УДК 343.34
ББК 67.401.114

ПРАВОВЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В. Ю. Голубовский
Всероссийский научно-исследовательский институт Министерства внутренних дел России (Москва, Россия)

За последнее десятилетие произошли громадные изменения в социальной и геополитической сферах, равно как и революционные изменения в технологиях, особенно в электронике и кибернетике, которые ознаменовали информационную революцию и резко вторглись в общественно-политические, социальные и иные сферы общественных отношений в мире в рамках отдельных стран и регионов, затронули сферы военного дела, военного искусства и стратегии. Установлено, что развитие информационных технологий и области их применения, разработка специфических целей и задач их использования и методов достижения этих целей в различных сферах, и особенно в области деятельности организованной преступности, создали потенциальную основу вызова и угрозы общественной и национальной безопасности.

Таким образом, возникшие нынешние опасения относительно потенциала информационных средств усилились благодаря распространению в мире технологий информационных средств и системы, в особенности благодаря соединению компьютерной техники с телекоммуникационной, что существенно углубило и расширило пространство и возможности информационной деятельности и позволило резко усовершенствовать информационные инфраструктуры, это и предопределило рассмотрение правовых аспектов защиты информационной безопасности.

Ключевые слова: защита, интернет, информационная безопасность, компьютерные преступления, правовое регулирование, преступление, расследование, цифровой суверенитет

LEGAL PROBLEMS OF INFORMATION SECURITY PROTECTION

V. Yu. Golubovsky
All-Russian Research Institute of the Ministry of Internal Affairs of Russia (Moscow, Russia)

Over the past decade, there have been enormous changes in the social and geopolitical spheres, as well as revolutionary changes in technology, especially in electronics and cybernetics, which marked the information revolution and sharply invaded the socio-political, social and other spheres of public relations in the world within individual countries and regions, affected the spheres of military affairs, military art and strategy. It has been established that the development of information technologies and the area of their application, the development of specific goals and objectives of their use and methods for achieving these goals in various areas and, especially in the area of organized crime, have created a potential basis for challenging and threatening public and national security.

Thus, the current concerns about the potential of information media have been intensified by the spread of information media and system technologies in the world, especially by the combination of computer technology with telecommunications, which has significantly deepened and expanded the space and possibilities of information activities and made it possible to sharply improve information infrastructures, which predetermined the consideration of the legal aspects of protecting information security.

Keywords: protection, internet, information security, computer crimes, legal regulation, crime, investigation, digital sovereignty

Doi: https://doi.org/10.14258/ralj(2025)1.5

По данным аналитического центра StormWall по итогам 2023 г. Россия находится на 12-м месте в рейтинге наиболее атакуемых хакерами стран мира [1]. В целом к концу года на фоне увеличения количества DDoS-атак в мире на 43% на Российскую Федерацию было совершено на 29% больше аналогичных нападений [2].

В числе высокотехнологичных преступлений 356 тыс. (52,6%) составляют мошенничества (в 2023 г. +38,2%), а раскрываемость их составляет всего 24,5% — при общей раскрываемости преступлений 52,3%.

По данным Национального агентства финансовых исследований в 2023 г. 91% россиян сталкивались с попытками мошенничества, что на 9% больше, чем годом ранее (82%) [3].

Согласно сведениям Центрального банка Российской Федерации за 2022 г. мошенники похитили у россиян 14 млрд руб. [4]. Утрата профилактических возможностей произошла и часто в связи с неоправданной либерализацией судебной практики, когда судами назначается даже за тяжкие преступления наказание ниже низшего предела на основании ст. 64 УК РФ [5, с. 70].

В Указе Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» [6] обращено внимание на необходимость разработки конкретных мер по реализации целого ряда принятых документов стратегического характера.

