Федеральное государственное казенное образовательное учреждение
высшего образования «Сибирский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра уголовного права и криминологии

Специальность 40.05.02. Правоохранительная деятельность
Специализация № 1 «Оперативно-розыскная деятельность»
Узкая специализация «Деятельность подразделения по контролю за оборотом наркотических средств и психотропных веществ органов внутренних дел»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
по теме:

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Выполнил:
Слушатель учебной группы П1402
младший лейтенант полиции
Огурцова Дарья Игоревна

Решение о допуске к защите:
К защите допускаем
Начальник кафедры
уголовного права и криминологии
полковник полиции
_____ С.М. Мальков
«30» апреля 2019 г.
Дата защиты:
«18» июня 2019 г.
Оценка: отлично

Руководитель:
кандидат юридических наук, доцент
профессор кафедры
уголовного права и криминологии
полковник полиции
Тепляшин Павел Владимирович

Председатель ГЭК
полковник полиции _____ В.В. Скиба
(специальное звание) (подпись) (инициалы, фамилия)

Красноярск 2019

Оглавление

ВВЕДЕНИЕ

Актуальность темы дипломного исследования. В нашей стране рынок IT-технологий начал развиваться только в начале 90-х годов, но первый платеж в России был осуществлен при помощи сети Интернет лишь в 1998 г., а доля интернет-пользователей не превышала и 1% (для сравнения в США в 1998 г. интернетом пользовались 30% населения). Это не могло не сказаться на низкой криминальной активности. Как следствие, длительное время работы исследователей были интересны лишь узкому кругу специалистов. Но уже на рубеже XX–XXI вв. произошел переход на информационно-коммуникационный путь развития наряду с другими странами мира. Подтверждением этому является стремительное распространение портативный устройств со свободным доступом в информационно-коммуникационную сеть Интернет. Данная ситуация привела к появлению и стремительному развитию качественно новых видов преступлений, которые в научном мире и юридической практике именуются термином «киберпреступления».

Современный мир в настоящее время сложно представить без различных гаджетов, средств связи, электронных устройств с помощью, который человек удовлетворяет свои потребности. Информационно - телекоммуникационные технологии, проникли уже во все сферы жизни человека и общества, являются его неотъемлемой частью, и обеспечивают управление информацией. Однако, совершенствование и развитие IT-технологий, расширение сферы их применения, доступность и широкая распространенность среди населения привело к появлению и неуклонному росту в последние годы преступлений, совершаемых с их использованием. Показателем такого роста является статистические данные, приведенные Генпрокуратурой РФ. Она сообщает, что в 2017 году число преступлений в сфере информационно-телекоммуникационных технологий увеличилось с 65

949 до 90 587. Их доля от числа всех зарегистрированных в России преступных деяний составляет 4,4% - это почти каждое 20 преступление. Распространение получили мошеннические действия, совершенные с использованием электронных средств платежа (статья 159.3 УК РФ). Их количество в первом полугодии 2018 г. возросло в 7 раз. При этом на 19,6% уменьшилось количество расследованных преступлений по указанным статьям (с 903 до 726), выросло на 30,5% (с 790 до 1031) число нераскрытых преступлений. Раскрываемость данных преступлений составила 41,3%. Имели место факты вынесения незаконных постановлений об отказе в возбуждении уголовного дела. Наибольшее число таких фактов зафиксировано, в том числе в Красноярском крае.[1] Исходя, из анализа приведённой выше статистике можно говорить о том, что темпы развития IT-технологий, существенно опережают нынешнее законодательство. И данный недостаток есть не только в уголовном законодательстве, но и в других нормативно-правовых актах, регламентирующих использование IT-технологий.

Повышается общественная опасность преступлений связанных с использованием информационных технологий, так как позволяет лицами занимающимися незаконной деятельностью за короткий период времени и с минимальными материальными затратами получать необходимые сведения для совершения преступлений. Также указанный способ обмена информацией позволяет преступникам напрямую не контактировать с заказчиками, что существенно затрудняет изобличение их законспирированной преступной деятельности. Большую роль в расследование преступлений связанных с использованием информационных технологий, играет уровень специальных знаний у должностных лиц правоохранительных органов, которым предстоит осуществлять поиск и изобличение лиц совершивших эти преступления. Правовая поддержка

[1]Официальный сайт Генеральной прокуратуры.- Российской Федерации URL: http://genproc.gov.ru/smi/news/news-1431104/

борьбы с преступлениями в Интернете, в последнее время, становится одной из приоритетных направлений в государственной политике РФ. Так в Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года, утвержденным Президентом РФ 24 июля 2013 г. Данный документ указывает, что основной угрозой в области международной информационной безопасности является использование информационных и коммуникационных технологий с вредоносными целями. Использование информационных технологий и информационно-телекоммуникационных сетей может быть положено в основу при выделении информационных преступлений как особой группы уголовно наказуемых деяний.[1] В Доктрине информационной безопасности от 5 декабря 2016 г. перечисляются основные сферы общества, в рамках которых совершаются преступления в Интернете: конституционные права и свободы человека и гражданина и кредитно-финансовая сфера[2].

В результате тема, посвященная исследованию уголовно-правовых положений преступлений, совершаемых с использованием информационных технологий, представляется актуальной как в практическом, так и в теоретических аспектах.

Объектом дипломного исследования является общественные отношения в сфере информационных технологий и их уголовно-правовая защита от преступных посягательств.

Предметом дипломного исследования являются уголовно - правовые нормы, устанавливающие ответственность за преступления совершаемых с использованием информационных технологий, соответствующая доктрина и правоприменительная практика.

---

[1] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24 июля 2013 г., N Пр-1753) // Система ГАРАНТ: http://base.garant.ru/70641072/#ixzz5eXRxLWsM

[2] Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 05.12.2016 № 646) // Собрание законодательства Российской Федерации 12.12.2016.

Цель дипломного исследования состоит во всестороннем комплексном изучении и анализе преступлений, совершаемых с использованием информационных технологий.

Достижение указанной цели обеспечивается решением следующих задач:

- рассмотрение общественной опасности преступлений, совершаемых с использованием информационных технологий;

- юридический анализ объективных и субъективных признаков составов преступлений, совершаемых с использованием информационных технологий;

- обобщение практики применения уголовного законодательства по делам о преступлениях, совершаемых с использованием информационных технологий;

- рассмотрение спорных вопросов квалификации общественно-опасных деяний, совершаемых с использованием информационных технологий;

- разработка предложений по совершенствованию соответствующих уголовно-правовых норм и практики их применения.

Методологическую основу дипломного исследования составил диалектический метод познания, а также основанные на нем общенаучные методы познания, анализа и синтеза. В работе нашли свое применение такие методы как системно-структурный, формально-логический и сравнительного правоведения, а также такие приемы сбора и обработки эмпирического материала, как анализ публикаций в периодической печати, анализ документов (решений судов).

Теоретическую основу дипломного исследования составили труды таких ученых как З.И. Хисамова, А.П. Кузнецова, И.В. Калюкарин, Е.А. Маслакова, П.В. Малышкин, В.А. Грошиков, Е.А. Русскевич, Н.Р. Шевко,

З.И. Читая, В.В. Зозуля и других. Вместе с тем, в число авторов, внесших безусловный вклад в развитие научных идей о преступлениях, совершаемых с использованием информационных технологий, можно назвать В.Б. Вехова, Г.И. Волкова, Ю.В. Гаврилина, А.В. Геллера, А.Г. Кибальника, В.П. Коняхина, И.Л. Кочои, В.Н. Кудрявцева, В.Д. Ларичева, О.С. Рудакову, Т.Л. Тропину, И.Г. Чекунова, А.Ю. Чупрову, Н.Г. Шурухнова и некоторых других.

Нормативную базу дипломного исследования составили международные правовые акты, Конституция РФ, Уголовный кодекс РФ, другие федеральные законы, постановления Пленума Верховного Суда РФ.

Практическое значение проводимого исследования заключается в том, что содержащиеся в нем выводы и предложения могут использоваться:

- в правотворческой деятельности по совершенствованию уголовного законодательства;

- в практической деятельности правоохранительных органов.

Структура дипломного исследования определена целями, задачами и логикой исследования. Диплом состоит из введения, трёх глав, объединяющих семь параграфов, заключения, библиографического списка.

Глава 1. Основы уголовной ответственности за преступления, совершаемые с использованием информационных технологий.

§1.1. Анализ международно-правовых актов в сфере противодействия преступлениям, совершаемым с использованием информационных технологий.

Зарубежных стран давно уже по сравнению с Российской Федерацией появились нормы регулирующие ответственность за преступления, совершаемые с использованием информационных технологий. Базовым нормативно-правовым источник в данной сфере можно выделить Конвенцию ООН против транснациональной организованной преступности 2000 г., в которой отражены основные направления межгосударственного сотрудничества в данной сфере.

Основополагающим международным нормативно-правовым актом по борьбе с преступлениями в глобальной сети является Будапештская Конвенция Совета Европы о киберпреступности 2001 г., в которой содержится перечень преступных деяний, состоящий из четырех групп: 1) преступления против конфиденциальности, целостности и доступности компьютерных данных (неправомерный доступ, незаконный перехват, воздействие на информацию и на функционирование систем); 2) преступления, связанные с использованием компьютерной техники (подлог и мошенничество с использованием компьютерных технологий); 3) преступления, связанные с содержанием данных, размещаемых в информационных ресурсах глобальных сетей; 4) преступления, связанные с нарушением авторского и смежных прав[1]. Она определяет киберпреступность как широкий спектр злонамеренных действий, включая незаконный перехват данных, системные помехи, которые нарушают

[1] Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) // Система ГАРАНТ: http://base.garant.ru/4089723/#ixzz5eXgUx0UQ

целостность и доступность сети, и нарушения авторских прав. Другие формы киберпреступности включают незаконные азартные игры, продажу запрещенных предметов, как оружие, наркотики или контрафактных товаров, а также вымогательство, производство, хранение или распространение детской порнографии[1]. На наш взгляд, данная трактовка является скорей не определением, а перечислением видов киберпреступлений. Российская Федерация к рассматриваемой Конвенции не присоединилась. С российской стороны большие нарекания вызывала норма статьи 32 Конвенции, позволяющая любому государству-участнику Конвенции получить доступ к данным, источник которых находится в другом государстве. Так, Б. Васильев считает, что «такого рода доступ к данным будет осуществляться без уведомления компетентных органов государства, в котором находится источник информации»[2].

В 2001 г. в г. Минске (Республика Беларусь) странами СНГ было подписано Соглашение о сотрудничестве в борьбе с преступлениями в области компьютерной информации. Государства-участники оговорили в данном международном документе такие понятия, как «преступления в сфере компьютерной информации», «вредоносные программы» и «неправомерный доступ», определили перечень уголовно наказуемых деяний и формы сотрудничества в области их предупреждения и пресечения. РФ ратифицировала данное соглашение лишь в 2008 г. с оговоркой, что возможен отказ в исполнении запроса компетентного органа другой стороны об оказании содействия в случае, если такое исполнение может нанести ущерб суверенитету или безопасности Российской Федерации[3].

Рассмотрение опыта зарубежных стран позволяет обогатить отечественную науку, критически осмыслить национальное

---

[1] Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве) Будапешт, 23 ноября 2001 года URL: http://mvd.gov.by/main.aspx?guid=4603 (дата доступа 31.01.2018)

[2] РФ поддерживает разработку конвенции по борьбе с киберпреступностью [Электронный ресурс]. — Режим доступа: https://ria.ru./politics/20141028/1030552154.html

[3] Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в области компьютерной информации (Минск, 1 июня 2001 г.) // Исполнительный комитет СНГ. — URL: http://www.cis.minsk.by/page.php?id=866

законодательство, выявить его слабые и сильные стороны. Однако не менее важным является и то, что отчётливое понимание особенностей установления и реализации ответственности за компьютерные преступления является непременным условием эффективного взаимодействия с правоохранительными органами и правовыми системами других государств.

Значительный материал по заявленной теме, конечно же, содержит уголовное законодательство США, которые, пожалуй, одними из первых обратили внимание на проблему действенного противодействия преступлениям, совершаемым с использованием компьютерных технологий. Ответственность за неправомерный доступ к компьютеру, компьютерной системе или компьютерной информации, которые могут быть отнесены к так называемой критической информационной инфраструктуре, предусмотрена §1030 Свода законов США. Данное преступление относится к категории так называемых федеральных преступлений. На уровне сводов законов отдельных штатов выделяются главы о киберпреступлениях (глава 16 Свода законов штата Южная Каролина, глава 815 Свода законов штата Флорида, глава 41 Свода законов штата Арканзас и др.), в рамках которых преступлениями преимущественно признаются неправомерный доступ к компьютерной информации, неправомерная модификация компьютерной информации, создание и распространение в любой форме компьютерной информации, которая заведомо предназначена для совершения преступлений, неправомерное распространение информации о сетевых идентификаторах. В ряду традиционных уголовно-правовых запретов, пожалуй, можно выделить специфический состав преступления, предусмотренный ст. 5-41-204 Свода законов штата Арканзас об ответственности за незаконное использование шифрования.

В отдельных штатах законодатель уделил особое внимание регламентации обстоятельств, которые могут выступать в качестве должной защиты от уголовного преследования за совершение деяния, посягающего на безопасность компьютерных данных. Так, например, Свод законов штата

Нью-Хемпшир в ст. 638.17 оговаривает, что лицо не может подлежать уголовной ответственности в случаях, если:

1) лицо было добросовестно убеждено, что правообладатель компьютера или компьютерной информации уполномочил его или должен был уполномочить на доступ к ним;

2) лицо не знало, не должно было и не могло знать, что доступ был осуществлён вопреки воли правообладателя компьютера или компьютерной информации[1].

Закон о неправомерном использовании компьютерных технологий Великобритании в качестве компьютерных преступлений называет: неправомерный доступ к компьютерной информации (ст. 1), неправомерный доступ в целях совершения иных преступлений (ст. 2), неправомерные действия в отношении компьютерных данных или нарушение правил эксплуатации средств хранения или обработки компьютерной информации (ст. 3) неправомерные действия в отношении компьютерных данных или нарушение правил эксплуатации средств хранения или обработки компьютерной информации, которые повлекли угрозу наступления тяжких последствий (ст. 3ZA), создание, приобретение или распространение компьютерных программ или компьютерной информации для совершения преступлений, предусмотренных статьями 1, 3 или 3ZA (ст. 3A)[2].

Уголовный кодекс Германии отдельно не выделяет группу компьютерных преступлений. В разных главах предусмотрена ответственность за фишинг (ст. 202b), неправомерную модификацию информации (ст. 303a), компьютерный саботаж (ст. 303b), а также выведение из строя особо важных объектов инфраструктуры (ст. 305a)[3].

В Сингапуре ответственность за совершение компьютерных преступлений определяется Законом Сингапура о неправомерном

[1] Электронный ресурс. – Justia Us Law. URL: http://law.justia.com/codes/new-hampshire/2015/title-lxii/chapter-638 (дата обращения: 18.02.2019).
[2] Электронный ресурс. – Legislation.gov.uk. URL: http://www.legislation.gov.uk/ukpga/1990/18/contents (дата обращения: 19.03.2019).
[3] Уголовный кодекс ФРГ // https://constitutions.ru/?p=5854&attempt=1

использовании компьютерных технологий и уголовным законодательством. Заимствуя опыт Великобритании, Закон Сингапура о неправомерном использовании компьютерных технологий устанавливает ответственность за неправомерный доступ к компьютерной информации (ст. 3), неправомерный доступ к компьютерной информации с целью совершения другого преступления (ст. 4), неправомерную модификацию компьютерной информации (ст. 5), несанкционированный доступ к сетям или услугам связи (ст. 6), неправомерное воспрепятствование использованию компьютера (ст. 7), неправомерное предоставление паролей, кодов доступа или иных аналогичных данных (ст. 8)[1].

В соответствии со ст. 3 указанного закона лицо подлежит ответственности за так называемое чистое хакерство, то есть преступление считается оконченным с момента самого неправомерного доступа и не требует наступления каких-либо общественно опасных последствий.

Действующее уголовное законодательство Китая предусматривает ответственность за: неправомерный доступ к компьютерной информации, содержащейся в критической информационной инфраструктуре (ст. 285.1), незаконное изменение данных, хранящихся в компьютерной информационной системе, и незаконный контроль над компьютерной информационной системой (ст. 285.2), распространение компьютерной информации, программ или иных средств для совершения преступлений, предусмотренных статьями 285.1–285.2 (ст. 285.3), неправомерное вмешательство в функционирование компьютерной системы (ст. 286). Самостоятельно криминализовано бездействие провайдеров в случаях их уклонения от исполнения обязательных решений контролирующих органов по блокированию соответствующих интернет-ресурсов, удалению запрещённой компьютерной информации и т.д. (ст. 286а).

[1] Закон Сингапура о неправомерном использовании компьютерных технологий // URL: http://statutes.agc.gov.sg

Кроме того, ст. 287 Уголовного кодекса Китая, не описывая признаков какого-либо компьютерного преступления, содержит общее указание о том, что использование информационно-коммуникационных технологий для совершения других преступлений подлежит юридической оценке по конкретным статьям об ответственности за данные преступления[1].

