УДК 340.1:004
ББК 67.408.01с51

ПРОТИВОДЕЙСТВИЕ СОВРЕМЕННЫМ КИБЕРПРЕСТУПЛЕНИЯМ

Е. В. Кунц

Научно-исследовательский институт Федеральной службы исполнения наказаний (Москва, Россия)

Развитие высоких технологий и их внедрение в различные сферы жизни породило множество серьезных проблем, одной из которых является стремительная криминализация научно-технической сферы. Следует отметить активное использование в преступных целях достижений научно-технического прогресса в процессе подготовки и совершения всевозможных преступлений, начиная от дистанционного мошенничества, заканчивая террористическими актами. Существующие нормативно-правовые акты рассчитаны преимущественно на физический мир, задавая определенные рамочные основы взаимоотношений и деятельности граждан. Далее они стали активно распространяться и на двумерную цифровую среду сети Интернет, охватывая основные вопросы кибербезопасности.

Констатируется, что рост количества преступлений в сфере компьютерной информации во многом связан с бурным прогрессом в технической и информационной сфере. Современный киберпреступник хорошо технически оснащен и образован в части применения информационных технологий. Соответственно логично предположить, что столь быстро должны совершенствоваться различные способы защиты населения, учреждений и организаций от преступных посягательств киберпреступников. Нужен системный подход в борьбе с преступлениями в информационной сфере, который должен учитывать причины и условия совершения преступлений данного вида, а также условия отбывания наказания лицами, осужденными за данные преступления.

Ключевые слова: интернет, киберпреступления, преступник, противодействие, осужденный

COUNTERING MODERN CYBERCRIMES

E. V. Kunts

Research Institute of the Federal Penitentiary Service (Moscow, Russia)

The development of high technologies and their implementation in various spheres of life has given rise to many serious problems, one of which is the rapid criminalization of the scientific and technical sphere. It should be noted that the achievements of scientific and technical progress are actively used for criminal purposes in the process of preparing and committing all kinds of crimes, from remote fraud to terrorist acts. Existing regulatory legal acts are designed primarily for the physical world, setting certain frameworks for the relationships and activities of citizens. Then they began to actively spread to the two-dimensional digital environment of the Internet, covering the main issues of cybersecurity.

It is stated that the increase in the number of crimes in the field of computer information is largely due to the rapid progress in the technical and information sphere. A modern cybercriminal is well technically equipped and educated in the use of information technology. Accordingly, it is logical to assume that various methods of protecting the population, institutions and organizations from criminal attacks by cybercriminals should be improved so quickly. A systematic approach is needed in the fight against crimes in the information sphere, which should take into account the reasons and conditions for committing a crime of this type, as well as the conditions for serving sentences by persons convicted of these crimes.

Keywords: Internet, cybercrimes, criminal, counteraction, convicted

Doi: https://doi.org/10.14258/ralj(2025)1.15

Злободневность проблемы и ее важность указана в пп. «д» п. 20 Указа Президента Российской Федерации от 1 декабря 2016 г. № 642 (в ред. от 15.03.2021) «О Стратегии научно технологического развития Российской Федерации» [1], где отмечается, что в ближайшие 10–15 лет приоритетами научно-технологического развития Российской Федерации следует считать те направления, которые позволят получить научные результаты, обеспечивающие противодействие техногенным, биогенным, социокультурным угрозам, терроризму и идеологическому экстремизму, а также киберугрозам и иным источникам опасности для общества, экономики и государства.

Следует отметить, что категория «киберпреступлений», или преступлений, совершенных с использованием киберпространства, вышла за рамки предусмотренных гл. 28 Уголовного кодекса Российской Федерации (Преступления в сфере компьютерной информации). Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646) [1] на настоящий момент имеет признаки некоторого устаревания, поскольку скорость развития компьютерной техники и порождаемых ей угроз превышает скорость научных и нормативных разработок. В настоящее время не в полной мере сформулирована концепция противодействия криминализации киберпространства, которая позволила бы оперативно реагировать на существующие и вновь возникающие угрозы криминалиации данной специфической сферы человеческой деятельности.

Компьютерные технологии компьютерных преступников являются весьма сложными и быстро эволюционирующими, что сводит к минимизации усилия правоохранительных и финансовых органов, направленные на удержание ситуации на должном уровне, что создает все большие возможности для онлайновых преступников [2, с. 13].