Сформулированные Президентом РФ В. В. Путиным на расширенном заседании коллегии МВД России в феврале 2022 г. цели актуальны и сегодня: «В целом вновь обращаю внимание на задачу кардинального повышения уровня раскрываемости преступлений. По итогам прошлого года добиться здесь качественных сдвигов, к сожалению, пока не удалось. А значит, нужна последовательная, более результативная работа по всем видам преступлений, которые представляют угрозу для нашего общества» [7].

Сущность информационной безопасности и ее обеспечение правовыми методами рассматривают в своих работах А. К. Дубень, И. И. Евкина, П. Н. Кобец, А. Ю. Ланецкая, Е. Н. Александрова, В. И. Литвиненко, В. С. Козлов, О. С. Павлов, Ю. И. Чернов, А. С. Шаталов и др.

Социально-психологическая характеристика киберпреступника представлена в научных статьях и монографиях Ю. В. Белевитиной, Н. А. Карповой, П. А., Муллаяровой, В. А. Семёнова, Е. Ю. Сурновой, Г. М. Третьякова и др.

Причины и условия совершения преступлений в сфере компьютерной информации анализируются в научных публикациях В. В. Бабурина, К. А. Ковтуна, Т. В. Молчановой, В. А. Аксёнова и др. Меры, направленные на предупреждение компьютерных преступлений, предлагаются в научных исследованиях Н. В. Дьяченко, А. С. Отакулова, И. С. Шатомирова, Т. Н. Кодзова, М. О. Николаевой, Т. В. Прокопьевой.

Однако серьезные изменения в информационной сфере, появление новых технологий, которые используют киберпреступники, новые вызовы в сфере информационной безопасности обусловливают потребность в проведении новых исследований в этой области.

Согласно статическому подходу информационная безопасность — это состояние защищенности информации, информационной среды, личности. Сторонники деятельностного подхода рассматривают информационную безопасность как процесс, практику обеспечения информационной безопасности, способность эффективно защитить ценности, ресурсы, интересы. Сторонники комплексного подхода исходят из того, что информационная безопасность включают в себя все аспекты, которые касаются защищенности объекта и процесса обеспечения этого состояния [8, с. 71].

Следует отметить, что под информационной безопасностью необходимо понимать способность государства обеспечивать защиту данных, во-первых, сведений независимо от формы их представления, во-вторых, это комплекс различных мероприятий по обеспечению безопасности информации, средств ее передачи, хранения, обработки и накопления.

Информационная безопасность должна быть обеспечена в различных сферах жизни общества и государства: политической, экономической, социальной и духовной. Следовательно, данный вид национальной безопасности должен постоянно совершенствоваться в соответствии с новыми опасностями и угрозами. Безопасное обращение с информацией предполагает необходимость проявлять осторожность при обращении с ней, поскольку существует большой риск того, что произойдет утечка данных.

Если разбирать подробнее саму систему производства, хранения и распространения информации, то в ней можно выделить два элемента: субъекты, а именно производители, распространители и владельцы информации, использующие механизмы ее защиты, и непосредственно сама база информации, т. е. компьютерные помещения, линии связи и обслуживающий персонал.

Меры по государственной защите информации в первую очередь должны быть направлены на защиту конфиденциальности данных, они включают в себя рекомендации по техническим и программным способам защиты, которые обязаны выполнять работники, осуществляющие обработку персональных данных и соблюдающие коммерческую или иную тайну. Рекомендации разрабатываются специальными службами, такими как Федеральная служба по техническому и экспортному контролю (ФСТЭК РФ), федеральный исполнительный орган власти, который осуществляет реализацию государственной политики в области государственной безопасности, и Федеральная служба безопасности Российской Федерации (ФСБ РФ) — осуществляет государственное управление в области обеспечения безопасности в Российской Федерации. Деятельность органов государственной власти в этой сфере многоаспектна, от обеспечения сохранности государственной и военной тайны до банковской тайны и обеспечения исключения неправомерного доступа к средствам граждан и компаний, которые хранятся на банковских картах и расчетных счетах [9, с. 350].