Закон о киберпреступлениях Австралии классифицирует все преступления, совершаемые с использованием информационно-коммуникационных технологий, на две группы: тяжкие компьютерные преступления и другие компьютерные преступления. К первой группе относятся: неправомерный доступ к компьютерной информации или компьютерной системе в целях совершения тяжкого преступления (ст. 477.1), неправомерная модификация компьютерной информации (ст. 477.2), неправомерное нарушение электронной связи (ст. 477.3). Можно отметить строгость наказаний за данные преступления – от 5 лет до пожизненного лишения свободы. При этом, особенностью санкции ст. 477.1 является то, что она построена по ссылочному принципу – вид и размер наказания определяется санкцией конкретного тяжкого преступления, которое намеревалось совершить лицо, используя информационно-коммуникационные технологии. К иным компьютерным преступлениям австралийский законодатель относит неправомерный доступ к защищённой компьютерной информации (ст. 478.1), неправомерную модификацию компьютерной информации (ст. 478.2), приобретение и хранение (ст. 478.3), а также создание или распространение компьютерной информации или программ с целью совершения киберпреступлений (ст. 478.4).

Уголовный кодекс Норвегии регламентирует ответственность за неправомерный доступ к компьютерной информации (ст. 145)[2]. В ст. 146 (б) самостоятельно выделен запрет на распространение сведений о сетевых идентификаторах (логинах и паролях). Кроме того, в статье 151 (б)

[1] Уголовный кодекс КНР // URL: http://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm
[2] Уголовный кодекс Норвегии // URL: http://www.un.org/depts/los/LEGISLATIONANDTREATIES/PDFFILES/NORpenal_code.pdf

регламентирована ответственность до 10 лет лишения свободы за уничтожение, повреждение или блокирование компьютерной информации или информационно-коммуникационного оборудования, которые повлекли существенное нарушение деятельности органов государственной власти или общественного порядка. Ни одна из Скандинавских стран не устанавливает ответственности за создание, использование и распространение вредоносных компьютерных программ.

В странах СНГ в настоящее время наиболее развёрнутую систему компьютерных преступлений содержит Уголовный кодекс Республики Молдова – всего 10 составов[1]. Отличительной особенностью УК Молдовы является криминализация только такого противоправного воздействия на компьютерные данные или систему, которое повлекло причинение ущерба в крупном размере. Так, уголовно-правовая норма о неправомерном доступе содержит указание на двухуровневые последствия – уничтожение, повреждение, модификацию, блокирование или копирование информации, нарушение работы компьютеров, информационной системы или сети и причинение ущерба в крупном размере. Равным образом уголовная ответственность наступает не просто за преднамеренное изменение, удаление или повреждение информационных данных, производство, импорт, продажу пароля, кода доступа или иных аналогичных данных, с помощью которых может быть получен доступ к информационной системе в целом или ее части, а только при условии, что эти действия повлекли причинение крупного ущерба.

Уголовный кодекс Республики Казахстан содержит девять составов преступлений, посягающих на отношения в сфере информатизации и связи (глава 7). Значимой особенностью уголовного законодательства Казахстана является то, что необходимым последствием неправомерного доступа к охраняемой законом информации, её уничтожения или модификации, а

[1] Уголовный кодекс Республики Молдова // URL: http://online.zakon.kz/Document/?doc_id=30394923#pos=2668;-85

также неправомерного завладения выступают общественно опасные последствия в виде существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства[1].

Практически идентичные списки уголовно-правовых запретов содержат УК Армении, УК Республики Беларусь и УК Таджикистана. При этом следует отметить удачное определение законодателем Таджикистана ответственности за нарушение правил эксплуатации компьютерной системы или сети. В диспозиции статьи содержится прямое указание на форму вины данного преступления – «если это повлекло по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования или причинение иного значительного ущерба». При этом деяния, связанные с умышленным посягательством на целостность и (или) доступность компьютерных данных, должны квалифицироваться либо как модификация компьютерной информации, либо как компьютерный саботаж.

Подводя итог рассмотрению норм уголовного законодательства зарубежных стран, можно отметить тот факт, что мировое сообщество в целом и каждое государство принимает меры по борьбе с преступлениями, совершаемыми с использованием информационных технологий. Но очевидно, что именно совместными усилиями и согласованными действиями можно добиться эффективных результатов в области совершенствования законодательства. И как точно указывает А.В. Чернякова, что принятые документы международных и региональных организаций характеризуются определенной степенью фрагментации с точки зрения криминализации деяний. Так одни больше внимания уделяют проблеме киберпреступности и говорят о ней в широком смысле, как о нарастающей угрозе международной безопасности, включая информационный терроризм, информационные

[1] Уголовный кодекс Республики Казахстан // URL: http://online.zakon.kz/m/Document/?doc_id=31575252#sub_id=2050000

войны. В других документах, нет единого подхода, к разрешению вопроса криминализации деяний, совершаемых в киберпространстве. Такие различия могут оказывать значительное влияние на то, каким образом положения международных документов будут учтены в национальных законодательствах. Большинство стран мирового сообщества согласно, что для борьбы с киберпреступностью требуется укрепление правовых мер, совершенствование законодательства, в том числе в области уголовного права[1].

Анализируя законодательства указанных выше государств, показывает, что зарубежные нормативные акты, в отличие от национальных актов Российской Федерации более тщательно на наш взгляд определяют круг противоправных деяний в сфере информационных технологий, что позволяет эффективнее противодействовать данной угрозе. Считаем необходимым, опираясь на положительный опыт зарубежных стран модернизировать действующее законодательство России в указанной области. Так как отечественное законодательство остро нуждается в коррекции. Не будет преувеличением утверждение, что УК РФ в действующей редакции не отвечает актуальным вызовам и угрозам в части обеспечения безопасности компьютерных данных и компьютерных систем.

§1.2. Социальная обусловленность и общественная опасность преступлений, совершаемых с использованием информационных технологий.

Нормы права создаются не произвольно, они определены социальными причинами и предпосылками. Поэтому использование информационных технологий при совершении преступления следует, рассматривать как

[1] Чернякова А.В. Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации // Юридическая наука и правоохранительная практика. 2018. № 4(46). С. 178.

социально обусловленное явление, являющееся отражением возникающих и существующих в обществе противоречий.

Главным законом, определяющим начала информационный отношений в России, является Конституция РФ от 12 июня 1993 г.[1]. В ней присутствуют краткие формулировки, которые описаны подробным образом в специальных законах и подзаконных актах. Так, в статье 24 установлен запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. В части 4 статьи 29 содержится формулировка о праве каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом; часть 5 этой же статьи провозглашает свободу массовой информации на всей территории суверенного государства. Статья 42 гарантирует право каждого на достоверную информацию о состоянии окружающей среды (ст. 42). Важная норма содержится в пункте «и» статьи 71, согласно которой к ведению Российской Федерации относятся так называемые федеральная информация и связь. По мнению М. А. Федотова, действующий Основной Закон России нуждается в детальной реформе по причине стремительных процессов развития информационного общества и информационного пространства; информационные отношения в Конституции регламентируются крайне скудно, ничего не говорится в ней и о киберпространстве[2].

Большинство ученых важнейшим основанием уголовно-правового запрета признают общественную опасность деяния, так как она выражает возможность наступления таких изменений, которые существенно нарушают условия существования системы, или создают реальную угрозу ее существованию[3]. Экспонентный рост технологий и практически безграничные возможности, открывающиеся в связи с их использованием, были оценены и преступниками. По данным В.С. Овчинского, ИТТ не просто

[1] Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.) (с поправками) // Собрание законодательства Российской Федерации от 4 августа 2014 г. N 31 ст. 4398

[2] Федотов М. А. Конституционные ответы на вызовы киберпространства // Lex Russica. 2016. № 3. С. 164–182.

[3] Коржанский, Н.И. Очерки теории уголовного права / Н.И. Коржанский // Волгоград. 1992. С. 45.

рассматриваются в качестве эффективного способа совершения преступления, но и становятся полноценным оружием ведения «кибервойн внутри преступного мира»[1]. Следует констатировать, что единичные (но масштабные) кибератаки 2017 г. (WannaCry, Petya, NotPetya) вызвали широкий общественный резонанс практически во всех странах.

О масштабах преступности в мире свидетельствуют данные, приведенные в новейших отчетах Международного валютного фонда (МВФ) и Европола. В частности, МВФ прогнозирует экономический ущерб порядка $ 53 млрд в случае глобальной кибератаки. Европол приводит данные о потерпевших от совершенной 12 мая 2017 г. планетарной кибератаки компьютерного вируса WannaCry — 300 тыс. компьютерных пользователей в 150 странах, включая такие объекты критической информационной инфраструктуры, как Национальная служба здравоохранения Великобритании, испанская телекоммуникация компания Telefónica и компания логистики FedEx[2].

Дж. Льюис, старший научный сотрудник Центра Стратегических и международных исследований, считает, что киберпреступность может быть названа одной из самых опасных угроз нашего времени[3]. В чем опасность преступлений, совершаемых с использованием информационных технологий? Отчет CSIS / McAfee за его авторством показал, что в 2017 г. две трети пользовотелей сети Интернет - более двух миллиардов человек – стали жертвами киберкраж, взломов или хищения личной информации. Как указано в отчете: «Киберпреступность неумолима, ничем не ограничена и вряд ли остановится. Это слишком просто и слишком полезно, и шансы быть пойманными и наказанными воспринимаются как слишком низкие. Высококвалифицированные киберпреступники так же технологичны, как и самые передовые компании в области информационных технологий, и,

[1] Страшнее пистолета [Электронный ресурс] // URL: https://www.kommersant.ru/doc/3428093
[2] IOCTA 2017 [Электронный ресурс] // URL: https://www.europol.europa.eu/iocta/2017/index.html
[3] Льюис Дж. Киберпреступность – глобальная угроза 2018 года. // URL: https://www.richardvanhooijdonk.com/en/blog/cybercrime-may-be-the-biggest-global-threat-of-2018/ (дата обращения: 31.01.2018).

подобно им, быстро перешли на внедрение облачных вычислений, искусственного интеллекта, программного обеспечения как услуги и шифрования. Киберпреступность остается слишком простой, поскольку многие пользователи технологий не принимают самых основных защитных мер, а многие технологические продукты не имеют адекватной защиты, в то время как киберпреступники используют как простые, так и передовые технологии для определения целей, автоматизации создания и доставки программного обеспечения и монетизации того, что они крадут[1]. Можно констатировать, что киберпреступность касается всех.

При этом преступления в сфере информационных технологий лидируют в соотношении риска к прибыли. Это преступление с низким уровнем риска, которое обеспечивает высокую отдачу. Квалифицированный киберпреступник может заработать сотни тысяч и даже миллионы долларов практически без шансов на арест или тюремное заключение. Кроме этого, нельзя забывать о моральной оценке таких деяний. В нашем обществе негативно относятся, скажем, к наркоторговцам (достаточно вспомнить дело «Приморских партизан», где основная линия защиты сводилась к тому, что убийства они совершали в отношении наркоторговцев). Хакеры такого социального неприятия не вызывают. Более того, как отмечает Г. Киркпатрик: «Без хакеров 1960-х индустрия ПК никогда бы не достигла успеха, которого она испытывает сегодня. Фактически, компьютерные любители написали большую часть оригинального программного обеспечения»[2]. Таким образом, преступления, совершаемые с использованием информационных технологий, с одной стороны выгодны, с другой – не вызывают этических трудностей, по сравнению с прочими

[1] Льюис Дж. Экономическое влияние киберпреступности не уменьшается. // URL: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd (дата обращения: 31.01.2018).

[2] Киркпатрик Г. Хакерская этика и дух цифрового времени. // URL: https://www.jstor.org/stable/24579606?Search=yes&resultItemClick=true&searchText=hackers&searchText=AND&searchText=subculture&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3Dhackers%2BAND%2Bsubculture%26amp%3Bacc%3Don%26amp%3Bwc%3Don%26amp%3Bfc%3Doff%26amp%3Bgroup%3Dnone&seq=1#page_scan_tab_contents (дата обращения: 31.01.2018).

преступными деяниями. Следовательно, популярность этого вида преступлений будет расти.

Облегчает их совершение доступ к анонимным, безопасным платежным системам, таким как Биткойн. Эта криптовалюта долгое время была излюбленной валютой для рынков DarkNet. Киберпреступники пользуются его анонимностью и децентрализованной организацией для проведения незаконных транзакций, получения платежей от жертв и отмывания доходов. Так, если мы зайдем в Joker.buzz[1] – биржу компромата, добытого, в том числе путем взломов электронных почтовых сетей, то увидим, что информацию продают за биткоины. Аналогичным образом ситуация обстоит и в магазине «Гидра» - крупнейшем русскоязычном магазине, продающим наркотические средства, поддельные денежные знаки и документы. Значит, отследить, кто является покупателем и продавцом, анализируя денежные транзакции, невозможно.

Массовое распространение компьютеров и компьютерных сетей, а также совершенствование программных инструментов для несанкционированного доступа привело к тому, что для совершения компьютерных преступлений перестало требоваться специальное образование: почти любой пользователь может освоить некоторые «хакерские» приемы; в итоге значительно расширился круг субъектов подобных деяний. При совершении деяний запрещенных уголовным законом с использованием информационных технологий лицо стремится, чтобы его личность оставалась анонимной, что препятствует выявлению, раскрытию и расследованию таких преступлений, следовательно, преступник не может быть привлечен к уголовной ответственности, так его личность неизвестна в связи, с чем смог избежать уголовного преследования и наказания предусмотренного законом. Потому данные категории преступлений носят высокий латентный характер. Для сокрытия личности используются чаще всего новейшее информационное программное компьютерное обеспечение.

[1] Joker.buzz // URL: http://jokerbuzzhyhl5cl.onion/?_locale=ru (дата обращения: 31.01.2018).

Наиболее частым способом сокрытия следов совершения преступлений, совершаемых с использованием информационных технологий является то, что лицо их совершающее использует технические возможности компьютерных сетей и специальные программы, которые осуществляют маскировку используемого IP-адреса посредствам переадресации на иного интернет-пользователя, который не имеет и не подозревает о совершении для того, чтобы при обнаружении преступления, совершении преступления, совершаемого с использованием информационных технологий. Приобретая опыт и оставаясь при этом безнаказанным, преступники совершенствуют свои способы сокрытия следов совершенных ими преступлений, что еще более усложняет задачу правоохранительных органов для их выявления, раскрытия и привлечения лиц к ответственности.

Вместе с тем киберпреступления наносят огромный ущерб. Например, компьютерный вирус «MyDoom» был впервые обнаружен еще в 2004 году и быстро распространился. Ущерб от вируса был оценен в 38,5 млрд долларов. Всего ущерб от киберпреступности только за 2017 г. оценивается в 600 млрд долларов, или 0,8% мирового ВВП[1]. Помимо финансовых убытков киберпреступники могут причинить вред, распространяя информацию, составляющую тайну частной жизни. Так, организации здравоохранения занимают первое место в списке наиболее уязвимых отраслей. Согласно Darkreading.com, сектор здравоохранения уязвим по ряду причин. Исторически здравоохранению не хватало безопасности. Многие организации здравоохранения используют устаревшие операционные системы и интернет-браузеры, создавая дополнительные уязвимости. Кроме этого, в силу специфики работы больницы и другие организации здравоохранения хранят много личной информации, например, записи пациентов. Эта информация может быть прибыльной для

[1] Льюис Дж. Экономическое влияние киберпреступности не уменьшается // URL: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd (дата обращения: 31.01.2018).

киберпреступников[1]. При этом, борьба с киберпреступлениями осложняется тем фактом, что часто преступные деяния санкционируются государством. К числу таких государств относят Северную Корею. Так, Д. Деннинг отмечает, что для этой страны преступления, совершаемые с использованием информационных технологий, способ удержать тонущую экономику на плаву. С введением экономических санкций профессиональные атаки, поддерживаемые правительством, могут принести бюджету необходимые деньги. По этой причине хакерские атаки координируются, организовываются и финансируются государством. Так, в начале 2016 года хакерами Северной Корей была предпринята попытка похищения 951 млн. долл. США у центрального банка Бангладеш через глобальную финансовую сеть SWIFT. К счастью, из-за опечатки им удалось похитить только 81 миллион долларов[2].

В 2017 году, по данным компании по разработке программного обеспечения в области информационной безопасности и защиты информации «Symantec», 978 миллионов человек в 20 странах пострадали от киберпреступности, т.е. 44% потребителей. Среди наиболее распространенных правонарушений данного вида выделяют: заражение технических устройств вирусом или другая угроза безопасности (53%), мошенничество с дебетовыми или кредитными картами (38%), незаконное использование паролей учетной записи (34%), несанкционированный доступ или взлом электронной почты или аккаунтов в социальных сетях (34%), покупки в интернете несуществующих товаров и услуг (33%), вход в мошенническую электронную почту или использование конфиденциальной (личной/финансовой) информации в ответ на мошенническую электронную почту (32%)[3] .

---

[1] Гринберг И. 12 фактов о киберпреступности. // URL: https://www.blue-pencil.ca/top-12-cyber-crime-facts-and-statistics/ (дата обращения: 31.01.2018).

[2] Деннинг Д. Растущая криминальная угроза в Северной Корее // URL: https://theconversation.com/north-koreas-growing-criminal-cyberthreat-89423 (дата обращения: 31.01.2018).

[3] TAdviser. Государство. Бизнес. IT [Электрон. ресурс] // URL: http://www.tadviser.ru/index.php/.(дата обращения: 01.04.2019).

