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 направлению подготовки / специальности)

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

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
(ДИПЛОМНАЯ РАБОТА)

на тему «Киберпреступность: понятие, состояние, криминалистический анализ отдельных видов»

Обучающийся Е.А. Лесовский
(Инициалы Фамилия) (личная подпись)

Руководитель канд. юрид. наук, доцент, П.А. Кабанов
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2022

Аннотация

Киберпреступность в современном мире технологий стремительно растет. Преступники Всемирной паутины используют личную информацию интернет-пользователей в своих корыстных целях. Они погружаются в «темную сеть», чтобы покупать и продавать нелегальные товары и услуги. Они даже получают доступ к секретной правительственной информации. Киберпреступность находится на рекордно высоком уровне, ежегодно обходясь компаниям и частным лицам в миллиарды долларов. Что еще более неприемлемо, так это то, что эта статистика в российском обществе только начала формироваться и очевидно будет только расти. Эволюция технологий и растущая доступность интеллектуальных технологий означают, что в отдельно взятом домовладении пользователя есть несколько точек доступа, которые хакеры могут использовать в преступных целях [80].

Одним из направлений исследования в дипломной работе является исследование актуального состояния киберпреступности, стремительный рост динамики которой отмечается в Российской Федерации за последние несколько лет (за 2017-2021 гг.) [58].

На основании статистики о состоянии киберпреступности, которая опубликована Министерством внутренних дел Российской Федерации, мы сравнили количество официально зарегистрированных за 2017-2020 гг. преступлений, совершённых в сфере компьютерной информации и с помощью информационно-коммуникационных технологий.

В результате исследования статистических данных был сделан вывод, что киберпреступность стремительно развивается в России в течении последних нескольких лет, а с появлением новой коронавирусной инфекции приобрела масштабы социальной проблемой и стала фактически угрозой национальной безопасности [42].

В работе сформулированы также факторы, в значительной степени поспособствовавшие возникновению данной негативной ситуации. К ним мы

отнесли низкий уровень компьютерной грамотности населения РФ на фоне ускорившейся во время пандемии компьютеризации населения; низкоэффективное противостояние киберпреступности (низкий уровень подготовленности кадров со стороны правоохранительных органов, несовершенность так называемой antifraud-инфраструктуры – комплекса технологий и программного обеспечения, разработанного для эффективного отпора киберпреступным действиям). Как следствие – невысокий процент раскрываемости киберпреступлений, низкая степень подготовки к работе на упреждение и оперативное пресечение киберпреступной активности [84].

Актуальность исследования подтверждается, таким образом, тем, что киберпреступная деятельность превращается в одну из самых серьёзных угроз современного российского общества и причиняет огромный ущерб российской экономике и благополучию граждан [68].

Целью дипломной работы является проведение всестороннего криминалистического анализа по киберпреступлениям; исследование особенностей киберпреступности, выявление современных тенденций на рынке киберпреступлений.

В рамках реализации цели можно выделить следующие основные задачи:

- определить понятие, состояние и криминалистическую классификацию преступлений в сфере ИТ-технологий;
- проанализировать динамику развития киберпреступности в Российской Федерации в 2017–2021 годах, опираясь на статистические данные Министерства внутренних дел о количестве зарегистрированных киберпреступлений в эти годы в РФ;
- охарактеризовать уголовно-правовые нормы по регулированию отношений в сфере киберпространства;
- исследовать становление и развитие правоотношений в сфере криминализации киберпреступлений;

- определить объективные и субъективные признаки киберпреступных деяний;
- выявить причины сложностей квалификации киберпреступлений;
- сформулировать и обосновать основные факторы, ставшие причиной ухудшения ситуации с киберпреступностью в РФ, усугубившейся за последние 5 лет.

Методология данной дипломной работы включает системный подход, а также использование логического, нормативно-догматического и сравнительно-правового методов познания.

Теоретическое и практическое значение результатов дипломной работы заключается в том, что здесь раскрыты основные положения о киберпреступлениях, проведен уголовной-правовой анализ отдельных его видов, сформированы рекомендации по совершенствованию законодательства, а также о мерах профилактики. Данные положения могут быть использованы в правоприменительной практике, также может быть использован в качестве материала для углубленного изучения курса «Уголовное право» студентами старших курсов по направлению подготовки «Юриспруденция» [38].

