федерации. В том числе автор отмечает, что увеличивающаяся степень общественной опасности обязывает проводить мероприятия по оптимизации и совершенствованию законодательства в целях реализации должного уровня противодействия угрозам настоящего и будущего в области информационной безопасности [13. С. 12].

В.В. Гришина полагает что безопасность – это продукт власти, обладающий качествами, которые возможно измерить, а также которыми возможно управлять. Как видится, по мнению исследователя, самым точным и надлежащим способом измерения уровня информационной безопасности выступает строго расписанная деятельность в информационной среде, которая имеет публично-правовой характер. К подобной деятельности следует относить, например, документирование и функционирование информационных ресурсов. Ключевыми же свойствами безопасности следует считать такие, как техническая, предметная и правовая совместимость информационных ресурсов, полнота, а также достоверность и актуальность ресурсной информации и защищенность информации [14. С. 12].

По мнению Т.А. Бражник, существующие подходы к толкованию понятия «информационная безопасность» являются не очень корректными и не отвечают основополагающим положениям информационного права. Так, например, само по себе приравнивание информационной безопасности к деятельности по реализации мер защиты информации и укреплению суверенитета в информационной среде, а также обеспечению надлежащей деятельности информационных и телекоммуникационных систем в корне неверно и как итог создает условия, при которых развитие всех элементов информационной безопасности невозможно. Следует учитывать, что требуется создание специальной терминологии в области обеспечения информационной безопасности, создание подобной совокупности терминов позволит проводить надлежащее разграничение безопасности личности от информационной безопасности, а также разграничит такие термины, как информационная безопасность и кибербезопасность [15. С. 17].

Обсуждение и результаты

Противоречивые суждения ученых и практиков во многом предопределяют и несовершенство законодательства Российской Федерации о безопасности в сфере информационных технологий в Российской Федерации [16. С. 120].

В первую очередь обращаем внимание на нормативный правовой акт с наивысшей юридической силой – Конституцию РФ от 12 декабря 1993 г. В этом нормативном правовом акте актуальны следующие положения. В первую очередь, это закрепление фактических обстоятельств, которые указывают, что сбор, хранение, а также распространение и использование информации о частной жизни лица возможно исключительно при наличии согласия такого лица. Во-вторых, отмечается, что органы как государственной власти, так и местного самоуправления, а также должностные лица наделяются обязанностью по обеспечению возможности ознакомления с документацией и материалами, которые фактически затрагивают права и свободы граждан.

Положения Конституции РФ, как правило, учитываются и в нормативных правовых актах с меньшей юридической силой.

Первоначально необходимо обратиться к Федеральному закону РФ «О безопасности» от 7 декабря 2010 г. [17]. Так, в рамках данного правового акта указывается, что его действие направлено на определение главенствующих принципов и раскрытие содержания деятельности по реализации безопасности государства. В том числе данный закон направлен на обеспечение общественной, экологической безопасности и безопасности личности, а также иных видов безопасности. Также регулируются полномочия и функции органов государственной власти на федеральном уровне в области обеспечения безопасности. Данное правило относится и к органам местного самоуправления, а также органам государственной власти субъектов нашей страны. В качестве же особого органа выделяется Совет Безопасности Российской Федерации, закрепляются его полномочия и функции.

В ФЗ РФ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. [18] фактически детализированы положения Федерального закона РФ от 7 декабря 2010 г.