С коммерческой тайной, как правило, сталкиваются предприятия, которые осуществляют деятельность по исполнению государственных контрактов, заказов, вследствие чего они имеют доступ к сведениям одной из следующих сфер, например, в военной области, экономике, науке и технике, в области внешнеэкономической деятельности.

В связи с бурным развитием информационных технологий, а также глобализацией информационных потоков возникает необходимость включения в законодательство Российской Федерации юридических норм, которые осуществляли бы регулирование общественных отношений, подвергающихся посягательствам в результате совершения преступлений в сфере компьютерных технологий.

Сфера информационной безопасности бурно начала развиваться с 80-х гг. прошлого века, что стало объективной закономерностью научно-технологического прогресса в сфере информационных технологий, глобальных систем телекоммуникаций, средств связи. При этом деятельность российского государства в современных условиях нацелена на то, чтобы создать национальную систему безопасности со всеми присущими ей элементами, а это предполагает повышенное внимание к важнейшему ее виду — информационной безопасности, без которой национальная безопасность не может быть обеспечена никакими средствами.

Наиболее тесно связаны между собой информационная и экономическая безопасность. Они переплетены и не могут быть изолированы друг от друга [10, с. 525].

Важно отметить также, что особую опасность представляют информационные угрозы государству и личности через распространение и навязывание идеологии международного терроризма, экстремизма и сепаратизма. Парирование этих угроз занимает важное место в обеспечении информационной безопасности и общей национальной безопасности России.

Компьютерные технологии нашли самое широкое применение со стороны деструктивных сил, осуществляющих подобную деятельность.

Одной из распространенных угроз в информационной сфере является использование компьютерных вирусов с целью хищения, уничтожения баз данных, лишения доступа к ним их обладателей. Определение понятия «вредоносная программа» дается в ст. 273 Уголовного кодекса Российской Федерации [11]. Это компьютерная программа либо иная компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Вирус — это самопроизводящийся программный код, который внедряется в установленные на устройстве программы без согласия пользователя [12, с. 376].

Еще одна разновидность вредоносных программ — это руткит. Особенность руткита в том, что для сокрытия вредоносного кода и его работы от пользователя и установленного защитного программного обеспечения применяется тесная его интеграция с операционной системой. Более того, некоторые рукиты могут запускаться перед загрузкой операционной системы.

Классический пример — это распространявшийся в 2000 г. почтовый червь LoveLetter. Электронное письмо, приходившее на электронный почтовый ящик, называлось «I love you». Пользователи,

получившие такое письмо, открывали его, так как хотели узнать, кто прислал им признание. В результате активировалась вредоносная программа. Результат «эпидемии» — почтовые серверы компаний не выдерживали нагрузку, поскольку червь рассылал свои копии по всем контактам из адресной книги пораженного компьютера. Другой пример — червь Swen, выдавший себя за сообщение от компании Microsoft и маскировавшийся под обновление, устраняющее ряд уязвимостей в операционной системе Windows.

Ключевым звеном в распространении преступлений, связанных с получением информации и ее безопасности, являются программы, которые носят вирусный характер, ведь посредством различных ссылок и атак, которым подвергаются лица, не обладающие специальными знаниями, злоумышленники проникают в их компьютеры и получают всю необходимую информацию.

За последние годы компьютерные технологии тесно вошли в нашу жизнь. Массовая компьютеризация началась еще в период с 1990-х и до конца 2000-х гг. Расширение компьютерной сферы привело к развитию рынка компьютеров, начали применяться электронно-вычислительные машины, которые в дальнейшем стали все чаще находить применение в сети широкого доступа.

Стали активно практиковаться работа с базами данных, обработка документов в служебной, производственной деятельности, так называемый документооборот. Компьютер стал помощником во всех сферах деятельности, с его помощью можно было получить очень много достоверной информации, он стал обязательным элементом рабочего стола в офисах, органах власти. Следствием этих процессов является криминализация сферы использования компьютерных технологий [13, с. 248].