Однако это лишь мотивы преступлений, а не их причины и условия. Первая причина — это недостаточность мер по защите электронно-вычислительных машин (далее — ЭВМ), систем и их сетей. Также недостаточность мер по обеспечению безопасности ЭВМ и программного обеспечения. Все это особо опасно на фоне возрастания информационного обмена с помощью мировой информационной сети Интернет. Нарушение правил работы с компьютерной информацией часто имеет место там, где низок уровень специальной подготовки должностных лиц и мало внимания уделяется защите информации и сетей коммуникации [3, с. 135].

Приведем типичные примеры из судебной практики. В сентябре 2018 г. Октябрьский районный суд г. Саранска приговорил вымогателя к году лишения свободы условно за вымогательство под угрозой уничтожения чужого имущества. Злоумышленник заблокировал несколько сайтов одного из предприятий, после чего связался с системным администратором и потребовал денежную сумму в размере 110 тыс. руб. за прекращение вредоносной атаки. После чего руководитель предприятия перечислил на электронный счет хакера 60 тыс. руб. [4, с. 125].

В декабре 2020 г. Хорошевский районный суд Москвы признал виновным Алексея Кузьмина по ст. 163 УК РФ (Вымогательство) и 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ), который произвел ряд DDoS-атак на компьютерную информацию, хранящуюся на ресурсах сайтов ЗАО Банк «Тинькофф Кредитные системы», ЗАО «Лаборатория Касперского», ОАО «Промсвязьбанк» и ЗАО «Издательский дом „Комсомольская правда”», а также требовал от владельца банка «ТКС» денежную сумму в размере 1 тыс. долл. за прекращение DDoS-атаки [5].

Большинство преступлений имеет латентный характер. Именно это обстоятельство объясняет высокий рост правонарушений, а также низкий уровень раскрываемости данных преступлений правоохранительными органами.

Например, некоторые ученые при исследовании данных отмечают, что по итогам 2022 г. по России нераскрытыми остались 71,0% от числа зарегистрированных преступлений в сфере компьютерной информации, в том числе по п. 1 ч. 1 ст. 208 УПК РФ (в связи с неустановлением лица) — 70,6%, снижение числа приостановленных (нераскрытых) по п. 1–3 ч. 1 ст. 208 УПК РФ уголовных дел в сравнении с аналогичным периодом прошлого года составило 4,7% (с 388 607 до 370 179)» [6, с. 413].

Если разбирать латентные преступления по видам, то первой их разновидностью является такая, при которой правоохранительные органы не осведомлены о совершении преступлений в компьютерной сфере, знают о них только те лица, которые виновны, а также их сообщники, не заинтересованные в разглашении сведений об этом. Даже жертвы преступлений не понимают, что являются таковыми. Следующий вид латентной преступности в этой сфере составляет огромный объем преступлений. Они хоть и известны должностным лицам и организациям, но ни те, ни другие

не осведомляют соответствующие органы о совершении преступлений в сфере компьютерной информации. В следующую разновидность латентной преступности в рассматриваемой сфере включена группа преступлений, которая уже известна правоохранительным органам, но в силу нехватки знаний по данному виду правонарушений либо неправильной юридической оценки и отсутствия достаточных профессиональных навыков не осуществляется нужная профилактическая работа, выявление и наказание преступников.

Во всех трех проявлениях может быть использована компьютерная информация различного рода.

Специалистами выявлено, что компьютерные преступники стали распространять свои действия на банкоматы, используя вредоносные программы, посредством которых взламывают систему и подбирают коды, нарушают целостность сайтов и получают доступ к денежным средствам, подвергая опасности денежные средства лиц, не знающих о данных технологиях.

Компьютерные технологии становятся средством совершения преступлений самого разного характера. Преступники никогда ранее не имели такого технологического оснащения, как в условиях цифровизации всех сфер жизни общества [7, с. 30].