В сфере бизнеса самыми критичными являются потери от кибератак на финансы компаний. По сведениям Europol, можно выделить основные тенденции киберпреступлений в финансовой сфере:

«Преступление-в-качестве-услуги»: «подпольные цифровые услуги» подкрепляются моделью «преступление-в-качестве-услуги», которая становится все более популярной и востребованной. Она объединяет между собой специализированных поставщиков хакерских утилит и организованные преступные группировки.

«Программы-вымогатели»: вымогательство и банковские «трояны» остаются главными угрозами среди вредоносного программного обеспечения.

Преступное использование данных: сведения остаются ключевым товаром для киберпреступников. Во многих случаях они используются для получения немедленной финансовой выгоды, но все чаще применяются для реализации более сложных схем мошенничества, зашифровываются с целью получения выкупа, либо используются непосредственно для вымогательства.

Платежное мошенничество: EMV (чип и PIN-код), геоблокировка и другие меры безопасности продолжают помогать в эффективной борьбе с карточным мошенничеством, но, тем не менее, растет и число атак, направленных против банкоматов. Организованные преступные группы начинают компрометировать платежи, связанные с использованием бесконтактных карт (NFC).

Социальная инженерия: правоохранительными органами был зарегистрирован рост числа фишингатак, направленные на цели, имеющие Уголовный закон: современное состояние и перспективы развития 249 высокую значимость. Главной угрозой стали атаки против руководящих сотрудников предприятий и организаций[1].

[1] Сивова А.А. Преступления в сфере компьютерных технологий и интернета как угроза национальной и экономической безопасности // Уголовный закон: Современное состояние и перспективы развития: Материалы II Международной научно-практической конференции, приуроченной ко дню принятия Уголовного Кодекса РФ. 2018 с. 248-249.

Также необходимо отметить не только о значительном причинение материального вреда государствам, организациям, теряющим в результате кибератак миллиарды долларов, но и том, что современные киберпреступники финансово заинтересованы и мотивированы на совершение преступлений совершаемые с использованием информационных технологий. Даже можно высказать предположение, что их деятельность стала, приближена к бизнесу и многие из них готовы заниматься ей всю жизнь, легально при этом, нигде не работая, либо лишь формально числиться в какой-нибудь организации в качестве сотрудника. Постепенно киберпреступность модернизировалась в широко разветвленный бизнес с доходами, сопоставимыми с доходами от наркоторговли. И при этом киберпреступнинки стали постоянными участниками организованной экономической преступной деятельности, которые предоставляют свои знания, умения в качестве услуг различного рода мошенникам, террористам, торговцам оружием, наркотиками ради достижения корыстных экономических целей в особо крупных размерах[1].

§1.3. Понятие и виды преступлений, совершаемых с использованием информационных технологий.

В условиях глобальной информатизации одним из важнейших факторов развития и повышения эффективности работы правоохранительных органов являются современные информационные и коммуникационные технологии. Прогресс в информационной сфере обуславливает возникновение негативных тенденций в преступном мире, которые приводят к появлению новых форм и видов преступных посягательств. В связи с этим

[1] Головинов О.Н., Погорелов А.В. Киберпреступность в современной экономике: состояние и тенденции развития // Вопросы инновационной экономики. 2016. №1. URL: https://cyberleninka.ru/article/n/kiberprestupnost-v-sovremennoy-ekonomike-sostoyanie-i-tendentsii-razvitiya (дата обращения: 16.04.2019).

появилась необходимость включение в уголовное законодательство ответственности за преступления связанные с использованием средств массовой информации, электронных или информационно-телекоммуникационных сетей (включая сеть "Интернет").

Развитие информационно-телекоммуникационной инфраструктуры вызвало появление новых форм общественно - опасных деяний, а также ранее не свойственных признаков личности преступника. В связи с этим Е.А. Русскевич в своей статье выделили такое понятие как, информатизация преступности – процесс проникновения кибернетических методов, а также инструментария информационно-коммуникационных технологий в механизм преступления[1]. Преступность, как и другие явления не стоят на месте, приобретают новые формы, используют новые способы совершения преступлений. Напрямую это касается именно тех преступлений, которые совершаются с использованием информационных технологий. Конечно, мы понимаем, что законодатель не способен предусмотреть абсолютно все ситуации, которые могут произойти на практике, но необходимо принимать меры, которые будут способствовать сдерживанию роста преступности по средствам уголовно-правовых предписаний. Для начала необходимо определить, что понимается под информационными технологиями, чтобы выделить преступления, которые относятся к тем, которые совершаются с использованием информационных технологий. Для этого проанализируем ряд нормативно-правовых актов, а также мнения учёных на этот счёт. Так в Указе Президента от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" дано понятие не информационным технологиям, а информационной сфере. Под "Информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно

[1] Русскевич Е.А. Актуальные проблемы уголовно-правовой политики в сфере противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий (ИКТ)// Уголовная политика и культура противодействия преступности материалы Международной научно-практической конференции. Краснодарский университет МВД России. 2016. С. 275.

телекоммуникационной сети "Интернет", сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений[1]". Данное определение включает в себя обширный перечень того, что относится к информационной сфере это и информация, и объекты информатизации, сайты в сети "Интернет", а главное сами информационные технологии. В законе о "Об информации, информационных технологиях и о защите информации" содержится следующее понятие информационных технологий - это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов[2]. Это определение очень схоже с тем, которое дано в Конвенции об обеспечении международной информационной безопасности (концепция), а именно «информационно-коммуникационные технологии» - совокупность методов, производственных процессов и программно-технических средств, интегрированных с целью формирования, преобразования, передачи, использования и хранения информации[3].

Согласно определению ЮНЕСКО, информационная технология – это комплекс взаимосвязанных, научных, технологических, инженерных дисциплин, изучающих методы эффективной организации труда людей, занятых обработкой и хранением информации; вычислительную технику и методы организации и взаимодействия с людьми и производственным оборудованием, их практические приложения, а также связанные со всем этим социальные, экономические и культурные проблемы.

---

[1] Указ Президента "Об утверждении Доктрины информационной безопасности Российской Федерации" от 05.12.2016 № 646.

[2] "Об информации, информационных технологиях и о защите информации". Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 18.12.2018).

[3] Конвенции об обеспечении международной информационной безопасности (концепция), а именно «информационно-коммуникационные технологии // URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения: 25.01.2019).

Следующее определение дает А.В. Суслопаров: «Информационными преступлениями являются общественно опасные противоправные деяния, причиняющие вред общественным отношениям по обеспечению информационной безопасности, способом совершения которых является информационное воздействие или (и) предметом которых является информация как особый нематериальный объект». На наш взгляд основная проблема данных определений заключается в том, что они не выделяют специфику преступлений совершаемых, с использованием информационных технологий. Например, при распространении тайны частной жизни информация также будет «особым нематериальным объектом». Однако, получить эту информацию можно, например, найдя бумажное письмо или подслушав чужой разговор. Таким образом, предложенные термины по большому счету соединяют и хакинг и сбор сведений обычным способом. До настоящего времени мировым сообществом не выработана единая терминология и единый подход к трактовке юридической категории «киберпреступление», употребляемой наряду с понятием компьютерное преступление. В зарубежных странах и в отечественном юридическом сообществе преступления, совершаемые в компьютерных и телекоммуникационных системах, именуются различными понятиями: преступления в сфере высоких технологий, компьютерные преступления, информационные преступления, киберпреступления, преступления в сфере безопасности обращения компьютерной информации, преступления в сфере компьютерной информации и т.д.[1]

Термин «киберпреступление» охватывает собой наиболее полный перечень преступлений в сфере информационных технологий, включая как компьютерные преступления, так и преступления в глобальных коммуникационных системах и сетях. Согласно исследованиям Т.Л. Тропиной, «киберпреступление — это виновно совершенное общественно

[1] Романовский Г. Б. Правовые основы противодействия терроризму в зарубежном праве // Экономика, педагогика и право. 2017. № 2. С. 2.

опасное, уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные, общественно опасные деяния, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера информационному пространству»[1]. Анализируя зарубежные нормативно-правовые источники можно привести определение киберпреступлениям, предложенное ЮНОДК, которые делят киберпреступность на три вида:

1. преступления, в которых компьютерное устройство является целью, например, для получения доступа к сети;

2. преступления, при которых компьютер используется в качестве орудия, например, для запуска атаки типа «отказ в обслуживании» (DoS);

3. преступления, при которых компьютер используется в качестве способа облегчить совершение преступления, например, использование компьютера для хранения незаконно полученных данных[2].

Законом не дано понятие информационных технологий в уголовно-правовом смысле, что вызывает проблемы при квалификации преступлений. Делая вывод из выше перечисленных терминов можно выделить такое определение: информационные преступления как запрещенные уголовным законодательством под угрозой наказания виновно совершенные общественно опасные деяния, механизм совершения которых предполагает использование информационных технологий и (или) информационно-телекоммуникационных сетей (ИТС).

Так же проблемой является то, что отсутствует конкретный перечень преступлений, которые считаются совершенные с использованием

[1] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Дис. … канд. юрид. наук. Владивосток, 2005. 235 с.
[2] ЮНОДК Киберпреступления. URL: https://www.unodc.org/southeastasiaandpacific/en/what-we-do/toc/cyber-crime.html

информационных технологий. Рассматривая составы преступлений через, уже закрепленные уголовным законодательством, можно выделить следующие группы информационных преступлений:

1) специфически информационные преступления — те деяния, которые могут быть совершены только с использованием информационных технологий и (или) ИТС. В первую очередь это компьютерные преступления, но к этой группе можно отнести и, например, компьютерное мошенничество; В нынешнем законодательстве существует глава, посвящённая преступлениям совершаемые в сфере компьютерной информации. Такие как неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ), неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1). Первым отличием данной группы от других в том, что компьютерные преступления содержаться в одной главе, а вот преступления, совершаемые с использованием информационных технологий, разбросаны по всему Уголовному кодексу. Термин «компьютерное преступление» не определен, что, в конечном счете, приводит к универсальности самого установления компьютерного преступления в широком смысле. Законодатель пошел по пути понимания компьютерных преступлений в узком смысле слова, что свидетельствует о выделении особого объекта посягательств. С другой стороны изменения гл. 28 УК РФ показывает, что законодатель расширяет объект преступного посягательства, уйдя от использования термина «ЭВМ».

2) преступления, в которых специальные признаки, предусмотренные в диспозиции статьи. 27 ноября 2016 г. совершила самоубийство, вовлеченная в суицидальную «игру» 12-летняя жительница г.

Северобайкальска Республики Бурятия[1]. Так, наличие суицидального контента было обнаружено на страницах двух школьниц 14 и 15 лет 26 февраля 2017 г. спрыгнувших с крыши 15-этажного дома в г. Усть-Илимске Иркутской области[2].

Участившиеся случаи детской смертности с 2015 по 2017 гг. побудили депутатов Государственной Думы принять качественно новый пакет поправок в УК РФ[3]. Так, в ч. 2 ст. 110 «Доведение до самоубийства» был введен п. «д», предусматривающий ответственность за доведение до самоубийства посредством использования сети Интернет. Также в УК РФ введены статьи 110.1 и 110.2, которые утвердили уголовную ответственность за склонение к совершению самоубийства и за побуждение к самоубийству путем использования информационных сетей (включая Интернет). Этими поправками введена ст. 151.2 УК РФ, предусматривающая ответственность за склонение и вовлечение несовершеннолетних в действия, представляющие опасность для их жизни путем использования информационных сетей (включая Интернет).

3) преступления общеуголовного характера, в которых применение информационных технологий и (или) ИТС существенно облегчает совершение преступного деяния или сокрытие его следов, дает возможность систематического и массового совершения преступных деяний. Например, развратные действия могут быть совершены как при непосредственном контакте, так и через средства интернет-коммуникации, однако, несомненно, во втором случае преступник избегает многих рисков и может воздействовать одновременно на значительное число малолетних. Еще один пример — получение взятки так называемыми «электронными деньгами» или даже денежными суррогатами, такими как криптовалюта Bitcoin. При таком способе совершения преступления исключается непосредственный

[1] URL: https://arigus.tv/news/item/89643/ (дата обращения: 30.04.2019).
[2] URL: http://www.myui.ru/blog/2017-02-27-1092 (дата обращения: 30.04.2019).
[3] ГД в первом чтении приняла законопроект об уголовном наказании за создание «групп смерти» [Электронный ресурс]. — Режим доступа: http://tass.ru./obschestvo/4195820

контакт между взяткодателем и взяткополучателем, крайне затруднительным становится установление факта получения материальной выгоды взяткополучателем.

Так же необходимо рассмотреть в данной группе, так называемые информационные преступления. По мнению В.В. Крылова под информационными преступлениями понимается - «общественно опасные деяния, запрещенные уголовным законом под угрозой наказания, совершенные в области информационных правоотношений»[1]. Информационные правоотношения же определялись им как «отношения, возникающие при: формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации»[2]. Недостатком данного определения является его широта, охват тех преступлений, которые под него подпадают. Кроме того, информационный ресурс – это отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)[3]. Исходя из буквального толкования этого термина «информационным преступлением» можно посчитать кражу книг из библиотеки.

Следует отметить, что на 10-м Конгрессе ООН по предупреждению преступности и обращению с правонарушениями (2000 г., Вена), были предложены сразу два определения киберпреступлений: 1) в узком смысле –

[1] Крылов В.В. Основы криминологической теории расследования преступлений в сфере информации. М. : МГУ, 1998. с. 50.

[2] Гребеньков А.А. Понятие информационных преступлений, место в уголовном законодательстве России и место признаков информации в структуре их состава // Lex Russica. 2018. №4 (137). URL: https://cyberleninka.ru/article/n/ponyatie-informatsionnyh-prestupleniy-mesto-v-ugolovnom-zakonodatelstve-rossii-i-mesto-priznakov-informatsii-v-strukture-ih-sostava (дата обращения: 09.04.2019).

[3] Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации" (с изменениями и дополнениями) (утратил силу).

любое противозаконное поведение в форме электронных операций, направленное против безопасности компьютерных систем и обрабатываемых ими данных; 2) в широком смысле – любое противозаконное поведение, осуществляемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное владение, предложение или распространение информации посредством компьютерной системы или сети.

4) преступления общеуголовного характера, при совершении которых могут использоваться информационные технологии и (или) ИТС, однако значительного влияния на преступный результат это не оказывает. Например, замышляя убийство группой лиц по предварительному сговору, соучастники могут обмениваться сообщениями по сети Интернет, однако существенной роли в механизме преступления это не играет: того же результата и приблизительно с теми же рисками можно было бы достичь и при личном общении, и при использовании телефонной связи. Тем самым, диспозиция статьи хоть и не содержит в себе указание на то, что преступление может совершаться с использованием информационных технологий, но это не является запретом для их использования злоумышленниками.

Законодателем были введены новые составы преступлений в действующий УК РФ и значительным образом отредактированы существующие составы в целях эффективного пресечения киберпреступлений и обеспечения информационной безопасности личности, государства и общества. Однако, для наиболее эффективной борьбы с данными преступлениями необходимо проводить постоянный мониторинг новых способов совершения киберпреступлений, своевременно вносить изменения в действующие составы УК РФ и создавать новые.

Делая вывод из всего вышеперечисленного можно говорить о том, что в настоящее время не существует нормативного определения, которое бы обозначало, что такое информационные технологии, следовательно, нет понимания, какие преступления совершенные с использованием

информационных технологий следует включать в данную категорию. В научной литературе тоже нет единого понимания об информационных технологиях и, что в них входит, но существует широкий выбор, таких определений как информационные, компьютерные, киберпреступления. Анализируя вышесказанное резонно предположить, что все эти группы преступлений связаны с информаций её передачей, хранением, неправомерным завладение, уничтожение и тд. в связи, с чем предлагается ввести понятие общее для этих видов деяний, а именно преступления, совершаемые с использованием информационных технологий.

Глава 2. Юридический анализ преступлений, совершаемых с использованием информационных технологий

§2.1. Уголовно - правовой анализ составов преступлений, совершаемых с использованием информационных технологий

Нормы о преступлениях в сфере компьютерной информации были включены в законодательство в 1996 г. с принятием Уголовного кодекса РФ[1]. За прошедшие с тех пор годы криминальная ситуация в данной сфере значительно изменилась[2].

Компьютерная преступность профессионализировалась: если раньше «хакингом» занимались одиночки-энтузиасты, то сейчас в России и в мире действует значительное число законспирированных организованных преступных групп, извлекающих значительный преступный доход из деятельности, связанной с посягательствами в информационной сфере. В распоряжении этих групп находятся так называемые «ботнеты» — сети из десятков или даже сотен тысяч компьютеров, над которыми установили контроль «хозяева» ботнета и которые скоординировано занимаются определенной деятельностью: подбором паролей, рассылкой рекламных сообщений либо атаками на другие компьютеры.

Компьютерная техника используется для совершения преступлений, посягающих на авторские права; на конституционные права и свободы человека; на экономические и государственные интересы. Имеются примеры использования информационных технологий для осуществления диверсий.

Понятия «информационные технологии» и «информационно-телекоммуникационные сети» определяются Федеральным законом от 27.07.2006 № 149 ФЗ «Об информации, информационных технологиях и

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ (с изменениями и дополнениями от 27.12.2018) // Собрание законодательства Российской Федерации от 17 июня 1996 г. N 25 ст. 2954

[2] Гребеньков А. А. Преступность в сфере высоких технологий: исторический аспект // Известия Юго-Западного государственного университета. Серия «История и право». 2015. № 1-1. С. 184—188.

