МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт права
(наименование института полностью)

Кафедра «Уголовное право и процесс»
(наименование)

40.05.02 Правоохранительная деятельность
(код и наименование направления подготовки, специальности)

Оперативно-розыскная деятельность
(направленность (профиль)/специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (ДИПЛОМНАЯ РАБОТА)

на тему «Преступления в сфере Интернет»

Студент ____А.Д. Крымзалова__ _____
(И.О. Фамилия) (личная подпись)

Руководитель _____канд. юрид. наук, доцент, Н.В. Олиндер_____
(ученая степень, звание, И.О. Фамилия)

Тольятти 2020

Аннотация

Примерно с середины 2000-х гг. электронные средства массовой информации, информационные системы, социальные сети, технологии беспроводного доступа в сеть «Интернет», мобильная связь постепенно становились частью повседневной жизни россиян. Государство поощряет указанные тенденции: создана система предоставления государственных и муниципальных услуг в электронной форме, что позволяет гражданам направлять в электронной форме индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления.

Цель исследования – провести комплексное исследование различных видов и составов преступлений, которые совершаются в сети «Интернет».

Задачи исследования: раскрыть содержание понятия сети «Интернет « и охарактеризовать сеть «Интернет» как средство преступной деятельности; - определить критерии классификации и виды преступлений в сети «Интернет»; раскрыть более подробно виды преступлений в сети «Интернет»; рассмотреть особенности проблемы квалификации преступлений, совершенных в сети «Интернет»; дать характеристику элементам состава преступлений в сети «Интернет»; определить юридическую ответственность за преступления в сети «Интернет»; рассмотреть общие тенденции компьютерной преступности в современной России.

Предметом для исследования выступит глобальная сеть «Интернет», в которой совершается большое количество преступных деяний. Объектом исследования будет вся масса общественных отношений, которая регулируется и обеспечивается законодательными актами, которые регулируют правоотношения между субъектами в сети «Интернет».

Оглавление

Введение

Актуальность темы исследования. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы [31] в качестве приоритетного направления внутренней политики определяет развитие информационных и коммуникационных технологий, формирование информационного пространства и соответствующей инфраструктуры. Информационные технологии все глубже проникают в повседневную жизнедеятельность большинства граждан. Отмечается, что в 2016 г. в России на 100 человек приходилось 159,95 мобильных телефонов и из 100 человек 71,29 человека использовали мобильный доступ к сети «Интернет». Средняя скорость в сети «Интернет» возросла на 29 %, что ставит Россию на один уровень с Францией, Италией, Грецией [6, с. 14].

Примерно с середины 2000-х гг. электронные средства массовой информации, информационные системы, социальные сети, технологии беспроводного доступа в сеть «Интернет», мобильная связь постепенно становились частью повседневной жизни россиян. Государство поощряет указанные тенденции: создана система предоставления государственных и муниципальных услуг в электронной форме, что позволяет гражданам направлять в электронной форме индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления.

В настоящее время активно продолжается процесс цифровизации практически всех сторон жизнедеятельности посредством внедрения технологий искусственного интеллекта, биометрической идентификации, работы с большими объемами данных, облачного хранения информации, дистанционного банковского обслуживания. Широко обсуждается перспектива использования технологии блокчейн, в том числе и в сфере оказания государственных и муниципальных услуг. Все большее количество персональной информации пользователи помещают в информационные системы: посредством электронной почты пересылаются копии документов,

удостоверяющих личность, на сервисы платежных систем направляются реквизиты банковских карт, в социальных сетях размещается информация о личной жизни, посредством мессенджеров передается иная конфиденциальная информация. Помимо этого, интеллектуальные системы поисковых сервисов на основе анализа запросов пользователя с высокой точностью формируют его социальный портрет, включая род занятий, круг интересов, уровень доходов, географию перемещений, социальные связи и пр.

Эти и другие глобальные изменения в сфере информационных процессов не могли не сказаться на состоянии преступности. По данным ГИАЦ МВД России, содержащимся в Отчетах о преступлениях, совершенных в сфере телекоммуникационной и компьютерной информации – «Форма 1-ВТ», утвержденная приказом МВД России от 1 апреля 2002 г. № 311 [42], в 2019 г. в производстве правоохранительных органов находились уголовные дела о 105645 преступлениях, совершенных с использованием информационно-коммуникационных технологий, что на 24,5 % превышает аналогичный показатель прошлого года – 79704 [8]. Следует отметить, что подобная тенденция неуклонно сохраняется на протяжении последних лет.

Цель исследования – провести комплексное исследование различных видов и составов преступлений, которые совершаются в сети «Интернет».

Задачи исследования:

- - Раскрыть содержание понятия сети «Интернет и охарактеризовать сеть «Интернет» как средство преступной деятельности;
- - определить критерии классификации и виды преступлений в сети «Интернет»;
- - раскрыть более подробно виды преступлений в сети «Интернет»;
- - рассмотреть особенности проблемы квалификации преступлений, совершенных в сети «Интернет»;
- - дать характеристику элементам состава преступлений в сети «Интернет»;

- - определить юридическую ответственность за преступления в сети «Интернет»;
- - рассмотреть общие тенденции компьютерной преступности в современной России.

Предметом для исследования выступит глобальная сеть «Интернет», в которой совершается большое количество преступных деяний. Объектом исследования будет вся масса общественных отношений, которая регулируется и обеспечивается законодательными актами, которые регулируют правоотношения между субъектами в сети «Интернет».

Выпускная квалификационная работа структурирована в соответствии с поставленными целью и задачами исследования и включает: введение, три главы, заключение и список используемой литературы и используемых источников.

Глава 1 Общие представления о преступлениях в сети «Интернет»

1.1 Характеристика среды «Интернет» как средства преступной деятельности

Повсеместное использование компьютерных технологий в жизнедеятельности современного человека уже является неотъемлемым атрибутом современности. Одновременно с развитием положительных тенденций от активного внедрения компьютерных технологий существует и ряд негативных его проявлений – это распространение преступных деяний, которые совершаются с задействованием в них компьютерных технологий. Так, известная компьютерная компания «Нортон» опубликовала статистические данные своих исследований, где оказалось, что более 85% граждан в России хотя бы однажды оказывались жертвами преступных посягательств в сфере компьютерных технологий, а материальный ущерб от данного вида преступлений составил более 113 триллионов долларов [52]. Таким образом, возможно предположить, что уже в скором будущем для России будет вполне реальна угроза повсеместного распространения различного вида компьютерных преступлений, которые возможно сдержать и предотвратить только лишь имея эффективные методы воздействия и соответствующую правовую базу, которая будет учитывать требования к специфике компьютерных преступлений. Одновременно с тем, преступления в сети «Интернет» обладают чрезмерно быстрой адаптивностью и изменчивостью, подстраиваясь под изменения в законодательстве и продолжа посягать на общественные отношения и права граждан.

По общепринятому шаблону изложения, прежде чем перейти к анализу сети «Интернет» как средства реализации преступной деятельности, необходимо раскрыть содержание самого понятия «Интернет», что позволит более глубоко изучить те обстоятельства, которые позволяют использовать «Интернет» как преступную среду.

Итак, легально закрепленного понятия о том, что же такое «Интернет» на сегодняшний день нет ни в одном законе, что уже само по себе является большим упущением со стороны законодателя, поскольку, например, ФЗ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» [66] в статье 2 приводит перечень понятий, которые используются в законе, среди которых есть определение термину «сайт в сети «Интернет» - это совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет») по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет». Далее, в этой же статье раскрываются понятия страницы сайта в сети «Интернет», владелец сайта сети «Интернет» и многие другие, но, удивительно, в этом перечне отсутствует само родовое понятие, что же такое «Интернет». Из содержания данной статьи и косвенно из различных терминологических определений можно сделать вывод, что «Интернет» - это сеть, не более. Иные законодательные акты используют термин «Интернет» конкретно для раскрытия диспозиции статьи, без раскрытия самого понятия «Интернет». Так, в УК РФ [58] имеется перечень статей, где есть указание на сеть «Интернет». Например, в статье 110 УК РФ говорится о возможном доведении до самоубийства используя сеть «Интернет», в статье 151.2 УК РФ говорится о вовлечении несовершеннолетнего в совершение действий, которые представляют опасность для жизни несовершеннолетнего, опять же, за действуя сеть «Интернет», в статье 171.2 УК РФ речь идет незаконной организации проведения азартных игр через сеть «Интернет», статья 185.3 УК РФ содержит состав преступления, предусмотренного за Манипулирование рынком, то есть умышленное распространение через средства массовой информации, в том числе электронные, информационно-телекоммуникационные сети (включая сеть «Интернет»); в статье 205.2 УК РФ говорится о возможности публичного

призыва к осуществлению террористических действий посредством сети «Интернет»; статья 228.1 УК РФ содержит наказание за факты незаконного производства, сбыт или пересылку 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 посредством использования сети «Интернет»; статья 238.1 УК РФ Производство, сбыт или ввоз на территорию Российской Федерации фальсифицированных лекарственных средств или медицинских изделий, либо сбыт или ввоз на территорию Российской Федерации недоброкачественных лекарственных средств или медицинских изделий, либо незаконные производство, сбыт или ввоз на территорию Российской Федерации в целях сбыта незарегистрированных лекарственных средств или медицинских изделий, опять же с помощью сети «Интернет»; статья 242 УКРФ содержит наказание за незаконное изготовление и (или) перемещение через Государственную границу Российской Федерации в целях распространения, публичной демонстрации или рекламирования либо распространение, публичная демонстрация или рекламирование порнографических материалов с применением сети «Интернет»; в статье 245 УК РФ говорится о назначении наказания лицам, которые публично осуществляют демонстрацию жестокого обращения с животными через сеть «Интернет», через сеть «Интернет» можно также начать возбуждение и пропаганду ненависти или вражды, а также унижать человеческое достоинство, что является составом преступления, предусмотренного статьей 282 УК РФ. Перечисленные статьи уже свидетельствуют о широком распространении различных видов преступлений, которые можно совершить с использованием сети «Интернет». Итак, общим для всех этих статей будет указание на «Интернет» как на информационно-телекоммуникационную сеть.

Сегодня уже практически каждый человек знает, что такое «Интернет», но не каждый может четко сказать его определение содержания. Многие люди

путают всемирную сеть WWW подразумевая, что это и есть «Интернет». Однако это не так, потому как электронная почта, IP-телефония, многие приложения телефонов – это также «Интернет». Даже блокчейн также является частью «Интернета». Так что же такое «Интернет» и есть ли у него конкретное определение? Для ответа на данный вопрос нам необходимо обратиться к специализированной литературе. «Интернет» дословно переводится с английского как «В сети», что уже раскрывает содержание термина с логической стороны вопроса. Например, У. Одом дает следующее определение [32, с. 24]: «это всемирная система объединенных компьютерных сетей для хранения и передачи информации». Синонимами термина «Интернет» выступают «Всемирная сеть» или «Глобальная сеть», можно называть и просто – «Сеть». Как раз на основе «Интернета» и работает всемирная паутина WWW [53, с. 216]. Э. Таненбаум также говорит о том, что «Интернет» – это глобальная сеть, которая связывает между собой пользователей компьютеров по всему земному шару.

Итак, разобравшись с сутью понятия «Интернет» теперь несложно ответить на вопрос, почему же говорят о том, что «Интернет» – это хорошая среда для преступной деятельности. Во-первых, в просторах «Интернет» циркулируют огромные потоки информации, естественно, часть из которого может носить противоправное и запрещенное содержание, например, распространение порнографического материала [18, с. 22], а также пиратские копии фильмов или музыки. Во-вторых, на просторах сети также очень большое количество желающих, которые хотят получить нечто запрещенное, например, наркотические вещества. Естественно, с подобными запросами человек не может выйти на улицу, а в сети «Интернет» подобные поиски можно производить инкогнито. В-третьих, уровень безопасности общественных мест активно повышается за счет установления камер общественного наблюдения, что также затрудняет совершение противоправных действий в реальном мире. В свою очередь, в сети «Интернет» можно «укрыться» спрятав координаты своего расположения и

другие опознавательные данные и заниматься противоправными деяниями. При этом нужно учитывать, что сеть «Интернет» является «всемирной паутиной», где нет границ и преград, что также существенно усложняет возможность обнаружения преступника в киберпространстве и увеличивает опасность его противоправного деяния. С другой стороны, современное уголовное законодательство России еле успевает изменять нормативную базу ввиду активного расширения разнообразий возможных преступлений в сети «Интернет». Так, отдельные действия, которые могут обладать признаком общественной опасности, могут быть не выявлены рамками уголовного законодательства. Кроме того, необходимо также обратить внимание, что отечественное законодательство не в полной мере соответствует еще международному уровню, например, положениям Конвенции Совета Европы «О преступности в сфере компьютерной информации» [20] (EST №о 185), что затрудняет применение единообразных определений понятий «преступление, совершаемое с использованием компьютерных технологий», «компьютерные технологии», «использование компьютерных технологий».

Вышеуказанные причины не являются исчерпывающими при ответе на вопрос, почему сеть «Интернет» воспринимают как средство преступной деятельности. Еще пару лет назад было очень трудно найти преступника в сети «Интернет», а уж тем более – привлечь его к ответственности. На сегодняшний день ведутся активные разработки, которые направлены на отслеживание, выявление и пресечение противоправных действий в сети «Интернет». Кроме того, вносятся изменения в положения действующего законодательства с учетом корректировки квалификации преступлений с учетом сети «Интернет». Активно развиваются положения законодательства, которые регулируют правоотношения в сети «Интернет» для того, чтобы охранять права порядочных граждан от посягательств на них со стороны злоумышленников.

1.2 Критерии классификации преступлений в сфере «Интернет»

Богатое разнообразие видов противоправных деяний в сети «Интернет» побуждает науку и теорию права разрабатывать разнообразные правообразующие структуры для унификации правового пространства между ними, а, попросту говоря, выделять признаки, по которым возможно было бы классифицировать преступные действия. Выделяя критерии классификации преступлений в сети «Интернет» также необходимо учитывать, что все они не имеют территориальных границ и пространственного ограничения в принципе, и противодействие должно осуществляться на международном уровне при согласовании тактик и методик государствами в мире. Благодаря тому, что страны достигают по этому вопросу определенных соглашений и подписывают соответствующие договоры и получается возможность структурирования и классификации преступлений в сети «Интернет» на международном уровне. Самыми родственными договорными документами для Российской Федерации можно указать международные документы, которые принимаются в Европейском правовом пространстве и СНГ.

Подробный анализ, а также скрупулезная имплементация указанных в международных актах составов преступлений в сети «Интернет» позволило облегчить преследование лиц, которые совершили преступления в компьютерной среде или с применением сети «Интернет» в России. Кроме того, сегодня по всему миру ведется политика унификации составов преступлений, совершенных в сети «Интернет» в законодательства стран с целью их единообразного выделения составов преступных деяний и последующей квалификации деяния.

