

## Борьба с посягательствами на компьютерную информацию.

Текст научной статьи по специальности «Право»

Кулумбегов Георгий Мерабович  
40.04.01 Юриспруденция  
Магистрант, МФПУ СИНЕРГИЯ

**Аннотация:** Киберпреступность признана глобальной международной проблемой. Наибольшая трудность, стоящая перед правоохранительными органами, заключается в невозможности эффективно координировать свои действия через государственные границы, рамки различных юрисдикций и законодательных систем. Противодействие киберпреступности подразумевает целую систему мероприятий, включающую в себя анализ объективных условий, порождающих преступление, механизмов их совершения, способов выявления, пресечения, расследования; опыт судебного рассмотрения. Необходимо также создать эффективные механизмы внедрения результатов уголовно-правовых и криминологических изысканий в законодательную и нормотворческую практику, а также обучение сотрудников правоохранительных органов. В рамках комплексного подхода к борьбе с киберпреступностью и Интернет-мошенничеством должен быть решен ряд общих и частных научно-практических задач.

**Abstract:** Cybercrime is recognized as a global international problem. The greatest difficulty facing law enforcement agencies is the inability to effectively coordinate their actions across State borders, the framework of various jurisdictions and legislative systems. Countering cybercrime implies a whole system of measures that includes an analysis of the objective conditions that give rise to a crime, the mechanisms of their commission, methods of detection, suppression, investigation; experience of judicial review. It is also necessary to create effective mechanisms for introducing the results of criminal law and criminological research into legislative and rule-making practice, as well as training law enforcement officers. As part of an integrated approach to combating cybercrime and Internet fraud, a number of general and particular scientific and practical tasks should be solved.

**Материалы и методы:** основу исследования составили Конституция Российской Федерации, уголовное и уголовно-процессуальное законодательство, судебные и нормативные правовые акты РФ, статистические данные о состоянии и динамике преступности в Российской Федерации.

**Materials and methods:** the basis of the study was the Constitution of the Russian Federation, criminal and criminal procedure legislation, judicial and regulatory legal acts of the Russian Federation, statistical data on the state and dynamics of crime in the Russian Federation.

**Методологической основой исследования** послужил общий диалектический метод научного познания, носящий универсальный характер, также методы логической дедукции, индукции, познавательные методы и приемы наблюдения, сравнения, анализа, обобщения и описания.

**The methodological basis of the research** was the general dialectical method of scientific cognition, which has a universal character, as well as methods of logical deduction, induction, cognitive methods and techniques of observation, comparison, analysis, generalization and description.

**Ключевые слова:** КИБЕРПРЕСТУПНОСТЬ / ИНТЕРНЕТ-МОШЕННИЧЕСТВО / РАССЛЕДОВАНИЕ / КРИМИНОЛОГИЯ / ИНТЕРНЕТ / CYBERCRIME / INTERNET-FRAUD / INVESTIGATION / CRIMINOLOGICAL RESEARCH / INTERNET

Современное общество невозможно представить без современных компьютерных технологий. Более того, общество 21 века по праву признается информационным. Вряд ли найдется представитель такого общества, который не сталкивался бы с передачей и получением информации через компьютерные сети. С ростом технического прогресса роль компьютеров как инструмента хранения, обработки и передачи данных давно вышла за свои пределы. Теперь это они представляют важную и неотъемлемую часть социальной жизни граждан, являются связующим звеном между индивидом и обществом. С ростом компьютеризации и развития сетевых технологий стало возможно учиться, работать и отдыхать, используя компьютерную технику и электронную связь, не покидая определенных территориальных границ. Теперь от надежной и бесперебойной работы компьютерной техники зависит не только сохранность и безопасность информации, но и функционирование коммерческих организаций, государственных органов, безопасность и обороноспособность страны в целом.