Н. С. Сорокун, О. В., Ермакова выделяют следующие факторы, способствующие росту преступлений в информационной сфере [3, с. 135]: всемирная популяризация безналичной оплаты товаров и услуг, использование банковских карт, онлайн-переводов и иных способов оплаты, это как раз и направляет преступников в эту сферу, так как именно здесь есть интересующие их финансовые потоки; низкий уровень цифровых компетенций граждан страны, что делает их уязвимыми для киберпреступников; недостаточно развитая квалификация правоохранительных органов, выражающаяся в неспособности оперативно пресекать киберпреступную деятельность и эффективно расследовать инциденты в цифровой среде — рост квалификации киберпреступников часто опережает динамику развития соответствующих компетенций тех, кто с ними борется; несовершенство законодательства, позволяющее преступникам во многих случаях избежать ответственности или получить более мягкое наказание, что также объясняется прежде всего тем, что законодатели просто не успевают вовремя адекватно отвечать на изменения в информационной среде; отсутствие установленных процедур международного сотрудничества между правоохранительными органами и экспертными организациями в разных странах, особенно на фоне резкого нарастания напряженности в отношениях России и стран коллективного Запада; сейчас ведется гибридная война против России со стороны ее противников, в условиях которой против государственных структур, бизнес-организаций и граждан работают иностранные спецслужбы и поощряемые ими хакерские группы.

Ряд авторов, среди которых Н. В. Дьяченко, А. С. Отакулов, И. С. Шатомиров, выделяя причины преступлений в информационном пространстве, делают акцент на таких внутренних установках киберпреступников, как желание получить признание в своей среде, и только потом в их мотивации стоит «добыть быстрые деньги» в условиях трудной идентификации личности преступника [8, с. 243].

Низкий контроль за деятельностью работников в сфере банковских услуг или других организаций, имеющих доступ к важной информации, создает условия для преступной деятельности.

Так, в 2021 г. по ч. 1 ст. 138 и ч. 2 ст. 272 УК РФ осужден А., который являлся продавцом-консультантом на точке продаж оператора сотовой связи. Он откликнулся на объявление в Телеграм-канале, в котором предлагалось денежное вознаграждение в размере 1000 руб. за каждую отправленную детализацию и замененную сим-карту. Осуществляя замену номеров сим-карт, А. получил в качестве вознаграждения 40 тыс. руб. [9]

Сочетание новейших технологий воздействия на психику людей и наличия интернета позволяет иностранным спецслужбам через сети вербовать своих агентов, навязывать им свои установки и манипулировать их сознанием вплоть до совершения ими преступления по заданию своих кураторов. Это реальность нашего времени [10].

Следовательно, причины и условия совершения преступлений, подрывающих информационную безопасность, многообразны. Разные эксперты по-своему их формулируют и группируют, что объясняется сложностью исследуемого феномена и той мировозренческой позицией, с которой проводит свое исследование тот или иной ученый.

В. В. Бабурин отмечает, что в настоящее время принято ограничиваться анализом причин и условий уже совершенных преступлений, описывать причины того, что уже произошло. Вместе с тем представляется актуальным не только анализ того, что уже прошло, а концентрация внимания

на том, что обязательно произойдет, исходя из тех условий, которые уже складываются для новых преступлений [11, с. 142].

По масштабам воздействия можно выделить следующие меры предупреждения компьютерных преступлений: общесоциальные, которые осуществляют государственные органы, прежде всего принимая и применяя соответствующие нормы законодательства, а также институты гражданского общества и СМИ; специально-криминологическое предупреждение, где задействованы специальные органы, например отдел «К» — подразделение Министерства внутренних дел РФ, борющееся с преступлениями в сфере информационных технологий, а также с незаконным оборотом радиоэлектронных средств и специальных технических средств. В субъектах Российской Федерации функционируют соответствующие структурные подразделения криминальной полиции — отделы «К».

С. Д. Бражник меры предупреждения компьютерных преступлений подразделяет на три основных группы: правовые; организационно-технические и криминологические [12, с. 35].

К первой группе профилактики преступлений этой категории относятся законодательные положения, предусматривающие дисциплинарную, гражданско-правовую, административную и уголовную ответственность за противоправные деяния.

Данные мероприятия включают выработку норм, которые регулируют отношения в сфере компьютерной информации, способствуют совершенствованию законодательства. К правовым мерам относятся также общественный контроль за создателями компьютерных систем и заключение международных договоров об их ограничениях, если они смогут оказать влияние на военные, экономические и социальные стороны жизни стран, подписавших соглашение.