В статье 2 Федерального закона РФ от 12 июля 2017 г. определены основные понятия, которые используются в данной сфере. Так, под автоматизированной системой управления понимается комплекс не только программных, но и программно-аппаратных средств, которые предназначены для контроля технологического и производственного оборудования, а также производных от этих средств процессов, в том числе и управления указанными процессами и оборудованием. Безопасность критической информационной инфраструктуры представляется как особое состояние защищенности подобной инфраструктуры, которое направлено на обеспечение ее устойчивого функционирования в условиях проведения компьютерных и информационных атак. В качестве значимого объекта критической информационной инфраструктуры представляется такой объект, который обладает каким-либо критерием значимости и который, соответственно, включен в реестр подобных объектов. Под компьютерной атакой следует понимать целенаправленное воздействие каких-либо программных или аппаратных приспособлений, воздействующих на объекты критической информационной инфраструктуры, а также сети электросвязи. Целью таких атак выступает нарушение или полное прекращение функционирования указанных объектов, также к целям относится создание угрозы безопасности информации, расположенной или обрабатываемой такими объектами. Компьютерный инцидент представляется как факт нарушения или полного прекращения функционирования объекта критической информационной инфраструктуры, а также сетей электросвязи; сюда же относятся и факты нарушения безопасности обрабатываемой информации, основой указанного инцидента выступает компьютерная атака. Под критической информационной инфраструктурой следует понимать такие объекты и сети электросвязи, которые представляют собой структурные элементы данной инфраструктуры. В качестве объектов критической информационной инфраструктуры представляются информационные системы, информационные и телекоммуникационные сети, а также автоматизированные системы управления, используемые субъектами критической информационной инфраструктуры. В данном ключе к таким субъектам следует относить государственные органы, учреждения, а также российские юридические лица и индивидуальных предпринимателей, которым по различным основаниям принадлежат информационные системы и информационно-телекоммуникационные сети, а также автоматизированные системы управления. Причем данные субъекты должны действовать в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере, а также в сферах финансового рынка, топливного и энергетического комплекса. Справедливым будет отнести сюда и представителей атомной энергетики, оборонной, ракетной, космической, добывающей, металлургической и химической промышленности. Также к субъектам будут относиться отечественные юридические лица и индивидуальные предприниматели, обеспечивающие взаимодействие указанных ранее систем и сетей.

В подзаконном нормативном правовом акте утверждена Доктрина информационной безопасности Российской Федерации, что регламентировано Указом Президента РФ № 646 от 5 декабря 2016 г. [19]. Указанная Доктрина представляется как особая система взглядов официальных представителей государства на вопрос обеспечения национальной безопасности России в области информационного развития. В рамках описываемой доктрины также содержится определение информационной сферы, под которой понимается общая совокупность информации, а также объектов информатизации, информационных систем, сайтов интернета, сетей связи, информационных технологий. В том числе сюда относятся и субъекты, функционирование которых связано с формированием и последующей обработкой информации, а также реализацией указанных технологий.

Заключение

Таким образом, научно-технический прогресс имеет для человечества не только позитивную сторону, но и негативную, что должно побуждать ученых к продолжению научных исследований и позволяет высказать несколько суждений.

Во-первых, состояние преступности в сфере компьютерной информации во многом определяется уровнем экономического развития любого государства, в том числе Российской Федерации как субъекта международного права.

Во-вторых, компьютерная информация как общественное отношение охраняется уголовным законодательством Российской Федерации.

В-третьих, противодействие в сфере компьютерной информации предполагает формирование специальных подразделений в ряде правоохранительных органов (в первую очередь, в органах государственной безопасности и органах внутренних дел), укомплектованных сотрудниками, обладающими дополнительными компетенциями в сфере компьютерных технологий.

ЛИТЕРАТУРА

1. *Олимпиев А.Ю., Мышко Ф.Г., Стрельникова И.А.* Цифровизация экономики в Российской Федерации: состояние и перспективы развития // Шаг в будущее: искусственный интеллект и цифровая экономика. Революция в управлении: новая цифровая экономика или новый мир машин : материалы II Междунар. науч. форума / под ред. П.В. Терелянского. М., 2018. С. 287–293.
2. *Олимпиев А.Ю., Михайленко Н.В.* Актуальные тренды реорганизации органов внутренних дел в условиях цифровой экономики // Вестник экономической безопасности. 2019. № 4. С. 46–47.
3. *Выступление* Президента России В.В. Путина на международном конгрессе по кибербезопасности (ICC), Москва, 06.07.2018 г. // Стенограмма выступления опубликована на официальном сетевом ресурсе Президента Российской Федерации. URL: http://www.kremlin.ru/events/president/news/57957 (дата обращения: 12.01.2021).
4. *Буряк В.В.* Цифровая экономика, хактивизм и кибербезопасность. Симферополь : ИП Зуева Т.В., 2019. 140 с.