Результаты проведенного анализа статистических данных о состоянии преступности в 2021 году говорят о том, что оперативная обстановка на территории Российской Федерации остаётся сегодня стабильной и контролируемой. Важно отметить заметное замедление темпов роста зафиксированных ИТ-преступлений, которые совершались с применением информационно-

телекоммуникационных технологий. По итогам 2021 года<sup>1</sup> их число увеличилось несущественно – на 1,4%. Ранее МВД России в своём докладе опубликовало информацию о том, что около 60% всех киберпреступлений связаны с применением Интернета. Причём доля подобных правонарушений выросла на 25%, если сравнивать с показателями 2020 года. В докладе также указано, что около 40% преступлений в информационно-телекоммуникационной сфере совершаются с использованием мобильной связи, но рост таких правонарушений составил только около 2%. Общее число ИТ-преступлений в 2021 составило более 494 тыс., что приблизительно на 7% больше в сравнении с показателями 2020 г. В МВД России также подчеркнули, что около 98,3% всех ИТ-преступлений, которые совершаются с использованием Интернета, выявляются правоохранительными органами. При этом 75% ИТ-преступлений связаны с кражей персональных данных, платёжной информации или денежных средств. Порядка 10% таких преступлений связаны с производством, реализацией, отправкой наркотической и иной запрещенной продукции.<sup>2</sup>

В январе - феврале 2022 года зарегистрировано 79,7 тыс.1 преступлений, совершенных с использованием информационно-

<sup>1</sup> «В 2021 году количество киберпреступлений в России увеличилось на 1,4% // Режим доступа: <https://cisoclub.ru/v-2021-godu-kolichestvo-kiberprestuplenij-v-rossii-uvelichilos-na-14-7/>» (дата обращения 19.03.2022)

<sup>2</sup> «В МВД заявили, что большинство ИТ-преступлений в РФ совершаются с использованием интернета» // Режим доступа: <https://tass.ru/proisshiestviya/13266279>? (дата обращения 19.03.2022)

телекоммуникационных технологий или в сфере компьютерной информации, что на 2,2% меньше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес остался на уровне января - февраля 2021 года и составил 26,3%.<sup>3</sup>

Все это означает, что в ближайшем будущем Россия вполне вероятно столкнется с ситуацией, в которой быстрый рост и повсеместное внедрение во все аспекты жизни общества современных компьютерных технологий приведет к еще более значительному скачку компьютерной преступности, на который правоохранные органы смогут адекватно отреагировать лишь при условии надлежащего правового обеспечения своей деятельности по противодействию преступности данного вида.

Не вызывает сомнений то обстоятельство, что преступления, совершаемые с использованием современных компьютерных технологий, имеют существенную специфику. Применение технических новинок для совершения противоправных действий позволяет преступникам посягать на наиболее важные охраняемые законом общественные отношения в сфере прав и интересов личности, общества и безопасности государства. Сложность обнаружения действий компьютерного преступника и его возможности совершать преступления в киберпространстве, не имеющем государственных границ, многократно увеличивают степень общественной опасности таких деяний. Многочисленные преимущества современных компьютерных технологий создали новые условия, которые содействуют совершению преступлений на национальном и международном уровнях. Доходы преступников, связанные с незаконным использованием новейших компьютерных технологий, занимают третье место в мире после доходов от торговли наркотиками и оружием.

Для борьбы с преступлениями связанными с компьютерной информацией необходимо также учитывать опыт других стран. В связи с этим, необходимо постоянно проводить мониторинг зарубежного законодательства, устанавливающего уголовную ответственность за компьютерные преступления.

Одной из важнейшей проблемы уголовно-правовых мер в обеспечении информационной безопасности выступает именно проблема, связанная с защитой информации от неправомерного доступа. Данная проблема заключается в том, что защите подлежит наиболее ценная охраняемая информация. Неправомерный

доступ к охраняемой законом информации влечет опасные последствия для общества, главным образом, нарушение ее конфиденциальности, целостности, а также доступности. На сегодняшний день современные уголовно-правовые меры защиты информации от неправомерного доступа основаны на приоритетности защиты информации, которая находится на определенных носителях, и в силу несоответствия такого подхода положениям информационного законодательства, непосредственно влечет отсутствие отчетливой системы уголовно-правовой защиты информации от неправомерного доступа.