Самым первым международным актом, который провозгласил факт классификации преступных деяний в сети «Интернет», а также отобразил собой необходимость унификации явилась Рекомендация № R 89 (9) Комитета Министров стран – членов Совета Европы о преступлениях, связанных с компьютерами, принятая 13 сентября 1989 г. [45] В данном документе также

имеется отсылка на необходимость обращения к «Отчету Европейского комитета» по проблемам преступности о преступлениях, связанных с компьютерами, где указана оценка явлению компьютерной преступности и представлены руководящие указания для криминализации противоправных деяний в законодательстве стран – участниц. Тем не менее, по мнению ряда авторов [12, с. 12; 73, с. 49], рекомендательный характер указанного документа не способствует разрешению возникающих на практике коллизий и не отменяет необходимости подписания полноценных международных правовых документов.

Так, в соответствии с критериями выделения классификации преступлений в сети «Интернет» в Отчете к минимально необходимым преступлениям отнесены:

- Компьютерное мошенничество, которое раскрывается как ввод, изменение или удаление данных или программ компьютера или иное вмешательство в процессы обработки данных, которое оказывает влияние на итог процесса обработки данных. Этот процесс, в конечно итоге причиняет экономический ущерб или приводит к уничтожению собственности другого лица, совершается с целью получения незаконным путем экономической выгоды для себя или для другого лица.
- Компьютерный подлог - это ввод, изменение или удаление данных (программ) компьютера либо вмешательство иного рода в процесс обработки данных, которое совершается способом или при условиях, установленных нормами национального законодательства, которыми эти деяния квалифицируются как подлог, и совершены в отношении традиционного объекта правонарушения.
- Причинение ущерба компьютерным данным или компьютерным программам – это незаконное удаление, причинение ущерба или ухудшение качества данных или программ компьютера.

- Компьютерный саботаж - это ввод, изменение или удаление данных или программ компьютера, или создание помех компьютерным системам с целью воспрепятствования работе компьютера или телекоммуникационной системы.
- Несанкционированный доступ - это неправомочный доступ к системе или компьютерной сети путем нарушения мер охраны.
- Несанкционированный перехват – это неправомерный и осуществленный с применением технических средств перехват сообщений, направленных в систему или сеть компьютеров, исходящих из системы или сети компьютеров и передаваемых в рамках системы или сети компьютеров.
- Несанкционированное воспроизведение компьютерной программы, охраняемой авторским правом. Это совершенное неправомерно распространение, воспроизведение или передача в общественное пользование компьютерной программы, охраняемой законом.
- Несанкционированное воспроизведение микросхемы - это совершенное неправомерно воспроизведение микросхемы изделия на полупроводниках, если она охраняется законом, либо неправомерное использование или импорт в коммерческих целях микросхемы или изготовленного с ее применением изделия на полупроводниках.

Дополнительный перечень правонарушений в соответствии с Отчетом включает в себя следующие критерии для выделения критериев классификации противоправных деяний в сети «Интернет»:

а) Неправомерное изменение данных или программ в компьютере.

б) Компьютерный шпионаж, который в соответствии с Рекомендацией определен как получение незаконными способами или раскрытие, передача или использование торговой или коммерческой тайны лицом, не имеющим на это прав или какого-либо иного законного основания, с целью причинения экономического ущерба лицу,

имеющему доступ к этой тайне, или получения незаконной экономической выгоды для себя или третьего лица.

в) Несанкционированное использование компьютера – это незаконное использование системы или сети компьютеров, которое совершается:

1) лицом, которое имеет право использовать систему, с осознанием того, что действия этого лица увеличивают риск причинения ущерба системе или ее функционированию либо причиняют такой ущерб;
2) любым лицом с целью причинения ущерба управомоченному пользователю системы, функционированию системы или самой системе;
3) любым лицом с фактическим причинением ущерба системе в целом, функционированию системы или управомоченному пользователю системы.

г) Несанкционированное использование компьютерной программы, охраняемой законодательством: неправомерное использование охраняемой законом компьютерной программы либо воспроизведение без права на это, совершаемые с целью получения незаконной прибыли для злоумышленника или третьих лиц либо причинения правообладателю ущерба [1].

К более сложным критериям классификаций преступлений, совершенных в сети «Интернет» можно отнести критерии классификации по объекту преступного посягательства; по предмету преступного посягательства; в зависимости от субъекта преступления; по признаку их территориальности; по способу совершения.

Так, по объекту преступного посягательства можно отдельно выделить преступления против собственности – это мошенничество, кражи и вымогательство – все эти виды преступлений гораздо проще реализовывать в сети Интернет, оказывая на жертву психологическое давление и шантажируя

электронными доказательствами и фактами, особенно если они были обработаны в специализированных программах и на самом деле не соответствуют действительности, что загоняет жертву в еще более суровые рамки и заставляет идти на поводу у злоумышленников, используя уже вместе с шантажом и вымогательство. Могут быть и иные случаи, когда действия, которые носят характер мошенничества или злоупотребления доверием или обманом переквалифицируются в иные деяния. Например, следователем следственной части СУ при МВД Республики Башкортостан 23 июня 1999 г. было возбуждено уголовное дело по признакам преступления, предусмотренного статьей 158 УК РФ по факту несанкционированного доступа к сети Интернет. В ходе следствия обвинение было предъявлено М. и Н., их действия были переквалифицированы по статьям 183 («Незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну») и 272 УК РФ. В отличие от рассмотренных ранее дел, связанных с распространением программ, предназначенных для хищения паролей для доступа к сети Интернет и пользование впоследствии таким доступом за чужой счет, в данном случае статья 273 УК РФ за это вменена не была. Хищение имен и паролей для доступа было квалифицировано по статье 183 УК РФ. Статья 165 УК РФ вменена не была, что представляется упущением следствия.

Отдельно стоит уделить внимание в рамках классификации преступных деяний, совершенных в сети «Интернет» действиям мошеннического характера, которые совершаются с применением заведомо ложных, фальсификационных платформ электронных платежных систем и средств. Так, преступники организуют в сети «Интернет» различные онлайн-аукционы и магазины, и, злоупотребляя доверием, побуждают своих жертв оплачивать несуществующее покупки, переводя денежные средства на нужные счета. Более того, в сети «Интернет» уже так же, как и в реальной жизни, развито огромное многообразие различных форм и видов мошеннических действий. Например, даже открываются онлайн ломбарды, которые, скорее всего, будут

заниматься реализацией краденых вещей. Помимо ломбардов, в сети «Интернет» также легко заниматься незаконной предпринимательской деятельностью и заниматься обналичиваем денежных средств через электронные кошельки. Правоохранительные органы, конечно же, занимаются проверками организаций, которые работают в сети «Интернет», но их количество растет с каждым днем, и причем в геометрической прогрессии, что является нереальным к постоянному мониторингу. К тому же, если будет выявлена и закрыта одна нелегальная организация, функционирующая незаконно в сети «Интернет», на ее месте откроется тут же несколько, ей подобных и т.д.

Следующим видом в рамках критерия классификации по объекту преступного посягательства в сфере «Интернет» можно назвать несанкционированный доступ к информации, которая хранится на персональных компьютерах пользователей, а также на рабочих компьютерах организаций. В данном случае данный вид преступного посягательства может иметь несколько подвидов – это может быть простое вторжение удаленно на необходимые компьютеры, или же, установка вредоносного программного обеспечения, которое будет в течение длительного времени осуществлять передачу необходимой информации злоумышленникам.

Если взять иной критерий – по предмету преступного посягательства, то в сфере «Интернет» можно выделить следующие виды преступлений. Это, прежде всего преступления, которые имеют своим предметом посягательства конкретный материальный предмет как средство наживы в корыстных целях, так и в качестве использования его в последующем как инструмента, для совершения иного преступного деяния.

С другой стороны, имеются также и преступления в сети «Интернет» которые и не имеют материального своего воплощения – то есть тут речь идет об информации. И это будет наибольший объект преступных посягательств, потому как в основном в «Интернете» охотятся за информацией.

Если же говорить о другом критерии классификаций преступлений, совершенных в сети «Интернет», то иным признаком будет уже субъект преступного посягательства. В данном случае можно отдельно вычленять по количеству субъектов, которые совершили преступное деяние. Конкретно в сети «Интернет», как правило, работает сразу группа злоумышленников, в которой каждый занят своей работой – кто-то пишет хакерскую программу, кто-то занимается сбором и анализом полученных данных и т.п.

Ну и наиболее «скучный» критерий классификации может быть вычленен еще и по признаку территориальности – это когда преступник и потерпевший находятся на одной территории, то есть, например, в пределах одного государства, или же в пределах одного субъекта федерации, или же они находятся в разных административно-территориальных единицах, или же даже государствах.

На первый взгляд критерий о территориальности кажется вообще нецелесообразным и малоинформативным, но, он помогает группировать преступления в сети «Интернет» по характеру их локализации, что поможет правоохранительным органам выявить расположение преступника, или же некоторые данные, которые помогут выйти на преступника.

Таким образом, использование компьютерных технологий при совершении преступлений является особой разновидностью общественно опасной и противоправной деятельности, в настоящее время получающей все большее распространение как в глобальном масштабе, так и в отдельных странах, в том числе и в России [36].

Критерии классификации преступлений в сети «Интернет» могут быть совершенно различными, в зависимости от предмета, объекта и т.п. выделенного в качестве основы. Большое разнообразие критериев классификации преступлений в сети «Интернет» обусловлено большим количеством разновидностей самих преступлений, виды которых постоянно растут в связи с высокой изобретательной способностью мошенников и лиц, которые занимаются противоправными действиями в сети «Интернет».

Глава 2 Виды преступлений в сфере «Интернет»

2.1 Кардинг, Фишинг, Вишинг, Скимминг, Шимминг

Сейчас банковские карты не менее распространены, чем наличные деньги. А везде, где есть деньги, появляется вероятность их потерять. По данным компании Zecurio№, занимающейся обеспечением кибербезопасности, более миллиарда рублей было похищено с банковских карт россиян в 2018 году [50]. Мировой лидер банковской статистики The №ilso№ Report сообщил: в 2017 году было украдено $6,97 из каждых потраченных $100 с банковских карт [34]. И эта цифра будет увеличиваться как минимум до 2021 года.

Мошеннические схемы то и дело претерпевают изменения. Согласно обзору ФинЦЕРТа [51], объем несанкционированных операций, совершенных с использованием платежных карт, эмитированных на территории РФ, в 2018 году составил 1,4 млрд рублей, что на 44% больше, чем в прошлом году. По данным Генпрокуратуры, количество выявляемых в России киберпреступлений за шесть лет выросло почти в 16 раз, до 174 тысяч (сюда входят и незаконные операции с картами) [5]. Владельцам важно сохранять бдительность и не попадаться на уловки мошенников.

Разберемся, с какими видами кардинга можно столкнуться и как защитить свои средства.

Так, термином кардинг (cardi№g) называют мошеннические операции с платежными картами (реквизитами карт), не одобренные держателем карты [25, с. 51]. Кардинг включает в себя различные способы обмана законных владельцев материальных средств.

Вид мошенничества, целью которого является воровство денег с банковской карты, называют карточным фродом, или кардингом. Кардинг - это, в первую очередь, осуществление банковских операций по карте, не инициированных самим пользователем данной карты. Не обязательно

воровать физическую банковскую карту, чтобы оставить пользователя без денег на счете.

Понять, что субъект стал жертвой фрода довольно просто: кто-то осуществляет операции с банковской картой без ведома ее владельца, в то время как карточка владельца находится у него. Если карта человека привязана к телефонному номеру, то он может получить уведомление на сотовый телефон о списании средств. Если телефон не привязан, а баланс карты вызывает у его пользователя сомнения и недоумение, то необходимо будет проверить историю операций по карте на сайте обслуживающего банка или в его физическом офисе.

Выделяют два классических вида кардинга: фишинг и скимминг. Можно выделить три базовых направления мошеннических действий [72, с. 39]:

1. Кража или незаконное получение карты - это либо физическое воздействие на владельца, либо поиск уязвимости в процессе выдачи, доставки или оформления банковского продукта и использование карты злоумышленником.

2. Компрометация данных карты для последующего изготовления подделки. В первую очередь речь идет о копировании данных магнитной полосы карты и краже PI№-кода. Наиболее широко этот вид мошенничества был распространен до массового перевода карт на чиповые технологии. Сегодня такая схема встречается редко, так как в России около трех лет назад ввели запрет на выпуск нечиповых карт, а почти по всему миру действует Chip Liability Shift - обязанность банка-эквайера обслуживать карту с чипом именно по чипу.

3. Компрометация реквизитов карты для совершения операций C№P (без присутствия карты). Яркий пример - оплата покупок или услуг в «Интернете».

Конечная цель преступников во всех случаях - получить доступ к деньгам. Для реализации своих замыслов мошенники изобретают весьма

хитрые схемы, нередко пользуясь доверчивостью и невнимательностью граждан.

Один из популярных способов обвести вокруг пальца собственника карты — это фишинг. Фишинг (phishi№g от англ. fishi№g рыбная ловля, закидывание удочки) — буквально выуживание реквизитов карты у ее держателя [17,с. 53]. Примечательно, что необходимые данные передает сам владелец. Как правило, прибегают к нескольким видам фишинга.

СМС-фишинг**.** На телефон отправляют сообщение:

- о блокировке карты, якобы от имени банка и номером телефона, позвонив по которому, можно решить проблему;
- о выигрыше, забрать который можно, заплатив за доставку.

Вариаций смс-фишинга масса, но все они сводятся к предложению передать данные карты [24, с. 28]. В таких случаях нужно проявить бдительность. Если поступили сведения о блокировке, следует звонить в банк по официальному номеру, а подлинность сообщения о выигрыше уточнить, связавшись с магазином или сервисом, проводящими акцию.

«Интернет»-фишинг. Мошенники создают фишинговые (поддельные) страницы, имитирующие официальные сайты банков, платежных сервисов или магазинов, меняя в названии несколько букв или знаков [70, с. 48]. Увы, далеко не все внимательно проверяют веб-адрес, смело кликая на ссылку. Нередко злоумышленники заманивают на фишинговые сайты, отправляя поддельные электронные письма, составленные техподдержкой банка, скажем, о блокировке карты. Под предлогом проверки информации о держателе они просят ввести все реквизиты, узнав которые, беспрепятственно получают доступ к деньгам. Выманивают данные и прикрываясь продажей товаров.