защите информации»[1]. Информационные технологии — это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Информационно-телекоммуникационная сеть — это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Данные преступления по своей природе являются высокотехнологичными, требующими наличия у преступника определенных знаний и опыта, специального оборудования и (или) компьютерных программ. Это позволяет говорить, что криминологическая характеристика такого вида преступлений будет существенно отличаться от общеуголовной.

Деяния первой группы можно рассматривать как посягающие на один объект: общественные отношения, связанные с использованием информационных технологий и ИТС в законных целях. Они выделены в отдельную главу Уголовного кодекса РФ. Для деяний второй преступления, специальные признаки, уже предусмотренные в диспозиции статьи. Для эффективной борьбы с наркобизнесом и защиты российского общества от наркотической угрозы в 2003 году в Особенную часть УК РФ введена новая статья 228.1, носящая в существующей редакции название «Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества». Часть 2 данной статьи содержит квалифицирующий признак, содержащий формулировку «с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей и сеть «Интернет» и устанавливающий верхний предел наказания в 12 лет лишения

[1] Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями от 18.12.2018) // Собрание законодательства Российской Федерации от 31 июля 2006 г. N 31 (часть I) ст. 3448

свободы. По мнению Н.Ш. Козаева, «дело в том, что преступления, представляющие ядро незаконного оборота наркотиков, и ранее характеризовались как экстерриториальные и транснациональные, а возможности Интернета и вовсе стерли все границы, поэтому такие высокие санкции носят обоснованный характер»[1].

Для преступлений третий группы применение информационных технологий и ИТС должно выступать признаком, дифференцирующим уголовную ответственность. В зависимости от того, насколько существенными являются особенности таких деяний при их совершении в информационной сфере, возможно выделение либо соответствующего квалифицирующего признака, либо специального состава преступления, совершенного с использованием информационных технологий и ИТС.

Для деяний четвёртой группы использование преступником или преступниками информационных технологий и ИТС является нейтральным признаком, который не должен влиять на уголовную ответственность.

В настоящее время, не определено в рамках какого признака состава информационного преступления следует рассматривать непосредственно информацию. Рассмотрим на примере статьи неправомерный доступ к компьютерной информации (ст. 272 УК РФ) относящийся к первой группе. Далее компьютерное мошенничество (ст. 159.6 УК РФ) и ст. 128.1 УК РФ клевета — ее можно отнести к категории общеуголовных преступлений, в которых применение информационных технологий и (или) ИТС существенно облегчает совершение преступного деяния, дает возможность систематического и массового совершения преступных деяний). В законодательной формулировке нормы ст. 128.1 УК РФ информация упоминается при характеристике преступного деяния, ст. 159.6 УК РФ — способа совершения деяния, ст. 272 УК РФ — как деяния, так и преступных последствий.

[1] Козаев Н. Ш. Изменения в уголовной политике в связи с проблемами обеспечения безопасности интернет-пространства // Вестник Санкт-Петербургского университета МВД России. 2015. № 1. С. 48–50.

Противоречивые мнения по данному вопросу могут встретиться даже на разных страницах одного и того же издания. Так, в одном из учебников по уголовному праву в главе, посвященной объекту преступления, говорится: «Поскольку предмет преступления составляют объективно существующие материальные вещи, то его не имеют такие деяния, как клевета (ст. 128.1 УК РФ)», а в разделе, посвященном непосредственно характеристике состава клеветы, указывается противоположное: «Предметом клеветы являются сведения о потерпевшем, которые порочат его честь и достоинство или подрывают его репутацию»[1]. Предметом клеветы такие сведения называют и некоторые другие авторы[2].

В монографии М.В. Демьянца, В.М. Елина и А.К. Жаровой указывается: «Как средство, то есть то, с помощью чего совершалось преступление, информация, к примеру, зафиксирована в составах ст. 128.1 “Клевета”»[3].

Часто информацию не относят к какому-либо конкретному признаку состава преступления, рассматривая характеристики информации в ходе анализа объективной стороны клеветы, переходя к их анализу после рассмотрения признака деяния[4].

Аналогичным образом поступают авторы, рассматривающие ст. 159.6 УК РФ: признаки информации при характеристике данного состава либо не раскрываются вообще, либо описываются в рамках толкования общих понятий и определений[5]. Имеются и иные мнения, так, М.А. Ефремова относит компьютерное мошенничество к группе преступлений, где

---

[1] Уголовное право России. Части Общая и Особенная: учебник / В. А. Блинников, А. В. Бриллиантов, О. А. Вагин [и др.] ; под ред. А. В. Бриллиантова. 2-е изд., перераб. и доп. М.: Проспект, 2015. 1184 с.

[2] Комментарий к Уголовному кодексу Российской Федерации : научно-практический (постатейный) / Н. И. Ветров, М. М. Дайшутов, Г. В. Дашков [и др.] ; под ред. С. В. Дьякова, Н. Г. Кадникова. М. : Юриспруденция, 2016. 912 с.

[3] Демьянец М. В., Елин В. М., Жарова А. К. Предпринимательская деятельность в сети Интернет: монография. М. : Юркомпани, 2014. 440 с.

[4] Комментарий к Уголовному кодексу Российской Федерации (постатейный) : в 2 т. / А. В. Бриллиантов, Г. Д. Долженкова, Э. Н. Жевлаков [и др.] ; под ред. А. В. Бриллиантова. 2-е изд. М. : Проспект, 2015. Т. 1. 792 с.; Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Г. Н. Борзенков, А. В. Бриллиантов, А. В. Галахова [и др.] ; отв. ред. В. М. Лебедев. М. : Юрайт, 2016. 1069 с.

[5] Колоколов Н. А. Преступления против собственности: комментируем новеллы УК РФ // Мировой судья. 2016. № 1. С. 6—15.

информация является средством совершения преступления[1]. А.Ю. Епихин указывает, что в данном составе «факт использования компьютерной информации — средство достижения корыстной цели»[2].

Например, И.Г. Чекунов предлагает рассматривать информацию не как предмет состава преступления, а как предмет уголовно-правовой охраны[3]. Интересным является также указание А.Я. Минина, который, хотя и признает информацию предметом преступления, указывает на то, что она представляет собой «благо особого рода»[4].

Фундаментальное свойство информации заключается в том, что любая «передача» информации на самом деле является ее копированием. Такое свойство информации делает неправомерными аналогии, связывающие информационное взаимодействие и отношения по поводу материальных объектов. Информацию нельзя украсть, в отношении нее не могут быть реализованы классические гражданско-правовые отношения купли-продажи и т.д. «Перемещение» информации представляет собой фикцию: оно представляет собой копирование информации с последующим ее уничтожением у передающего субъекта. Можно выделить следующие признаки информации: самостоятельность сведений, возможность многократного использования, возможность математического анализа, системность и т.д., однако наиболее значимым является именно сохранение информации у передающего и принимающего субъекта.

Поскольку информация не является материей, она нематериальна. Данное логическое построение, хотя и является очевидным, имеет далеко идущие следствия. Нематериальные объекты не могут существовать сами по себе, в объективной реальности они всегда связаны с определенным

[1] Ефремова М. А. Мошенничество с использованием электронной информации // Информационное право. 2016. № 4. С. 19—21.
[2] Епихин А. Ю. Уголовно-правовые аспекты дополнения уголовного закона специальными видами мошенничества // Современное право. 2016. № 10. С. 134—137.
[3] Чекунов И. Г. Понятие и отличительные особенности киберпреступности // Российский следователь. 2014. № 18. С. 53—56.
[4] Минин А. Я. Кибербезопасность и защита информационных систем // Право и кибербезопасность. 2016. № 2. С. 28—35.

материальным субстратом или носителем. Носителем информации является материальный объект или среда.

Предмет преступления — это «то, что непосредственно подвергается преступному воздействию для нанесения вреда объекту посягательства»[1]. Если раньше общепринятым было понимание предмета исключительно как вещи материального мира, то в последнее время стало распространяться более широкое понимание данной категории, которое включает неовеществленные явления внешнего мира и даже субъективные права[2], любые доступные для восприятия, измерения, фиксации и оценки явления внешнего мира, путем воздействия на которые причиняется или может быть причинен вред объекту посягательства[3].

Предмет преступления — это не любой объект, на который воздействует преступник, а лишь тот, в котором «проявляются определенные стороны, свойства общественных отношений (объекта преступления)», что и позволяет причинить путем воздействия на него вред объекту уголовно-правовой охраны. Это свойство предмета является главным в его теоретической характеристике. Оно позволяет отграничить предмет преступления от орудий и средств преступления[4], от иных объектов, с которыми взаимодействует преступник в ходе реализации преступного намерения. Особенности последних характеризуют механизм совершения преступления, а в уголовном праве их признаки раскрываются в рамках характеристики способа совершения преступления[5]. Поэтому предметом преступления может быть признано лишь то, что: а) не совпадает с объектом преступления (общественными отношениями), б) непосредственно выражает

[1] Уголовное право Российской Федерации. Общая часть : учебник для вузов / Н. Н. Белокобыльский, Г. И. Богуш, Г. Н. Борзенков [и др.] ; под ред. В. С. Комиссарова, Н. Е. Крыловой, И. М. Тяжковой. М. : Статут, 2015. С. 86.

[2] Бикмурзин М. П. Предмет преступления: теоретико-правовой анализ. М. : Юрлитинформ, 2016. С. 50—51

[3] Калмыков Д. А. К вопросу о необходимости корректировки понятия «предмет преступления» // Противодействие преступности: уголовно-правовые, криминологические и уголовно-исполнительные аспекты : материалы Российского конгресса уголовного права / отв. ред. В. С. Комиссаров. М., 2014. С. 44.

[4] Энциклопедия уголовного права. СПб : Издание профессора Малинина, 2015. С. 194.

[5] Князьков А. С. Криминалистическая характеристика преступления в контексте его способа и механизма // Вестник Томского государственного университета. Серия «Право». 2014. № 1. С. 51—64.

в себе свойства данного объекта, в) позволяет путем воздействия на него причинить вред объекту преступления.

Исходя из этого и из свойств информации, в качестве предмета преступления ее можно рассматривать только при наличии ее непосредственной связи с объектом посягательства и при условии, что именно информационное воздействие причиняет вред объекту уголовно-правовой охраны.

Рассмотрим характеристики информации в составе клеветы. Чтобы она была признана предметом посягательства необходимо: а) чтобы эта информация непосредственно выражала свойства чести и достоинства как объекта посягательства; б) чтобы воздействие на эту информацию причиняло ущерб данному объекту. Честь и достоинство находят отражение не в заведомо ложной информации о человеке, а в его самосознании и оценке его другими людьми. Воздействие на них и причиняет вред объекту преступления.

Не следует рассматривать заведомо ложные сведения как средство совершения клеветы. В этом случае любая информация, используемая для воздействия на психику людей, является средством совершения преступления. Можно переформулировать диспозицию ст. 128.1 УК РФ следующим образом: «Унижение чести и достоинства лица, подрыв его деловой репутации путем распространения заведомо ложных сведений». В составе клеветы признаки распространяемых лицом сведений следует рассматривать при характеристике способа совершения преступления.

В 2012 году Федеральным законом № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» введена статья 159.6 УК РФ под названием «Мошенничество в сфере компьютерной информации». Способом совершения данного уголовно-наказуемого деяния названы ввод, удаление, блокировка, модификация компьютерной информации, вмешательство иного характера в нормальную работу компьютерных систем и их устройств.

Данный состав явно подразумевает совершение объективной стороны деяния путем использования сети Интернет. Необходимо различать ситуации, когда компьютерная информация вводится в информационную систему и когда осуществляется воздействие уже на имеющуюся в данной системе компьютерную информацию. В первом случае компьютерная информация действительно может рассматриваться как средство совершения преступления, точно так же, как можно рассматривать в качестве средства совершения кражи «электронную отмычку», используемую для открытия кодового замка на входе в хранилище.

В случае с неправомерным доступом к компьютерной информации данная информация близка к предмету преступления. Преступник, осуществляя неправомерный доступ, получает возможность ознакомиться с информацией и совершить определенные действия с ней. Можно говорить о тесной связи информации и общественных отношений по ее охране, которые являются объектом данного преступления.

Информация в формулировке ст. 272 УК РФ фигурирует дважды: при описании действия и последствия. Не всегда фактически это будет одна и та же информация: неправомерный доступ может осуществляться к одной информации, а модифицироваться, блокироваться, уничтожаться или копироваться может и иная информация, обрабатываемая в той же информационной системе. Последствия вполне могут наступить в результате действий лица, получившего неправомерный доступ к информационной системе, но не к информации, в ней обрабатывающейся. Например, путем ввода системных команд лицо может уничтожить или заблокировать информацию, при этом, не имея возможности ознакомиться с ней или воспользоваться ею иным образом.

Ликвидировать этот пробел и избежать «опредмечивания» информации можно изменив формулировку ст. 272 УК РФ, следующим образом: «Неправомерный доступ к информационной системе, повлекший уничтожение, блокирование, модификацию или копирование компьютерной

информации». В такой формулировке характеристика информации будет отнесена к последствиям преступления, а предметом будет выступать информационная система.

Среди законов и нормативно-правовых актов РФ прослеживается определенная система политико-правового регулирования информационных отношений, возникающих в сфере информационных технологий, включая пользование компьютерными и иными устройствами со свободным доступом в сеть Интернет.

Рассмотрим федеральные законы, регулирующие отношения в информационной сфере[1].

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Он регулирует общественные отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, при применении информационных технологий, а также при обеспечении защиты информации.

Федеральный закон от 28 декабря 2010 № 390-ФЗ «О безопасности»[2]. В нем определяются основные принципы и содержание деятельности по обеспечению безопасности личности, общества и государства.

Закон РФ от 27 декабря 1991 г. № 2124-I «О средствах массовой информации»[3]. Данный федеральный нормативно-правовой акт применяется в отношении средств массовой информации, созданных в России и за ее пределами — в части, касающейся распространения продукции СМИ в РФ.

Федеральный закон от 07 июля 2003 № 126-ФЗ «О связи»[4]. Устанавливает правовые основы деятельности в области связи, определяет

[1] Романовский Г. Б. Принципы правотворческой политики: проблемы реализации // Российский журнал правовых исследований. 2015. № 2. С. 45–50.

[2] Федеральный закон от 28 декабря 2010 г. N 390-ФЗ "О безопасности" (с изменениями и дополнениями от 05.10.2015) // Собрание законодательства Российской Федерации от 3 января 2011 г. N 1 ст. 2

[3] Закон РФ от 27 декабря 1991 г. N 2124-I "О средствах массовой информации" (с изменениями и дополнениями от 27.12.2018) // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации от 13 февраля 1992 г. N 7 ст. 300

[4] Федеральный закон от 7 июля 2003 г. N 126-ФЗ "О связи" (с изменениями и дополнениями от 27.12.2018) // Собрание законодательства Российской Федерации от 14 июля 2003 г. N 28 ст. 2895

полномочия органов государственной власти в области связи, права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»[1]. В соответствии с ним, на территории России запрещено распространять среди детей информацию, побуждающую к причинению вреда их здоровью, самоубийству; способную развить порочные наклонности (употребление алкоголя, наркотиков и др.). Регламентируются возрастные ограничения в отношении изображения (описания) насилия, преступлений, смерти, заболеваний, самоубийств, несчастных случаев, аварий, катастроф.

С 2018 года в России действует ФЗ «О безопасности критической информационной инфраструктуры»[2], который создан для обеспечения защищенности объектов критической информационной инфраструктуры государства.

Среди подзаконных нормативно-правовых актов по защите информации предусмотрены рядом следует обозначить указы Президента РФ, постановления Правительства РФ, государственные стандарты, организационно-распорядительные документы ФСБ России и др.

Главным национальным правовым источником по борьбе с киберпреступлениями является Уголовный кодекс Российской Федерации. Данный закон является единственным кодифицированным нормативным правовым актом, устанавливающим преступность и наказуемость деяний на территории России. Кодекс содержит специальную главу 28, в которой перечислены преступления в сфере компьютерной информации: ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание,

[1] Федеральный закон от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" (с изменениями и дополнениями от 18.12.2018) // Собрание законодательства Российской Федерации от 3 января 2011 г. N 1 ст. 48.

[2] Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" // Собрание законодательства Российской Федерации от 31 июля 2017 г. N 31 (часть I) ст. 4736.

использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей».

Как считает Т.М. Хусяинова, «развитие современных информационно-коммуникационных технологий существенно опережает любое законодательное регулирование, так как требует немедленного правового реагирования, а общественная опасность преступлений виртуального характера существенно повышается в связи с постепенным проникновением сети Интернет во все сферы жизни общества, государственные структуры и жизнь каждого человека и гражданина»[1]. Поэтому федеральным законодателем введены новые составы преступлений в действующий УК РФ и значительным образом отредактированы существующие составы. Так, в 2010 г. Федеральным законом от 30.10.2009 № 241-ФЗ была введена новая статья 185.3, именующаяся в действующей редакции «Манипулирование рынком», которая в диспозиции указывает на распространение ложной информации путем пользования информационно-телекоммуникационными сетями, включая сеть «Интернет».