Перечисленные факторы предопределили актуальность темы исследования.

Недостаток комплексных мер противодействия, их противоречивость и фрагментарность, высокая латентность преступности в сфере компьютерной информации приводят к неэффективности выработанных мер ее предупреждения, обуславливая трудности в противодействии и борьбе с данным видом общественно опасных деяний.

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы<sup>4</sup> в качестве приоритетного направления внутренней политики определяет развитие информационных и коммуникационных технологий, формирование информационного пространства и соответствующей инфраструктуры.

Существенное значение для изучения преступлений, совершаемых с использованием компьютерных технологий, имеет анализ истории их развития.

Говоря о ретроспективе преступного использования компьютерных технологий и его законодательного ограничения, следует принимать во внимание, что динамика данных процессов существенно различалась в России и в странах, где компьютерные технологии стали частью общественной жизни значительно раньше. В нашей стране еще в период существования СССР компьютерные технологии в основном использовались для работы в правоохранительной и банковской сферах, в целях обеспечения обороноспособности страны и полного контроля государством, в то время как в зарубежных странах компьютер практически сразу стал существенной частью жизни обычных граждан. Таким образом, в мире проблема противодействия преступлениям, совершаемым с использованием компьютерных технологий, проявилась гораздо раньше и до конца 1990-х гг. стояла гораздо острее, чем в России.

<sup>3</sup> Приложение 1,2 (Показатели сформированы в соответствии с Перечнем N 25, введенным в действие указанием Генеральной прокуратуры Российской Федерации и Министерства внутренних дел Российской Федерации «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» от 29 декабря 2021 г. № 790/11/1)

<sup>4</sup> О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Рос. Федерации от 9 мая 2017 г. № 203 // Собр. законодательства Рос. Федерации. 2017. № 20. Ст. 2901.

В соответствии с результатами нашей исследовательской деятельности мы полагаем, что киберпреступность является актуальной проблемой современного мира, поскольку затрагивает различные сферы общественной жизни и с каждым годом приобретает различные новые формы и вариации, становится более сложной в вопросе борьбы с ней, уменьшения прогрессии, а также поиска и наказуемости преступников. Однако, вместе с развитием киберпреступности растет и количество мер борьбы с ними, что, по нашему мнению, в скорейшем времени позволит научиться продуктивно бороться с ее наиболее часто встречающимися формами.

По степени реализации общественно опасные последствия, как известно, подразделяется на реальный ущерб (вред) и угрозу или опасность их причинения. В трех из четырех случаях главы 28 УК, законодатель предусмотрел в качестве особо отягчающего обстоятельства наступление «тяжких последствий или создание угрозы их наступления» (ст. 272- 274 УК). В этих случаях, достаточно угрозы наступления тяжких последствий. Составы угрозы причинения вреда конструируются законодателем обычно в случаях посягательств на особо ценные объекты (ст. 205. Террористический акт; ч.2 ст. 225. Ненадлежащее исполнение обязанностей по охране ядерного, химического или других видов оружия массового поражения; ст. 247. Нарушение правил обращения экологически опасных веществ и отходов и др.).

Анализ исследуемого состава дает основание утверждать, что законодатель крайне небрежно подошел к формулированию особо квалифицированных признаков ч. 5 ст. 274.1 УК, не используя, устоявшуюся в законодательной практике формулу «если оно (т.е. деяние) повлекло тяжкие последствия или создало угрозу их наступления». Вполне обосновано, на наш взгляд, законодатель использует данную конструкцию «создающих опасность» в составах ст. 272-274 УК, тогда как при охране более значимого объекта (ст. 274.1 УК) законодатель попросту ее игнорирует. Представляется, что в процессе развития уголовного законодательства эта ошибка должна быть исправлена.