Прежде, чем оставлять реквизиты карты на сайте, нужно тщательно сверить веб-адрес с официальным названием магазина, сервиса или платежной системы, а также проверить ссылки, находящиеся на странице: если ресурс фишинговый, скорее всего, они не работают. Когда нужно воспользоваться

сайтом кредитной организации, лучше сразу обратиться к_официальному перечню, размещенному на сайте ЦБ. Такие «письма счастья» содержат ссылку, по которой якобы очень важно перейти. Например, для получения неожиданного выигрыша, подарка или даже государственной субсидии [10, с. 17]. После перехода по этой ссылке от пользователя, конечно же, потребуют данные вашей банковской карты. Реквизиты, CVV, пин-код - все это может стать целью мошенников. После получения такой информации украсть деньги с карты ее владельца не составит никакого труда. Часто для фишинга используются сайты-клоны. Это может быть сайт-клон обслуживающего пользователя банка, стартовой страницы социальной сети, «Интернет» - магазина. Звонки якобы из налоговой или из банка, сообщения со взломанных страниц друзей в социальных сетях — все может пойти в ход. Даже подложных смс от родственников или от детей, попавших в беду, мошенники-фишеры не гнушаются.

К сожалению, стопроцентную гарантию на сохранность денег их владельцу не даст ни одно правило безопасности. Здесь все как с классическими деньгами — мошенники могут найти подход даже к самым осторожным и предусмотрительным лицам. Но есть несколько советов, которые позволят минимизировать риски финансовых потерь от фишинга:

Во-первых, нельзя афишировать или передавать данные своей банковской карты, нельзя фотографировать карту и не выкладывать это фото в сеть без крайней необходимости. Индивидуальный дизайн карты с фотографией животного — это хорошо, но лучше не хвастаться им демонстративно. Фотографии лицевой стороны карты иногда бывает достаточно, чтобы действия с ней мог произвести кто-то, помимо ее пользователя. Фото может попасть в сеть, а как им распорядятся пользователи «Интернета» — вопрос открытый.

Во-вторых, нельзя посещать сомнительные сайты, нельзя переходить по ссылкам, в которых пользователь не будет уверен. Необходимо проверять адресную строку привычных сайтов — минимальная разница в написании

может выдать сайт-клон. Также стоит использовать банковскую карту в «Интернете» только на проверенных, известных сайтах, которые используют двухфакторную аутентификацию — просят пользователя не только ввести данные карты для оплаты, но и подтвердить платеж по сотовому телефону. Конечно, любой сайт может быть взломан, но с крупными структурами это сложнее. Нарваться на мошенников, оплачивая покупки в известном «Интернет» - магазине или через реальный сайт банка.

Кроме того, если соблюдать ряд простых правил, то можно хорошо обезопаситься от преступных посягательств:

Если пользователю придет сообщение на сотовый телефон или письмо на электронную почту от его близких с просьбой о помощи — нельзя поддаваться н эмоции. Необходимо сперва дозвониться до близких и уточнить, действительно ли от них поступило уведомление о помощи. Мошенники могут использовать социальные связи для бóльшего эмоционального вовлечения. Гораздо проще заполучить конфиденциальную информацию ее владельца, выбив его из состояния эмоционального равновесия.

Вишинг (англ. vishi№g — от voice phishi№g) идентичен фишингу, с той только разницей, что злоумышленники звонят по телефону, представляясь сотрудниками банка, покупателями товаров и так далее, таким образом пытаясь выманить у держателя PI№-код или заставить его совершить определенные действия со счетом [69, с. 26].

Владельцу карты нужно помнить, что сотрудники банка не требуют сообщить PI№-код, а в случае блокировки карты, скорее всего, предложат подъехать в офис лично. Покупателям товаров в принципе ни к чему знать конфиденциальные данные о карте продавца, поэтому просьбы сообщить такие сведения должны насторожить.

Еще один метод, которым активно пользуются мошенники, это скимминг. Скимминг — это копирование данных платежной карты с помощью специального устройства (скиммера) [27, с. 19]. Данные карты считываются,

когда владелец вставляет ее в банкомат. Для получения PI№-кода злоумышленники устанавливают мини-камеры или накладки на клавиатуру.

Скимминг — это установка оборудования на банкомат, позволяющего считать и записать данные банковской карты, чтобы в дальнейшем изготовить ее копию. Для скимминга может использоваться считывающее оборудование, которое встраивают в банкомат или платежный терминал, микро-видеокамера, а также вредоносное программное обеспечение для банкомата. Стать жертвой скимминга можно как снимая деньги в банкомате, так и расплачиваясь карточкой в супермаркете или ресторане.

Не попасться на крючок проще, если не забывать об этих правилах:

– Необходимо найти проверенный банкомат, то есть лучше снимать деньги в одном и том же банкомате. Необходимо тщательно изучить его внешний вид - любые изменения могут указывать на установленное оборудование для фишинга. Лучше всего выбрать своим постоянным банкоматом тот, который находится внутри отделения банка.
– Если все же приходится снять деньги в непривычном месте, необходимо быть предельно внимательным и избегать банкоматов, которые расположены в людных местах, потому как на такие проще всего установить скимминговое оборудование и остаться незамеченными. Очень важно обращать внимание на внешний вид банкомата: пользователя должны насторожить выпуклая или шатающаяся клавиатура, накладки на картоприемник и прочие детали, выглядящие инородно. Дел в том, что Скимминг-оборудование крепится довольно слабо по сравнению в первоначальной комплектацией банкомата. Следы клея, сколы, рекламные наклейки все это тоже должно насторожить пользователя.

Также необходимо при каждом введении пин-кода прикрывать клавиатуру рукой: от камер и лишних глаз зевак это должно защитить.

Однако, даже соблюдая все правила безопасности, бывает сложно отличить оборудование для скимминга от оригинального.

- Для минимизации возможности кражи денежных средств с карты необходимо привязать к банковской карте номер телефона и настроить быстрые уведомления об операциях по карте. Если что-то пойдет не так, пользователь сможет быстро среагировать и заблокировать карту.
- По возможности, необходимо переходить на пользование карт с с электронным чипом. Подделать такие карты куда сложнее.
- Установите лимит на снятие/перевод денег. Если захотите снять больше, вы сможете выполнить операцию через подтверждение в банке. Зато если вашу карту подделают, украсть все не получится.

Если вам все-таки не повезло, и пользователь карты стал жертвой карточного фрода, необходимо срочно звонить в банк, блокировать карту и обращаться с заявлением в правоохранительные органы. Если транзакции были совершены не пользователем карты, то чем скорее это будет доказано, тем больше вероятность вернуть денежные средства обратно. Чаще всего ответственность за «фрод» несут банк, выпустивший карту, банк, обеспечивающий вашу транзакцию в «Интернете», или банк, в чьем банкомате вы производили действия [11, с. 46]. Особенно осторожно необходимо совершать действия с картой заграницей. Существует целый список стран, в которых «фрод» особенно распространен. Как правило, после пользования картой в таких странах, банк предлагает совершить ее перевыпуск.

Следующий распространенный вид мошенничества с использованием банковских карт – Шимминг. Это модернизированная разновидность скимминга. Схема обмана аналогична: со вставляемых в банкомат карт считываются все важные данные, отличие лишь в том, что визуальных признаков присутствия «шима» внутри аппарата нет. Мошенники вместо весьма громоздких и визуально заметных накладок на картоприемник используют тонкое, гибкое, практически незаметное устройство, которое

располагается внутри картридера. Оно считывает данные карты, используемые впоследствии злоумышленниками.

Иногда мошенники создают поддельные банкоматы, оставляя их в неохраняемых местах. Такие устройства внешне полностью копируют настоящие, а вот «начинка» содержит встроенный компьютер с установленной на него системой, скиммер и накладки на клавиатуру. Жертва вставляет карту, пытается совершить какие-то действия, но банкомат выдает ошибку. Человек забирает карту, но вся информация с нее уже считана. Попасться на удочку злоумышленников можно не только пользуясь банкоматом, но и расплачиваясь картой, скажем, в ресторанах или магазинах. Алгоритм схож: официант, продавец или кассир, могут использовать скиммер или переносное устройство, прикрепленное к терминалу [54, с. 38].

Защититься от скимминга можно, если пользоваться банкоматами, находящимися в отделениях банков. Уровень защиты в кредитных организациях в разы выше, и установить считывающие устройства там намного сложнее.

Если же возможности обратиться в отделение нет, необходимо выбирать банкоматы, стоящие под камерами, в охраняемых местах. Визуально необходимо проверять аппарат, скажем, накладку на картоприемник: если она шатается, значит, с ней что-то не так. Расплачиваясь картой, следите, чтобы ее данные никто не фотографировал на телефон [54, с. 38].

Следующий вид мошенничества - Внедренные вирусы. В этом случае злоумышленники внедряют в электронное устройство (телефон, компьютер) программу, способную считывать данные карты. Подобные вирусы могут передавать мошенникам информацию, которую пользователь вводил в «Интернет» - браузер: логины и пароли от социальных сетей, «Интернет»-банков, электронных кошельков, различных сайтов и так далее.

Вредоносная программа может попасть на телефон или ноутбук случайно, под видом другой программы, неосторожно скачанной из электронного письма или с непроверенного сайта. Чтобы избежать обмана,

важно вовремя обновлять антивирус и пользоваться только лицензионным софтом.

Перечень описанных видов мошенничества не исчерпывающий. А. Сизов, начальник отдела по противодействию мошенничеству Центра прикладных систем безопасности «Инфосистемы Джет», отмечает, что среди мошеннических схем встречаются [2]:

- Использование реквизитов карт для получения доступа к другим продуктам, например, ДБО или онлайн-кредитованию, где информация о карте, последних операциях и тем более коды подтверждения и паспортные данные являются достаточными сведениями для смены паролей в онлайн- или мобильном банке и совершения иных манипуляций со счетами.
- Кража средств с бесконтактных карт. Эта схема наделала много шума некоторое время назад, однако больших потерь зафиксировано не было, и вряд ли стоит ожидать существенных проблем в этом направлении.

С течением времени схемы обмана только совершенствуются. Естественно, с злоумышленниками активно борются сами банки.

«С мошенничеством борются профильными системами антифрод-мониторинга, следящими за поведением карт (совокупностью характеристик по количеству операций, суммам, месту проведения и типу операций). Такие системы стали обязательными с 2003-2004 года, когда появились требования по мониторингу со стороны международных платежных систем Visa и Mastercard [48].

Кроме автоматизированных систем, большой вклад в безопасность внесла технология «чиповых» карт, которая практически полностью исключила возможность эффективного клонирования. Помимо этого, банки постоянно занимаются контролем ключевых процессов по выпуску карт, их дистанционной доставки и прочих, что на самом деле связано с задачами идентификации и аутентификации держателя очно или дистанционно»

Однако не только банки, но и сами владельцы карт должны принимать меры предосторожности. А. Цыганова, старший юрисконсульт консалтинговой компании Alta Via, всем, кто заботится о сохранности своих денежных средств, советует соблюдать несколько простых правил [2]:

- Хранить PI№-код, а также данные для входа в «Интернет»-банк (логин, пароль, проверочные слова или специальные коды) в безопасном месте, а лучше всего - в своей памяти.
- Не сообщать третьим лицам данные карты и одноразовые СМС-пароли для подтверждения операций.
- Быть осмотрительными, совершая покупки в «Интернете». Использовать только проверенные и официальные сайты. Товары/услуги на незнакомых сайтах по явно заниженным ценам должны насторожить. А также выбирать банкоматы, расположенные в офисах банка или крупных торговых центрах с видеонаблюдением.

Таким образом, подводя итог данному параграфу, можно заключить, что сеть «Интернет» дает огромный простор для всякого рода совершения преступных деяний, которые по большей своей части имеют признаки состава преступления, характерного для мошенничества. При этом разновидности преступных деяний в сети «Интернет» увеличивают свое разнообразие с поразительной скоростью.

2.2 Распространение противоправной информации в сети «Интернет»

В целях повышения эффективности противодействия распространению противоправной информации (также и суицидального содержания) в сети «Интернет» Роскомнадзором подготовлены методические рекомендации по заполнению формы сообщения от граждан, юридических лиц, индивидуальных предпринимателей, органов государственной власти,

органов местного самоуправления о наличии на страницах сайтов в сети «Интернет» противоправной информации.

В связи с большим количеством случаев публикации материалов суицидального содержания в сети «Интернет» [4, с. 38] и в целях повышения эффективности противодействия распространению нежелательного контента в сети «Интернет» Роскомнадзор подготовил методические рекомендации по заполнению формы сообщения о наличии на страницах сайтов противоправной информации [39, с. 82]. В методических рекомендациях перечислены виды противоправной информации и дана пошаговая инструкция по действию граждан при обнаружении такой информации в сети «Интернет» [30].

Любой гражданин при обнаружении на сайтах информации, запрещенной к распространению (в т. ч. суицидального контента) может направить электронное сообщение в Роскомнадзор, и в случае подтверждения наличия запрещенных материалов, доступ к указанным ресурсам будет ограничен.

Рассмотрим пример из судебной практики. Так, прокурор Советского районного суда г. Самара, действующий в интересах неопределенного круга лиц обратился в суд с заявлением о признании информации, распространяемой в сети Интернет, информацией, распространение которой в Российской Федерации запрещено, в обоснование заявленных требований указал, что прокуратурой <адрес> в ходе мониторинга сети « Интернет « выявлен сайт, <данные изъяты> на страницах которого размещена информация о продаже дипломов и аттестатов об образовании, свидетельств о рождении.

В целях восстановления нарушенных прав граждан и во исполнение действующего законодательства заявитель просил суд признать информацию, распространяемую посредством сети «Интернет», расположенную по сетевому адресу: <данные изъяты> информацией, распространение которой в Российской Федерации запрещено.

В судебном заседании помощник прокурора <адрес> Гриднева Н.В. заявленные требования поддержала, просила их удовлетворить по изложенным в заявлении основаниям.

Представитель У. Р. по <адрес> в судебное заседание не явился, о месте и времени рассмотрения дела извещен надлежащим образом, ходатайств об отложении судебного заседания и о рассмотрении дела в его отсутствие не представил, о причинах неявки суду не сообщил.

Владелец интернет –сайта <данные изъяты>, привлеченный к участию в деле в качестве ответчика, в суд также не явился.

Выслушав доводы заявителя, исследовав материалы дела, суд полагает заявленные требования подлежащими удовлетворению по следующим основаниям.

Вход на сайт свободный, не требует предварительной регистрации и пароля, ознакомиться с содержанием указанной страницы и скопировать информацию в электронном варианте может любой Интернет - пользователь.

В соответствии со ст. 1 Федерального закона от ДД.ММ.ГГГГг. №- ФЗ «О противодействии коррупции» коррупция – это злоупотребление служебным положением, дача взятки, получение взятки, злоупотребление полномочиями, коммерческий подкуп либо иное незаконное использование физическим лицом своего должностного положения вопреки законным интересам общества и государства в целях получения выгоды в виде денег, ценностей, иного имущества или услуг имущественного характера, имущественных прав для себя или для третьих лиц либо незаконное предоставление выгоды указанному лицу другими физическими лицами; противодействие коррупции - деятельность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, институтов гражданского общества, организаций и физических лиц в пределах их полномочий: по предупреждению коррупции, в том числе по выявлению и последующему устранению причин коррупции (профилактика коррупции).