Структура работы обусловлена целью и задачами дипломной работы и включает в себя введение, две главы, объединяющих в себе 7 параграфов, заключение и список используемой литературы и используемых источников.

Оглавление

Введение

В основе любого общества лежит межличностное общение. Люди используют его, в том числе, для получения информации и информационных продуктов. Несмотря на то, что во время стремительного прогресса в сфере передовых технологий информация играет огромную роль для развития индивида, общества и государства, глобальная цифровизация имеет и отрицательные последствия в виде серьёзных угроз как для отдельных индивидов, так и для общества в целом. Внедрение цифровизации во все области нашей жизни спровоцировало изменения как в развитии полезной деятельности общества, так и в развитии преступности.

Практически каждое четвертое преступление в Российской Федерации совершается с использованием информационных технологий. В 2021 году в РФ зарегистрировано около 518 тысяч киберпреступлений, что составляет на 1,4% больше, чем в 2020 году, однако, сразу в 1,8 раза превосходит показатель 2019 года [58]. Эти данные подтверждают и данные компании RTM Group, которая проводила оценку на основе возбужденных уголовных дел, связанных с использованием ИТ-технологий.

В частности, количество заявлений о мошенничестве выросло на 5,11%, превысив 249 тысяч. Однако, количество заявлений о возбуждении уголовных дел в связи с киберпреступлениями со взломом сократилось на 10,5%, до 157 тысяч. Около четверти всех преступлений было связано с другими составами, в том числе с незаконной организацией и проведением азартных игр.

Эксперты оценили ущерб России от действий хакеров в 150 млрд. рублей по итогам 2021 года. По данным авторитетного аналитического агентства в области оценки влияния киберпреступлений на экономику по итогам 2022 года можно предугадать рост числа результативных кибератак не менее, чем на 30–40% [58]. Такой рост происходит, в том числе за счет развития схем социальной инженерии и применения новых инструментов.

В марте 2021 года президент России Владимир Путин заявил, что за последние 6 лет число преступлений в сфере информационных технологий выросло в 10 раз и потребовал повысить показатели раскрываемости таких преступлений, но «не благодаря бумажной отчетности, а благодаря кропотливой работе на земле». Нарушители становятся все более агрессивными и сохраняют анонимность, тщательно скрывая свои следы.

В связи с вышесказанным, исследование причин стремительного развития, анализ криминалистической характеристики киберпреступлений и варианты преодоления киберугроз становятся крайне актуальными задачами и находят свое отражение в работах А.А. Куклина, Л.И. Абалкина, В.К. Сенчагова, А.И. Татаркина и других авторов [81].

Целью дипломной работы является представление наиболее всестороннего криминалистического анализа по киберпреступлениям; исследование особенностей киберпреступности, выявление современных тенденций на рынке киберпреступлений.

В рамках реализации цели можно выделить следующие основные задачи:

- определить понятие, состояние и криминалистическую классификацию преступлений в сфере ИТ - технологий;
- проанализировать динамику развития киберпреступности в Российской Федерации в 2017-2021 годах, опираясь на статистические данные Министерства внутренних дел о количестве зарегистрированных киберпреступлений в эти годы в РФ;
- охарактеризовать уголовно-правовые нормы по регулированию отношений в сфере киберпространства;
- исследовать становление и развитие правоотношений в сфере криминализации киберпреступлений;
- определить объективные и субъективные отдельных признаки киберпреступных деяний;
- выявить причины сложностей квалификации киберпреступлений;

– сформулировать и обосновать основные факторы, ставшие причиной ухудшения ситуации с киберпреступностью в РФ, усугубившейся за последние 5 лет.

Предметом данной работы выступают нормы российского уголовного законодательства, устанавливающие уголовную ответственность за киберпреступления, совершённых с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», а также, нормы законодательства РФ в сфере кибербезопасности и информационных технологий.

Объектом исследования выступают общественные отношения, осуществляющие противодействие киберпреступной деятельности.

Для анализа, в рамках дипломной работы, в качестве одного из источников статистических данных, была использованы показатели по преступлениям, совершённым с использованием ИТ-технологий, которая опубликована в разделе отчётов о состоянии преступности в стране [58].