Изначально ст. 274.1 УК РФ введена в главу 28 с целью предусмотрения ответственности за деяния, обладающие повышенной общественной опасностью по сравнению с деяниями, отраженными в ст. 272-274 УК РФ и затрагивающими государственные интересы. И эта разница в общественной опасности должна была найти свое отражение в первую очередь в жесткости санкций указанных составов.

Но при сравнении санкций общих и специального состава, эта разница в общественной

опасности прослеживается не достаточно четко. Это касается сравнения ч. 1 ст. 273 УК РФ и ч. 1 ст. 274.1 УК РФ – оба преступления средней тяжести, и санкция вновь вводимого состава позволяет судам назначать наказание меньшее, чем пять лет лишения свободы (от двух до пяти).

Отсутствие нижнего предела размера наказания предусмотренного ч. 3 ст. 274.1 УК РФ - лишение свободы сроком до шести лет, является недостатком, позволяющим сопоставить данную часть с ч. 1 ст. 274 УК РФ, так как у судов есть возможность назначать наказание в виде лишения свободы сроком на два года. И тогда исчезает грань в оценке уровня общественной опасности при квалификации деяния, как по общему, так и специальному составу преступления против компьютерной информации.

Аналогичная ситуация складывается (суд может назначить равные сроки наказания в виде лишения свободы) и при назначении наказания за данные преступления, совершенные групповым способом (за преступления, предусмотренные ч. 4 ст. 274.1 УК РФ и ч. 3 ст. 272, ч. 2 ст. 273 УК РФ).

В заключение остается напомнить о том, что ошибки, допущенные в процессе правотворчества, приводят к снижению качества действующего уголовного законодательства, дефектам правового регулирования, что, в свою очередь, может породить ошибки в правоприменительной деятельности, а это прямой путь к нарушениям прав и законных интересов субъектов правоотношений. Выявленные недостатки законодательной техники при построении уголовно-правовой нормы, закрепленной ст. 274.1 УК РФ, должны быть устранены.

Учитывая, что рассматриваемая статья в УК РФ достаточно новая по сравнению с точкой отсчета появления в свет 28 главы, а преступные посягательства и различного рода кибератаки на критическую информационную инфраструктуру набирают свои обороты и во многом приобретают политический характер, законодателю предстоит еще много вносить поправок в ее содержание.

На наш взгляд, самым эффективным методом профилактики является постоянное упоминание в СМИ о новых способах совершения киберпреступлений. Одной из причин того, что злоумышленники почти перестали звонить, писать сообщения и т.д. своей жертве, является информирование населения о распространенных способах обмана. Например, при поступлении в социальных сетях предложения о вложении инвестиций в какой-либо проект преступники не сообщают практически никакой конкретной информации о проекте, либо отсутствуют данные о самом злоумышленнике. Вторым способом являются разработка и последующее

распространение в СМИ определенных кратких схем, в которых была бы указана информация о безопасном поведении в сети «Интернет» и безопасном использовании мобильных устройств. Третий способ - разработка специальных компьютерных программ, которые либо блокировали бы неправомерный доступ к данным пользователя, либо уведомляли бы о нем. Однако этот способ является самым неэффективным, так как с помощью современных технологий можно обойти практически любую защитную программу.

Таким образом, рассмотренные нами общесоциальные, особенные и индивидуальные меры предупреждения преступлений в сфере компьютерной информации всегда нацелены на решение комплексной задачи. С одной стороны - это противодействие криминогенным детерминантам, создающим ситуации, объективно благоприятствующие совершению преступлений в сфере компьютерной информации или формированию среди определенного контингента, группы, у конкретного лица готовности их совершить. С другой стороны - это воздействие на личность, у которой прогнозируется или конкретно диагностируется склонность к совершению преступлений, с целью ее удержания от совершения.

Система мер предупреждения преступлений в сфере компьютерной информации определяется особенностями данных общественно опасных деяний, личностью преступников, причинами и условиями, способствующими совершению преступлений. Охватываемые данной системой меры являются достаточно многочисленными, они различаются по целям, уровням применения, масштабам, правовой урегулированности, характеру осуществления.