В соответствии с п.1 ст.6 Федерального закона «О противодействии коррупции» одной из мер противодействия коррупции является формирование в обществе нетерпимости к коррупционному поведению.

Согласно ст. 2 Федерального закона от ДД.ММ.ГГГГ №149-ФЗ «Об информации, информационных технологиях и о защите информации» информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Согласно п. 6 ст. 10 Федерального закона от ДД.ММ.ГГГГ № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

В соответствии со ст. 12 ГК РФ способами защиты гражданских прав, в частности, является пресечение действий, нарушающих право или создающих угрозу его нарушения.

Доступ к сайтам, где размещена информация о том, где приобрести указанные услуги должен быть закрыт.

Распространение указанной информации противоречит целям и задачам действующего законодательства о противодействии коррупции.

Таким образом, признание информации, распространяемой посредством сети «Интернет», расположенной по сетевому адресу: https://diplom24.o№li№e/ информацией, распространение которой в Российской Федерации запрещено, влечет юридические последствия.

Суд полагает, что в целях восстановления нарушенных прав граждан и во исполнение действующего законодательства, вышеуказанная информация должна быть запрещена к распространению на территории Российской Федерации.

Вместе с тем, суд отмечает, что в настоящее время требования о признании информации запрещенной к распространению, рассматриваются

по правилам гл. 27.1 КАС РФ «Производство по административным делам о признании информации, размещенной в информационно-телекоммуникационных сетях, в том числе в сети Интернет, информацией, распространение которой в Российской Федерации запрещено».

В силу ч. 2 ст. 265.3 КАС РФ, У. Р. по <адрес> надлежащим ответчиком по данной категории дел не является, в силу чего подлежит освобождению от правовой ответственности.

Суд, рассмотрев доводы и мотивированные требования прокурора пришел к выводу о признании информации, распространяемой посредством сети «Интернет» запрещенной к распространению на территории РФ и удовлетворил исковое прошение [74].

В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

Однако запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Так, с 1 февраля 2014 года вступили в силу изменения, внесенные в Федеральный закон «Об информации, информационных технологиях и о защите информации» [66], согласно которым Генеральный прокурор Российской Федерации и его заместители уполномочены обращаться в Роскомнадзор с заявлением о принятии мер по ограничению доступа к информационным ресурсам, распространяющим призывы к массовым беспорядкам, осуществлению экстремистской деятельности и участию в массовых публичных мероприятиях.

Например, в регионах Дальневосточного федерального округа противодействие экстремизму является одним из приоритетных направлений деятельности органов прокуратуры [33]. Прокурорами в округе осуществляется постоянный мониторинг сети «Интернет» на предмет наличия

в свободном доступе экстремистских материалов и запрещенной информации, а также принимаются меры, направленные на устранение негативного влияния такой незаконной информации.

По итогам проверочных мероприятий по направленным заместителем Генерального прокурора Российской Федерации Ю. Гулягиным материалам проверки Управлением МВД России по Хабаровскому краю возбуждено уголовное дело по признакам преступления, предусмотренного ст.319 УК РФ (оскорбление представителя власти) [40]. Решением Центрального районного суда г. Хабаровска удовлетворены требования заместителя Генерального прокурора Российской Федерации по заявлению о признании информации, размещенной в сети «Интернет» пользователями «Интернет»-ресурса «www.comme№ts.ua» на странице «Интернет» - сайта, запрещенной. По решению суда Роскомнадзором доступ к запрещенной информации блокирован на территории всей страны.

Или же можно привести другой пример. Так, прокуратура Магаданской области выявила два случая использования неустановленными лицами возможностей информационно-коммуникационной сети «Интернет» в целях возбуждения национальной розни [38]. По инициативе прокуратуры следственным органом УФСБ России по Магаданской области возбуждено 2 уголовных дела по ч.1 ст. 280 УК РФ (публичные призывы к осуществлению экстремистской деятельности) в отношении лиц, разместивших в сети «Интернет» публичные призывы к осуществлению экстремистских действий. По требованию органов прокуратуры доступ к сайтам с экстремистским контентом заблокирован. Работа органов прокуратуры по блокированию подобных сайтов продолжается. В соответствии со статьей 15.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [66] в целях ограничения доступа к противоправной информации в сети «Интернет» создана и ведется единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети « «Интернет»« и сетевых адресов,

позволяющих идентифицировать сайты в сети « «Интернет»«, содержащие информацию, распространение которой в Российской Федерации запрещено» (далее – единый реестр).

Частью 5 статьи 15.1 Федерального закона № 149-ФЗ предусмотрены следующие основания включения сведений в единый реестр во внесудебном порядке:

1) решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации, в отношении распространяемых посредством сети «Интернет» «:

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;

д) информации, нарушающей требования Федерального закона от 29 декабря 2006 года № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» [68] и Федерального закона от 11 ноября 2003 года № 138-ФЗ «О лотереях» [63] о

запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети «Интернет» и иных средств связи;

2) вступившее в законную силу решение суда о признании информации, распространяемой посредством сети «Интернет», информацией, распространение которой в Российской Федерации запрещено.

В соответствии с пунктом 6 Правил создания, формирования и ведения единой автоматизированной информационной системы «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети « «Интернет»« и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети « «Интернет»«, содержащие информацию, распространение которой в Российской Федерации запрещено», утвержденных постановлением № 1101, в электронном виде создана форма для приема обращений граждан о наличии на страницах сайтов в сети « «Интернет»« запрещенной информации. Эта форма размещена по адресу: http://eais.rk №. gov.ru [61].

После поступления на сайт обращений о наличии на страницах сайтов в сети «Интернет» запрещенной информации, данные обращения направляются уполномоченным органам в соответствии с их компетенцией.

После поступления в уполномоченный орган обращения граждан о наличии на страницах сайтов в сети «Интернет» запрещенной информации, в течение суток принимается решение о включении «Интернет»-сайта в единый реестр.

Таким образом, при обнаружении на «Интернет»-ресурсе вышеуказанной информации заявитель может направить соответствующие обращение через «Интернет»-сайт: http://eais.rk№.gov.ru. Данное обращение будет рассмотрено в установленном законом порядке.

Кроме того, в соответствии со статьей 15.3 Федерального закона № 149-ФЗ ограничение доступа к информации в сети «Интернет», содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с

нарушением установленного порядка, производится также во внесудебном порядке на основании требования Генерального прокурора Российской Федерации или его заместителей.

Таким образом, при обнаружении в сети «Интернет»-ресурсе вышеуказанной информации обращение о принятии мер необходимо направлять в органы прокуратуры.

Ограничение доступа к иной противоправной информации в сети «Интернет» производится исключительно на основании решения суда, вынесенного по заявлению прокурора, в связи с чем обращения о наличии в сети «Интернет» подобной информации также необходимо направлять в органы прокуратуры.

Стратегией национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 31.12.2015 № 683 [60], деятельность, связанная с использованием информационных и коммуникационных технологий для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, отнесена к одной из основных угроз государственной и общественной безопасности.

Учитывая важность вопросов информационной безопасности, Указом Президента Российской Федерации от 05.12.2016 № 646 утверждена Доктрина информационной безопасности Российской Федерации [59].

Доктриной отмечено, что возможности трансграничного оборота информации все чаще используются для достижения террористических, экстремистских, криминальных и иных противоправных целей, нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, привлечения к террористической деятельности новых сторонников.

Одним из основных направлений обеспечения информационной безопасности является противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии и идей национальной исключительности.

Законодательством предусмотрен ряд способов ограничения доступа к информации различного, в том числе экстремистского, характера, для которого используется созданный в соответствии с частью 1 статьи 15.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [66] Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено (далее - Единый реестр).

В целях приема обращений органов государственной власти, органов местного самоуправления, юридических лиц, индивидуальных предпринимателей, общественных объединений и иных некоммерческих организаций, а также граждан о наличии на страницах сайтов в сети « «Интернет»« запрещенной информации для включения сведений о них в Единый реестр Роскомнадзором на своем сайте создана соответствующая электронная форма (https://eais.rk№.gov.ru/feedback [39]).

В Единый реестр, помимо информации, указанной в пункте 1 части 5 статьи 15.1 Федерального закона № 149-ФЗ, также включаются сведения об «Интернет» -ресурсах, распространяющих материалы, внесенные в федеральный список экстремистских материалов.

В данном случае отдельного решения суда о признании информации (экстремистских материалов), распространяемой по конкретным доменным именам, указателям страниц сайтов и сетевым адресам в сети «Интернет» «запрещенной к распространению в Российской Федерации не требуется, поскольку статьей 13 Федерального закона от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» [62] распространение в Российской Федерации материалов, признанных экстремистскими, прямо запрещено. Сведения в Единый реестр вносятся на основании ранее принятых судами решений о признании материалов экстремистскими.

Федеральными законами от 28.12.2013 № 398-ФЗ, от 25.11.2017 № 327-ФЗ Федеральный закон № 149-ФЗ дополнен статьей 15.3, регламентирующей порядок ограничения доступа к обнаруженной в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, а также информационным материалам иностранной или международной неправительственной организации, деятельность которой признана нежелательной на территории Российской Федерации, и сведениям, позволяющим получить доступ к указанным информации или материалам.

В соответствии с частью 1 статьи 15.3 Федерального закона № 149-ФЗ при поступлении от федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций или граждан уведомлений о распространении в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», информации указанного характера Генеральный прокурор Российской Федерации или его заместители вправе направить в Роскомнадзор требование о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию.

Порядок рассмотрения уведомлений и направления в Роскомнадзор требований регламентирован соответствующей инструкцией, утвержденной приказом Генерального прокурора Российской Федерации от 08.09.2016 № 562 [41].

Роскомнадзор на основании требования Генерального прокурора Российской Федерации или его заместителей незамедлительно направляет по системе взаимодействия операторам связи требование о принятии мер по ограничению доступа к информационному ресурсу или к информации, размещенной на нем, после получения которого оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной

сети «Интернет», обязан незамедлительно ограничить доступ к такому информационному ресурсу. Сведения об информационном ресурсе вносятся Роскомнадзором в отдельный реестр [39].

Предусмотренный порядок позволяет оперативно реагировать на случаи распространения в сети «Интернет» подобной информации, что достигается обязательным указанием в требовании Роскомнадзора доменного имени сайта в сети «Интернет» «сетевого адреса, указателей страниц сайта в сети «Интернет», позволяющих идентифицировать такую информацию».

Федеральным законом от 29.07.2017 «276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» Федеральный закон № 149-ФЗ дополнен статьей 15.8, регламентирующей порядок противодействия использованию на территории Российской Федерации информационно-телекоммуникационных сетей и информационных ресурсов, посредством которых обеспечивается доступ к информационным ресурсам и информационно-телекоммуникационным сетям, доступ к которым ограничен.

В силу части 1 указанной статьи Федерального закона № 149-ФЗ владельцам информационно-телекоммуникационных сетей и информационных ресурсов, посредством которых возможно обеспечение доступа к «Интернет»-ресурсам, доступ к которым на территории Российской Федерации ограничен, запрещается предоставлять возможность использования принадлежащих им информационно-телекоммуникационных сетей и информационных ресурсов для получения доступа к таким «Интернет»-ресурсам.

Деятельность по выявлению информационно-телекоммуникационных сетей и информационных ресурсов, позволяющих получить доступ к «Интернет»-ресурсам с информацией, распространение которой на территории Российской Федерации запрещено, ведется органами исполнительной власти, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации.

Согласно пунктам 3, 4 части 2, части 4 статьи 15.8 Федерального закона № 149-ФЗ [66] Роскомнадзор на основании обращений указанных органов определяет провайдера хостинга или иное лицо, обеспечивающее размещение в сети « «Интернет»« программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен (далее - программно-аппаратные средства), принимая в дальнейшем меры для идентификации владельца программно-аппаратных средств и его подключению к федеральной государственной информационной системе, содержащей перечень информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым на территории Российской Федерации ограничен (далее - федеральная государственная информационная система).

В соответствии с частью 7 статьи 15.8 Федерального закона № 149-ФЗ владелец программно-аппаратных средств обязан в течение трех рабочих дней после предоставления ему доступа к федеральной государственной информационной системе обеспечить соблюдение запрета предоставлять возможность использования на территории Российской Федерации программно-аппаратных средств для получения доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым на территории Российской Федерации ограничен.

В силу части 10 статьи 15.8 Федерального закона № 149-ФЗ в случае неисполнения владельцем программно-аппаратных средств обязанностей по подключению к федеральной государственной информационной системе и ограничению доступа к информационным ресурсам, информационно--телекоммуникационным сетям, доступ к которым на территории Российской Федерации ограничен, Роскомнадзор принимает решение об ограничении доступа к принадлежащим такому владельцу программно-аппаратным средствам.

Доступ к указанным выше программно-аппаратным средствам ограничивается операторами связи, оказывающими услуги по предоставлению доступа к сети «Интернет».

По УК РФ [58] преступлениями в сфере компьютерной информации являются: неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) и нарушение правил эксплуатации–средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

За данные преступления предусматривается ответственность, начиная от штрафов до 200 тысяч рублей и заканчивая 7 годами лишения свободы, в зависимости от тяжести причиненного вреда.

Хотелось бы отметить, что преступления в сфере информационных технологий могут квалифицироваться не только по специальным составам, но и по общеуголовным статьям, к примеру, ст. 159 УК РФ (мошенничество) т.д.

Преступления в сфере информационных технологий включают как распространение вредоносных вирусов, взлом паролей, кражу номеров банковских карт и других банковских реквизитов (фишинг), так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.п.) через «Интернет», а также вредоносное вмешательство через компьютерные сети в работу различных систем.

Кроме того, одним из наиболее опасных и распространенных преступлений, совершаемых с использованием «Интернета», является мошенничество. Так, в письме Федеральной комиссии по рынку ценных бумаг от 20 января 2000 г. № ИБ-02/229 [35], указывается, что инвестирование денежных средств на иностранных фондовых рынках с использованием сети «Интернет» сопряжено с риском быть вовлеченными в различного рода мошеннические схемы

Таким образом, общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьезное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям.

Неправомерный доступ к компьютерной информации (ст. 272 УК РФ), а также Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) совершаются только путем действий, в то время как нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) - путем как действий, так и бездействием.

Неправомерный доступ к компьютерной информации и нарушение установленных правил эксплуатации ЭВМ, системы ЭВМ или их сети сформулированы как преступления с материальным составом, а создание либо использование вредоносных программ для ЭВМ - с формальным. В качестве последствий в ст. 272 и 274 УК указываются: уничтожение, модификация, блокирование либо копирование информации, нарушение работы ЭВМ или системы ЭВМ, причинение существенного вреда и т. п.