Теоретическое и практическое значение результатов дипломной работы заключается в том, что здесь раскрыты основные положения о киберпреступлениях, проведен уголовной-правовой анализ отдельных его видов, сформированы рекомендации по совершенствованию законодательства, а также о мерах профилактики. Данные положения могут быть использованы в правоприменительной практике, также может быть использован в качестве материала для углубленного изучения курса «Уголовное право» студентами старших курсов по направлению подготовки «Юриспруденция».

Научные исследования в рамках выявления криминалистических особенностей компьютерных преступлений проводились по ряжу направлений разными авторами: вопросы, касающиеся выделения данных преступных деяний в отдельно группу в рамках криминалистической классификации; описание методики расследования киберпреступлений; криминалистический учёт киберпреступлений, предопределённых

особенностями использования возможностей Интернет-сети; вероятность использования виртуальных следов, и другие. В работе использовались научные достижения следующих авторов: А.С. Вражнова, В.Ю. Агибалова, В.В. Крылова, М.А. Бабакова, В.Б. Вехова, Д. А. Илюшина, А.А. Васильева, Ю.В. Гаврилина, А.А. Косынкина, В.А. Мещерякова, В.В. Поповой, А.Н. Семикаленовой, В.В. Степанова, А.И. Усова и другими исследователями [8].

В данном дипломном исследовании, мною был проведён анализ норм уголовного законодательства РФ, который характеризует отдельные признаки совершения преступлений для выделения киберпреступлений с точки зрения уголовного права России и в целях улучшений уголовного законодательства РФ в части совершения преступлений в сфере высоких технологий [37].

Методология данной дипломной работы включает системный подход, а также использование логического, нормативно-догматического и сравнительно-правового методов познания [7].

Структура работы обусловлена целью и задачами дипломной работы и включает в себя введение, две главы, объединяющих в себе 6 параграфов, заключение и список используемой литературы и используемых источников.

Глава 1 Понятие, состояние, признаки киберпреступности и её виды

1.1 Понятие, состояние и признаки киберпреступности

В Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы [56], сказано о том, что информационные системы и социальные сети стали важной частью повседневной жизни граждан нашей страны. Интернет – это революционная коммуникационная и сетевая технология, которая позволила людям по всему миру активно взаимодействовать: общаться, подключаться, покупать и продавать.

Дату начала работы Интернет-пространства сложно определить. Никола Тесла и другие авторитетные программисты в начале 1900-х разработали беспроводную систему, которая могла бы соединять машины по всему миру. Первый прототип признанной глобальной компьютерной сети – ARPANET, иногда ошибочно называемый DARPANET, стал реальностью в 1969 году [2].

Однако другие специалисты считают, что официальное начало интернета было в 1983 году, когда протокол управления (TCP/ IP) впервые позволил использовать универсальный язык для общения во всех сетях. Сегодня интернет позволяет пользователям получать доступ к веб-страницам на настольных компьютерах, ноутбуках, смартфонах, планшетах и многих других устройствах с помощью сигналов Wi-Fi, сотовых сигналов или прямого оптоволоконного соединения.

Так, Тропина Т.Л. обращает внимание: «… прообразом сети Интернет является первая высокоскоростная континентальная компьютерная сеть ARPANet, созданная в DARPA – Армейском агентстве передовых исследовательских проектов по заказу министерства обороны США. Идея создания такой сети родилась в 1964 г. у Ларри Робертса и заключалась в создании децентрализованной системы, состоящей из отдельных независимых сегментов, где не было бы главного компьютера, который может быть уничтожен в случае ядерной войны. В случае выхода из строя одного

компьютера, передача должна была осуществляться по обходным каналам связи. В 1969 г. состоялся успешный обмен данными путем подсоединения двух компьютеров между собой. В этом же году был проведен аналогичный эксперимент, но с компьютерами, находящимися в разных городах. С этого момента ARPANet начала свою работу» [64, с. 31].

В 1962 году специалисты по информатике Массачусетского технологического института начали работу над созданием новаторского прототипа сети. Такие специалисты как Lawrence G. Roberts, Thomas Merrill и Leonard Kleinrock стали одними из самых известных участников этого сетевого соединения.