Меры правового характера занимают особое место в числе других мер по предупреждению преступлений в сфере компьютерной информации. Изучение обстоятельств, способствующих совершению преступлений в рассматриваемой сфере, свидетельствует о том, что многие из них связаны с имеющимися пробелами в уголовном, а также базовом «информационном» законодательстве, несовершенством и противоречивостью отдельных норм, регулирующих отношения в сфере защиты государственных, коммерческих секретов.

Данное обстоятельство предопределяет необходимость дальнейшего совершенствования их правового регулирования, связанного с реализацией уже принятых и действующих нормативно - правовых актов в данной сфере, наведением должного порядка в ведомственном и корпоративном регулировании вопросов защиты государственных, коммерческих секретов,

закреплением определенного порядка в толковании норм, регламентирующих процесс обеспечения режима секретности (конфиденциальности) проводимых работ, секретного делопроизводства, противодействия преступлениям в сфере компьютерной информации, разработки рекомендаций по их предупреждению.

Анализ статей 272, 273, 274, 274.1 УК РФ показывает, что именно копирование, модификация, блокирование и уничтожение – все эти свойства охраняются главой 28 УК РФ.

По нашему мнению, такое действие, как «ознакомление» может нанести существенный вред владельцу информации. Поэтому, анализируя все выше сказанное, для более точной квалификации данного преступления я считаю, что необходимо внести изменения в ч. 1 ст. 272 и изложить ее в следующей редакции:

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло несанкционированное ознакомление, уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Так же в ч. 4 ст. 272 УК устанавливается, что деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, наказываются лишением свободы на срок до семи лет. Однако законодатель не раскрывает понятие, о каких тяжких последствиях идет речь, что затрудняет применение данной нормы.

2. Нужно включить в состав ч. 2 ст. 272 УК РФ отношения собственности, тем самым признав потерпевшего обязательным признаком объекта состава преступления и дополнив ст. 272 УК РФ новым квалифицирующим признаком "с причинением значительного ущерба гражданину..."

Все эти факторы доказывают еще раз, что глава 28 УК РФ требует весомых доработок и изменений.

Преступления в сфере компьютерной информации, предусмотренные Уголовным кодексом РФ в главе 28 на сегодняшний день являются одними из наиопаснейших преступлений нового типа. В связи с постоянно развивающимся рынком цифровых технологий для правильной, соразмерной и более точной квалификации данных деяний необходимо в ногу со временем анализировать, прогнозировать и вносить изменения в статьи указанной главы Уголовного кодекса. Это положительно отразится на борьбе с данными видами преступлений и приведет к более качественной защите электронной информации и безопасности.

Деяние, предусмотренное ст. 274 УК РФ,

часто выступает как способ для совершения других преступлений, чаще всего против собственности (хищения денежных средств из банкоматов, платежных терминалов, с банковских счетов и т.д.). В связи с этим считаем целесообразным включить в диспозицию ч. 1 ст. 274 УК РФ мотив "деяние... совершенное из корыстной заинтересованности", по примеру уголовно-правовых норм ст. ст. 272, 273 УК РФ, а также такие мотивы и цели, как "из хулиганских побуждений" и "с целью скрыть другое преступление или облегчить его совершение".

Объективная сторона состава преступления, предусмотренного ч. 1 ст. 274.1 УК РФ, выражается в создании, распространении и (или) использовании вредоносных компьютерных программ либо иной компьютерной информации. Она полностью совпадает с объективной стороной состава преступления, предусмотренного ст. 273 УК РФ.