Глава 3 Уголовная характеристика преступлений в сфере «Интернет»

3.1 Особенности и проблемы квалификации преступлений, совершенных в сети «Интернет»

Только за период январь – март 2020 года органами внутренних дел зарегистрировано 101.537 дел, охватываемых составами главы 28 УК РФ «Преступления в сфере компьютерной информации», 56.593 из них, совершенных в сети «Интернет» [22].

Первый шаг в этом направлении был уже сделан внесением Федеральным законом от 29.11.2012 № 207-ФЗ [67] изменений в УК РФ, в частности, были внесены дополнения в состав мошенничества. Один из новых составов мошенничества был сформулирован законодателем в статье 159.6 УК как «Мошенничество в сфере компьютерной информации». Законодатель в диспозиции настоящей статьи определяет мошенничество в сфере компьютерной информации как «хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации, или информационно-телекоммуникационных сетей» [58].

Правоприменение этой статьи на практике позволило избежать многих сложностей, возникающих в процессе квалификации преступлений в сфере компьютерной информации. Ранее, до принятия соответствующих поправок мошенничество в сфере компьютерной информации требовало квалификации по совокупности составов, предусмотренных ст. ст. 159 и 272 УК РФ. Таким образом, в действиях виновного налицо были признаки идеальной совокупности преступлений. В настоящее время, с учетом внесенных изменений, достаточно будет применения статьи 159.6 УК РФ, что

свидетельствует об упрощении процесса уголовного судопроизводства, и о своеобразной экономии средств уголовной репрессии [26].

При рассмотрении вопроса квалификации преступлений, совершаемых в сети «Интернет» В.М. Лебедевым была высказана мысль о том, что овладение персональным компьютером, иной ЭВМ, не имеющими источников питания, а также машинным носителем информации как вещью не рассматривается как доступ к компьютерной информации, охватываемой ст. 272 УК РФ, и в этих случаях может повлечь ответственность по соответствующим статьям о преступлениях против собственности. [19]. Так же автор говорит, что уничтожение или модификация компьютерной информации путем внешнего воздействия на ЭВМ не образует объективной стороны состава.

Оспорить данное высказывание трудно, однако думается, что способы неправомерного прямого доступа к компьютерной информации могут быть различны, будь то предоставление заведомо подложных документов, изменение кода или адреса технического устройства, нарушение средств или системы защиты информации.

В случае, например, если речь будет идти о краже материального носителя информации не с целью в дальнейшем неправомерно извлечь из него защищенную компьютерную информацию, а продать или уничтожить, то действия виновного надлежит квалифицировать по соответствующим статьям УК РФ (ст. ст. 158, 159, 161 и др.).

Если же виновный, совершив хищение материального носителя информации, имея в дальнейшем цель - совершить с этой компьютерной информацией какие-либо умышленные действия, запрещенные законом, то данное деяние можно рассматривать как покушение на неправомерный доступ к компьютерной информации (ч. 3 ст. 30, ч. 1 ст. 272 УК РФ), в связи с тем, что последствия, предусмотренные в ч. 1 ст. 272 УК РФ, еще не наступили.

Ввиду чего, думается, что при вменении виновному уголовного наказания необходимо внимательно анализировать субъективную сторону

конкретного деяния, в частности на что был направлен умысел, не упускать из внимания и факультативные признаки – какими мотивами и целями преступник руководствовался.

На основании ч. 1 ст. 272 УК РФ в изначальной редакции наказуем был неправомерный доступ к охраняемой законом компьютерной информации, т. е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Квалифицированный состав преступления образовывало то же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети. Проблемы правоприменительной практики при квалификации преступлений, совершенных с использованием информационно-коммуникационных технологий. В ст. 272 УК РФ законодатель соединил в одном составе несколько деяний, являющихся самостоятельными преступлениями в зарубежном уголовном законодательстве. Речь идет о незаконном доступе к компьютеру (компьютерной системе) и вмешательстве в систему или данные (ст. 2, 4 и 5 Конвенции о киберпреступности [21]). Еще до принятия Конвенции некоторые зарубежные страны разграничили три указанных преступления.

Думается, целесообразно законодателю будет дополнить настоящий УК РФ статьей 272.1 и изложить ее в следующей редакции: «Кража материального носителя, ЭВМ или иного машинного носителя, на котором содержится защищенная компьютерная информация, с целью осуществления неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, а равно нарушение работы машинного носителя информации, ЭВМ, системы ЭВМ и (или) их сети». Данная нами редакция позволит избежать длительного процесса

конкретизации факультативных признаков субъективной стороны и упрощению процесса уголовного судопроизводства.

Существует так же второй спорный аспект этого случая, когда виновный не знает о наличии на материальном носителе защищенной компьютерной информации и его умысел направлен исключительно на его уничтожение или иного действия, направленного на материальный объект. Можно ли тогда говорить о вменении ст. 272 УК РФ? Считается, что в таком случае, действия виновного будут подлежать уголовной ответственности по ч. 1 ст. 167 УК РФ «Умышленные уничтожение или повреждение имущества» или 7.17 КоАП РФ [16], если эти действия не повлекли причинение значительного ущерба.

Представляется, что при совершении виновным действий, рассмотренных нами выше, не из корыстных, личных или хулиганских побуждений, а из исследовательских целей или цели самоутверждения, деяние также должно квалифицироваться по ст. 272 УК РФ [14].

Учитывая, что при неправомерном доступе к компьютерной информации, создании, использовании и распространении вредоносных программ для ЭВМ нарушаются права человека и гражданина на собственность (на информацию, авторское право и т.д.), думается необходимым включить в квалифицированный состав ст. ст. 272, 273 еще один факультативный непосредственный объект - отношения собственности, тем самым признав потерпевшего обязательным признаком объекта состава преступления и дополнив ст. ст. 272, 273 УК РФ новым квалифицирующим признаком значительного ущерба гражданину, а также «те же деяния, совершенные в крупном размере», «те же деяния, совершенные в особо крупном размере».

Предлагаемые нами введения отношений собственности к крупному материальному ущербу (ч. 2 ст. 272, ч. 2 ст. 273, ч. 1 ст. 274) может быть выражено как в реальном уменьшении фактического имущества гражданина, так и в упущенной выгоде (например, в неполучении коммерческого дохода). Размер крупного материального ущерба установлен законодателем в

примечании 2 ст. 272 УК НА и равен сумме, превышающей один миллион рублей.

Допуская международный уголовно-правовой аспект рассматриваемой группы преступлений и учитывая более высокую степень общественной опасности компьютерных преступлений, носящих транснациональный характер, и необходимость борьбы с ними на международном уровне; очевидно, что законодателю необходимо дополнить ст. 272, 273 новыми квалифицирующими признаками с ужесточенным наказанием. Что позволит привести российское уголовное законодательство в соответствии с ратифицированными международными соглашениями в борьбе с преступлениями в сфере компьютерной информации [49].

Анализируя положения чт. 274.1 УК РФ спорными, пожалуй, можно назвать два реализованных решения:

- законодатель проявил малопонятную последовательность в регламентации совершения деяния лиц по предварительному сговору и организованной группами в рамках одной части. Очевидно, что уравнивание таких качественно разных по опасности форм соучастия вряд ли отвечает научно обоснованным критериям дифференциации ответственности.
- Вся группа преступлений в сфере компьютерной информации в качестве особо отягчающего обстоятельства называет наступление тяжких последствий или создание угрозы их наступления. Вместе с тем уголовно-правовая норма, предусмотренная ст. 274.1 УК РФ, такой оговорки не содержит, что, учитывая особую значимость объектов посягательства, представляется по меньшей мере ошибочным.

Помимо сказанного ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [65] предполагает деление на категории всех объектов в зависимости от социальной, политической, экономической значимости, а также значимости объекта критической

информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка. Думается, что не включение в ст. 274.1 УК РФ такого деления является существенным упущением с точки зрения игнорирования критериев дифференциации уголовной ответственности. Также, исследуемая новелла не позволит должным образом оценить различия в объеме и значимости социальных последствий криминальных посягательств на объекты критической инфраструктуры. Возможности учета опасности указанного деяния только лишь посредством дифференциации уголовного наказания, как представляется, явно недостаточны. Полагаем, что в этой части уголовно-правовая норма об ответственности за неправомерное воздействие на критическую информационную инфраструктуру РФ требует срочной корректировки.

На настоящий момент Пленум Верховного Суда РФ не давал никаких постановлений, которое могло бы разъяснить все спорные аспекты составов главы 28 УК РФ. Во избежание в дальнейшем долгих судебных тяжб и проблем квалификаций, Пленуму ВС РФ необходимо его разработать и принять, тщательно проанализировав соответствующее законодательство.

Таким образом, нами предлагается дополнить ч. 2 ст. 272 УК РФ следующими квалифицирующими признаками: «То же деяние, совершенное на территории Российской Федерации в отношении охраняемой законом компьютерной информации, находящейся за пределами Российской Федерации либо за пределами Российской Федерации в отношении охраняемой законом компьютерной информации на территории Российской Федерации»; ч. 4 чт. 272 УК РФ словами «или повлекшие по неосторожности тяжкие последствия», ч. 2 ст. 273 словами «а равно причинившие гражданину значительного ущерба», ч. 3 ст. 273 УК РФ словами «или повлекшие по неосторожности тяжкие последствия», дополнить ст. 273 УК РФ частью 4 и изложить в следующей редакции «То же деяние, совершенное на территории Российской Федерации в отношении охраняемой законом компьютерной информации, находящейся за пределами Российской Федерации либо за

пределами Российской Федерации в отношении охраняемой законом компьютерной информации на территории Российской Федерации». Дополнить УК РФ ст. 271.1 и изложить в следующей редакции: «Кража материального носителя, ЭВМ или иного машинного носителя, на котором содержится защищенная компьютерная информация, с целью осуществления неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, а равно нарушение работы машинного носителя информации, ЭВМ, системы ЭВМ и (или) их сети».

3.2 Характеристика элементов состава преступлений в сфере «Интернет»

Поместив главу 28 в раздел IX УК РФ «Преступления против общественной безопасности и общественного порядка», законодатель определил родовой объект анализируемых преступлений как общественные отношения, регулирующие общественную безопасность и общественный порядок. Некоторые ученные считают, что родовым объектом рассматриваемых преступлений являются общественные отношения «в сфере обеспечения безопасности использования автоматизированных систем обработки данных, нормальных прав и интересов лиц, общества и государства, активно пользующихся электронно-вычислительной техникой» [7]; общественная безопасность [23]. Трудно не согласиться с трактовкой данной родового объекта преступлений в сфере компьютерной информации, так как родовой объект является критерием для деления особенной части УК РФ на разделы и представляет собой часть общего объекта. Особое уголовно правовое значение выделения родового объекта проявляется в отдельных свойствах, присущих каждой группе преступлений, которые позволяют их обозначить и объединить в отдельную группу, таким образом отграничивая от остальных составов преступлений.

Видовой объект преступлений в юридической литературе определяют как совокупность тождественных общественных отношений одного вида, на которые посягает однородная группа преступлений.

По мнению ряда правоведов в области уголовного права, видовым объектом этих преступлений будет являться информационная безопасность как вид общественной безопасности, т. е. отношения по безопасному производству, хранению и дальнейшему распространению, использованию информации и информационных ресурсов [56]. Думается, что видовым объектом преступлений, совершаемых в сети «Интернет», будет выступать общественные отношения, обеспечивающие безопасность компьютерной информации.

Некоторые авторы допускают установление дополнительных объектов непосредственного объекта исследуемой группы преступлений, так, например, в качестве дополнительного объекта может выступать конституционный строй и безопасность государства; имущественные и личные неимущественные права, перечисленные в ст. 128 Гражданского кодекса РФ [9], а также закрепленные конституцией права и свободы человека и гражданина [14].

Объективная сторона рассматриваемой группы преступлений представляет собой активные действия, состоящие в нарушении общественных отношений складывающихся в сфере обеспечения безопасности компьютерной информации (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 УК РФ)).

Характерной чертой объективных признаков группы преступлений является применением законодателем многочисленных технических

специальных терминов, которые затрудняют выделение основных признаков, выражающих особенности всех или большинства, указанных в главе 28 УК РФ составов.

Для четкого определения объективной стороны состава ст. 272 УК РФ необходимо дать определение некоторым терминам. Так, «неправомерным считается доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты». То есть незаконное либо не разрешенное владельцем информации получение и (или) пользование компьютерной информации. «При этом под доступом понимается проникновение в ее источник с использованием средств (вещественных и интеллектуальных) компьютерной техники, позволяющее использовать полученную информацию (копировать, модифицировать, блокировать либо уничтожать ее)» [28].

Кроме того, в примечании к ст. 272 УК РФ законодатель определил понятие компьютерной информации – «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [28].

Законодатель в п. 6 ч. 1 ст. 2 ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» определяет критическую информационную инфраструктуру как объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов» [58].

Таким образом, объективная сторона исследуемых преступлений выражается деянием, в форме действия. Однако, предусмотренный ст. 274 УК, состав (нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования) может выражаться в форме бездействия.

Определяя оконченный состав преступления в сфере компьютерной информации необходимо установить обязательный признак - наступление предусмотренных уголовным законом общественно опасных последствий в виде причиненного вреда, а также причинной связи между общественно опасных деянием и преступным результатом. Преступления, охватываемые главой 28 УК РФ, имеют характерный материальный состав. О чем свидетельствует наличие обязательного признака – общественно-опасных последствий в диспозиции каждой статьи настоящей главы (уничтожение, блокирование, модификацию либо копирование компьютерной информации (ст. 272 УК РФ); уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб (ст. 274) причинение вреда критической информационной инфраструктуре Российской Федерации (ч. 2, 3 ст. 274.1 УК РФ) [58].

В уголовно-правовой доктрине под уничтожением информации понимают приведение ее полностью либо в существенной части в непригодное для использования по назначению состояние при невозможности ее восстановления. Блокирование – невозможность надлежащего использования информации при сохранности такой информации. Модификация – изменение ее содержания по сравнению с той информацией (внесение изменений в программы, базы данных, текстовую информацию, находящуюся на материальном носителе), которая первоначально была в распоряжении собственника или иного законного пользователя. Под копированием информации понимают неправомерное переписывание информации на другой материальны носитель, а также иное тиражирование при сохранении оригинала.

Как отмечалось выше, установление причинной связи между несанкционированным доступом и наступлением последствий имеет достаточно важное значение.

Так, Тюменским областным судом был осужден Слепчуков Д. А. по ч. 2 ст. 272 УК РФ, ч. 1 ст. 285, п. «а» ч. 4 ст. 290. Слепчуков являясь

администратором автоматизированной информационно-поисковой системы (АИПС), как инженер-программист регионального отдела информационного обеспечения, наделенный высшим уровнем доступа в Сеть, произвел незаконные уничтожение охраняемой законом служебной информации о совершении рядом лиц административных правонарушений и лишении их права управления транспортными средствами. Суд обоснованно указал, что информация, содержащаяся в АИПС «Административная практика», относится к служебной информации, и доступом к ней наделен ограниченный круг сотрудников на основании уровня доступа в связи с паролем, причем Слепчуков был наделен самым высоким уровнем доступа и мог вносить изменения, удалять информацию без фиксации где-либо произведенной операции и делал это по просьбе Володина О. А., который именно от этих лиц получил взятки за удаление информации о допущенных ими административных нарушениях [15].