К январю 1973 года через ARPANET было подключено всего 35 узлов. К 1976 году количество подключенных хостов увеличилось до 63.

В 1989 году Тимом Бернерсом-Ли был разработан язык гипертекстовой разметки (HTML) и унифицированного указателя ресурсов (URL). Это значительно расширило сетевые возможности сети интернет.

Винт Серф и Роберт Кан, известные как «отцы» интернета, совместно изобрели протоколы TCP/IP в DARPA. Это важное событие позволило Интернету превратиться из сети исследовательских компьютеров DARPA в глобальное явление.

С целью расширения возможностей для передачи данных специалисты сегодня производят не надстройки сети, а меняют описание изменений веб-платформ. Одна из которых обознается как Web 2.0. Этот термин используется для описания изменений в веб-платформах и взаимодействиях. По мере того, как интернет развивался, там были представлены различные социальные сети, службы потокового видео и другие интерактивные платформы. Примерно в 2004 году все эти изменения были объединены термином Web 2.0 для переопределения удобства использования Интернета.

Платформы будущего интернета называются Web 3.0. Специалисты рассматривают Web 3.0 как полностью интерактивную децентрализованную версию интернета, работающую с использованием искусственного интеллекта

и машинного обучения. Многие считают, что блокчейн – это будущее Интернета, и он предлагает множество преимуществ. Блокчейн – это то, где устройства являются не только частью сложного сетевого соединения, но и используют общедоступный реестр, охватывающий всю сеть [3]. Такие технологичные изменения обещают создать безопасную базу для криптовалют и невзаимозаменяемых токенов (NFT), которые будут использоваться в качестве валюты. Критики отмечают, что у децентрализации сети интернет есть свои плюсы и минусы, поскольку может быть сложнее отслеживать или регулировать незаконную деятельность.

Федотов М. А. обращает наше внимание на весьма интересный факт: «… чтобы представить темпы проникновения интернет-технологий в современное общество, достаточно сравнить скорость распространения современных телекоммуникационных сетей с темпами развития сети приема традиционных аудио- и аудиовизуальных СМИ. Так, в США радиовещание смогло расширить число своих пользователей до 50 млн. человек за 38 лет, телевидение – за 13 лет, Интернет – за 4 года» [77, с. 166].

К 2020 году число пользователей во всем мире достигло примерно 4,5 миллиардов, что составляет более половины населения мира. Существует много споров о том, оказывает ли интернет в целом положительное, отрицательное или нейтральное влияние на мир. Очевидно, одно, что эта глобальная динамично развивающая сеть, позволяет пользователям по всему миру получать доступ к веб-страницам, сообщениям в социальных сетях, изображениям, видео и другому контенту [2].

В период своего развития Интернет-сеть претерпела множество обновлений и улучшений, отдельные ее компоненты могут влиять на безопасность не только отдельно взятой компании или физического лица, но и затрагивать интересы государства.

Верно отмечает А. Г. Серго «... что появление кириллической доменной зоны имеет целый ряд недостатков. Во-первых, домены в зоне Российской Федерации останутся недоступными для иностранных пользователей

интернета, не имеющих кириллической клавиатуры. Во-вторых, дополнительные проблемы появятся даже у пользователей интернета в других странах, использующих кириллицу (Беларусь, Болгария, Сербия, Украина и др.), поскольку их алфавит содержит не все буквы русского языка» [2, с. 175].

Интернет способен передавать множество типов информации по сетям на множество различных устройств. Это способствует развитию различных мошеннических схем, в практике существует такой термин «дистанционное мошенничество», который охватывает высокотехнологичные виды киберпреступлений в том числе: киберзапугивания, распространение вредоносных программ, преднамеренная дезинформации и другие виды манипуляции.

В 1996 году Конгресс США принял Закон о пристойности в средствах массовой информации, чтобы ограничить «непристойные или непристойные» сообщения лицами моложе 18 лет. Он также стремился ограничить использование «явно оскорбительных» материалов. Многие из положений были отменены в 1997 году как неконституционные, но некоторые остаются. После анализа всех «за» и «против» было решено, что некоторые акты включали слишком много ограничений свободы слова.