5. *Корниенко А.А., Глухов А.П., Диасамидзе С.В.* Кибербезопасность и защита от компьютерных атак на железнодорожном транспорте : учеб. пособие. СПб., 2015. 49 с.
6. *Евдокимов А.А.* Информационная безопасность в России: особенности или уникальность? // Право и кибербезопасность. 2013. № 1. С. 36–38.
7. *Лопатин В.Н.* Информационная безопасность в электронном государстве // Информационное право. 2018. № 2. С. 14–19.
8. *Багоян Е.Г.* Информационная безопасность и применение технологии блокчейн: зарубежный опыт и необходимость правового регулирования в Российской Федерации // Юрист. 2019. № 3. С. 42–49.
9. *Мазитов Р.Р.* Информационная безопасность Российской Федерации на современном этапе // Российская юстиция. 2009. № 11. С. 4–7.
10. *Керценбаум К.М.* Информационная безопасность, или Просто о сложном // Право и кибербезопасность. 2012. № 1. С. 30–32.
11. *Тонконогов А.В.* Кибернетическая безопасность: понятие и сущность феномена // Право и кибербезопасность. 2013. № 2. С. 36–43.
12. *Чеботарева А.А.* Научные подходы к определению понятия «информационная безопасность» // Информационное право. 2011. № 1. С. 3–5.
13. *Паненков А.А.* Кибертерроризм как реальная угроза национальной безопасности России // Право и кибербезопасность. 2014. № 1. С. 12–19.
14. *Гришина В.В.* Правовое обеспечение информационной безопасности // Административное и муниципальное право. 2008. № 5. С. 10–14.
15. *Бражник Т.А.* Правовые вопросы обеспечения информационной безопасности личности // Информационное право. 2018. № 4. С. 17–21.
16. *Галузо В.Н.* Конституционно-правовой статус России: проблема именования государства // Вестник Московского университета МВД России. 2010. № 5. С. 119–123.
17. *Федеральный* закон РФ «О безопасности» от 7 декабря 2010 г. // СЗ РФ. 2011. № 1. Ст. 2.
18. *Федеральный* закон РФ «О безопасности критической информационной инфраструктуры Российской Федерации» от 12 июля 2017 г. // СЗ РФ. 2017. № 31 (ч. I). Ст. 4736.
19. *Указ* Президента РФ № 646 от 5 декабря 2016 г. // СЗ РФ. 2016. № 50. Ст. 7074.

Статья принята к публикации 24.05.2021.

Cybersecurity and Its Maintenance in the Russian Federation

Ugolovnaya yustitsiya – Russian Journal of Criminal Law, 2021, no. 17, pp. 104–109. DOI: 10.17223/23088451/17/21

Anatoly Yu. Olimpiev, Institute of Social Sciences (Moscow, Russian Federation). E-mail: a.olimpiev@yandex.ru
Irina A. Strelnikova, Higher School of Economics (Moscow, Russian Federation). E-mail: irina.a.strelnikova@mail.ru

Keywords: criminal legislation, Criminal Code of Russian Federation, corpus delicti, crime, social interaction, computer information, security, “cybersecurity”

The problematic issues of ensuring cybersecurity in the Russian Federation are investigated in the article. Based on the analysis of legal literature and normative legal acts on crimes in the field of computer information in the criminal legislation of the Russian Federation and countering them, several judgments are made. The state of crime in the field of computer information is largely determined by the level of economic development of any state, including the Russian Federation as a subject of international law. Computer information, as social interaction, is protected by the criminal legislation of the Russian Federation. Counteraction in the field of computer information involves the formation of special units in a number of law enforcement agencies (first of all, in the state security bodies and in the internal affairs bodies) staffed with employees with additional competencies in the field of computer technology.