Федеральным законодателем в 2011 г. введен состав преступления в УК РФ — ст. 171.2 «Незаконные организация и проведение азартных игр». Диспозиция данной статьи информирует о том, что данное преступное деяние совершается путем незаконной организация и реального проведение азартных игр. Здесь присутствует формулировка «совершенное путем использования информационно-телекоммуникационных сетей, в том числе сети «Интернет».

Сегодня Интернет стал популярной общественной площадкой для свободного распространения материалов порнографического характера. Федеральным законом от 29.02.2012 № 14-ФЗ были отредактированы ст. ст.

[1] Хусяинов Т. М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования: материалы Всероссийского круглого стола. Иркутск, 2015. С. 120–125.

242 «Незаконные изготовление и оборот порнографических материалов или предметов» и 242.1. «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних». В данные составы добавлены квалифицирующие признаки, содержащие специальную формулировку «с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей, включая сеть «Интернет», что автоматически переводит такие преступления в разряд киберпреступлений.

В августе 2014 года вступил в силу ФЗ «О внесении изменений в статью 280.1 Уголовного кодекса Российской Федерации», который внес значительные коррективы по борьбе с киберэкстремизмом. Так, в статью 280.1. «Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации» введена ч. 2, предусматривающая уголовную ответственность за публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации, которые совершаются посредством использования средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая Интернет). Также в 2014 г. ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства» УК РФ претерпела существенные изменения: в диспозицию добавлена формулировка про информационно-телекоммуникационные сети и про Интернет, что автоматически вводит данное общественно опасное деяние в ранг киберпреступлений.

Из-за роста случаев призывов к совершению террористических актов через сеть Интернет Федеральным законом от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» в ст. 205.2 «Публичные призывы к осуществлению террористической деятельности или публичное оправдание

терроризма» введена ч. 2, которая содержит диспозицию следующего содержания: «Те же деяния, совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет». Вместе с новой частью статьи федеральным законом внесено специальное примечание, содержащее легальную трактовку дефиниции «публичное оправдание терроризма».

В 2017 г. УК РФ дополнен ст. 274.1, которая предусматривает ответственность за противозаконное воздействие на объекты критической информационной инфраструктуры страны.

Таким образом, развитие информационного пространства на территории России стало поводом для появления новых видов общественно–опасных деяний — киберпреступлений[1]. Уголовный кодекс РФ, как единственный отечественный источник уголовного права, содержит соответствующие составы киберпреступлений (включая как главу 28 «Преступления в сфере компьютерной информации», так и отдельные составы), за совершение которых предусматривается соответствующие виды наказания: от денежного штрафа различной градации до лишения свободы.

§2.2. Проблемы квалификации преступлений, совершаемых с использованием информационных технологии

Роль информации в жизни личности, общества и государства в последние годы значительно возросла[2]. В нашей стране вслед за ведущими мировыми державами начался процесс генезиса информационного общества[3]. В настоящее время информационно-телекоммуникационные

[1] Романовская О.В. Акт о патриотизме: ограничения права на неприкосновенность частной жизни в США в целях противодействия терроризму // Наука. Общество. Государство. 2017. Т. 5. № 2.
[2] Жестеров П. В. Манифест уголовной репрессии эпохи дополненной реальности. М.: Проспект, 2017. С. 224
[3] Кобец П. Н. Противодействие угрозам кибersталкинга — важнейшей проблеме, исследуемой в рамках совершенствования аспектов информационной безопасности регионов в условиях глобализации информационного пространства // Вестник Прикамского социального института. 2017. № 1 (76). С. 27–35.

технологии (ИТТ), будучи разнонаправленными высокодоходными способами оборота информации, проникли практически во все сферы человеческой жизнедеятельности.

В России основным источником информации о киберпреступлениях служит статистическая форма 1-ВТ «Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации», которая включает в себя сведения о преступлениях, предусмотренных ч. 1 ст. 138, ст. 138.1, 146, 158, 159, 159.3, 159.6, 165, 1712, 183, 242, 242.1, 242.2, 272, 273, 274 УК РФ.

Киберпреступность продолжает принимать новые формы и новые направления. Например, в Доктрине информационной безопасности Российской Федерации прогнозируется, что в будущем получит развитие трансграничный оборот информации, облегчающий достижение криминальных целей (п. 10). Особую опасность представляют преступления террористического характера[1]. Использование террористами ИТТ способствовало появлению новой криминологической категории — кибертерроризма.

Ведущую роль в противодействии киберпреступности принадлежит мерам уголовно-правового воздействия, эффективность которого, в свою очередь, зависит от оптимальности уголовно-правовой политики в данной сфере правоохранительной деятельности. Как было указано выше, Уголовный кодекс Российской Федерации впервые в себя группу норм, направленных на обеспечение информационной безопасности от общественного опасных посягательств, объединенных в рамках главы 28 «Преступления в сфере компьютерной информации». Отечественный законодатель признал особую общественную опасность деяний, совершенных с использованием информационных технологий. Уголовно-правовые нормы из разных глав УК РФ были дополнены за последние пять

[1] Кобец П. Н. Анализ природы терроризма и его детерминирующих факторов в условиях середины второго десятилетия XXI столетия // Полицейская деятельность. 2016. № 6. С. 596–602.

лет такими признаками составов преступлений, как: использование информационно-телекоммуникационных сетей, в том числе сети Интернет (ч. 3 ст. 137, ч. 1 ст. 159.6, ч. 1 ст. 171.2, ч. 1 ст. 185.3, ч. 2 чт. 205.2, п. «б» ч. 2 ст. 228.1, п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242.1, п. «г» ч. 2 ст. 242.2, ч. 2 ст. 280, ч. 2 ст. 280.1, ч. 1 ст. 282 УК РФ); использование электронных сетей (ч. 1 ст. 185.3, ч. 2 ст. 205.2, п. «б» ч. 2 ст. 228.1, ч. 2 ст. 280.1 УК РФ); использование средств связи, в том числе подвижной связи (ч. 1 ст. 171.2 УК РФ). В настоящее время в Государственной Думе Российской Федерации обсуждается предложение по криминализации понуждения несовершеннолетних к действиям сексуального характера через сеть «Интернет», создание и оборот порнографических видеоматериалов с несовершеннолетними, что в полной мере отражает общемировые тенденции законодательного регулирования противодействия киберпреступности.

Проблема противодействия преступлениям, совершаемым в сфере использования информационно-коммуникационных технологий, продолжает оставаться одной из наиболее злободневных. Федеральным законом от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» введена ответственность за квалифицированные виды мошенничества, среди которых и преступления, совершаемые с использованием информационно-коммуникационных технологий: ст. 159.3 «Мошенничество с использованием платежных карт» и ст. 159.6 «Мошенничество в сфере компьютерной информации».

Инициатором изменений выступил Верховный Суд РФ. Позиция судебного органа объясняется тем, что «конкретизация в УК РФ составов мошенничества, в зависимости от сферы правоотношений, в которой они совершаются, должна была уменьшить число ошибок и злоупотреблений при

возбуждении уголовных дел о мошенничестве, способствовать повышению качества работы по выявлению и расследованию таких преступлений»[1].

В своей статье В.В. Хилюта отмечает сомнительность наличия такого неотъемлемого признака мошенничества, как «обман»: «Компьютер, как и замок у сейфа, нельзя обмануть, поскольку технические устройства лишены психики»[2]. Возможен обман только физического лица, которое вследствие введения его в заблуждение передает добровольно свое имущество преступнику. Н.Ш. Козаев также отмечает экстраполяцию общих признаков мошенничества на рассматриваемый состав[3].

Противники указанной позиции отмечают, что обман, напротив, имеет место быть, т.к. при несанкционированном видоизменении компьютерной информации возникает искажение действительности в сознании человека, эксплуатирующего модифицированную систему, что можно отнести к обману, как к искажению истины[4].

Отсутствие системности в действиях законодателя привело к тому, что ряд составов, предусматривающих ответственность за незаконные манипуляции с использованием информационно-коммуникационных технологий, находятся в отношениях полной или частичной конкуренции.

Перечень альтернативных действий по совершению мошенничества в сфере компьютерной информации гораздо шире перечня последствий, возможных при неправомерном доступе. Особенно это противоречие наблюдается при неоконченном преступлении, когда установить умысел на хищение чужого имущества достаточно сложно. Конкурируют между собой и квалифицирующие признаки указанных статей: неправомерный доступ к охраняемой законом компьютерной информации, повлекший указанные в

---

[1] О проекте Федерального закона № 53700-6 «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации»: письмо Верховного Суда РФ от 25 мая 2012 г. № 2-ВС-2733/12. // СПС «КонсультантПлюс».

[2] Хилюта В.В. Уголовная ответственность за хищения с использованием компьютерной техники // Журн. рос. права. 2014. № 3. С. 111–118.

[3] Козаев Н.Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): / под. ред. А.В. Наумова. М., 2015. С. 88.

[4] Воронцова С.В. К вопросу о квалификации преступлений в сфере электронных платежей // Банковское право. 2015. № 1. С. 35–37.

законе последствия, причинивший крупный ущерб или совершенный из корыстной заинтересованности, идентичен по содержанию мошенничеству в сфере компьютерной информации, совершенному в крупном размере. Так, если лицо из корыстных побуждений осуществило неправомерный доступ к системе «Банк-клиент», повлекший модификацию информации о средствах на счету законного пользователя системы в пользу злоумышленника, то его действия содержат признаки хищения, т.к. имущественные права на активы, переведенные со счета законного владельца, были нарушены. Был осуществлен неправомерный доступ из корыстной заинтересованности, повлекший модификацию информации и, как следствие, причинение крупного ущерба. В анализируемой ситуации имеет место коллизия уголовно-правовых норм, поскольку фактически они устанавливают ответственность заодно и то же деяние.

Ст. 159.6 УК РФ является специальной по отношению к ст. 272, 273 УК РФ, поскольку неправомерный доступ к компьютерной информации из корыстной заинтересованности представляет собой действия, направленные на хищение, т.е. компьютерная информация, выступает средством доступа к чужому имуществу, что охватывается объективной стороной ст. 159.6 УК РФ, ввиду чего в силу ч. 3 ст. 17 УК РФ дополнительной квалификации по ст. 272, 273 УК РФ преступных посягательств в IT-сфере не требуется.

Относительно ситуации, связанной с использованием подложной карты для оплаты товаров в торговых и иных организациях, можно отметить, что законодателем указанные неправомерные действия криминализованы в рамках ст. 159.3 УК РФ, однако под объективную сторону рассматриваемой статьи подпадает мошенничество конкретно указанным способом – путем обмана сотрудника кредитной, торговой или иной организации в подлинности карты и ее принадлежности. Под уголовно-правовой запрет подпадают действия, характеризующиеся сознательным сообщением заведомо ложных, не соответствующих действительности сведений

работнику банка, например оператору, либо сотруднику магазина или кассиру.

Иные виды незаконных действий по использованию платежной карты под действие данной нормы не подпадают и должны быть квалифицированы либо по ст. 158 УК РФ как тайное хищение – при использовании банкомата (в соответствии с разъяснениями, данными в постановлении Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате»[1]), либо по ст. 159.6 УК РФ – при иных видах хищений и использовании различных видов информационно-коммуникационных технологий.

Правоохранительные органы также сталкиваются со случаями совершения преступлений путем использования нескольких разновидностей информационно-коммуникационных технологий: возможностей сети Интернет с созданием и распространением вредоносных программ, влекущих неправомерный доступ к компьютерной информации, которая впоследствии необходима для создания поддельной (подложной) карты, используемой через систему АТМ-банкинга либо для осуществления платежей с использованием онлайн-банкинга. Деяния должны быть квалифицированы по совокупности различных составов УК РФ. Если с квалификацией действий злоумышленников по использованию вредоносных программ и неправомерному доступу ситуация более или менее ясная, то вопрос, как быть с изготовлением подложной карты и использованием ее реквизитов, требует изучения.

8 июня 2015 г. был принят Федеральный закон № 153-ФЗ «О внесении изменений в ст. 187 Уголовного кодекса РФ», вступивший в силу 19 июня 2015 г. Данным законом полностью изменены название ст. 187 УК РФ и диспозиция, в то время как санкция осталась прежней. Так, в статью включен ряд противоправных и альтернативных действий со средствами платежа,

[1] Постановление Пленума Верховного Суда РФ от 27 декабря 2007 г. N 51 “О судебной практике по делам о мошенничестве, присвоении и растрате” // ГАРАНТ.РУ: http://www.garant.ru/products/ipo/prime/doc/1685377/#ixzz5eXnB4h9J

таких как приобретение, хранение, транспортировка в целях использования или сбыта, а статья получила название «Неправомерный оборот средств платежей».

Указание в диспозиции рассматриваемой нормы на создание компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств создает конкуренцию со ст. 273 УК РФ, предметом которой является «компьютерная программа либо иная компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации».

Неправомерный оборот средств платежей выражен рядом альтернативных действий: изготовление, приобретение, хранение, транспортировка в целях использования или сбыта, а равно сбыт средств платежей, таких как поддельные платежные карты, распоряжения о переводе денежных средств, документов или средств оплаты, электронные средства, электронные носители информации, технические устройства, компьютерные программы, предназначенные для неправомерного осуществления приема, выдачи и перевода средств.

К числу первоочередных мер следует отнести криминализацию компьютерного саботажа и неправомерного изменения идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создания, использования, распространения программ для изменения идентификационного кода абонентского устройства.

Глава 3. Оптимизация уголовной ответственности за преступления, совершаемые с использованием информационных технологий

§3.1 Оптимизация уголовной ответственности на основе взаимодействия с международными организациями в сфере противодействия преступлениям, совершаемым с использованием информационных технологий.

По данным Международного союза электросвязи (МСЭ), специализированного агентства по информационно-коммуникационным технологиям ООН, в 2010 году более 62 млн жителей России регулярно пользовались Интернетом. К концу 2018 года количество пользователей составило 110 млн, что соответствует 76.2% населения России. Распространение мобильной широкополосной связи также продолжает расти и к концу 2019 года составило свыше 227 млн абонентов.

Фрагментация на международном уровне и разнообразие национального законодательства в области борьбы с преступностью, совершённой с использованием информационных технологий, привели к тому, что в последние годы было обнародовано множество документов, в том числе международных по вопросам борьбы с указанными преступлениями, в частности Конвенция Совета Европы «О киберпреступности» 2001 года[1], Директива ЕС «О нападениях на информационные системы» 2013 года, однако четкой и согласованной рамочной основы по-прежнему не хватает. Еще одним фактором является восприятие “низкого риска”, связанного с преступлениями в сфере информационных технологий ввиду их большой латентности. Мы уже указывали выше на то, что киберпреступность имеет по определению транснациональный характер. И в своей статье В.А.

[1] Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) // СПС КонсультантПлюс

Номоконов и Т.Л. Тропина говорят о том, что как «Борьба же с преступностью в области международных компьютерных сетей усложняется по оценкам экспертов ООН, по трём основным причинам. 1) Для расследования преступлений в электронной среде требуются специальные знания и опыт. 2) Интернет представляет собой открытую среду, дающую пользователям возможности совершать определённые действия за пределами границ государства, в котором они находятся. В то же время следственные действия правоохранительных органов в целом ограничиваются пределами собственного государства. 3) Открытые структуры международных компьютерных сетей позволяют пользователям выбирать такую правовую среду, которая оптимальным образом соответствует их целям. Т.е. пользователи могут выбирать такие страны, в которых определённые деяния, совершаемые в электронной среде, не влекут за собой уголовную ответственность. Наличие подобных «информационных убежищ» может сдерживать усилия других государств по борьбе с преступностью с использованием компьютерных сетей»[1].

Правовые меры играют важную роль в борьбе с преступностью в сфере информационных технологий и должны охватывать различные области, начиная от материального аспекта и заканчивая уголовно-процессуальным правом, а также вопросы юрисдикции. Однако необходимо уделять должное внимание трем вопросам: профилактике путём оценки угроз, информационно-пропагандистской деятельности и повышению осведомлённости.

В 2017 года Европол принял довольно структурированную методологию стратегического анализа особенностей организованной преступности (SOCTA). Данная методология, разработанная для анализа угрозы, создаваемой организованными преступными группами, может быть

[1] Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. №24. URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza (дата обращения: 15.04.2019).

использована с учетом соответствующих различий для изучения специфики угроз преступлений в сфере информационных технологий[1].

Интернет сделал географические соображения практически не актуальными, ввиду чего необходимо, чтобы правоохранительные органы взаимодействовали как с государственными, так и с частными заинтересованными структурами, возможно через создание координационного центра.

В рамках ЕС эту роль выполняет Европейский центр по борьбе с Киберпреступностью (ЕС3), который, после его основания в январе 2013 года является коллективным органом ЕС в борьбе с киберпреступностью. ЕС3 поддерживает операции, активно участвует в исследованиях, обучении сотрудников и профилактике преступлений, а также регулярно поддерживать связь с рядом учреждений и органов ЕС. Схожая инициатива предпринята 20.07.2018 по результатам заседания Совета министров внутренних дел стран СНГ, в ходе которого запланировано открытие в России дополнительного учебного заведения для подготовки сотрудников для органов внутренних дел стран Содружества.

Зачастую преступления в сфере компьютерной информации являются результатом деятельности транснациональной организованной преступности, правоохранительным органам при раскрытии таких преступлений не обойтись без взаимодействия с иностранными коллегами. Правоохранительные органы получают информацию через Национальное центральное бюро Интерпола России из Международного банка криминальной информации, который обеспечивает закрытая глобальная компьютерная Система криминальной информации[2].