Относительно разработки понятийного аппарата Шевченко Е.С. обоснованно утверждает: «Выполняя коммуникативную и познавательную функцию, определение (понятие, термин) выражает некоторую категорию сведений об объекте познания и понятно для лиц, не обладающих узко криминалистическими знаниями» [86, с. 15].

М.А. Федотов обоснованно считает, что: «...для того, чтобы государство смогло выработать правовые нормы, устанавливающие эффективные правила работаты в сети, оно должно сначала найти себя в киберпространстве и определить, где здесь проходят границы его суверенитета и юрисдикции. Трансграничный интернет не признает государственных границ. Государственный суверенитет не знает понятия киберпространства и не ощущает своих границ в этом» [50].

Специфика киберпространства заставляет пересмотреть этот подход, поскольку в интернет-среде понятие «пространство» лишается однозначной географической определенности, понятие «время» не привязано ни к какому часовому поясу, а понятие «круг лиц» оказывается включающим не физических и юридических лиц, а компьютеры и другие устройства, участвующие в сетевом взаимодействии и идентифицируемые по их IP-адресам и другим технологическим деталям» [82, с. 167].

Отечественная и зарубежная наука по-разному именует преступления, совершенные в виртуальном мире: киберпреступления, информационные преступления, компьютерные преступления, преступления, совершенные в виртуальном пространстве, преступления в сфере высоких технологий [39].

«Киберпреступление» – термин иностранного происхождения, состоящий из двух частей «кибер» и «преступление». В словаре Оксфорда слово «кибер» определено, как: «относящийся к компьютерам, информационным технологиям, виртуальной реальности» [79, с. 33-38].

В законодательстве РФ для описания и характеристики виртуального пространства и высоких технологий применяются прилагательные «цифровое» и «информационное».

По мнению Шевченко Е.С. «киберпреступление – это общественно опасное деяние, совершаемое в киберпространстве, посягающее на общественную безопасность, собственность, права человека, другие охраняемые законом отношения, необходимым элементом механизма подготовки, совершения, сокрытия и отражения которого является компьютерная информация, выступающая в роли предмета или средства преступления» [86, с. 36].

Кочкина Э.Л. определяет киберпреступление как: «... совокупность преступлений, запрещенных Уголовным кодексом РФ, совершаемых в киберпространстве, где основными непосредственными объектами преступного посягательства выступают:

– конституционные права и свободы человека и гражданина;

– общественные отношения в сфере компьютерной информации и информационных технологий;
– общественные отношения в сфере экономики и экономической деятельности;
– общественные отношения в сфере государственной власти;
– общественные отношения в сфере здоровья населения и общественной нравственности» [35, с. 167].

Исходя из положений уголовного законодательства РФ, под киберпреступностью понимается реализация неправомерных деяний в отрасли информационных процессов, являющихся посягательством на информационную безопасность частных пользователей, групп или целой инфраструктуры и совершаются с помощью использования компьютерных сетей и систем [65].

Согласно Доктрине информационной безопасности Российской Федерации, под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации; развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений [56].

Рассматривая признаки киберпреступлений, авторы научных исследований выделяют несколько характерных признаков:

– киберпреступления совершаются с использованием средств компьютерной техники и в отношении информации, находящейся (используемой и/или обрабатываемой) в интернет-сети». Компьютерные устройства и все возможные информационо-коммуникационные и социальные сети являются средствами

совершения преступления; применение вредоносных программ выступает орудием совершения преступления;

- присутствуют два объекта посягательства: общественные отношения в сфере киберзащиты и общественные отношения, связывающие её с реальным миром;
- применение специальных навыков в компьютерной сфере или же применение специальных программных комплексов с целью осуществления данных преступных деяний;
- умышленный характер действий киберпреступника, который осознаёт общественную опасность своего деяния в полной мере и способен предвидеть наступление вредных для общества или отдельного человека последствий и желает этого или же относится к ним безразлично. Совершение киберпреступлений по небрежности или легкомыслию исключается. Основная отличительная черта киберпреступления от иных противоправных деяний является использование информационных технологий и сети «Интернет» при совершении преступления.

Основные виды информационно-технических инструментов, используемых в кибертеррористической деятельности представлены в таблице 1. При этом под Интернет-ресурсами мы понимаем такие как виды как интернет-сайты, интернет-хостинги, социальные сети, сайты знакомств, форумы.