В настоящее время действуют федеральные законы «О связи» от 7 июля 2003 г. № 126-ФЗ [13] и «Об информации, информационных технологиях и о защите информации» от 27 июня 2006 г. № 149-ФЗ [14]. В указанных законах содержатся определения основных компонентов информационных технологий, закреплены категории доступа определенных субъектов к конкретным видам сведений и установлены уровни секретности информации.

Важным элементом предупреждения преступлений данной категории считают Уголовный кодекс Российской Федерации, вступивший в силу 1 января 1997 г. В указанном законе компьютерная информация закреплена как объект уголовно-правовой охраны [15].

Принятие данного документа привело отечественное законодательство в соответствие с общепринятыми международными правовыми нормами. При этом, как указывает С. Ю. Чимаров, Уголовный кодекс Российской Федерации имеет ряд несовершенств из-за того, что законодатель не успевает за изменениями в информационной сфере, в связи с этим возникают проблемы, которые затрудняют предупреждение и расследование компьютерных преступлений [16]. Это в полной мере касается также Кодекса об административных правонарушениях Российской Федерации [17], Гражданского кодекса Российской Федерации [18] и иных нормативных правовых документов, в той или иной степени регулирующих отношения в информационной сфере.

В законодательстве по-прежнему есть пробелы, оставляющие лазейки для преступников. Среди них, например, отсутствие эффективных мер наказания организаторов и участников трэш-стримов — тех, кто выкладывает в интернет сцены жестокости. Действующее законодательство не учитывает, что это несет серьезную угрозу общественной безопасности, достоинству личности, жизни и здоровью граждан, нравственной атмосфере в социуме.

Второй группой мероприятий по защите средств компьютерной информации от противоправных посягательств считают меры организационно-технического характера, которые подразделяются на организационные, технические и комплексные методы профилактики [19, с. 325].

Организационные меры служат эффективным средством сохранения информации, поскольку наиболее важной причиной, способствующей совершению компьютерных преступлений, в большинстве случаев является недостаточная организация контроля за работой подчиненных сотрудников.

Неплохо зарекомендовал себя риск-ориентированный подход в сфере обеспечения информационной безопасности. Содержание информационно-правового риска как компонента риск-ориентированного подхода является основой для правового осмысления вопросов обеспечения национальной информационной безопасности в Российской Федерации. Однако определение информационно-правового риска дается только в подзаконных нормативных актах, что, по мнению А. К. Дубеня, недостаточно для обеспечения всеми субъектами однозначного понимания этого феномена [20, с. 126].

Одним из способов защиты национальной информации может стать использование отдельно созданных платформ передачи различных видов информации, усиление контроля за различными уже созданными платформами передачи информации, создание своих собственных закрытых средств связи для передачи особо важных данных [21, с. 299].

Самыми известными и широко распространенными программными профилактическими методами защиты информационных ресурсов от компьютерных вирусов являются программные антивирусные средства. Современные программы в кратчайшие сроки могут обнаружить и распознать вирус в информационных ресурсах, а также вылечить его.

При этом совместно с антивирусной программой нужно применять комплексные организационно-технические меры, которые заключаются в уведомлении сотрудников о возможном риске при совершении вирусного посягательства; запрете приносить на рабочее место неправомерные программные средства; проверке всех файлов, которые поступают из внешней компьютерной сети; создании архивов копий программ, которые используются в непосредственной работе организации; проведении проверки файлов; установке на персональном компьютере системе защиты информационных данных [22, с. 88].

Программные методы защиты идентифицируют личность пользователя и определяют операции, какие он может выполнять и к каким данным у него имеется допуск. Выборочно используются четыре метода, позволяющие установить личность пользователя, а именно: по предмету, которым он владеет; личному идентификационному коду, по антропологическим характеристикам личности, а также по электронной цифровой подписи, которая основана на использовании криптографической системы с открытым ключом.

Сотрудниками правоохранительных органов выработана система способов для предотвращения совершения любого компьютерного преступления. Это подтверждается анализом международного опыта борьбы с преступностью. В качестве профилактики используются различные меры, которые направлены на выявление и устранение причин, способствующих совершению противоправных деяний. Правильно организованная профилактическая работа оказывает позитивное воздействие на уровень, структуру и динамику преступности, поскольку данные мероприятия сконцентрированы на истоках преступности [23, с. 224].