References

1. Olimpiev, A.Yu., Myshko, F.G. & Strel’nikova, I.A. (2018) [Digitalization of the economy in the Russian Federation: State and development prospects]. *Shag v budushchee: iskusstvennyy intellekt i tsifrovaya ekonomika. Revolyutsiya v upravlenii: novaya tsifrovaya ekonomika ili novyy mir mashin* [Step into the future: Artificial intelligence and digital economy. A revolution in management: A new digital economy or a new world of machines]. Proceedings of the II International Scientific Forum. Moscow: State University of Management. pp. 287–293. (In Russian).
2. Olimpiev, A.Yu. & Mikhaylenko, N.V. (2019) The current trends in the reorganization of the internal affairs bodies in the digital economy. *Vestnik ekonomicheskoy bezopasnosti.* 4. pp. 46–47. (In Russian).
3. Kremlin.ru. (2018) *Speech by the President of Russia, V.V. Putin, at the International Cybersecurity Congress (ICC), Moscow, July 06, 2018.* [Online] Available from: http://www.kremlin.ru/events/president/news/57957 (Accessed: 12th January 2021). (In Russian).
4. Buryak, V.V. (2019) *Tsifrovaya ekonomika, khaktivizm i kiberbezopasnost’* [Digital Economy, Hacktivism and Cybersecurity]. Simferopol: IP Zueva T.V.
5. Kornienko, A.A., Glukhov, A.P. & Diasamidze, S.V. (2015) *Kiberbezopasnost’ i zashchita ot komp’yuternykh atak na zheleznodorozhnom transporte* [Cybersecurity and protection against computer attacks on railway transport]. St. Petersburg: St. Petersburg State Transport University.
6. Evdokimov, A.A. (2013) Informatsionnaya bezopasnost’ v Rossii: osobennosti ili unikal’nost’? [Information security in Russia: features or uniqueness?]. *Pravo i kiberbezopasnost’.* 1. pp. 36–38.
7. Lopatin, V.N. (2018) Information security in an electronic state. *Informatsionnoe pravo – Informational Law.* 2. pp. 14–19. (In Russian).

8. Bagoyan, E.G. (2019) Information security and application of blockchain technologies: Foreign experience and the need for legal regulation in the Russian Federation. *Yurist – Jurist.* 3. pp. 42–49. (In Russian). DOI: 10.18572/1812-3929-2019-3-42-49
9. Mazitov, R.R. (2009) Informatsionnaya bezopasnost' Rossiyskoy Federatsii na sovremennom etape [Information security of the Russian Federation at the present stage]. *Rossiyskaya yustitsiya – Russian Justitia.* 11. pp. 4–7.
10. Kertsenbaum, K.M. (2012) Informatsionnaya bezopasnost', ili Prosto o slozhnom [Information Security, or On the complex in simple words]. *Pravo i kiberbezopasnost'.* 1. pp. 30–32.
11. Tonkonogov, A.V. (2013) Kiberneticheskaya bezopasnost': ponyatie i sushchnost' fenomena [Cybersecurity: concept and essence of the phenomenon]. *Pravo i kiberbezopasnost'.* 2. pp. 36–43.
12. Chebotareva, A.A. (2011) Nauchnye podkhody k opredeleniyu ponyatiya "informatsionnaya bezopasnost' " [Scientific approaches to defining "information security"]. *Informatsionnoe pravo – Informational Law.* 1. pp. 3–5.
13. Panenkov, A.A. (2014) Cyber terrorism as a real menace to the national security of Russia. *Pravo i kiberbezopasnost'.* 1. pp. 12–19. (In Russian).
14. Grishina, V.V. (2008) Pravovoe obespechenie informatsionnoy bezopasnosti [Legal issues of ensuring information security of the individual]. *Administrativnoe i munitsipal'noe pravo – Administrative and Municipal Law.* 5. pp. 10–14.
15. Brazhnik, T.A. (2018) Legal Issues of Ensuring Information Security of an Individual. *Informatsionnoe pravo – Informational Law.* 4. pp. 17–21. (In Russian).
16. Galuzo, V.N. (2010) Konstitutsionno-pravovoy status Rossii: problema imenovaniya gosudarstva [Constitutional and legal status of Russia: the problem of naming the state]. *Vestnik Moskovskogo universiteta MVD Rossii.* 5. pp. 119–123.
17. Russian Federation. (2011) Federal'nyy zakon RF "O bezopasnosti" ot 7 dekabrya 2010 g. [Federal Law of the Russian Federation "On Security" of December 7, 2010]. *Sobranie zakonodatel'stva RF.* 1. Art. 2.
18. Russian Federation. (2017) Federal'nyy zakon RF "O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii" ot 12 iyulya 2017 g. [Federal Law of the Russian Federation "On the Security of the Critical Information Infrastructure of the Russian Federation" of July 12, 2017]. *Sobranie zakonodatel'stva RF.* 31 (I). Art. 4736.
19. Russian Federation. (2016) Ukaz Prezidenta RF № 646 ot 5 dekabrya 2016 g. [Decree of the President of the Russian Federation No. 646 of December 5, 2016]. *Sobranie zakonodatel'stva RF.* 50. Art. 7074.

Received: 24 May 2021.