Конструкция объективной стороны ч. 1 ст. 274.1 УК РФ такова, что предполагает «хорошо известное»/«несомненное» знание виновным вредоносных качеств компьютерной программы или компьютерной информации, предназначенных для неправомерного воздействия именно на КИИ РФ, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или для нейтрализации средств защиты указанной информации. В настоящее время, когда уровень развития компьютерной техники столь высок, а программы достигли чрезвычайной сложности, одни и те же действия часто приводят к разным последствиям (в зависимости от состояния ЭВМ, степени её надежности и защищенности) – воздействие на КИИ, а равно ее уничтожение, блокирование, модификация или копирование может произойти по самой непредсказуемой причине. В подобной ситуации, как нам представляется, презумпция знания закона («хорошо известное»/«несомненное» знание виновным вредоносных качеств компьютерной программы или компьютерной информации) оказывается вполне опровержимой. Исходя из изложенного, представляется целесообразным исключить из диспозиций ст. 273 и

ч. 1, 2 ст. 274.1 УК указание на «заведомость», чтобы избежать проблем при квалификации указанных деяний, которые с неизбежностью будут возникать управомоченителя.

Учитывая, что статья 274.1 в УК РФ достаточно новая по сравнению с точкой отсчета появления в свет 28 главы, а преступные посяательства и различного рода кибератаки на критическую информационную инфраструктуру набирают свои обороты и во многом приобретают политический характер, законодательно предстоит еще много вносить поправок в ее содержание.

Киберпреступность можно считать одной из актуальных и серьезных проблем современного глобального мира, поэтому борьба с преступлениями, посягающими на информационную безопасность, имеет межгосударственное значение. Необходимо выработать международные правила и стандарты противодействия киберпреступности, сформировать единую терминологию и категоризацию преступлений в сфере IT-технологий. Для оказания консультативной помощи при осуществлении нормотворческой деятельности необходимо повысить уровень участия государств в международном правотворчестве по вопросам кибербезопасности и противодействию киберпреступности.

Кроме того, на национальном уровне необходимо качественно повысить уровень специализированной, в том числе криминалистической, подготовки кадров. Следует своевременно улучшать технические возможности подразделений, специализирующихся на расследовании киберпреступлений, что в будущем существенно повлияет на формирование условий, способствующих снижению количества киберпреступлений и их предупреждению.

#### Нормативно - правовые акты:

1. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 09.03.2022) (с изм. и доп., вступ. в силу с 17.03.2022)//"Российская газета", N 113, 18.06.1996, N 114, 19.06.1996, N 115, 20.06.1996, N 118, 25.06.1996
2. Федеральный закон от 04.07.1996 N 85-ФЗ (ред. от 29.06.2004) "Об участии в международном информационном обмене"// "Собрание законодательства РФ", 08.07.1996, N 28, ст. 3347, Прим. Документ утратил силу в связи с принятием Федерального закона от 27.07.2006 N 149-ФЗ.
3. Федеральный закон РФ от 09.07.1993 N 5351-1 (ред. от 20.07.2004) "Об авторском праве и смежных правах"// "Российская газета", N 147, 03.08.1993, Прим. Документ утратил силу с 1

января 2008 года в связи с принятием Федерального закона от 18.12.2006 N 231-ФЗ.

4. Федеральный закон РФ от 23.09.1992 N 3523-1 (ред. от 02.02.2006) "О правовой охране программ для электронных вычислительных машин и баз данных"// Прим. Документ утратил силу с 1 января 2008 года в связи с принятием Федерального закона от 18.12.2006 N 231-ФЗ.

5. Федеральный закон от 07.12.2011 N 420-ФЗ (ред. от 03.07.2016) "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации"// "Собрание законодательства РФ", 12.12.2011, N 50, ст. 7362

6. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" // "Российская газета", N 167, 31.07.2017.

7. Федеральный закон от 26.07.2017 N 194-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" // "Российская газета", N 167, 31.07.2017.

8. Федеральный закон РФ от 21.07.1993 N 5485-1 (ред. от 11.06.2021) "О государственной тайне"// "Российские вести", N 189, 30.09.1993г.

9. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 30.12.2021) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2022) // "Собрание законодательства РФ", 31.07.2006, N 31 (1 ч.), ст. 3448

10. Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 30.12.2021) "О связи" (с изм. и доп., вступ. в силу с 01.03.2022) // "Собрание законодательства РФ", 14.07.2003, N 28, ст. 2895.

11. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" // "Собрание законодательства РФ", 12.12.2016, N 50, ст. 7074

12. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Рос. Федерации от 9 мая 2017 г. № 203 // Собр. законодательства Рос. Федерации. 2017. № 20. Ст. 2901.

13. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО «Издательство «Юрлитинформ», 2001. – 496 с.

14. Гаврилов О.А. Курс правовой информатики. М., 2000; Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право /под ред. Б.Н. Топорнина. Спб., 2001.

15. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Под ред. Г.А. Есакова. 8-е изд., перераб. и доп. [Электронный ресурс]. - М.: Проспект, 2020. // СПС КонсультантПлюс 2020.

16. Кочои С.М. Ответственность за корыстные преступления против собственности /С.М. Кочои. - М., 1998. С. 132.

17. Осипенко, А. Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт / А. Л. Осипенко. – Москва : Юридическое издательство "Норма", 2004. – 432 с.

18. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы /под ред. В.А. Садовнического, В.П. Шерстюка. М., 2002. С. 23-37.

19. Уголовное право зарубежных государств. Общая часть : учебник для вузов / А. В. Наумов [и др.] ; под редакцией А. В. Наумова, А. Г. Кибальника. — Москва : Издательство Юрайт, 2021. — 285 с. — (Высшее образование). — ISBN 978-5-534-06320-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/474186> (дата обращения: 19.03.2022).

20. Уголовное право зарубежных государств. Особенная часть: Учебн. пособие.//Под ред. Ипредисл. КозочкинаИ.Д. –М, 2004. С.49-50.

21. Уголовное право. Общая часть. В 2 т. Том 2 : учебник для вузов / И. А. Подройкина [и др.] ; ответственные редакторы И. А. Подройкина, Е. В. Серегина, С. И. Улезько. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 280 с. — (Высшее образование). — ISBN 978-5-534-12767-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/470469> (дата обращения: 19.03.2022).

Диссертации, авторефераты диссертаций

22. Бессонов, В. А. Виктимологические аспекты предупреждения преступлений в сфере

компьютерной информации : специальность 12.00.08 "Уголовное право и криминология; уголовно-исполнительное право" : диссертация на соискание ученой степени кандидата юридических наук / Бессонов Владимир Анатольевич. – Нижний Новгород, 2000. – 249 с.

23. Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: Дис. ... канд. юрид. наук / С.Д. Бражник. - Ижевск, 2002. С.89.

24. Гайфутдинов Р.Р. Понятие и квалификация преступлений против безопасности компьютерной информации: Дис. ... канд. юрид. наук / Р.Р. Гайфутдинов. - Казань, 2017. С. 308.

25. Егорышев А.С. Расследование и предупреждение неправомерного доступа к компьютерной информации: автореф. дис. канд. юрид. наук. Самара, 2004. С.10.

26. Малыковцев М. М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: Дис. ... канд. юрид. Наук / М.М. Малыковцев. - М., 2007. С. 10.

27. Маслакова Е. А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: дис.. канд. юрид. наук. - Орел, 2008. - 198 с

28. Мещаряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. канд. юрид. наук. Воронеж, 2001, С. 14-15.

29. Мусаева У.В. Розыскная деятельность следователя по делам о преступлениях в сфере компьютерной информации: автореф. дис. канд. юрид. наук. Тула. 2002. С. 18

30. Остроушенко А.В. Организационные аспекты методики расследования преступлений в сфере компьютер-ной информации: автореф. дис. канд.юрид. наук. Волгоград, 2000, С. 4.

31. Рогозин В.Ю. Особенности расследования и предупреждения преступлений в сфере компьютерной ин-формации: автореф. дис. канд. юрид. наук. Волгоград, 1998. С.4

32. Степанов-Егиянц В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект): Дис. ... д- ра юрид. наук. / В.Г. Степанов-Егиянц. - М., 2016. С.396.

33. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : автореферат дис. ... кандидата юридических наук : 12.00.08 / Дальневост. гос. ун-т. - Владивосток, 2005. - 26 с.