Известно, что преступления в сфере компьютерной безопасности имеют очень высокую степень латентности, что способствует постоянную росту количества совершенных преступлений данной категории.

Следует объективно признать, что многие работники органов внутренних дел, в том числе сотрудники следственных подразделений, на недостаточном профессиональном уровне подготовлены к осуществлению профилактических мероприятий. Для выработки правильного алгоритма действий, направленных на профилактику совершения преступлений данной категории, правоохранительным органам следует знать причины и условия, которые способствуют совершению компьютерных преступлений.

В последнее десятилетие отмечается увеличение количества компьютерной техники как в различных организациях, так и у граждан, в связи с чем возрос объем обрабатываемой и хранящейся информации. Указанные обстоятельства влекут рост обмена информационными данными через телекоммуникационные сети.

Анализ современного состояния свидетельствует о несовершенстве профилактических мер, направленных на защиту компьютерных систем и их сетей, а также программного обеспечения. Требует постоянного совершенствования государственная политика в сфере обеспечения информационной безопасности, она должна отвечать на актуальные вызовы в этой сфере. Кроме того, не выработан необходимый алгоритм использования в работе на компьютере программного обеспечения, базы данных и аппаратных средств поддержания сетевых технологий. При этом при осуществлении работы с компьютерными сведениями, которые охраняются законом, пользователи нарушают установленные правила [24, с. 54].

Целесообразно выделить и другие условия, способствующие совершению противоправных действий данного вида: недостаточная защищенность электронной почты; при работе на компьютере пользователи допускают небрежность; кадровая политика при приеме людей на работу характеризуется некачественной работой по изучению личности кандидатов; обязанности по разработке про-

граммного обеспечения и эксплуатация техники зачастую возлагается на одного сотрудника; пользователи редко меняют пароли или они недостаточно надежны; ЭВМ необоснованно используется в конкретных технологических процессах и операциях; администрация не осуществляет надлежащего контроля за деятельностью своих сотрудников, которые задействованы на различных стадиях обработки компьютерной информации; руководство неправильно организует межличностные взаимоотношения с подчиненными. Преодоление этих недостатков возможно с помощью усиления регламентации деятельности должностных лиц, усиления контроля в сочетании с обучением персонала и разъяснительной работой [25, с. 39].

На сегодняшний день законодательство нуждается в большей разработке. С учетом развития, передачи, хранения и распространения информации общество подвергается все большей опасности, возможна криминализация иных общественно опасных деяний в сфере компьютерной информации.

Безусловно, компьютерные преступления являются распространенным видом преступлений, механизм их расследования требует опыта и знания предмета деятельности. Более того, перечень преступлений, закрепленных в законах в соответствующих главах, постоянно изменяется и дополняется, что, в свою очередь, требует дополнительных сведений и профессионального мастерства. Поэтому повышение квалификации в этой сфере работников правоохранительных органов должно носить перманентный характер.

Исходя из того, что преступления, совершаемые с применением компьютерных технологий, давно вышли за пределы национальных границ, необходимо объединить усилия с представителями зарубежных государств и подключить к борьбе с данным видом преступлений международные сообщества путем ратификации международных договоров и включения унифицированных норм международного права в данной области.

Можно обозначить основные правила в процессе устранения киберпреступлений [26, с. 119]. Тот факт, что кибератака была запущена из информационной системы, расположенной на территории государства, является доказательством того, что атака приписывается этому государству. Если кибератака была запущена или, другими словами, была произведена в рамках правительственной киберинфраструктуры, существует опровержимая презумпция, что государство связано с этой операцией. Государству, таким образом, нужно рассматривать ситуацию, при которой оно может нести ответственность за кибератаки или другие действия, в которых могут использоваться их информационные структуры. Страны могут поднять свой собственный уровень кибербезопасности созданием более строгого контроля за использованием и эксплуатацией информационной инфраструктуры в своей юрисдикции. Баланс между интересами экономики и безопасности должен рассматриваться в каждом отдельном случае. Принцип атрибуции существует в международном законодательстве по вопросам государственной ответственности. Два главных стандарта — это эффективный и всеобъемлющий контроль.