Основные виды угроз информационной безопасности можно распределить по различным признакам. Непреднамеренные, т. е. неумышленные, случайные угрозы, которые возникают в результате ошибок проектирования компьютерной системы и ее элементов, ошибок в программном обеспечении, ошибок в действиях персонала.

Преднамеренные, т. е. умышленные угрозы, связанные с корыстным умыслом преступников. Источниками могут служить различные компоненты, как внутренние, так и внешние, элементы самой компьютерной системы либо вредоносные программы, персонал и аппаратура [14, с. 293].

Среди источников угроз информационной безопасности России следует различать внешние и внутренние угрозы [15, с. 192]. К внешним угрозам относят: деятельность иностранных структур, направленную против интересов Российской Федерации в информационной сфере; стремление ряда стран к доминированию в мировом информационном пространстве; обострение международной конкуренции за обладание информационными технологиями и ресурсами; деятельность международных террористических организаций; деятельность космических, воздушных и наземных технических и иных средств (видов) разведки иностранных государств; ведение рядом государств информационной войны против Российской Федерации.

К внутренним угрозам информационной безопасности следует отнести: неподготовленность отечественных отраслей промышленности к вызовам в сфере информационной безопасности; неблагоприятную криминогенную обстановку в России; недостаточную координацию деятельности органов власти по реализации единой политики в области информационной безопасности; недостаточно развитую нормативную базу в информационной сфере; недостаточный государственный контроль за развитием информационного рынка; отставание России от ряда стран по уровню информатизации всех сфер деятельности и жизни.

В наши дни особую угрозу представляют информационные войны, которые ведут против России ее противники. Информационная война предполагает наличие специализированных формирований, а также предпринимаемых враждебных действий для достижения информационного превосходства над неприятелем. Их цель — обеспечить нанесение урона противнику с помощью воздействия на информацию и информационные системы. Для всех участников информационных войн важно укреплять собственную систему информационной безопасности. Информационная война характеризуется тем, что имеет наступательные и оборонительные составляющие. Она предполагает наличие особого управления и коммуникаций, соответствующей материальной базы, осуществления разведки и контрразведки, обеспечивающих превосходство над противником [16]. Неконтролируемые, по существу, криминальные группировки или отдельные лица, использующие методы и средства информационной войны, следует разбить на три группы: компьютерные взломщики (хакеры), группировки организованной преступности и политические подпольные группировки.

К группе «хакеров» принадлежат как организованные преступные группировки, так и индивидуальные преступники. Эта группа далеко не однородна по составу, целям и задачам деятельности. Сюда относят всех тех, кто обладает знаниями, опытом и специальными методами манипулирования в специализированных компьютерных системах, телекоммуникационных сетях для решения своих личных или групповых задач, например разведка, изъятие или подмена информации в военных сетях, базах данных, изъятие денег в банках, особенно для целей обхода механизмов защиты, обеспечения безопасности систем. «Хакеры» по своей сути — это «солдаты на передовом фронте борьбы» в составе любой группировки, которая в своих целях интересуется методами и средствами информационной войны.

Неконтролируемые группировки, используя профессионалов в области новейших технологий (компьютерные и телекоммуникационные системы), в последние годы стали сами создавать весьма сложные, разветвленные и хорошо защищенные компьютерные и коммуникационные системы.

Таким образом, в сфере национальной безопасности существует множество угроз, которые делятся на внешние и внутренние, создаваемые преднамеренно и возникающие вследствие сбоев техники и просчетов персонала. Каждая из них должно быть вовремя выявлена, требует своего глубокого анализа и предполагает адекватную реакцию со стороны органов государственной власти, гражданского общества и всех членов социума. Все это требует постоянного совершенствования нормативно-правовой базы обеспечения информационной безопасности, анализ которой представлен далее.