---

[1] European union serious and organised crime threat assessment 2017. URL: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.

[2] Менжега М. М. Информационное взаимодействие работников правоохранительных органов при расследовании преступлений в сфере высоких технологий / М. М. Менжега // Международный научно-исследовательский журнал. — 2012. — №5 (5). — С. 9. — URL: https://research-journal.org/law/informacionnoe-vzaimodejstvie-rabotnikov-pravooxranitelnyx-organov-pri-rassledovanii-prestuplenij-v-sfere-vysokix-texnologij/ (дата обращения: 01.05.2019).

Органы внутренних дел направляют запросы при раскрытии и расследовании преступлений в области высоких технологий, имеющих международный характер:

- неправомерный доступ или подключение к ЭВМ, системе ЭВМ или их сети;
- нарушение правил эксплуатации компьютерной или телекоммуникационной системы с целью избежать оплаты полученных услуг;
- внесение в технические средства или программное обеспечение компьютерных систем изменений, приводящих к уничтожению, блокированию или модификации информации (компьютерные "бомбы" и вирусы);
- компьютерные мошенничества и фальсификации с банкоматами, платежными средствами, игровыми автоматами;
- компьютерные мошенничества с базами данных, компьютерными и телекоммуникационными системами;
- неправомерное воспроизведение элементов компьютерной техники, программного обеспечения, в том числе компьютерных игр;
- сознательное неисполнение должностным лицом своих обязанностей, правил эксплуатации технических или программных средств компьютерных систем;
- использование ЭВМ, их систем и сетей, всемирной сети Интернет в противозаконных целях, для размещения и обмена нелегальным программным обеспечением, хакерской информацией, детской порнографией;
- хищение профессиональных тайн и промышленных секретов (промышленный шпионаж)[1].

[1] Приказ МВД России № 221 от 28 февраля 2000 г. «О мерах по совершенствованию сотрудничества по линии Интерпола» // СПС «Гарант»

Таким образом, компьютерные преступления являются одним из самых распространенных видов преступлений. Это в первую очередь связано с массовостью распространения компьютеров, ведь в настоящее время компьютер стал столь же обычной принадлежностью нашего быта, как и холодильник или, скажем, телевизор. В связи с этим вполне обоснованно появились рассуждения о потенциальных возможностях, которые таят в себе компьютерные сети. Нечистоплотная, а тем более преступная манипуляция компьютерной информацией представляет сегодня реальную опасность информационной безопасности не только для отдельного человека, но и для всего российского общества и государства. Развитие компьютерных технологий просто немыслимо без внедрения и развития информационного поля Интернет[1].

В своей статье К.И. Попов, указывает на то, что в настоящее время отсутствует унифицированная система, которая включала бы в себя формулировки конкретных условий, принципов, требований, стандартов и критериев для обозначения и подробного описания феномена компьютерной преступности, а также однозначно характеризующая, фиксирующая и регистрирующая все совершенные компьютерные преступления, процесс их подготовки и попытки осуществления[2]. Так как преступлений данной категории причиняют ущерб и наносят вред интересам не только отдельного взятого государства, а всего мирового сообщества в целом, а также проблемой является то, что субъект, совершающий противоправные деяния зачастую находится на территории другого государства. Совершенствование правовых механизмов: улучшение правовой базы борьбы с данным видом преступлений, оптимальное решение проблем криминализации общественно

[1] Попов К.И. Компьютерные преступления — преступления мирового масштаба // Правопорядок: история, теория, практика. 2013. №1 (1). URL: https://cyberleninka.ru/article/n/kompyuternye-prestupleniya-prestupleniya-mirovogo-masshtaba (дата обращения: 25.04.2019).

[2] Попов К.И. . Компьютерные преступления — преступления мирового масштаба // Правопорядок: история, теория, практика. 2013. №1 (1). URL: https://cyberleninka.ru/article/n/kompyuternye-prestupleniya-prestupleniya-mirovogo-masshtaba (дата обращения: 25.04.2019).

опасных деяний, закрепление процессуальных механизмов и т.п[1]. Например, в целях дальнейшей модернизации и развития НЦБ Интерпола МВД России необходимо создания единой системы информационно-аналитического обеспечения деятельности структурных подразделений ОВД.

Изучение проблемы преступности в сфере информационных технологий, позволяет говорить о необходимости дальнейшей разработки и внесения изменений в национальное законодательство в соответствии с международным законодательством в целях повышения эффективности борьбы в данной поле. Поэтому, для усиления на территории Российской Федерации юридической ответственности за данный вид преступлений необходимо проводить комплекс мер, направленный на борьбу с противоправными действиями со стороны преступников.

§ 3.2 Совершенствование национального уголовного законодательства в сфере противодействия преступлениям, совершаемым с использованием информационных технологий.

В борьбе с преступностью в сфере информационных технологий крайне важное значение имеет укрепление доверия между Интернет-отраслью и правоохранительными органами государства.

Также имеет большое значение просвещение пользователей Интернета, а именно не только как использовать современные информационные технологии, но и о том, как защитить себя от преступных посягательств. Борьба с преступлениями в сфере информационных технологий - это не прерогатива, которая ложится на правоохранительные органы в одиночку.

Государство должно запустить рекламные кампании, чтобы помочь людям защитить себя от подобных преступлений. Простые меры

[1] Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. №24. URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza (дата обращения: 01.05.2019).

безопасности, особенно среди молодежи, могут значительно снизить уровень преступности. Повышение осведомленности через средства массовой информации, социальные сети, которые сейчас находится на пике популярности и это лишь один из вариантов достижения цели.

Вопрос о категориальном определении преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, не решён. При этом данная проблема может быть представлена сразу на двух уровнях. Первый связан с отсутствием общего видения относительно самой терминологии. В трудах отечественных авторов можно обнаружить использование совершенно разных категорий: компьютерные преступления, информационные преступления[1], киберпреступления[2], преступления в сфере высоких технологий[3], интернет-преступления[4]. Второй уровень касается самого наполнения данной группы преступлений – учёные существенно расходятся во мнениях относительно того, какие деяния следует признавать «компьютерными», а какие при внешней схожести таковыми всё же не являются.

Одним из известных подходов является определение компьютерных преступлений как деяний, исключительно посягающих на безопасность компьютерной информации[5].

Вместе с тем, А.А. Жмыхов отмечает, что указания на направленность посягательства объективно недостаточно, поскольку, таким образом к компьютерным преступлениям необходимо будет относить и уничтожение физических носителей информации. В связи с этим он предпринимает попытку конкретизировать содержание явления, обосновывая, что это не

[1] Букалерова Л. А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы: дис.…д-ра юрид. наук. М., 2007. 574 с.
[2] Чекунов И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореф. дис.…канд.юрид.наук. М., 2013. 22 с.
[3] Козаев Н. Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): монография. М.: Юрлитинформ, 2015. 224 с.
[4] Гузеева О. С. Преступления, совершаемые в российском сегменте сети Интернет: монография. М.: Акад. Ген. прокуратуры, 2015. 136 с.
[5] Гаджиев М. С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): автореф. дис. ...канд. юрид. наук. Махачкала, 2004. 21 с.

просто совокупность преступлений, посягающих на безопасность компьютерной системы или сети, но и совершаемых с помощью компьютерной системы или сети, а также в рамках компьютерной системы или сети.

Используя другую терминологию (киберпреступность), однако похожим образом определяет данные преступления Т.Л. Тропина – совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей или компьютерных данных[1].

Таким образом, по мнению авторов, компьютерная природа преступления определяется как содержанием объекта посягательства, так и признаками средства и обстановки.

Такой подход нельзя признать удачным, так как в указанной интерпретации исследователи проблематику «виртуальной» преступности искусственно концентрируют на деяниях, посягающих исключительно на безопасность компьютерных данных и систем, то есть предусмотренных Главой 28 УК РФ[2].

В отечественной теории уголовного права можно обнаружить подход, связанный с определением «компьютерных» преступлений через своего рода «сетевой» аспект. Так, Н.В. Летелкин оперирует категорией «преступления, совершаемые с использованием информационно-телекоммуникационных сетей (включая сеть Интернет)». Автор раскрывает данную группу деяний как умышленные, наказуемые деяния, запрещённые Особенной частью уголовного закона, наряду с основным объектом уголовно-правовой охраны, посягающие на общественные отношения в сфере правомерного

[1] Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. №24. URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza (дата обращения: 10.04.2019).

[2] Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ (с изменениями и дополнениями от 27.12.2018) // Собрание законодательства Российской Федерации от 17 июня 1996 г. N 25 ст. 2954

использования информационно-телекоммуникационных сетей, отличающиеся повышенной степенью общественной опасности ввиду использования при их совершении технологических систем, предназначенных для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[1].

Выделяет два критерия признания преступления «компьютерным» Н.В. Летелкин – использование соответствующих технологических систем, а также направленность деяния на причинение вреда дополнительному объекту уголовно-правовой охраны – отношениям в сфере информационной безопасности. Наиболее уязвимым моментом предлагаемого подхода является, пожалуй, тезис о необходимой двуобъектности преступления, поскольку, как известно, многие из современных преступлений, совершаемых с использованием сетевого оборудования, угрозы для самой информационной инфраструктуры не представляют. Например, сбыт наркотических средств, совершаемый путём так называемых «закладок» с использованием сети Интернет.

При наличии определённых достоинств, строго догматический подход обладает очевидным и существенным недостатком – он не позволяет учесть реальных масштабов проблемы, значительно и искусственно преуменьшая палитру «компьютерной» преступности. Это может привести к недостаточному вниманию теории уголовного права к охране общественных отношений, обеспечивающих личные и общественные интересы в информационной сфере, а также к недооценке тенденций развития отечественного уголовного законодательства. Кроме того, догматический подход не позволит построить эффективную стратегию предупреждения преступлений, совершаемых с использованием информационно-

[1] Летелкин Н. В. К вопросу об определении понятия преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») // Уголовное право: стратегия развития в XXI веке: материалы XV Международной научно-практической конференции. М.: Юрлитинформ, 2018. С. 617 – 619.

коммуникационных технологий. Наша точка зрения такова, что преступления которые совершаются с использованием информационных технологий не находится только в главе 28, они есть и в 25 касающаяся незаконного производство, сбыта или пересылки наркотических средств, психотропных веществ или их аналогов, и в 21 статьи 159.3 и 159.6 и др.

Например, А.Г. Волеводз среди преступлений, совершаемых с применением компьютерных технологий и использованием компьютерной информации, выделяет не только преступления в сфере компьютерной информации, посягающие на информационные компьютерные отношения, но и иные преступления, для которых характерно использование компьютерной информации или составляющих ее элементов информационного пространства при совершении деяний, посягающих на иные охраняемые уголовным законом правоотношения[1].

Также относит к данным преступлениям Т.М. Лопатина, все совершённые на определённой территории за определённый период деяния, непосредственно посягающие на отношения по сбору, обработке, накоплению, хранению, поиску и распространению компьютерной информации, а равно преступления с использованием компьютера в целях извлечения материальной выгоды или иной личной заинтересованности[2].

Развитие информационных отношений существенно увеличивает их значимость для общества и государства. Учитывая масштабы «виртуализации жизнедеятельности», в социальном плане можно рассматривать такие общественные отношения как единые, обеспечивающие одновременно и физические блага личности, и экономические отношения, и общественные, а также государственные интересы. Они представляют собой разные, но весьма взаимосвязанные отношения, одни из которых обеспечивают права и законные интересы личности, другие – конкретные общественные или государственные интересы. Поскольку на такие

[1] Волеводз А. Г. Противодействие компьютерной преступности. М.: Юрлитинформ, 2015. С. 96.
[2] Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис. ...д-ра юрид. наук. М., 2006. 418 с.

взаимосвязанные общественные отношения посягают преступления, совершаемые с использованием информационно-коммуникационных технологий, не входящие в Главу 28 УК РФ, постольку с точки зрения повышения эффективности охраны подобного рода общественных отношений уголовным правом представляется целесообразным исходить из понимания «компьютерных» преступлений не в формально-догматическом понимании, а в более широком смысле, как совокупности всех общественно опасных деяний, совершаемых полностью или частично в виртуальном пространстве посредством использования информационно-коммуникационных технологий.

Правовое регулирование в области информационных отношений реализуется многочисленными нормативными актами: Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1], Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»[2], Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»[3] и др. Уголовная ответственность в рассматриваемой сфере регулируется Уголовным кодексом Российской Федерации.

В российском законодательстве не применяется термин «компьютерные преступления», гл. 28 УК РФ называется «Преступления в сфере компьютерной информации». Главным признаком таких преступлений является не компьютер, используемый в качестве орудия преступления, а информационные отношения, формирующиеся в ходе создания, обработки, накопления, хранения, поиска, распространения и предоставления потребителю компьютерной информации, а также создания и применения

[1] Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями от 18.12.2018) // Собрание законодательства Российской Федерации от 31 июля 2006 г. N 31 (часть I) ст. 3448

[2] Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (с изменениями и дополнениями от 31.12.2017) // Собрание законодательства Российской Федерации от 31 июля 2006 г. N 31 (часть I) ст. 3451

[3] Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" (с изменениями и дополнениями от 23.06.2016) // Собрание законодательства Российской Федерации от 11 апреля 2011 г. N 15 ст. 2036, в "Парламентской газете" от 8 апреля 2011 г. N 17

информационных технологий, средств их обеспечения и, в первую очередь, защиты охраняемой законом компьютерной информации[1].

В юридической литературе предлагаются различные трактовки понятия преступления в сфере компьютерной информации. Так, В.С Комиссаров к таким преступлениям относит сознательные общественно опасные деяния, наносящие вред или создающие угрозу нанесения вреда общественным отношениям, регулирующим безопасное производство, хранение, применение или распространение информации и информационных ресурсов или их охрану[2].

По мнению М.А. Зубовой, преступления в области компьютерной информации – это виновно совершенные общественно опасные деяния, посягающие на нормальный порядок обращения охраняемой законом компьютерной информации, за которые в УК РФ назначено наказание[3].

Определяет такие преступления как общественно опасные противоправные деяния А.В. Суслопаров, дополнительным родовым объектом которых выступают общественные отношения по обеспечению информационной безопасности общества, покушающиеся на естественный порядок хранения, обработки и передачи данных в компьютерах (компьютерных системах)[4].

Понятийно-терминологический аппарат нуждается в обновлении и конкретизации, так как не соответствует существующей действительности. По их мнению, компьютер выступает одной из разновидностей информационного оборудования. Проблемами его использования не охватывается весь комплекс отношений в сфере конфиденциальной компьютерной информации. В статьях 272—274 УК РФ довольное большое количество спорных моментов. Как и было сказано выше нет единого

[1] Расследование преступлений повышенной общественной опасности: пособие для следователя / Под ред. Н.А. Селиванова, А.И. Дворкина. М., 2014. С. 334.
[2] Комиссаров В.С. Преступления в сфере компьютерной безопасности; понятие и ответственность // Юрид. мир. 2014. № 2. С. 22.
[3] Зубова М.А. Компьютерная информация как объект уголовно-правовой охраны: Автореф. дис. канд. юрид. наук. Казань, 2008. С. 10.
[4] Суслопаров А.В. Информационные преступления: Автореф. дис. канд. юрид. наук. Красноярск, 2008. С. 9.

понимания ни компьютерных преступлений, ни информационных, а в законе нет легального определения. В связи, с чем возникают недопонимания, споры и неопределённости. Так как при совершении всех этих преступлений используются те или иные информационные технологии резонно использовать термин преступления, совершаемые с использованием информационных технологий. И все же большинство правоведов к компьютерным преступлениям относят противозаконные действия в сфере автоматизированной обработки информации и выделяют в качестве главного классифицирующего признака, позволяющего объединить эти посягательства в обособленную группу, общность способов, орудий, объектов посягательств, т. е. «объектом посягательства является информация, обрабатываемая в компьютерной системе, а сам компьютер служит орудием посягательства»[1].

Например, М.Ю. Дворецкий предлагает применять дефиницию «преступления в сфере информационных ресурсов», а В.В. Крылов – «информационные преступления» в качестве базового термина. По их мнению, следует абстрагироваться от определенных технических средств и учесть саму специфику данных деяний, отграничивая их от других преступлений.

Предлагает определять преступления в сфере компьютерной информации как «преступления в сфере информационных технологий» - Д.В. Добровольский. К таким преступлениям он предлагает относить установленные уголовным законодательством виновные общественно опасные деяния, имеющие целью нарушение неприкосновенности охраняемой законом электронной информации и ее материальных носителей, осуществляемые в ходе формирования, применения и распространения электронной информации, а также имеющие целью нарушение работы ЭВМ, системы ЭВМ или их сети, наносящие вред законным интересам собственников или владельцев, жизни здоровью, правам и свободам человека

[1] Колмыков В.В.Статья Уголовно-правовые средства борьбы с преступлениями, совершаемыми в сфере информационных технологий — 2006 г.

и гражданина, национальной безопасности[1]. По мнению Д.В. Добровольского использование понятия «преступления в сфере компьютерной информации», не позволяет точно установить конкретный вид преступлений, т.к. на сегодняшний день компьютеры присутствуют практически во всех сферах жизнедеятельности общества.