Если кибератака была проведена через информационные системы, расположенные на территории какого-либо государства, создаются обязательства по сотрудничеству с государством, являющимся жертвой атаки. Существование глобальной информационной инфраструктуры делает невозможным для любого государства защиту от кибератаки без сотрудничества с другим государством, чья инфраструктура может быть использована для осуществления атаки. Более эффективное сотрудничество требуется между общественными институтами, так же как между правительствами разных стран и международными организациями. Необходимо также взаимодействие между юридическими, политическими, военными и техническими экспертами.

Каждый имеет право на самозащиту, пропорциональную и необходимую в случае угрозы. В уголовном праве если жертва обоснованно верит, что неправомерная сила может быть применена против нее, не существует ответственности за действия, производимые в целях самозащиты. Это не означает, что каждый «киберответ» на атаку может подходить под эту концепцию. Каждый пользователь должен обеспечивать разумный уровень безопасности в своей информационной инфраструктуре.

Существуют обязательства сообщать потенциальным жертвам об известных и надвигающихся кибератаках. Общественность имеет право быть информированной об угрозе жизни, безопасности и благополучию.

Правовые нормы для доступа к информации будут являться важным аспектом кибербезопасности в плане стратегической коммуникации и общественной осведомленности. Каждое государство

имеет обязательство включать наиболее общие киберпреступления в положения уголовного права. Правило криминализации — это скорее напоминание, чем что-то качественно новое. Уже хорошо известно в уголовном праве, что кибератаки могут расследоваться и дела передаваться в суд только в том случае, если эти действия квалифицируются как уголовные преступления.

Таким образом, практически невозможно для государства направить санкции против кого-то индивидуума, участвовавшего в кибератаке, если только не была осуществлена специфическая деятельность, рассматриваемая как уголовная в рамках действующего права. Политически мотивированная киберпреступность присуща большинству угроз общественности, а не отдельным личностям или организациям и может потребовать другой реакции по сравнению с экономически мотивированным киберпреступлением.

Способность организации действовать на основании мандата — это правило релевантно для определения и координации международных усилий по обеспечению мировой кибербезопасности. В частности, его практическое значение заключается в сфере создания новых и ревизии существующих положений в области кибербезопасности.

Результаты анализа существующих законов и политических средств, связанных с кибербезопасностью, выявили пробелы в международном координировании. Киберзащита обходится во много раз дороже, чем подготовка самой атаки, и поскольку правительственная информационная инфраструктура все чаще становится целью атаки, развитие национальной и международной системы безопасности становится вопросом инвестиционным [26, с. 120].

Учет этих положений должен повысить осведомленность экспертов о существующих правовых сложностях, когда рассматриваются вопросы кибербезопасности и пути ее преодоления, служить основой для обсуждения и координации и являться достаточно обоснованным предложением для разработки дополнительного законодательства на международном уровне.

Информационная инфраструктура в рамках государства является предметом территориального суверенитета государства. Электронные коммуникации, криминальные санкции, уровень расследования, взаимодействие с Интернет-провайдерами и многие другие существенные элементы успешной киберзащиты зависят от качества национального законодательства. Пока все опции исполнения и интерпретации национального законодательства не будут полностью использованы, трудно определить, на какие средства нужно соглашаться на международном уровне. Принцип территориальности дает возможность странам навязывать свой суверенитет информационной инфраструктуре, находящейся в пределах их территории, или действовать в соответствии с их юрисдикцией. Ответственность государства за безопасность своих сетей поддерживается принятыми международными принципами невмешательства и суверенитета.

Современной информационной угрозе можно противостоять, объединив положения, средства защиты и правовую практику четырех ключевых областей законодательства. Достаточно длительное время ученые активно обсуждали существующие законы, а не акцентировали внимание на создании нового законодательства. Ряд таких вопросов можно отнести к правовым, таких как компетенция, идентификация или криминальное взаимодействие, хотя они связаны с политическими или техническими аспектами и должны рассматриваться с точки зрения конструктивных решений. Некоторые вопросы являются новыми для законодательства, более того, могут быть решены путем интерпретации или исключений из существующего законодательства вместо разработки совершенно нового законодательства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. О Стратегии научно-технологического развития Российской Федерации : Указ Президента РФ от 01.12.2016 № 642. URL: http://www.kremlin.ru/acts/bank/41449 (дата обращения: 21.11.2024).