Среди нерешенных проблем правового регулирования сферы национальной безопасности отметим, что на сегодняшний день назрела необходимость принятия новых международных документов в области обеспечения информационной безопасности с учетом практики ведущих государств в данной сфере. Предпосылками данных изменений служит неуклонный рост международной информационно-телекоммуникационной преступности, которая, в свою очередь, угрожает безопасности всех государств мира. Однако этому шагу препятствует рост конфронтации между развитыми мировыми державами, в том числе в информационной сфере. Это вредит всем членам мирового сообщества. Однако по-прежнему национальные корыстные интересы превалируют над интересами мировой информационной безопасности.

Ввиду стремительного развития интернета цифровое пространство стало неотъемлемой частью жизни общества. Оно не имеет физических территориальных границ. В этой связи вопрос содержания и пределов национального суверенитета в цифровом пространстве встает особенно остро.

В настоящее время мнения по поводу суверенитета в киберпространстве разделились. В России и Китае действует подход, согласно которому на цифровое пространство распространяется национальный суверенитет. Подход США и Великобритании сосредоточен на свободе и открытости киберпространства, а также на недопустимости распространения на него суверенитета. Несмотря на разницу в подходах в Докладе Группы правительственных экспертов ООН «О развитии в области информации и телекоммуникаций» (24 июня 2013 г.) UN Doc A/68/98 было отмечено следующее: «Государственный суверенитет и международные нормы, и принципы, вытекающие из принципа государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием ИКТ, а также на юрисдикцию государств над ИКТ, как инфраструктурой на их территории» [17]. Неопределенность вносит тот факт, что киберпространство — это совершенно новая область, и вопрос суверенитета в киберпространстве не полностью соответствует сухопутному и морскому суверенитету. В то же время формальное признание суверенитета в киберпространстве, его практическая реализация осложняется разобщенностью на мировом уровне и отсутствием необходимого правоприменительного опыта ввиду специфики киберпространства. Оно имеет виртуальные и нематериальные характеристики, и как позиционировать суверенитет стран в такой области — это проблема, с которой сталкиваются все правопорядки. Развитие информационного пространства формулирует проблемы, которым раньше не уделялось достаточного внимания, некоторые из них вообще не существовали. Увеличилось число преступлений, связанных с нарушением прав неприкосновенности частной жизни при обработке персональных данных с использованием информационных технологий. Очевидно, что в отсутствие реализации цифрового суверенитета присутствуют как внешняя, так и внутренняя угрозы национальному суверенитету.

В этой связи необходим алгоритм защиты компьютерной информации, который позволил бы минимизировать риски. Так, например, если криптографические методы были вполне эффективными

еще несколько десятилетий назад, то нельзя сказать это применительно к настоящему времени, поскольку они морально и физически устарели с учетом того, что современная компьютерная техника стала более мощной, более распространенной.

В настоящее время методы качественного контроля программных средств используются до, во время или после создания новой программы с целью проверки правильности ее поведения. Но ни одна современная программа не будет совершенной, и очевидные изъяны в некоторых популярных программах свидетельствуют о том, что их качественный контроль мог бы быть на более высоком уровне. Следует опасаться тех поставщиков программного обеспечения, которые не могут дать документального подтверждения его качества, необходимо больше доверять отечественному производителю.

Целесообразно обращаться к отечественным компаниям, занимающимся вопросами защиты, хотя при этом следует иметь в виду, что ключевые зоны, вероятнее всего, будут закрытыми для анализа.

При использовании сети Интернет для передачи электронного письма обычно имеет место передача информации об отправителе, получателе и некоторые данные о маршруте. Это позволяет отслеживать многие истинные источники электронной почты, что может быть нежелательным для отправителя. Для этого существуют службы электронного посредничества, которые маскируют или полностью закрывают источник электронного сообщения. Необходимо сохранять электронные сообщения с угрозами, полученные организацией, в том случае, если в заголовках содержится полезная информация. Правоохранительные органы, занимающиеся расследованием компьютерных преступлений, безусловно, одобрят, если будет сохранено что-либо, что можно использовать в качестве вещественных доказательств. В качестве главного фактора-причины следует отметить социально-психологические свойства и качества самого преступника [5, с. 69].