Современное состояние правоотношений в области информационных технологий. Помимо компьютеров к числу технических устройств, с помощью которых можно осуществлять доступ к информации относятся мобильные телефоны, смартфоны, разного рода гаджеты, радиотрансляционные приемники, датчики охранной и пожарной сигнализации, а также их линии и сети электропроводки.

На сегодняшний день инновации в области сервиса в значительной степени стимулируются и обеспечиваются развитием информационно-коммуникационных технологий – ИКТ. Сформировалось новое направление развития ИКТ, получившее название «интернет вещей» (ИВ). Концепция ИВ подразумевает, что многие отдельные объекты, а также взаимосвязи внутри групп таких объектов и между ними могут получить уникальную идентификацию посредством применения радиометок, датчиков и различных срабатывающих устройств, что обеспечит возможность виртуально отобразить их как в проводных, так и беспроводных информационных сетях.

В ходе обсуждений проблем становления интернета основное внимание на данном этапе уделяется технологиям реализации, необходимой инфраструктуре и поставщикам разрабатываемых технологий. Значительно меньше усилий тратится на попытки представить себе и осознать, как будут функционировать процессы, основанные на применении ИВ, в том числе и связанные с этими технологиями преступные действия.

Интернет вещей представляется многим исследователям одной из самых многообещающих и перспективных инноваций. Основным движущим

[1] Добровольский Д. В. Актуальные проблемы борьбы с преступностью (уголовно-правовые и криминологические проблемы): дис.... канд. юрид. наук. М., 2005. С. 19.

фактором этой парадигмы является интеграция нескольких технологий и коммуникационных решений. Интернет вещей открывает новые возможности в объединении деятельности, ресурсов и действующих субъектов в бизнес-сетях. Комплекс разнообразных устройств, датчиков и вычислительных мощностей, относящихся к различным отраслям, получит новые возможности при подключении к формирующимся системам интернета вещей; работа этих систем потребует установления и поддержания огромного количества связей между этими устройствами. Технология интернета вещей охватывает множество областей практического применения, зачастую – в совместном использовании с другими технологиями. Это безопасность, трекинг и иные формы отслеживания положения и перемещений, выполнение платежей, здравоохранение, удаленный контроль и обслуживание, измерения и управление. Все это может привести к расширению видов и форм преступности в той сфере, которая сейчас называется сферой компьютерной информации. Непосредственно компьютеры в инновационных технологиях в своем традиционном виде использоваться не будут. В подтверждение вышесказанного стоит сказать о виртуальных объектах в уголовно-правовом поле, таких как биткоины. Нет единого подхода в понимании данной валюты. Так, 6 февраля 2014 г. на заседании экспертной группы при Межведомственной рабочей группе по противодействию преступлениям в сфере экономики в Генеральной прокуратуре РФ при участии представителей Центрального банка РФ было решено подготовить и реализовать комплекс мероприятий, направленных на предотвращение использования виртуальных валют в противозаконных операциях, в том числе при легализации (отмывании) доходов, полученных преступным путем[1]. Логичным продолжением решения, принятого на заседании стал опубликованный 11 марта 2016 г. Министерством финансов РФ проект федерального закона «О внесении изменений в отдельные

[1] Блокчейн и биткоин в России. Центробанк не запрещал биткоины. URL: http://cryptorussia.ru/news/centrobank-ne-zapreshchal-bitkoin

законодательные акты Российской Федерации», предусматривающий введение понятия «денежный суррогат», а также опубликованный 28 марта 2016 г. текст проекта федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации», предусматривающий дополнение Уголовного кодекса Российской Федерации ст. 187.1 «Оборот денежных суррогатов»[1].

В Германии Министерство финансов в ответе на запрос немецкого парламента указало, что биткоины не могут быть отнесены к электронной, национальной или иностранной валюте, но к ним может быть применим термин «Rechnungseinheit», означающий финансовый инструмент[2].

Ещё в 1990-х были представлены массовые многопользовательский онлайн-игры, их появлению способствовал выросший уровень скорости подключения к всемирной паутине и модернизация самих электронно-вычислительных машин (ЭВМ). С тех пор прошло уже около 20 лет, как в искусственных онлайновых вселенных, используемых как игры, выделился класс многопользовательских сетевых приложений — так называемых серьезных игр, или Глобальных многопользовательских виртуальных миров (Massively Multiplayer Online World — MMOW), по сути, модифицированных «отражений» реального мира, симуляторов жизни (Entropia, Neocron, There, Second Life и др.), где люди через своих аватаров (виртуальных персонажей) живут и работают, учатся и преподают, занимаются творчеством и бизнесом и, конечно, совершают «правонарушения»[3]. И так как игры являются симуляторами жизни в них также как и в реальности совершаются преступления, которые касаются материальной составляющей (собственность участников, финансовые средства, накопленные ими и

[1] Федеральный портал проектов нормативно-правовых актов. URL: http:// regulation.gov.ru/projects#npa=46853

[2] См.: Германия официально признает биткоин как «частные деньги». URL: https://cryptochan.org/germaniya-ofi cialno-priznaet-bitcoin-kak-chastnye-dengi/

[3] Батурин Ю. М., Полубинская С. В. Статья Что делает виртуальные преступления реальными // Труды Института государства и права РАН. — 2018. — № 2.

находящимися на балансе них учетной записи и другими элементами гражданского оборота). Можно привести пример, что в декабре 2016 г. пресс-служба управления МВД по Красноярскому краю сообщила о возбуждении уголовного дела в связи с разбойным нападением на участника соревнований по компьютерным играм — у молодого человека под угрозой огнестрельного оружия потребовали передачи «внутриигровых предметов компьютерной игры», которыми оказались два вида виртуального оружия стоимостью 27 тыс. руб[1].

Технически реализуемые возможности инноваций могут спровоцировать изменения в коммерческой деятельности, социальных взаимодействиях, а также в правовых отношениях. Инновационные технологии, в том числе интернет вещей будут распространяться очень широко, но этот процесс потребует некоторого времени: следует учитывать институциональные соображения, возможности существующих сетевых структур и процессов, а также необходимость внесения изменений и дополнений в законодательство, в том числе регламентирующее уголовную ответственность за преступления в рассматриваемой сфере.

В связи с этим необходимо заменить понятие «преступления в сфере компьютерной информации» на «преступления в сфере информационных технологий». Это позволит более оперативно реагировать на криминализацию общественно опасных деяний в тех областях науки, техники, производства, которые только формируются, точно и своевременно разрабатывать нормы уголовного закона применительно к появляющимся новым формам преступлений в этой сфере.

Отсутствие четкого разделения ответственности за неосторожное и умышленное уничтожение, блокирование, модификацию или копирование информации при неправомерном доступе является серьезным изъяном действующей редакции ст. 272 УК РФ. Заимствование опыта стран

[1]В Красноярске полицейские задержали злоумышленников, напавших на участника компьютерного турнира. 22 декабря 2016 г. URL: https://24.xn--b1aew.xn--p1ai/news/item/9145006

Содружества Независимых Государств могло бы способствовать успешному устранению данной проблемы.

Отечественное законодательство об ответственности за неправомерный доступ к компьютерной информации (ст. 272 УК РФ) нуждается в коррекции. К числу первоочередных мер, на наш взгляд, следует отнести:

1) разделение ответственности за неправомерный доступ к компьютерной информации в зависимости от психического отношения субъекта к наступлению общественно опасных последствий (умысла или неосторожности);

2) дифференциацию ответственности за неправомерный доступ к информации в зависимости от наступивших последствий:

а) уничтожение, блокирование, приведение в непригодное состояние компьютерной информации,

б) ее модификация (изменение) и в) копирование (завладение);

3) в целях устранения смысловой неопределенности из диспозиции ст. 272 УК РФ необходимо исключить указание на то, что предметом данного преступления является исключительно охраняемая законом (т. е. конфиденциальная) информация. Общедоступная информация отнюдь не является информацией, лишенной защиты в части ее доступности и целостности.

ЗАКЛЮЧЕНИЕ

Проведенное дипломное исследование позволяет сформулировать ряд следующих основных выводов и предложений:

1. Преступления, совершаемых с использованием информационных технологий являются одним из самых специфических, динамично развивающихся видов преступности в связи с их высокотехнологичным характером. Данные преступления в настоящее время остаются серьезнейшей угрозой, не только для отдельных государств, но и для всего мирового сообщества в целом. Анализируя всю представленную статистику, делаем вывод о том, что имеется тенденция по увеличению количества преступлений совершаемых с использованием информационных технологий. В связи, с чем необходимо предпринимать меры по совершенствованию уголовно-правового закона. В целях упорядочения терминологии, обеспечения единства и системности уголовного законодательства, предлагается легитимизация понятия преступления, совершаемые с использованием информационных технологий, возможно сопровождающиеся пленумом Верховного суда, который разъяснил бы, что такое информационные технологии и какие именно преступления указанные в Уголовном кодексе РФ следует к ним относить.

2. Считаем необходимым изменить наименование главы 28 УК РФ, предложив следующую редакцию «Преступления в сфере использования информационных технологий», а также статью 159.6 УК РФ «Мошенничество в сфере информационных информации».

3. Ущерб, причиняемый действиями лиц совершающих преступления, с использованием информационных исчисляется миллиардами долларов, как было отмечено выше. Но это не единственный аспект вреда, который причиняют преступления с использованием информационных технологий. Во-первых, он выражается не только в денежном эквиваленте, а также в угрозе похищения и рассекречивания персональных данных о лицах,

например о держателях кредитных карт в банках, чьими услугами они пользуются. А во-вторых, нарушения нормальной работы электронных вычислительных машин с помощью вредоносных программ, так называемые «черви» и «трояны» и др. Считаем необходимым выделение статистики преступлений, совершаемых с использованием информационных технологий наряду с преступлениями сфере незаконного оборота наркотиков, оружия, террористической и экстремисткой направленностью и др.

4. Говоря о субъекте преступлений, совершаемых с использованием информационных технологий можно отметить тот факт, что на сегодняшний день необязательно, чтобы у лица имелось высшее техническое образование или средне специальное (колледж). Преступники и сами неплохо занимаются самообразование и развитием своих способностей, просто сидя дома за компьютером. Стали очень популярны курсы онлайн-обучения, информация может, предоставляется как на бесплатной основе, так и за плату, но по сравнению с государственным образованием в разы дешевле, что для лиц совершающих преступления является более простой и доступной формой обучения. Преимуществом такого учебного процесса и в том, что нет необходимости непосредственно присутствовать на занятиях, приведенный пример обучения позволяет учиться дистанционно. Что по-нашему мнению является причиной ускоренного процесса подготовки лиц совершающих противоправные деяния в сфере информационных технологий, а также это приводит к увеличению количества совершаемых ими преступлений. Ещё одной особенностью является конфиденциальности лица. Она выражается в том, что лицо скрывает свою подлинную личность, путём использованием различных компьютерных программ, браузеров (Tor), прокси-серверы и др. В связи, с чем преступники чувствуют себя в безопасности от правоохранительных органов и не бояться быть обнаруженными. В этом и состоит проблема безнаказанности лиц за их преступную деятельность, так как они продолжают оставаться в тени. Не будет же сотрудник ждать пока лицо само допустит ошибку, которая приведёт к расшифровки его личности,

поэтому необходимо использовать при проведение не только оперативно-розыскных мероприятий, но и при осуществлении предварительного следствия передовой опыт коллег из зарубежных стран, а также практиковать использование знаний специалистов в области информационных технологий. В целях подготовки высококвалифицированных сотрудников в сфере противодействия преступлениям, совершаемым с использованием информационных технологий предлагается ввести в специализированные высшие учебные заведения дисциплины, которые помогу сформировать у обучающихся знания об информационных технологиях, умениям и навыкам их применения в будущей профессиональной деятельности. Предлагаем следующие наименования учебных дисциплин: «Информационные технологии в правоохранительной деятельности», «Расследование и раскрытие преступлений, совершаемых в сфере использования информационных технологий», «Особенности осуществления оперативно-розыскной деятельности по преступлениям, совершенным в сфере использования информационных технологий», «Практикум по документированию действий лиц, совершающих преступления в сфере использования информационных технологий» и др.

5. В целях повышения эффективной борьбы с данной категорией преступлений необходимо совершенствование законодательства, а именно расширения перечня преступлений в сфере информационных технологий. Приведенный анализ законодательства зарубежных государств показывает, что нормативные акты более детально определяют круг противоправных деяний в сфере информационных технологий, что по-нашему мнению позволяет более продуктивно противодействовать данной угрозе. Предлагаем добавить п. «г» ч. 4 статью 162 УК РФ, квалифицирующий признак: «с использованием информационных технологий виртуальных объектов, с применением насилия, опасного для жизни или здоровья, либо с угрозой применения такого насилия».

6. Диспозиция статьи 282 УК РФ говорит, что: «с использованием средств массовой информации либо информационно - телекоммуникационных сетей, в том числе сети «Интернет», но данная формулировка не совпадает с тем, что указанно в Федеральном законе от 25 июля 2002 г. «О противодействии экстремистской деятельности». Согласно ст. 12 Федерального закона «О противодействии экстремистской деятельности» запрещается использование сетей общего пользования для осуществления экстремистской деятельности. Проблема состоит в том, что Интернет в законодательстве к средствам массовой информации не относится. Следовательно, необходимо отнести в законодательном порядке компьютерные сети Интернет к средствам массовой информации, поменяв при этом и диспозицию статьи 282 Уголовного Кодекса России.

7. Нуждается в дальнейшем совершенствование международное сотрудничество, которое может выражаться в:

- развитие международного сотрудничества посредством заключения соглашений об обеспечении информационной безопасности, а также участие в конвенциях и договорах, которые касаются не только безопасности, но и самих преступлений совершаемых с использованием информационных технологиях.

- создание международной базы данных, в которой содержатся сведения о преступлениях данной категории и лицах их совершающих.

- обсуждение в рамках научных конференций в целях привлечения внимания к данной проблеме.

8. Важной составляющей в профилактики любого вида преступлений, а именно с использованием информационных технологий является проведение разъяснительной работы в среде интернет-пользователей. Научно-исследовательская, консультативная и пропагандистская деятельность среди населения о том, как не стать жертвой мошенника и как защитить свои электронные устройства от незаконных посягательств преступников.

Проблематика преступлений, совершаемых с использованием информационных технологий, нуждается в дальнейших исследованиях. Особенное внимание следует уделить специфическим признакам составов данных преступлений. При этом следует избегать придания давно разработанным в теории уголовного права институтам не свойственных им функций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативно-правовые акты

1. Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве) Будапешт, 23 ноября 2001 года URL: http://mvd.gov.by/main.aspx?guid=4603 (дата обращения: 31.01.2018)
2. Конвенции об обеспечении международной информационной безопасности (концепция), а именно «информационно-коммуникационные технологии // URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения: 25.01.2019).
3. Конвенция об обеспечении международной информационной безопасности (концепция) // URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения: 25.01.2019).
4. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) // Система ГАРАНТ: http://base.garant.ru/4089723/#ixzz5eXgUx0UQ.
5. Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в области компьютерной информации (Минск, 1 июня 2001 г.) // Исполнительный комитет СНГ. — URL: http://www.cis.minsk.by/page.php?id=866.
6. Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.) (с поправками) // Собрание законодательства Российской Федерации от 4 августа 2014 г. N 31.
7. Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ (с изменениями и дополнениями от 27.12.2018) // Собрание законодательства Российской Федерации от 17 июня 1996 г. N 25.

8. "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации" Федеральный закон от 29.11.2012 N 207-ФЗ (ред. от 03.07.2016).
9. "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" Федеральный закон от 26.07.2017 N 194-ФЗ.
10. О проекте Федерального закона № 53700-6 «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации»: письмо Верховного Суда РФ от 25 мая 2012 г. № 2-ВС-2733/12. // СПС «КонсультантПлюс».
11. Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации" (с изменениями и дополнениями) (утратил силу).
12. "Об информации, информационных технологиях и о защите информации". Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 18.12.2018) // Собрание законодательства Российской Федерации от 31 июля 2006 г. N 31.
13. Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" // Собрание законодательства Российской Федерации от 31 июля 2017 г. N 31 (часть I).
14. Федеральный закон от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" (с изменениями и дополнениями от 18.12.2018) // Собрание законодательства Российской Федерации от 3 января 2011 г. N 1.
15. Федеральный закон от 28 декабря 2010 г. N 390-ФЗ "О безопасности" (с изменениями и дополнениями от 05.10.2015) // Собрание законодательства Российской Федерации от 3 января 2011 г. N 1.

16. Федеральный закон от 7 июля 2003 г. N 126-ФЗ "О связи" (с изменениями и дополнениями от 27.12.2018) // Собрание законодательства Российской Федерации от 14 июля 2003 г. N 28.
17. Закон РФ от 27 декабря 1991 г. N 2124-I "О средствах массовой информации" (с изменениями и дополнениями от 27.12.2018) // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации от 13 февраля 1992 г. N 7.
18. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 05.12.2016 № 646) // Собрание законодательства Российской Федерации. 12.12.2016.
19. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24 июля 2013 г., N Пр-1753) // Система ГАРАНТ: http://base.garant.ru/70641072/#ixzz5eXRxLWsM.
20. Приказ МВД России № 221 от 28 февраля 2000 г. «О мерах по совершенствованию сотрудничества по линии Интерпола» // СПС «Гарант».
21. Уголовный кодекс Австрии https://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/10002296/StGB%2c%20Fassung%20vom%2017.07.2014.pdf.
22. Кодекс Соединенных Штатов http://uscode.house.gov/view.xhtml;jsessionid=A85801239AAD3996A66CDEA7174237A3?req=granuleid%3AUSC-prelim-title18-part1&saved=%7CZ3JhbnVsZWlkOlVTQy1wcmVsaW0tdGl0bGUxOC1zZWN0aW9uMTAyOQ%3D%3D%7C%7C%7C0%7Cfalse%7Cprelim&edition=prelim.
23. Уголовный кодекс ФРГ // https://constitutions.ru/?p=5854&attempt=1.
24. Закон Сингапура о неправомерном использовании компьютерных технологий // URL: http://statutes.agc.gov.sg.