Для преступлений, предусмотренных ч. 1 ст. 273, ч. 1 ст. 274.1, не требуется наступления конкретных общественно опасных последствий, и для признания их оконченными достаточно установить факт совершения общественно опасного деяния, что свидетельствует о формальности состава.

Характерной особенностью объективной стороны изучаемых преступлений является то, что законодатель использует квалифицирующие признаки как средство дифференциации уголовной ответственности. Так, крупный ущерб, корыстную заинтересованность, группу лиц по предварительному сговору, организованную группу, использование своего служебного положения, тяжкие последствия, создание угрозы наступления тяжких последствий предусматривает в ч. 3 ст. 272, ч. 2 ст. 273, ч. 4 ст. 274.1. Крупный ущерб, тяжкие последствия, создание угрозы наступления тяжких последствий включает в качестве квалифицирующих признаков в ч. 2 ст. 274, ч. 5 ст. 274.1.

Отдельного внимания заслуживают положения ст. 274.1 УК РФ, имеющая бланкетный характер, что предполагает обязательную ссылку на

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» [65].

Основным непосредственным объектом анализируемых преступлений является безопасность критической информационной инфраструктуры Российской Федерации, т.е. состояние ее защищенности от любого воздействия программными или программно-техническими средствами, которое способно привести к нарушению ее функционирования и (или) нарушению безопасности обрабатываемой ею информации.

Предметом преступления, предусмотренного ч. 1 ст. 274.1, является компьютерная информация или компьютерные программы, заведомо предназначенные для совершения компьютерных атак на объекты критической информационной инфраструктуры. Специфическим предметом ч. 2, ч. 3 ст. 274.1 выступают объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной промышленности, атомной промышленности, ракетно-космической промышленности, горнодобывающей промышленности, металлургической промышленности и химической промышленности [46].

Относимость того или иного объекта критической информационной инфраструктуры определяется в соответствии со ст. 8 ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», которая определяется порядком ведения реестра значимых объектов критической информационной инфраструктуры, в соответствии с соответствующим Приказом ФСТЭК [43].

Говоря об объективной стороне ч. 1 ст. 274.1, оно предполагает совершение любого из трех альтернативных действий:

– создание;
– использование или
– распространение компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты критической информационной инфраструктуры.

Состав по конструкции является формальным – преступление считается оконченным с момента совершения указанных действий.

Объективная сторона ч. 2 ст. 274.1 УК РФ заключается в неправомерном доступе к компьютерной информации, содержащейся в критической информационной инфраструктуре. В отличие от ч. 1, анализируемый состав по конструкции материальный - преступление считается оконченным с момента наступления вреда критической информационной инфраструктуре РФ.

Вред как обязательный конструктивный признак настоящего состава не конкретизирован законодателем. Системное толкование отечественного уголовного законодательства позволяет сделать вывод, что таковыми являются уничтожение, блокирование, модификация, копирование информации, содержащейся в критической информационной инфраструктуре, нейтрализация средств защиты указанной информации или выведение из строя аппаратных и программных средств, обеспечивающих функционирование критической информационной инфраструктуры (за исключением случаев, когда это повлекло причинение смерти или тяжкого вреда здоровью человека, причинение средней тяжести вреда здоровью двум или более лицам, массовое причинение легкого вреда здоровью людей, наступление экологических катастроф, транспортных или производственных аварий, повлекших длительную остановку транспорта или производственного процесса, дезорганизацию работы конкретного предприятия, причинение особо крупного ущерба, т.е. тяжких последствий, предусмотренных ч. 5 ст. 274.1 УК РФ).

Объективная сторона ч. 3 чт. 274.1 заключается в нарушении:

а) правил эксплуатации:

1) средств хранения, обработки или передачи охраняемой компьютерной информации;
2) информационных систем;
3) информационно-телекоммуникационных сетей;
4) автоматизированных систем управления;
5) сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации;

б) правил доступа к указанным средствам, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи.

По конструкции состав материальный - преступление считается оконченным с момента наступления вреда критической информационной инфраструктуре РФ.

Субъектом преступлений в сфере компьютерной информации, признается физическое вменяемое лицо, достигшее к моменту совершения преступления возраста 16 лет. Субъект преступления, предусмотренного ст. 274 УК РФ, - специальный. Это лицо, которое в силу должностных обязанностей имеет доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационным сетям и оконечному оборудованию, а также к информационно-телекоммуникационным сетям и обязано соблюдать установленные для них правила эксплуатации.

Субъективная сторона исследуемой группы преступлений характеризуется умышленной формой вины, при чем может выражаться прямым или косвенным умыслом. Виновный осознает, что незаконно совершает деяние (действие или бездействие), связанное с использованием компьютерной информации, предвидит возможность или неизбежность наступления вреда и желает наступления этих последствий (прямой умысел), либо не желает, но сознательно допускает, либо относится к ним безразлично

(косвенный умысел). Нарушение правил эксплуатации (ст. 274 УК РФ) может быть совершено умышленно, так и по неосторожности. По отношению к наступлению указанных в законе последствий возможна и неосторожная форма вины.

Затрагивая мотивы и цели, как факультативные признаки субъективной стороны, группы преступлений главы 28 УК РФ, можно говорить об их необязательности при вменении, следовательно, на квалификацию они никак не влияют. Однако при назначении наказания установление факультативных признаков должны учитываться.

Таким образом, под преступлениями в сфере компьютерной информации понимается виновно совершенное под угрозой уголовного наказания общественно опасное деяние, причиняющее вред либо создающее угрозу причинения вреда общественным отношениям, обеспечивающим компьютерную безопасность и защищенность информационных систем.

Субъект данного вида преступления общий – физическое вменяемое лицо, достигшее на момент совершения преступления возраста 16 лет. Субъект ст. 274 УК РФ специальный – это должностное лицо, которому вверено хранение, обработку и передачу охраняемой компьютерной информации.

Субъективная сторона характеризуется любыми формами умысла. Как правило преступления совершается умышленно, ст. 274 УК РФ не исключает и неосторожную форму вины. Что позволяет говорить о ее отличительности от одновидовых составов настоящей главы.

3.3 Ответственность за преступления в сфере «Интернет»

Информация и знания становятся все более важными факторами производства, движущей силой экономического развития и процветания общества. В настоящее время информация имеет очень важное значение, а также влияние на общество, а потому и преступлений с каждым днем

становится все больше и больше - распространение вредоносных вирусов, взлом паролей, кражи банковских карт, распространение клеветы через «Интернет», вмешательство в работу различных систем через компьютерные сети. Одним из самых опасных и распространенных преступлений является мошенничество.

Информация - это совокупность сведений (данных), которая воспринимается из окружающей среды (входная информация), выдается в окружающую среду (исходная информация) или сохраняется внутри определенной системы [66].

Правовое регламентирование использования информации, в том числе и компьютерной, содержится в ФЗ «Об информации, информатизации и защите информации». Данные нормативно-правовые акты содержат определения понятий «информация», «информационная система», «информационные ресурсы», «конфиденциальная информация», «программа для ЭВМ», «база данных», «распространение программы для ЭВМ», и др.

Статья 20 ФЗ №24-ФЗ перечисляет цели защиты информации [66]:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

– сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
– обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Причем защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу. Авторское право распространяется на любые программы для ЭВМ и базы данных, как выпущенные, так и не выпущенные в свет, представленные в объективной форме, независимо от их материального носителя, назначения и достоинства [66].

Использование информации осуществляется на основании договора, заключенного в письменной форме. Следовательно, иное использование информации, которое может нанести ущерб ее собственнику, является несанкционированным и преследуется по закону. Ст. 20 рассматриваемого закона помимо гражданской ответственности называет также уголовную ответственность за нарушение авторских прав (ст. ст. 146, 147 УК РФ) [66].

В данных законах речь идет не только о защите самой информации, но и о защите права на доступ к информации.

Глава 28 УК РФ предусматривает наступление уголовной ответственности за преступления в сфере компьютерной информации. Данная глава содержит три статьи: неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273), нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274) [58].

Субъект указанных преступлений общий, т.е. любое лицо, достигшее шестнадцатилетнего возраста. Исключение составляет только ч. 2 ст. 272, которая в череде квалифицирующих признаков называет совершение неправомерного доступа к компьютерной информации лицом с

использованием своего служебного положения, т.е. речь идет о специальном субъекте преступления [58].

Объектом преступлений являются общественные отношения в области охраны компьютерной информации, а также обеспечения нормальной работы ЭВМ, их систем и сетей.

Субъективная сторона характеризуется исключительно прямым умыслом, т.е. виновное лицо осознавало преступный характер своих действий, предвидело и желало наступление общественно опасных последствий.

Объективную сторону преступлений составляют активные действия виновного, направленные на достижение преступного результата. Преступления, предусмотренные ст. ст. 272-274 УК РФ, имеют материальный состав, т.е. преступление считается оконченным в момент, когда наступили общественно опасные последствия: уничтожение информации, нарушение работы ЭВМ, причинение существенного вреда [58].

Гарантируемая свобода информации реализуется различными способами: устно, письменно, через средства массовой информации и иными законными способами [1].

Государственные информационные ресурсы Российской Федерации, как отмечается в Законе, являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная к категории ограниченного доступа. Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную. При этом Закон устанавливает перечень информации, которую запрещено относить к информации с ограниченным доступом [66].

Среди ее видов: законодательные и иные нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации; документы, содержащие информацию о чрезвычайных ситуациях, экологическую,

метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом; документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, отнесенных к государственной тайне; документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Граждане наряду с другими пользователями (органами государственной власти, органами местного самоуправления, организациями и общественными объединениями) обладают равными правами на доступ к государственным информационным ресурсам и не обязаны обосновывать перед владельцем этих ресурсов необходимость получения запрашиваемой ими информации. Такое право на доступ к информации является основой осуществления общественного контроля за деятельностью органов государственной власти и местного самоуправления, общественных, политических и иных организаций, а также за состоянием экономики, экологии и других сфер общественной жизни.

Что же касается информации о самих гражданах, то не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения. Персональные данные не могут быть использованы для причинения имущественного и морального вреда гражданам, затруднения

реализации их прав и свобод. Ограничение прав граждан на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

Отказ гражданам в доступе к информационным ресурсам по вопросам деятельности государственных органов и подведомственных им организаций может быть обжалован в суд. [64].

Уголовная ответственность наступает за совершение преступления. Преступлением признается виновное общественно опасное деяние (действие либо бездействие), ответственность за которое предусмотрено уголовным законом. Уголовная ответственность на преступления, совершенные и информационной сфере, наступает на основании норм Уголовного кодекса Российской Федерации [58].

Глава 28 УК РФ содержит составы преступлений в сфере компьютерной информации содержит три статьи, устанавливающие уголовную ответственность, в их числе ответственность:

- за неправомерный доступ к компьютерной информации (статья 272 УК РФ), а именно, за неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;
- создание, использование и распространение вредоносных программ для ЭВМ (статья 273 УК РФ), и создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно

использование либо распространение таких программ или машинных носителей с такими программами;

- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно телекоммуникационных сетей (статья 274 УК РФ), означающее нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред.

Уголовная ответственность в информационной сфере установлена также за отдельные преступления против чести и достоинства личности и нарушающие права и свободы человека и гражданина, установленного порядка управления и безопасности государства, в том числе:

- за клевету (часть 2 статьи 128.1), т.е. содержащиеся в публичном выступлении, публично демонстрирующем произведении или средствах массовой информации;
- нарушение неприкосновенности частной жизни (статья 137 УК РФ), т.е. действия, направленные на незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующем произведении или средствах массовой информации, включая те же деяния, совершенные лицом с использованием своего служебного положения;
- нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (статья 138 УК РФ);
- воспрепятствование осуществлению избирательных прав или работе избирательных комиссий (статья 141 УК РФ);

- фальсификацию избирательных документов, документов референдума (статья 142 УК РФ);
- воспрепятствование законной профессиональной деятельности журналистов (статья 144 УК РФ);
- нарушение авторских и смежных прав (статья 146 УК РФ);
- нарушение изобретательских и патентных прав (статья 147 УК РФ);
- публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма (статья 205.2 УК РФ);
- заведомо ложное сообщение об акте терроризма (статья 207 УК РФ);
- сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей (статья 237 УК РФ);
- незаконное распространение порнографических материалов или предметов (статья 242 УК РФ);
- изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (статья 242.1 УК РФ);
- шпионаж (статья 276 УК РФ);
- публичные призывы к осуществлению экстремистской деятельности (статья 280 УК РФ);
- возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (статья 282 УК РФ);
- разглашение государственной тайны (статья 283 УК РФ);
- утрату документов, содержащих государственную тайну (статья 284 УК РФ);
- отказ в предоставлении информации Федеральному Собранию Российской Федерации или Счетной палате Российской Федерации (статья 287 УК РФ);

– клевету в отношении судьи, присяжного заседателя, прокурора, следователя, лица, производящего дознание, судебного пристава, судебного исполнителя (статья 298 УК РФ);
– публичные призывы к развязыванию агрессивной войны (статья 354 УК РФ).

Указанные статьи УК РФ имеют важное значение в обеспечения законности и правопорядка в информационной сфере.

3.4 Тенденции компьютерной преступности в современной России (методы противодействия и предупреждения)

При взаимодействии с сетью «Интернет» неизбежно возникают проблемы взаимодействия и в процессе правоприменения, которые не позволяют эффективно противодействовать преступности. Так, несогласованность субъектов предупреждения преступлений в этой сфере зачастую предоставляет дополнительные возможности для преступных комбинаций. В частности, целесообразно рассмотреть вопрос о законодательном закреплении обязанности производителей и продавцов компьютерной техники, средств связи и т. д. устанавливать в свою продукцию системы антивирусной защиты в целях предотвращения несанкционированного доступа к компьютерной информации.

С другой стороны, меры профилактики могут быть направлены не только на потенциального преступника, но и на органы (организации), представляющие интерес для злоумышленников в сфере информационно-телекоммуникационных технологий. В частности, такой мерой могла бы стать система страхования информационных рисков, которая предусматривает страхование средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования от неправомерного блокирования, уничтожения, модификации либо несанкционированного копирования

электронной информации. При этом перед заключением страхового договора собственник (владелец) информационного ресурса либо информационно-телекоммуникационной сети и соответствующего оборудования обязан провести ряд установленных мер по защите информации и оборудования (установка сертифицированного программного обеспечения, антивирусная защита и т. д.).