34. Чекунов И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности : диссертация ... кандидата юридических наук : 12.00.08 / Чекунов Игорь Геннадьевич; [Место защиты: Моск. ун-т МВД РФ]. - Москва, 2013. - 223 с.

Периодические издания

35. Болгов Р. В. Сообщества пользователей интернет-проектов // Вестник МГИМО. 2013. №1 (28). URL: <https://cyberleninka.ru/article/n/soobshchestva-polzovateley-internet-proektov> (дата обращения: 19.03.2022).

36. Бражник С.Д., Пилясов И.А. Техничко-юридический анализ нормы о неправомерном воздействии на критическую информационную инфраструктуру Российской Федерации (ст.274.1 УК РФ) / С.Д. Бражник, И.А. Пилясов// Евразийское Научное Объединение. 2019. -№8-3 (54). С. 198.

37. Булай Ю. Г., Булай Р. И. Профилактика и противодействие киберпреступности, а также международным киберугрозам // Академическая мысль. 2017. №1. URL: <https://cyberleninka.ru/article/n/profilaktika-i-protivodeystvie-kiberprestupnosti-a-takzhe-mezhdunarodnym-kiberugrozam> (дата обращения: 19.03.2022).

38. Вехов Б.В. Компьютерные преступления: способы совершения, методика расследования. М., 1996. С. 44; Федоров В.И. Борьба с транснациональной организованной преступностью в сфере «высоких технологий» // прокурорская и следственная практика. 1999. №3. С.31.

39. Волеводз А.Г. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации / А.Г. Волеводз // Российский судья. – 2002. - № 9. С. 39.

40. Воробьев В.В. О проблемах реализации уголовно-правовых запретов в сфере компьютерной информации как следствие недостатков в юридической технике // Юридическая техника. 2018. №12. URL: <https://cyberleninka.ru/article/n/o-problemah-realizatsii-ugolovno-pravovyh-zapretov-v-sfere-kompyuternoy-informatsii-kak-sledstvie-nedostatkov-v-yuridicheskoy-tehnike> (дата обращения: 19.03.2022).

41. Гайнелзянова В. Р. Возможности судебной компьютерно-технической экспертизы при расследовании преступлений в сфере компьютерной информации // Вестник УЮИ. 2021. №1



(91). URL: <https://cyberleninka.ru/article/n/vozmozhnosti-sudebnoy-kompyuterno-tehnicheskoy-ekspertizy-pri-rassledovanii-prestupleniy-v-sfere-kompyuternoy-informatsii> (дата обращения: 19.03.2022).

42. Гобозов А.З. Проблема разграничения неправомерного доступа к охраняемой законом компьютерной информации от смежных составов преступления // StudNet. 2020. №9. URL: <https://cyberleninka.ru/article/n/problema-razgranicheniya-nepravomernogo-dostupa-k-ohranyaemoy-zakonom-kompyuternoy-informatsii-ot-smezhnyh-sostavov-prestupleniya> (дата обращения: 19.03.2022).

43. Гончар В. В. Отдельные вопросы совершенствования подготовки кадров, специализирующихся на расследовании преступлений, совершаемым с использованием информационных технологий: сборник статей Международной научно-практической конференции // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения). М., 2018. С. 75.

44. Гребеньков А.А. Копирование информации как признак составов информационных преступлений // Наука, техника и образование. 2016. №9 (27). URL: <https://cyberleninka.ru/article/n/kopirovanie-informatsii-kak-priznak-sostavov-informatsionnyh-prestupleniy> (дата обращения: 19.03.2022).

45. Евдокимов К. Н. К вопросу о причинах компьютерной преступности в России // Известия БГУ. 2010. №5. URL: <https://cyberleninka.ru/article/n/k-voprosu-o-prichinah-kompyuternoy-prestupnosti-v-rossii> (дата обращения: 19.03.2022).

46. Евдокимов К.Н. Особенности субъективной стороны состава преступления при нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) / К.Н. Евдокимов //Мировой судья. – 2019. - №6. С.31.