25. Уголовный кодекс КНР // URL: http://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm.
26. Уголовный кодекс Норвегии // URL: http://www.un.org/depts/los/LEGISLATIONANDTREATIES/PDFFILES/NOR penal_code.pdf.
27. Уголовный кодекс Республики Молдова // URL: http://online.zakon.kz/Document/?doc_id=30394923#pos=2668;-85.
28. Уголовный кодекс Республики Казахстан // URL: http://online.zakon.kz/m/Document/?doc_id=31575252#sub_id=2050000.

Судебная практика

29. Постановление Пленума Верховного Суда РФ от 27 декабря 2002 г. N 29 "О судебной практике по делам о краже, грабеже и разбое" // URL: http://base.garant.ru/1352873/#ixzz5ee1wJCRC (дата обращения 01.02.2019).
30. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 “О судебной практике по делам о мошенничестве, присвоении и растрате” // URL: http://www.garant.ru/products/ipo/prime/doc/71723288/#ixzz5ee0jpzA7 (дата обращения 01.02.2019).
31. Постановление Пленума Верховного Суда РФ от 27 декабря 2007 г. N 51 “О судебной практике по делам о мошенничестве, присвоении и растрате” //ГАРАНТ.РУ: http://www.garant.ru/products/ipo/prime/doc/1685377/#ixzz5eXnB4h9J.

Монографии, учебники, учебные пособия

32. Уголовное право России. Части Общая и Особенная: учебник / В. А. Блинников, А. В. Бриллиантов, О. А. Вагин [и др.] ; под ред. А. В. Бриллиантова. 2-е изд., перераб. и доп. М.: Проспект, 2015. С. 1184.

33. Уголовное право Российской Федерации. Общая часть : учебник для вузов / Н. Н. Белокобыльский, Г. И. Богуш, Г. Н. Борзенков [и др.] ; под ред. В. С. Комиссарова, Н. Е. Крыловой, И. М. Тяжковой. М. : Статут, 2015. С. 86.
34. Коржанский, Н.И. Очерки теории уголовного права // Волгоград. 1992. С. 45.
35. Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 2 т. / А. В. Бриллиантов, Г. Д. Долженкова, Э. Н. Жевлаков [и др.] ; под ред. А. В. Бриллиантова. 2-е изд. М. : Проспект, 2015. Т. 1. С. 792.
36. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Г. Н. Борзенков, А. В. Бриллиантов, А. В. Галахова [и др.]; отв. ред. В. М. Лебедев. М: Юрайт, 2016. С. 1069.
37. Комментарий к Уголовному кодексу Российской Федерации: научно-практический (постатейный) / Н. И. Ветров, М. М. Дайшутов, Г. В. Дашков [и др.]; под ред. С. В. Дьякова, Н. Г. Кадникова. М.: Юриспруденция, 2016.С. 912.
38. Энциклопедия уголовного права. СПб: Издание профессора Малинина, 2015. С. 194.

Научные публикации и статьи в иных периодических изданиях

39. Антонян Ю.М. Комплексный анализ состояния преступности в Российской Федерации по итогам 2017 года и ожидаемые тенденции её развития: аналитический обзор. М.: ФГКУ «ВНИИ МВД России», 2018. С. 76.

40. Батурин Ю.М., Полубинская С. В. Статья Что делает виртуальные преступления реальными // Труды Института государства и права РАН. 2018. — № 2.
41. Бикмурзин М. П. Предмет преступления: теоретико-правовой анализ. М. : Юрлитинформ, 2016. С. 50—51.
42. Букалерова Л.А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы: дис.... д-ра юрид. наук. М., 2007. 574 с.
43. Воронцова С.В. К вопросу о квалификации преступлений в сфере электронных платежей // Банковское право. 2015. № 1. С. 35–37.
44. Волеводз А.Г. Противодействие компьютерной преступности. М.: Юрлитинформ, 2015. С. 96.
45. Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): автореф. дис... канд. юрид. наук. Махачкала, 2004. С. 21.
46. Головинов О.Н., Погорелов А.В. Киберпреступность в современной экономике: состояние и тенденции развития // Вопросы инновационной экономики. 2016. №1. URL: https://cyberleninka.ru/article/n/kiberprestupnost-v-sovremennoy-ekonomike-sostoyanie-i-tendentsii-razvitiya (дата обращения: 16.04.2019)..
47. Гребеньков А.А. Преступность в сфере высоких технологий: исторический аспект// Известия Юго-Западного государственного университета. Серия «История и право». 2015. № 1-1. С. 184—188.
48. Гребеньков А.А. Понятие информационных преступлений, место в уголовном законодательстве России и место признаков информации в структуре их состава// Lex Russica. 2018. №4 (137). URL: https://cyberleninka.ru/article/n/ponyatie-informatsionnyh-prestupleniy-mesto-v-ugolovnom-zakonodatelstve-rossii-i-mesto-priznakov-informatsii-v-strukture-ih-sostava (дата обращения: 09.04.2019).

49. Гузеева О.С. Преступления, совершаемые в российском сегменте сети Интернет: монография. М.: Акад. Ген. прокуратуры, 2015. С 136.
50. Демьянец М.В., Елин В. М., Жарова А. К. Предпринимательская деятельность в сети Интернет: монография. М. : Юркомпани, 2014. С 440.
51. Добровольский Д.В. Актуальные проблемы борьбы с преступностью (уголовно-правовые и криминологические проблемы): диссертация канд. юрид. наук. М., 2005. С. 19.
52. Епихин А.Ю. Уголовно-правовые аспекты дополнения уголовного закона специальными видами мошенничества // Современное право. 2016. № 10. С. 134—137.
53. Ефремова М.А. Мошенничество с использованием электронной информации // Информационное право. 2016. № 4. С. 19—21.
54. Жестеров П.В. Манифест уголовной репрессии эпохи дополненной реальности. М.: Проспект, 2017. С. 224
55. Зверянская Л.П. Дискуссионные проблемы выявления и предупреждения киберпреступлений// Гуманитарные, социально-экономические и общественные науки. 2015. №8. С. 160-161.
56. Зозуля В.В. К вопросу об уголовной ответственности в России за совершение преступления с использованием информационно-телекоммуникационных технологий.
57. Зубова М.А. Компьютерная информация как объект уголовно-правовой охраны: Автореф. дис.... канд. юрид. наук. Казань, 2008. С. 10.
58. Калмыков Д.А. К вопросу о необходимости корректировки понятия «предмет преступления» // Противодействие преступности: уголовно-правовые, криминологические и уголовно-исполнительные аспекты: материалы Российского конгресса уголовного права / отв. ред. В.С. Комиссаров. М., 2014. С. 44.
59. Князьков А.С. Криминалистическая характеристика преступления в контексте его способа и механизма // Вестник Томского государственного университета. Серия «Право». 2014. № 1. С. 51—64.

60. Кобец П.Н. Анализ природы терроризма и его детерминирующих факторов в условиях середины второго десятилетия XXI столетия // Полицейская деятельность. 2016. № 6. С. 596–602.
61. Кобец П.Н. Противодействие угрозам кибersталкинга — важнейшей проблеме, исследуемой в рамках совершенствования аспектов информационной безопасности регионов в условиях глобализации информационного пространства // Вестник Прикамского социального института. 2017. № 1 (76). С. 27–35.
62. Козаев Н.Ш. Изменения в уголовной политике в связи с проблемами обеспечения безопасности интернет-пространства // Вестник Санкт-Петербургского университета МВД России. 2015. № 1. С. 48–50.
63. Козаев Н.Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): / под. ред. А.В. Наумова. М., 2015. С. 88.
64. Колоколов Н. А. Преступления против собственности: комментируем новеллы УК РФ // Мировой судья. 2016. № 1. С. 6—15.
65. Крылов В.В. Основы криминологической теории расследования преступлений в сфере информации. М.: МГУ, 1998. 50 с.
66. Комиссаров В.С. Преступления в сфере компьютерной безопасности; понятие и ответственность // Юрид. мир. 2014. № 2. С. 22.
67. Летелкин Н.В. К вопросу об определении понятия преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») // Уголовное право: стратегия развития в XXI веке: материалы XV Международной научно-практической конференции. М.: Юрлитинформ, 2018. С. 617 – 619.
68. Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис.... доктора юрид. наук. М., 2006. 418 с.
69. Малышкин П.В. Особенности сокрытия следов совершенных преступлений, совершаемых с применением информационных

компьютерных технологий // Мир науки и образования. 2016. №4 (8). URL: https://cyberleninka.ru/article/n/osobennosti-sokrytiya-sledov-sovershennyh-prestupleniy-sovershaemyh-s-primeneniem-informatsionnyh-kompyuternyh-tehnologiy (дата обращения: 01.02.2019).

70. Менжега М.М. Информационное взаимодействие работников правоохранительных органов при расследовании преступлений в сфере высоких технологий / М. М. Менжега // Международный научно-исследовательский журнал. 2012. №5 (5). С. 9. URL: https://research-journal.org/law/informacionnoe-vzaimodejstvie-rabotnikov-pravooxranitelnyx-organov-pri-rassledovanii-prestuplenij-v-sfere-vysokix-texnologij/ (дата обращения: 01.05.2019).
71. Минин А.Я. Кибербезопасность и защита информационных систем // Право и кибербезопасность. 2016. № 2. С. 28—35.
72. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. №24. URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza (дата обращения: 15.04.2019).
73. Селиванова Н.А., Дворкина А.И. Расследование преступлений повышенной общественной опасности: пособие для следователя. 2014. С. 334.
74. Романовская О.В. Акт о патриотизме: ограничения права на неприкосновенность частной жизни в США в целях противодействия терроризму // Наука. Общество. Государство. 2017. Т. 5. № 2.
75. Романовский Г.Б. Правовые основы противодействия терроризму в зарубежном праве // Экономика, педагогика и право. 2017. № 2. С. 2.
76. Романовский Г.Б. Принципы правотворческой политики: проблемы реализации // Российский журнал правовых исследований. 2015. № 2. С. 45–50.

77. Русскевич Е.А. Актуальные проблемы уголовно-правовой политики в сфере противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий (ИКТ).
78. Русскевич Е.А. Уголовная ответственность за преступления в сфере компьютерной информации по законодательству китайской народной Республики: сравнительно-правовой анализ // Журнал зарубежного законодательства и сравнительного правоведения. 2018. №5 (72). С. 121-127.
79. Савин Г.Е. Экономические преступления, совершаемые с использованием информационных технологий, и способы их предотвращения. // Вестник Академии экономической безопасности МВД России. 2010 № 10. С. 70-77.
80. Сивова А.А. Преступления в сфере компьютерных технологий и интернета как угроза национальной и экономической безопасности // Уголовный закон: Современное состояние и перспективы развития: Материалы II Международной научно-практической конференции, приуроченной ко дню принятия Уголовного Кодекса РФ. 2018 с. 248-249.
81. Суслопаров А.В. Информационные преступления: автореф. дис. канд. юрид. наук. Красноярск, 2008. С. 8.
82. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис.... канд. юрид. наук. Владивосток, 2005. 235 с.
83. Турышев А. А. Информация как признак составов преступлений в сфере экономической деятельности: автореф. дис.... канд. юрид. наук. Омск, 2006. С. 9.
84. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис.... канд.юрид.наук. Владивосток, 2005. 235 с.
85. Федотов М.А. Конституционные ответы на вызовы киберпространства // Lex Russica. 2016. № 3. С. 164–182.
86. Хисамова З.И. О конструкции норм уголовного законодательства, предусматривающих ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий.

87. Хисамова З.И. Об особенностях квалификации преступлений, совершаемых в сфере использования информационно-коммуникационных технологий // Общество и право. 2016. №1 (55).С. 117-120.
88. Хисамова З.И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий: дис.... канд. юр. наук. Краснодар, 2016. С. 31.
89. Хилюта В.В. Уголовная ответственность за хищения с использованием компьютерной техники // Журн. рос. права. 2014. № 3. С. 111–118.
90. Хусяинов Т.М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования: материалы Всероссийского круглого стола. Иркутск, 2015. С. 120–125.
91. Чернякова А.В. Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации // Юридическая наука и правоохранительная практика. 2018. № 4(46). С. 178.
92. Чекунов И.Г. Понятие и отличительные особенности киберпреступности // Российский следователь. 2014. № 18. С. 53–56.
93. Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореф. диссертации канд.юрид.наук., 2013. С. 22.

Интернет ресурсы

94. РФ поддерживает разработку конвенции по борьбе с киберпреступностью [Электронный ресурс]. — Режим доступа: https://ria.ru./politics/20141028/1030552154.html.

95. Страшнее пистолета [Электронный ресурс] // URL: https://www.kommersant.ru/doc/3428093.
96. IOCTA 2017 [Электронный ресурс] // URL: https://www.europol.europa.eu/iocta/2017/index.html.
97. ГД в первом чтении приняла законопроект об уголовном наказании за создание «групп смерти» [Электронный ресурс]. — Режим доступа: http://tass.ru./obschestvo/4195820.
98. В Красноярске полицейские задержали злоумышленников, напавших на участника компьютерного турнира. 22 декабря 2016 г. URL: https://24.xn--b1aew.xn--p1ai/news/item/9145006.
99. Законодательство о киберпреступности во всем мире https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx
100. Киркпатрик Г. Хакерская этика и дух цифрового времени. // URL: https://www.jstor.org/stable/24579606?Search=yes&resultItemClick=true&searchText=hackers&searchText=AND&searchText=subculture&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3Dhackers%2BAND%2Bsubculture%26amp%3Bacc%3Don%26amp%3Bwc%3Don%26amp%3Bfc%3Doff%26amp%3Bgroup%3Dnone&seq=1#page_scan_tab_contents (дата обращения: 31.01.2018).
101. Официальный сайт Генеральной прокуратуры.- Российской Федерации URL: http://genproc.gov.ru/smi/news/news-1431104.
102. Федеральный портал проектов нормативно-правовых актов. URL: http://regulation.gov.ru/projects#npa=46853.
103. См.: Германия официально признает биткоин как «частные деньги». URL: https://cryptochan.org/germaniya-ofi cialno-priznaet-bitcoin-kak-chastnye-dengi/.
104. Блокчейн и биткоин в России. Центробанк не запрещал биткоины. URL: http://cryptorussia.ru/news/centrobank-ne-zapreshchal-bitkoin.

105. Joker.buzz // URL: http://jokerbuzzhyhl5cl.onion/?_locale=ru (дата обращения: 31.01.2018).
106. Гринберг И. 12 фактов о киберпреступности. // URL: https://www.blue-pencil.ca/top-12-cyber-crime-facts-and-statistics/ (дата обращения: 31.01.2018).
107. Деннинг Д. Растущая криминальная угроза в Северной Корее // URL: https://theconversation.com/north-koreas-growing-criminal-cyberthreat-89423 (дата обращения: 31.01.2018).
108. Интернет: российская аудитория в анфас и профиль http://www.advlab.ru/articles/article88.htm.
109. Количество пользователей интернета в России http://www.bizhit.ru/index/users_count/0-151.
110. Попов К.И. Компьютерные преступления — преступления мирового масштаба // Правопорядок: история, теория, практика. 2013. №1 (1). URL: https://cyberleninka.ru/article/n/kompyuternye-prestupleniya-prestupleniya-mirovogo-masshtaba (дата обращения: 25.04.2019).
111. Обзор по несанкционированным переводам денежных средств за 2017 г. // http://www.cbr.ru/statichtml/file/14435/survey_transfers_17.pdf.
112. Льюис Дж. Киберпреступность – глобальная угроза 2018 года. // URL: https://www.richardvanhooijdonk.com/en/blog/cybercrime-may-be-the-biggest-global-threat-of-2018/ (дата обращения: 31.01.2018).
113. Льюис Дж. Экономическое влияние киберпреступности не уменьшается. // URL: https://csis- prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd (дата обращения: 31.01.2018).
114. Пояснительная записка к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации (в части усиления уголовной ответственности за хищение денежных средств с банковского счета или электронных денежных средств)» // http://sozd.duma.gov.ru/bill/410960-7.

115. ЮНОДК Киберпреступления. URL: https://www.unodc.org/southeastasiaandpacific/en/what-we-do/toc/cyber-crime.html.
116. URL: https://arigus.tv/news/item/89643/ (дата обращения: 30.04.2019)
117. URL: http://www.myui.ru/blog/2017-02-27-1092 (дата обращения: 30.04.2019).
118. European union serious and organised crime threat assessment 2017 URL: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.
119. TAdviser. Государство. Бизнес. IT [Электрон. ресурс] // URL: http://www.tadviser.ru/index.php/.(дата обращения: 01.04.2019)