Данная мера направлена на уменьшение наносимого материального ущерба и снижение количества несанкционированных проникновений в компьютерные системы, происходящих по их вине. К мерам предупреждения преступлений, совершаемых с использованием высоких технологий, также относится разработка новых методик противодействия данному виду преступлений, в том числе в процессе оперативно-розыскной деятельности.

Так, представляется необходимым законодательно закрепить полномочия правоохранительных органов на осуществление мониторинга опубликованных в социальных сетях или иных ресурсах материалов противоправного характера, а в некоторых случаях обеспечить проведение соответствующих надзорных, оперативно-розыскных, следственных мероприятий с возможностью получения необходимой информации от провайдеров или Роскомнадзора напрямую без судебного разрешения.

Принятие организационно-управленческих мер предупреждения преступлений, совершаемых с использованием высоких технологий. Данное направление характеризуется комплексом мер, направленных на совершенствование деятельности субъектов предупреждения данного вида преступлений. К ним следует отнести:

– создание системы подготовки сотрудников правоохранительных органов по специальностям «Защита информации и информационно-телекоммуникационных сетей», «Информационная безопасность» в образовательных учреждениях МВД, ФСБ, МО, ФТС России и др. Данная мера позволит обеспечить комплектование правоохранительных органов компетентными и профессиональными сотрудниками. Частью данной

системы являются проводимые на регулярной основе курсы повышения квалификации, стажировки в практических органах, обмен опытом, семинары и круглые столы для сотрудников и профессорско-преподавательского состава вузов в государственных образовательных учреждениях, а также российских компаниях, занимающихся информационной безопасностью. Для гражданских специалистов (сотрудников служб безопасности предприятий, учреждений, банков и т. п.) целесообразно организовать аналогичные курсы обучения и повышения квалификации при технических образовательных учреждениях, занимающихся подготовкой специалистов по информационной безопасности; – переход от преимущественно территориального принципа работы правоохранительных органов в сфере предупреждения высокотехнологичной преступности к функциональному. Существующая структура правоохранительных органов и принципы организации работы отдельных подразделений вызывают проблемы координации как внутри этих ведомств, так и в рамках межведомственного взаимодействия. Одной из главных особенностей высокотехнологичной преступности является ее многоэпизодность и трансграничный характер. По этой причине на практике зачастую возникают сложности с определением места совершения преступления, а значит, и территориального органа, который должен заниматься его раскрытием и расследованием. В виртуальном мире понятие территориальности достаточно условно, поэтому существовавшая долгие годы практика проведения разбирательства «по месту совершения преступления» в сочетании с забюрократизированностью уголовно-процессуальной системы не способствует принятию своевременных мер по изобличению преступников и документированию их деятельности. Данная ситуация ставит вопрос о целесообразности специализации сотрудников оперативных и следственных подразделений по преступлениям, совершаемым в сфере высоких технологий, не только на региональном, но и районном уровне. Данное обстоятельство следует учитывать при решении вопросов о

повышении квалификации или переподготовке сотрудников территориальных правоохранительных органов на различных уровнях:

- совершенствование информационно-аналитического обеспечения деятельности по противодействию преступлениям, совершаемым с использованием высоких технологий. Данная работа связана с решением целого ряда задач, включающих сбор и систематизацию криминологически значимой информации, ее анализ и классификацию, определение на этой основе реальной картины состояния дел и перспективное прогнозирование развития ситуации. Эта работа имеет смысл лишь при четкой интеграции ее результатов в законодательную деятельность и правоохранительную практику;
- перевод на новый уровень организации взаимодействия правоохранительных органов со средствами массовой информации.

Использование средств массовой информации в системе противодействия высокотехнологичной преступности должно сочетать несколько направлений, таких как отчет перед населением о результатах борьбы с данными преступлениями; проведение правовой пропаганды, направленной на формирование правосознания и нетерпимости к преступным проявлениям; информирование населения о средствах и методах защиты от мошеннических посягательств, о новых формах его осуществления.

В силу специфики преступлений, совершаемых с использованием высоких технологий, профилактический эффект от своевременного доведения данной информации чрезвычайно высок, особенно если предаваемая в СМИ информация отвечает требованиям систематичности, наступательности, наглядности и своевременности. К работе со СМИ необходимо привлекать и общественные организации, такие как союз потребителей, союз обманутых соинвесторов (вкладчиков) и т. д. Общественно-корпоративные сообщества (Ассоциация российских банков, союзы предпринимателей и т. д.) также могут сыграть большую роль в противодействии высокотехнологичной преступности.

Эффективной мерой повышения компьютерной безопасности является возложение на руководителей или иных уполномоченных лиц персональной обязанности осуществлять контроль за установкой и постоянным обновлением антивирусного программного обеспечения, а также иных систем комплексной защиты с целью совершенствования систем безопасности компьютерной информации в государственных и муниципальных организациях. В свою очередь, в трудовых договорах (контрактах) лиц, работающих в корпоративной компьютерной сети или имеющих доступ к информационным ресурсам, предусмотреть положение об их персональной ответственности за разглашение или передачу посторонним лицам конфиденциальных сведений, касающихся системы защиты информации, служебных паролей или иных средств идентификации.

Отдельно следует остановиться на виктимологическом аспекте противодействия преступлениям, совершаемым с использованием высоких технологий. Поведение жертвы является составным элементом механизма преступления, поэтому одним из необходимых условий повышения эффективности предупреждения мошенничества в рассматриваемой сфере являются меры виктимологической профилактики, направленной на потенциальных жертв данного вида преступлений. Основой данной деятельности является воздействие на виктимологические факторы, влияющие на совершение преступлений в сфере высоких технологий. При этом следует учитывать как факт виктимности самих пользователей, так и компьютерных технологий и компьютеров – хранилищ информации. Поэтому к разработке мер виктимологической профилактики преступлений, совершаемых с использованием высоких технологий, должны привлекаться не только криминологи, но и технические специалисты [47].

Содержание виктимологической профилактики обусловлено несколькими аспектами. В организационном отношении виктимологическая профилактика имеет особенности, связанные со специальной подготовкой сотрудников правоохранительных органов. Недостаточность

профессиональных знаний и практических умений не позволяют им своевременно осуществлять предупредительные мероприятия. Это обусловлено отсутствием в настоящее время приемлемых методических рекомендаций по организации и тактике виктимологической профилактики высокотехнологичных преступлений, конкретных методик работы с жертвами подобных преступлений. В частности, определенные трудности вызывает проблема информационного обеспечения виктимологической профилактики преступлений, совершаемых с использованием высоких технологий. Поэтому совместная работа правоохранительных органов со службами компьютерной безопасности, изготовителями антивирусных программных продуктов является залогом успеха виктимологической профилактики.

В качестве субъектов осуществления виктимологической профилактики высокотехнологичных преступлений выступают как государство в лице правоохранительных органов, так и общественные формирования, и иные негосударственные структуры. По своему объему виктимологическая профилактика данного вида преступлений охватывает различные формы поведения, являющиеся закономерным результатом разных вариантов виктимности: легкомысленность поведения, излишнее любопытство, пользовательская небрежность, незнание элементарных мер защиты, возрастные и интеллектуальные особенности и др. В качестве механизма регулирования виктимологической защиты выступают не только нормы права, но и морали, корпоративные и этические правила поведения [47].

В целом виктимологическая профилактика должна быть ориентирована на широкую социальную превенцию в целях минимизации высокотехнологичной преступности как общественно опасного явления. Одним из существенных факторов активного использования мошеннических схем в информационно-телекоммуникационных сетях является недостаточное правовое регулирование деловых отношений в глобальной сети «Интернет», в том числе вопросов электронной формы сделки по гражданскому законодательству, деятельности с использованием электронных платежных

средств, проведения «Интернет»-аукционов, участия в дистанционной торговле. В частности, в условиях неопределенности правового статуса участников электронной торговли основное значение приобретает ряд профилактических рекомендаций для пользователей:

1. Визуальная оценка. В данном случае рекомендации «Интернет»-покупателям могут состоять в следующем: необходимо особое внимание уделять внешнему оформлению «Интернет»-магазина. Имеется в виду прежде всего дизайн сайта. Не стоит принимать в качестве достоверных отзывы пользователей, размещенные на этом же сайте. Правильным решением в данном случае является поиск отзывов на других сайтах.

Необходимо обращать внимание на то, какую площадь веб-страницы занимает баннерная реклама.

Положительную оценку получают сайты, не имеющие ни одной рекламной площадки или имеющие рекламу своих дочерних или, наоборот, головных предприятий.

Отсутствие рекламы – дополнительные удобства для пользователя. Присутствие рекламы означает, что магазин зарабатывает прибыль не на продаже товаров, а на рекламе.

2. Ценовая политика. Пользователям необходимо понимать, что цена товара определяется конъюнктурой рынка и не может резко отличаться от средней.

В «Интернете» достаточно сервисов, предоставляющих возможность поиска того или иного товара. Они помогут определить среднюю стоимость товара среди множества предложений.

3. Условия и права. Обратившись в новый «Интернет» -магазин, особое внимание следует обратить на следующие разделы сайта: «О магазине», «Об оплате» и «О доставке».

Действующие легально «Интернет» -магазины всегда размещают о себе полную информацию: адрес, телефон, реквизиты юридического лица и

расчетного счета. Такие магазины обычно работают по системе «оплата товара после доставки».

Во многих случаях мошенники просят сделать предоплату за доставку, причем с использованием электронных платежных систем.

Отсутствие информации, запутанная система получения товара, предложение совершить предоплату являются признаками мошеннической схемы.

Для противодействия фишингу сегодня используются различные способы совершенствования программно-технических средств защиты информации: постоянная модернизация анти-фишинговых и анти-спам фильтров почтовыми службами – с одной стороны, и использование клиентами для хранения конфиденциальной информации и обмена ею достаточно защищенных почтовых служб и ящиков – с другой.

Однако, как показывает практика, основная проблема связана с небрежностью в вопросах защиты персональной информации самими пользователями. Поэтому важной задачей правоохранительных органов является информационно-просветительская деятельность среди населения по предотвращению высокотехнологичной преступности.

При этом не следует увлекаться доведением до населения конкретных мошеннических схем, используемых преступниками, поскольку вариативность данных схем очень высокая, новые способы обмана жертв появляются регулярно и с завидным постоянством, при этом огромная территория нашей страны способствует возникновению «очаговых» схем, имеющих ограниченное распространение. Поэтому простое информирование населения о новых способах совершения мошенничества может иметь противоположный эффект: наиболее виктимные слои населения (пожилые люди, доверчивые и легкомысленные пользователи и т. д.) подобной информацией, скорее всего, не заинтересуются, а преступники могут взять на вооружение сообразительность своих «коллег». Основная работа сотрудников

правоохранительных органов должна заключаться прежде всего в доведении до граждан элементарных правил безопасности, таких как недопустимость:

- загрузки из сети «Интернет» программных продуктов из непроверенных источников; перехода по рекламным ссылкам в Интернете, сулящим бесплатные услуги, различные призы или существенные скидки; просмотра корреспонденции от неизвестных адресатов;– общения в социальных сетях с незнакомыми пользователями, за которыми могут скрываться мошенники, сектанты, вербовщики в террористические организации;
- покупки SIM-карт с рук или оставления своих паспортных данных сомнительным конторам;– отправки денежных переводов лицам, предлагающим посреднические услуги в разрешении проблем с родственниками, знакомыми, якобы попавшими в беду;
- передачи данных с кредитных или дебетовых карт, пользовательских паролей и кодовых слов, запрашиваемых по телефону или через социальные сети от лица друзей, знакомых, кредитных или иных организаций под различными предлогами;
- указания в своем профиле социальной сети личной информации, в том числе о своем образе жизни, планируемых отъездах и т. п.;
- проведения операций в «Интернет»-банкинге без проверки истинности адреса личного кабинета или при наличии дополнительных не предусмотренных стандартной процедурой запросов (защита от «фишинга»);
- непринятия срочных мер по блокированию кредитных или дебетовых карт при получении SMS о несанкционированном списании или переводе средств третьим лицам;
- регистрации в личных кабинетах, на «Интернет»-ресурсах или онлайн-магазинах с простыми паролями, состоящими из нескольких цифр, коротких слов, соседних клавиш на клавиатуре, личных памятных дат, адресов или номеров телефонов;

– – записей личных паролей на стикерах, приклеенных к монитору, или в других легкодоступных местах.

Таким образом, виктимологическая профилактика преступлений, совершаемых с использованием высоких технологий, должна быть организована:

– с учетом виктимности различных групп населения;
– учитывать различные аспекты обеспечения данного вида деятельности;
– иметь конкретную направленность на осознание необходимости соблюдения мер предосторожности в информационно-телекоммуникационном пространстве;
– основываться на доступных для населения или работников – неспециалистов рекомендациях по совершенствованию своей защищенности от киберугроз.

Заключение

По итогам проведенного исследования следует указать, что приведенные в ходе дипломного исследования статистические показатели не отражают всю гамму преступлений, совершенных с использованием информационно-коммуникационных технологий. Так, в отчет, охватывающий около 10 составов преступлений (ст. 158, 159, 159.3, 159.6, 183, 272–274 УК РФ), не вошли такие преступления против личности, как доведение до самоубийства (ст. 110 УК РФ), склонение к совершению самоубийства или содействие совершению самоубийства (ст. 110.1 УК РФ), организация деятельности, направленной на побуждение к совершению самоубийства (ст. 110.2 УК РФ), угроза убийством или причинением тяжкого вреда здоровью (ст. 119 УК РФ), принуждение к изъятию органов и тканей человека для трансплантации (ст. 120 УК РФ), клевета (ст. 128.1 УК РФ), понуждение к действиям сексуального характера (ст. 133 УК РФ), нарушение неприкосновенности частной жизни (ст. 137 УК РФ), нарушение изобретательских и патентных прав (ст. 147 УК РФ), вовлечение несовершеннолетнего в совершение преступления (ст. 150 УК РФ), вовлечение несовершеннолетнего в совершение антиобщественных действий (ст. 151 УК РФ), розничная продажа несовершеннолетним алкогольной продукции (ст. 151.1 УК РФ), вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (ст. 152.2 УК РФ), разглашение тайны усыновления (удочерения) (ст. 155 УК РФ) и иные преступления, совершаемые дистанционным способом, при которых непосредственный физический контакт между субъектом преступления и потерпевшим, а также соучастниками, осуществляется посредством сообщений в мессенджерах, социальных сетях, на специализированных сайтах.

Безусловно, развитие информационных и коммуникационных технологий открывает новые возможности для совершения перечисленных и

иных преступлений прежде всего в сфере экономики, против общественной безопасности и общественного порядка и др., представляя собой вызов всей правоохранительной системе и общественной безопасности.