Достаточно эффективным способом нарушения защиты системы технологической компании является так называемый культурный способ, когда методом убеждения лица, знающего пароль, добиваются, чтобы тот сообщил его. Это и есть социальная техника, которая наиболее легко осуществляется по мобильным каналам. Представившись тем, кто имеет право знать пароль, социальные техники могут уговорить сотрудника выдать необходимую информацию. Типичными приемами при этом являются: представление в качестве специалиста, имеющего предписание устранить возникшую проблему в сети; представление сотрудником телемаркетинговой компании. Этим приемом в настоящее время активно пользуются компьютерные мошенники.

Довольно часто злоумышленники могут легко получить внутренние телефонные списки, которые они используют для последовательного обзвона, пока не найдут такого сотрудника, который окажется недостаточно бдительным и поддастся на их предложение. Для противодействия такой тактике телефонные абоненты должны иметь возможность сообщать в соответствующую инстанцию о подозрительных звонках или электронных сообщениях. Без такого централизованного сбора вряд ли будет возможно выявить попытку нарушения защиты. Если сотрудник планомерно контролирует использование сети, то должен заметить систематические попытки нарушить защиту ваших информационных серверов.

В настоящее время почти все пользователи сталкивались с проблемой вирусов. Они имеют тенденцию суперлинейного распространения и поэтому с большей вероятностью могут широко распространяться и передаваться кому-то за пределами компании. Имеются вирусы, которые заражают дискеты, программные файлы, документацию Word, крупномасштабные таблицы Excel и др. Современное противовирусное программное обеспечение является необходимым средством для любого учреждения, организации.

Таким образом, правовые акты в сфере информационной безопасности Российской Федерации нацелены на создание всех условий для свободного поиска, получения, передачи, производства и распространения информации любым законным способом во всех сферах жизни общества. Одновременно они направлены на пресечение противоправной деятельности в этой сфере. Тем не менее отмеченные пробелы в законодательстве требуют дальнейшего совершенствования правового обеспечения национальной безопасности Российской Федерации.

Необходимо установить приоритеты: защита правительственных систем, защита национальной инфраструктуры и создание систем, помогающих гражданам безопасно работать в киберпро-

странстве. Правительство Российской Федерации должно иметь официальные организации, отвечающие за две проблемы. Первая — это создание сильного мониторинга и способности обнаружения атак. Способность обнаружения должна охватывать диапазон всех слоев коммуникации, и в частности уровень приложений. Вторая — это ответственность властей за создание стандартов безопасности, которые свяжут любые правительственные организации, когда добавляется новая связь с общественностью. Им также необходимы приоритеты в работе национальных коммуникаций против атак, вызывающих отказ в обслуживании. В частности, они должны обеспечить достаточное внутреннее резервирование, достаточный избыток защитного контроля, определяемый в результате оценки процесса риска, чтобы направить ресурсы туда, где самый высокий уровень риска или самый низкий уровень безопасности.

Очень важной является защита данных и приложений. Гражданские и военные базы данных — это национальное достояние. Правительство Российской Федерации должно быть уверено, что эти данные, например номера счетов, информация о здоровье или другая персональная информация, надежно защищены. Это предполагает необходимость точного определения, что считается чувствительной информацией, и установления требований по контролю безопасности. Необходимо также принимать во внимание интеллектуальную собственность. Похитители интеллектуальной собственности — это часто бизнес-конкуренты, компании-жертвы, они будут просить помощи у государства, которую оно должно будет предоставить в соответствии с принятыми законами.

Получение разведывательных данных на хакеров также очень важно. Анализ деятельности хакеров, технических средств, мест запуска атак и целей позволит представителям правоохранительных органов вовремя определить предполагаемую значительную атаку на компьютерные системы. Основываясь на информации, полученной от разведки, представители власти могут обеспечить руководство по созданию соответствующих механизмов защиты.