2. Голубовский В. Ю. Уголовно-правовые проблемы защиты общества от компьютерных преступлений // Проблемы уголовной ответственности и наказания : сб. материалов Междунар. науч.-практ. конф., посвящ. памяти профессоров В. А. Елеонского и Н. А. Огурцова, Рязань, 24 мая 2024 г. Рязань : Академия права и управления ФСИН, 2024. С. 12–17.

3. Сорокун Н. С., Ермакова О. В. Особенности квалификации, выявления, устранения причини условий совершения киберпреступлений на современном этапе // Алтайский юридический вестник. 2023. № 3. С. 133–138.

4. Лопатина Т. М. Условно-цифровое вымогательство, или кибершантажа // Журнал российского права. 2015. № 1. С. 118–126.

5. Осужден студент, разоривший DDoS-атаками Тинькова и Касперского на 11 млн руб. URL: https://pravo.ru/news/view/114299/ (дата обращения: 10.11.2024).

6. Павлова А. А., Игнатьева Т. И. Особенности динамики компьютерной преступности и проблемы ее латентности // Право и государство: теория и практика. 2023. № 7 (223). С. 411–415.

7. Дворецкий М., Копырюлин А. Проблемы квалификации преступлений, сопряженных с созданием, использованием и распространением вредоносных программ // Уголовное право. 2007. № 4. С. 29–33.

8. Дьяченко Н. В., Отакулов А. С., Шатомиров И. С. Причины киберпреступлений и методы предосторожности // Modern Science. 2019. № 5–3. С. 242–245.

9. Приговор Солнцевского районного суда г. Москвы от 16.06.2021 по делу № 1–339/2021 // Архив Солнцевского районного суда г. Москвы за 2021 г.

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

11. Бабурин В. В. Причины и условия преступлений, совершаемых в сфере информационно-коммуникационных технологий // Вестник Карагандинской академии Министерства внутренних дел Республики Казахстан им. Баримбека Бейсенова. 2022. № 4. С. 140–143.

12. Бражник С. Д. Преступление в сфере компьютерной информации: проблемы законодательной техники : дис. … канд. юрид. наук. Ижевск, 2022.

13. О связи: Федеральный закон от 07.07.2003 № 126-ФЗ (действ. ред.). URL: http:// www.consultant.ru (дата обращения: 30.11.2024).

14. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.06.2006 № 149-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/?ysclid=m4e52tzjwb468035272) дата обращения: 30.11.2024).

15. Уголовный кодекс Российской Федерации от 13.06.96 № 63-ФЗ. URL: https://consultant.ru (дата обращения: 29.11.2024).

16. Чимаров С. Ю. О новом уровне информационной безопасности России в контексте современных решений по правовому регулированию отрасли квантовых коммуникаций // Международный журнал гуманитарных и естественных наук. 2023. № 7–2. С. 239–241.

17. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 14.10.2024) (с изм. и доп., вступ. в силу с 21.10.2024). URL: https://www.consultant.ru/document/cons_doc_LAW_34661/?ysclid=m2ora1lmxb256082525 (дата обращения: 21.11.2024).

18. Гражданский кодекс Российской Федерации. URL: https://www.consultant.ru/document/cons_doc_LAW_5142/?ysclid=m2orc4y9wo702178414 (дата обращения: 21.11.2024).

19. 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.

20. Дубень А. К. Обеспечение информационной безопасности правовыми методами регулирования // Право и государство: теория и практика. 2023. № 10. С. 125–127.

21. Павлов О. С., Чернов Ю. И. Вопросы административно-правового регулирования в области информационной безопасности // Эпомен. 2021. № 57. С. 295–300.

22. Евдокимов К. Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. 2019. № 1 (35). С. 86–93.

23. Кодзов Т. Н. Совершенствование методов противодействия киберпреступлениям в современных условиях // Пробелы в российском законодательстве. 2023. Т. 16, № 5. С. 222–226.

24. Николаева М. О. Информационная безопасность: современная картина проблемы информационной безопасности и защиты информации // Мониторинг. Образование. Безопасность. 2023. Т. 1, № 1. С. 51–57.

25. Суслов В. А. Информационная безопасность как форма экономической безопасности // Наука через призму времени. 2023. № 4. С. 38–40.

26. Полетаева И. В. Десять правил кибербезопасности // Survival. 2011. Т. 53, № 3. С. 119–132.