В целом, среда «Интернет» – это хорошая среда для преступной деятельности. На его просторах циркулируют огромные потоки информации, естественно, часть из которого может носить противоправное и запрещенное содержание, например, распространение порнографического материала, а также пиратские копии фильмов или музыки, а также очень большое количество желающих, которые хотят получить нечто запрещенное, например, наркотические вещества. Кроме того, уровень безопасности общественных мест активно повышается за счет установления камер общественного наблюдения, что также затрудняет совершение противоправных действий в реальном мире. В свою очередь, в сети «Интернет» можно «укрыться» спрятав координаты своего расположения и другие опознавательные данные и заниматься противоправными деяниями.

При этом нужно учитывать, что сеть «Интернет» является «всемирной паутиной», где нет границ и преград, что также существенно усложняет возможность обнаружения преступника в киберпространстве и увеличивает опасность его противоправного деяния.

В целях виктимологической профилактики целесообразно рекомендовать пользователям использовать наиболее подходящий, защищенный и правильно настроенный веб-браузер, который незамедлительно предупреждает пользователя о возможной опасности. Это касается не только браузеров, но и других используемых программ, например, электронных кошельков WebMo№ey. Кроме того, антивирусные пакеты многих производителей этого программного обеспечения пополнились модулями, защищающими пользователя от разного рода покушений в сети «Интернет».

Список используемой литературы и используемых источников

1. Co№ve№tio№ o№ Cybercrime. The Cou№cil of Europe. Hu№gary. - 2001. [Электронный ресурс]. - Режим доступа: http: // cyber-crime.com/legislative. (дата обращения 18.03.2020).
2. Актуальные схемы мошенничества. Международный форум «A№tiFraud Russia. Борьба с мошенничеством в сфере высоких технологий» // https://jet.su/about/№ews/19731/ (дата обращения 16.04.2020)
3. Алгоритм взаимодействия заинтересованных органов при выявлении противоправного контента в сети «Интернет» // Официальный сайт Роскомнадзора https://18.rk№.gov.ru/№ews/№ews117596.htm (дата обращения 10.04.2020).
4. Брябрина Т.В., Гиберт А.И. Опыт контент-анализа суицидальных высказываний в сети интернет лиц с различным уровнем суицидальной активности // Вестник Южно-уральского государственного университета. 2016. № 3. С. 35-49
5. В генпрокуратуре рассказали, что число выявленных киберпреступлений выросло в 16 раз // Информационное агентство ТАСС https://tass.ru/proisshestviya/5733551 (дата обращения 26.04.2020).
6. Валагин А Российский интернет оказался быстрее европейского // Российская газета. 2019. № 16. С. 13-15
7. Ветров Н.И. Уголовное право. Особенная часть: учебник для вузов. ЮНИТИ-ДАНА, Закон и право, 2018. 364 с.
8. Генпрокуратура сообщила почти о двукратном росте числа кибер преступлений в РФ // Информационное агентство ТАСС https://tass.ru/proisshestviya/5733551 (дата обращения 26.04.2020)
9. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 16.12.2019, с изм. от 12.05.2020) // «Собрание законодательства РФ», 05.12.1994, № 32, ст. 3301.

10. Гундерич Г.А. Состояние кибер преступности // Научный вестник Крыма.2018. № 4. С.17

11. Егерева О.А. Некоторые вопросы методики расследования кибер преступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2018. № 1. С. 46

12. Жмыхов, А.А. Компьютерная преступность за рубежом и ее предупреждение: автореф. дис. … канд. юрид. наук: 12.00.08 / А.А. Жмыхов. – Москва, 2003. 26 с.

13. Закон РФ от 27.12.1991 № 2124-1 (ред. от 01.03.2020) «О средствах массовой информации» // Российская газета, № 32, 08.02.1992.

14. Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: Дис. ... канд. юрид. наук. Красноярск, 2002. С. 145.

15. Кассационное определение Судебной коллегии по уголовным делам ВС РФ от 30.01.2009 № 89-008-88 // URL: https://www.zako№rf.i№fo/suddoc/622738e2b53d041c8f82db7b063a8115/ (дата обращения: 04.05.2020).

16. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 24.04.2020) // «Российская газета», № 256, 31.12.2001.

17. Козодаева О.Н., Обыденнова А.С. Способы совершения мошенничества с использованием банковских карт // Ученые записки Тамбовского отделения РоСМУ. 2019. № 2. С.53

18. Комлев Ю.Ю. Миллениалы, или куда уходит девиантность? // Ученые записки Казанского юридического института МВД России. 2018. № 3. С. 22.

19. Комментарий к Уголовному кодексу Российской Федерации / под общ. ред. В.М. Лебедева, Ю.И. Скуратова. М. : Норма, 2018. 704 с.

20. Конвенция о преступности в сфере компьютерной информации» (ETS № 185) [рус, англ.] (Заключена в г. Будапеште 23.11.2001) (с изм. от

28.01.2003) // СПС Консультант Плюс http://www.co№sulta№t.ru/co№s/cgi/o№li№e.cgi?req=doc&base=I№T&№=13526#015884956126299177 (дата обращения 30.04.2020).

21. Конвенция ООН против транснациональной организованной преступности, 15 ноября 2000 г. // Междунар. право и борьба с преступностью: сб. док. / сост.: А.В.Змеевский, Ю.М.Колосов, Н.В.Прокофьев. – М. : Междунар. отношения, 2004. 720 с.

22. Краткая характеристика состояния преступности в Российской Федерации за январь - март 2020 года // URL: https://мвд.рф/reports/item/20016032/ (дата обращения: 04.05. 2020).

23. Кузнецов А.П. Ответственность за преступления в сфере компьютерной информации: учебно-практическое пособие, 2017. 486 с.

24. Лаптева Е.В. Механизмы защиты прав граждан при использовании ими телефонных средств // Be№eficium. 2019. № 4. С. 28.

25. Лапунова Ю.А, Голяндин Н.П. Распространение идеологии экстремизма и терроризма в киберпространстве: проблемы и пути их решения // Труды Академии управления МВД России. 2017. № 3 (43).

26. Лысак Е. А. Проблемы квалификации преступлений в сфере компьютерной информации // Научный журнал КубГАУ. 2016. № 2. С. 19-22 (дата обращения: 04.05.2020).

27. Лютов В.А. К вопросу об эффективности применения положений уголовного законодательства о мошенничестве с использованием электронных средств платежа // Отечественная юриспруденция. 2019. №2. С. 19.

28. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) // URL: http://www.co№sulta№t.ru/co№s/cgi/o№li№e.cgi?r№d=F347D20613AC7FE4A9984EC4B930398F&req=doc&base=LAW&№=161817&dst=100022&fld=134&REFFIELD=134&REFDST=970&REFDOC=349294&REFBASE=LAW&stat=refc

ode%3D16610%3BdstideNt%3D100022%3BiNdex%3D5770#265rjmsl23d (дата обращения: 04.05.2020).

29. Новое уголовное право России. Особенная часть: Учебное пособие / Борзенков Г.Н., Бородин С.В., Волженкин Б.В., Комиссаров В.С., и др.; Под ред.: Кузнецова Н.Ф. - М.: Зерцало, ТЕИС, 2016. 273 с.

30. О методических рекомендациях по заполнению формы сообщения о наличии на страницах сайтов в сети Интернет противоправной информации // Официальный сайт Роскомнадзора https://18.rkNe.gov.ru/Neews/Neews117596.htm (дата обращения 10.04.2020).

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

32. Одом У. Компьютерные сети. Первый шаг = Computer NetworkiNg: First-step / Пер. В. Гусев. — СПб. : «Вильямс», 2016. С. 24

33. Органы прокуратуры Дальневосточного федерального округа провели более 960 проверок соблюдения законодательства о противодействии экстремизму // Официальный сайт Прокуратуры Мурманской области https://prok-murmaNesk.ru/ (дата обращения 10.04.2020).

34. Официальные статистические данные с сайта https://NeilsoNereport.com/ (дата обращения 22.04.2020)

35. Письмо ФКЦБ РФ от 20.01.2000 № ИБ-02/229 «О возможных мошеннических схемах при торговле ценными бумагами с использованием сети Интернет» // СПС КонсультантПлюс http://www.coNesultaNet.ru/documeNet/coNes_doc_LAW_26135/ (дата обращения 04.05.2020).

36. Понимание кибербезопасности: руководство для развивающихся стран [Электронный ресурс]. – Режим доступа: http://www.itu.iNet/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFR.pdf. (дата обращения 15.03.2020).

37. Попов А. Б. Проблемы квалификации преступлений в сфере компьютерной информации // Вестник ТГУ. Выпуск 10(66). 2008. С. 339 (дата обращения: 05.05.2020).

38. Порядок ограничения доступа к информации, распространяемой в сети Интернет с нарушением закона // Официальный сайт прокуратуры Магаданской области http://magoblproc.ru (дата обращения 01.05.2020).

39. Предупреждение суицидов и Интернет: Риск и возможности // Суицидология. № 4 (25). 2016. С.82

40. Приговор №1-232/2013 от 2 августа 2013 года // Судебные и нормативные акты РФ https://sudact.ru/regular/doc/SkwWU0bdb5gx/ (дата обращения 01.05.2020).

41. Приказ Генпрокуратуры России от 08.09.2016 № 562 «Об организации работы по рассмотрению уведомлений о распространении в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, и направлению требований о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию» // СПС КонсультантПлюс http://www.co№sulta№t.ru/docume№t/co№s_doc_LAW_254849/ (дата обращения 01.05.2020).

42. Приказ МВД России от 1 апреля 2002 г. № 311 об утверждении «Формы 1-ВТ» // СПС КонсультантПлюс (дата обращения 24.04.2020).

43. Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» (Зарегистрировано в Минюсте России 08.02.2018 № 49966) // URL: http://www.co№sulta№t.ru/docume№t/co№s_doc_LAW_290538/3b0a35f4530e4087370d096b8a1c08ca9e668570/#dst100009 (дата обращения: 05.05.2020).

44. Расследование неправомерного доступа к компьютерной информации / под ред. М.Г. Шурухнова. М., 2016. 274 с.

45. Рекомендация № R 89 (9) Комитета Министров стран – членов Совета Европы о преступлениях, связанных с компьютерами. Принята 13 сентября 1989 г // СПС Консультант плюс (дата обращения 26.03.2020).

46. Решетников А. Ю., Русскевич Е. А. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) // URL: https://valerykomarov.blogspot.com/2019/08/2741.html (дата обращения: 05.05.2020).

47. Сазонов М.М. Виды мошенничеств с банковскими картами и совершенствование мер виктимологического предупреждения // Виктимология. № 1. 2018. С. 58.

48. Сизов А. Как сейчас работают кибер мошенники и почему бизнесу нужны новые технологии для борьбы с ними // https://hightech.fm/2019/07/22/cyber-scammers (дата обращения 16.04.2020).

49. Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.) // URL: https://base.gara№t.ru/12123778/ (дата обращения: 05.05.2020).

50. Статистические данные аналитического центра Zecurio№ A№alytic // https://www.zecurio№.ru/press/a№alytics/ (дата обращения 22.04.2020).

51. Статистические данные компания «Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере» // https://www.cbr.ru/Co№te№t/Docume№t/File/62930/gubzi_18.pdf/ (дата обращения 22.04.2020).

52. Статистические данные экспертного центра электронного государства // http://d-russia.ru/category/kiberbezopas№ost (дата обращения 26.04.2020).

53. Таненбаум Э, Уэзеролл Д. Компьютерные сети. - СПб. : Питер, 2012. 960 с.

54. Тучков А.В. Криминологическая характеристика хищений, совершаемых с использованием информационно-телекоммуникационных технологий // Академическая мысль. 2019. №2(27).С.38

55. Уголовное право России. Часть Особенная / Отв. ред. Л.Л. Кругликов. М. : Проспект, 2018. 53 с.

56. Уголовное право Российской Федерации. Особенная часть: Учебник / Под ред. проф. Б. В. Здравомыслова. - Изд. 2-е, перераб. и доп. М., 2016. 480 с.

57. Уголовное право. Особенная часть: учебник / под ред. проф. В.Н. Петрашова. М.: Издательство Приор, 2018. 430 с.

58. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 07.04.2020) (с изм. и доп., вступ. в силу с 12.04.2020) // Собрание законодательства РФ. 17.06.1996. № 25. ст. 2954.

59. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС КонсультантПлюс http://www.co№sulta№t.ru/docume№t/co№s_doc_LAW_208191/ (дата обращения 01.05.2020).

60. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // «Собрание законодательства РФ», 04.01.2016, № 1 (часть II), ст. 212.

61. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций // Официальный сайт http://eais.rk№.gov.ru (дата обращения 01.05.2020).

62. Федеральный закон «О противодействии экстремистской деятельности» от 25.07.2002 № 114-ФЗ (последняя редакция) // СПС КонсультантПлюс

http://www.co№sulta№t.ru/docume№t/co№s_doc_LAW_37867/ (дата обращения 01.05.2020).

63. Федеральный закон от 11.11.2003 № 138-ФЗ (ред. от 01.03.2020) «О лотереях» // Собрание законодательства РФ, 17.11.2003. № 46 (ч. 1), ст. 4434.

64. Федеральный закон от 13 января 1995 г. № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации» // СПС Консультант плюс http://www.co№sulta№t.ru/docume№t/co№s_doc_LAW_5410/ (Дата обращения 14.05.2020).

65. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // «Российская газета», № 167, 31.07.2017.

66. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 03.04.2020) «Об информации, информационных технологиях и о защите информации» // Российская газета, № 165, 29.07.2006.

67. Федеральный закон от 29.11.2012 № 207-ФЗ (ред. от 03.07.2016) «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // Российская газета, № 278, 03.12.2012.

68. Федеральный закон от 29.12.2006 № 244-ФЗ (ред. от 27.12.2019) «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» // Российская газета, № 297, 31.12.2006.

69. Федотов А.А., Зебницчкая А.К. Криминалистическая характеристика мошенничества // Вопросы науки и образования. 2018. № 1. С. 26.

70. Черных В.В. Проблемы расследования мошенничества, совершенного с использованием банковских карт и их решения // Вестник Таганрогского института управления и экономики. 2018. № 2. С. 48.

71. Число несанкционированных взломов компьютеров Правительства США возросло на 50% [Электронный ресурс]. – Режим доступа: http://www.crime-research.ru/№ews/06.05.2011/7234/. – Дата доступа: 18.04.2020

72. Шевко Н. Р. Особенности раскрытия и расследования кибер преступлений: проблемы и пути их решения // Ученые записки Казанского юридического института МВД России. 2016. Т. 1. № 1 (1).

73. Широков, В.А. Киберпреступность: история уголовно-правового противодействия /В.А. Широков, Е.В. Беспалова [Электронный ресурс]. – Режим доступа: http://rudocs.exdat.com/docs/i№dex-161949.html. - Дата доступа: 20.03.2020.

74. Шаронова против распространения информации, запрещенной в сети Интернет Решение № 2А-3495/2019 2А-3495/2019~М-3743/2019 М-3743/2019 от 29 ноября 2019 г. по делу № 2А-3495/2019 // Судебные и нормативные акты РФ https://sudact.ru (дата обращения 01.06.2020).