Для анализа информации должны применяться различные процессы и средства. Получение данных от граждан, и особенно от сетевых курьеров, может способствовать усилению анализа со стороны правительственной хакерской разведки. Дальнейшее сотрудничество может включать выявление атак, которые берут начало в стране, и искоренение их на регулярной основе. Логично возникает вопрос: что правительство может сделать для усиления правоохранительных органов, занимающихся киберпреступностью? Во-первых, законодательство по киберпреступлениям должно быть интегрировано с законами уголовного права; во-вторых, правительство должно координировать деятельность правоохранительных органов с деятельностью институтов гражданского общества. То, что может показаться небольшой кибератакой, на самом деле может быть частью большой криминальной попытки, которую могут распознать только правоохранительные органы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Россия вошла в число самых атакуемых хакерами стран // Лента.ру. URL: https://lenta.ru/news/2024/02/06/rossiya-voshla-v-chislo-samyh-atakuemyh-hakerami-stran/ (дата обращения: 27.11.2024).

2. В 2023 году больше всего выросло количество DDoS-атак на российские телеком-сферу, транспортный и государственный секторы // SERVERNEWS. URL: https://servernews.ru/1099012 (дата обращения: 23.11.2024).

3. 91% россиян сталкивался с попытками мошенничества в 2023 году — опрос // Вслух. ru. URL: https://vsluh.ru/novosti/obshchestvo/91-rossiyan-stalkivalsya-s-popytkami-moshennichestva-v-2023-godu-opros_399249/?ysclid=m1f4p7ivhx177360318 (дата обращения: 21.11.2024).

4. Россияне сдали мошенникам рекордные ₽14 млрд // РБК. URL: https://www.rbc.ru/newspaper/2023/02/15/63eb5da89a794701b759621f?ysclid=m1f4rc86og374377764 (дата обращения: 21.11.2024).

5. Костюк М. Ф., Кунц Е. В. Криминологические аспекты дистанционного мошенничества // Проблемы права. 2022. № 3. С. 69–71.

6. О Стратегии национальной безопасности Российской Федерации : Указ Президента РФ от 02.07.2021 № 400. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 21.11.2024).

7. Расширенное заседание коллегии МВД России. URL: http://www.kremlin.ru/events/president/transcripts/comminity_meetings/67795 (дата обращения: 20.11.2024).

8. Литвиненко В. И., Козлов В. С. Основы информационной безопасности. М. : Кнорус, 2022. 199 с.

9. Иксанов Р. А., Бакирова Р. Р. Кражи как разновидность экономических преступлений // Аллея науки. 2018. Т. 2, № 4. С. 355–358.

10. Криминология. Особенная часть : учебник для курсантов и слушателей образовательных организаций высшего образования системы МВД России / А. Е. Шалагин, Р. Р. Абдулганеев, О. В. Артюшина [и др.] ; под общ. ред. Ф. К. Зиннурова. 2-е изд., перераб. и доп. Казань : Казанский юридический институт МВД РФ, 2016. 524 с.

11. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. URL: http://www.consultant.ru/ (дата обращения: 30.11.2024).

12. Евкина И. И., Шарыпова Т. Н. Киберпреступность как угроза информационной безопасности // Инновации. Наука. Образование. 2021. № 36. С. 375–377.

13. Чайковский П. П. Средства реализации угроз информационной безопасности // Вестник науки. 2022. Т. 4, № 11. С. 248.

14. Аванесов Г. А. Криминология. М. : Юнити-Дана, 2020. 447 с.

15. Ланецкая А. Ю., Александрова Е. Н. Современные угрозы информационной безопасности // Международный журнал гуманитарных и естественных наук. 2022. № 7–2. С. 192–195.

16. Лукин А. Н., Медведев А. Н. Информационная война против России: уроки, которые необходимо извлечь // Бизнес и общество. 2022. № 1.

17. Доклад группы правительственных экспертов за 2012/2013 годы был издан в виде документа A/68/98*. URL: https://disarmament.unoda.org/ru/ (дата обращения: 25.11.2024).