Таблица 1 Динамика числа лиц, совершивших преступление в состоянии опьянения в России за 2018-2022 год

Виды информационно-технических инструментов, используемых для совершения киберпреступлений					
Интернет-ресурсы	Мессенджеры	СМИ	Навигационная аппаратура	Беспилотные летательные аппараты	Смартфоны

С помощью мессенджеров Viber и Whatsp осуществили вербовку студентки Московского государственного университета В. Карауловой, отправившейся в Сирию с целью выйти замуж за человека, который был знаком ей лишь виртуально. Надо заметить, что обычно вербовщик находится за пределами Российской Федерации.

Указанная схема вербовки показала весьма высокую эффективность в течении всего периода прохождения боевых действий на территории Ирака и Сирии. Помимо мессенджеров, в качестве метода вербовки, террористы используют мусульманские сайты брачных знакомств (к примеру, www.nikyah.ru, www.nikah.su, www.muslima.com) и социальные сети достаточно активно. Главное предпочтение при проведении вербовок в Сети отдаётся возможности создания «фейковых» страниц и аккаунтов, ведь они усложняют поиск и установление данной категории лиц силами спецслужб.

В последнее время стали чаще происходить случаи звонков анонимного характера о «минировании» административных зданий и социально важных объектов с помощью IP-телефонии (через Интернет, не через социальные сети).

С помощью проведённых оперативно-разыскных мероприятий, российские спецслужбы определяли, что «компьютерный след» ведёт на территории некоторых иностранных государств (в частности, Сирия и Украина). Анонимные звонки такого рода могут использоваться террористическими элементами для нанесения экономического урона и нарушения стабильности общественного порядка, которые ведут к нарушению функционирования всех ветвей власти.

После реализации диверсионно-террористического акта террористические группировки активно пользуются информационным пространством с целью воздействия на общественное мнение, для придания «ореола мученичества» (в случае совершения террористической акции террористом-смертником), а также для перекладывания ответственности за случившееся на силовой блок.

Обвиняющие правоохранительные органы в совершении террористических актов информационные вбросы, как было замечено, происходят после каждого резонансного террористического акта [76].

Максимальная их эффективность достигается в течение 10-12 дней после совершения громких террористических актов [77].

В связи с вышеизложенным, в качестве мер противодействия считаем целесообразным использовать меры информационной контрпропаганды с использованием широких возможностей СМИ (средств массовой информации), блогеров, тематических групп в соцсетях, которые могут и должны давать альтернативную точку зрения на произошедшее, полностью освещать вопросы, представляющие интерес для тех людей, кто является целью террористической пропаганды [60].

Однако, полагаем, что рост потока данных, воспринимаемым конкретным пользователем, снижает критичность оценки им информации. Применение манипулятивных технологий террористскими и экстремистскими формированиями дают им возможность оказывать воздействие на общество более эффективно [77].

Для киберпреступника ИТ-технологии – это возможность получения доступа к практически любым секретам – как государственным, так и личным, на любом расстоянии от источника информации. Количество и виды преступлений в мире высоких технологий продолжают только расти. Пока правоохранительные органы обнаруживают пути решения одних информационных преступлений, хакеры уже придумывают новые [30].

Данные статистики о состоянии киберпреступности в 2020 году говорят о том, что, число преступлений, которые были совершены с помощью высоких технологий, выросло на 94,7 %, в том числе тяжких и особо тяжких – на 129,7 %.

Кроме того, министр внутренних дел России Владимир Колокольцев сообщает, что «на общую раскрываемость негативно повлияло увеличение количества преступлений, совершенных с использованием IT-технологий, и

сложности в установлении причастных к совершению таких преступлений лиц. Доля киберпреступлений повышается и достигла 23 %» [40].

В основном, это связано, как нам представляется, с переходом в условиях пандемии Covid-19 многих людей на дистанционный формат работы и обучения.

Виртуальный террор является достаточно новым оружием для террористов и очень прогрессивным. Бывает довольно трудно установить личность преступника, к тому же киберпреступление может быть совершено абсолютно из любой точки мира, где есть Интернет.

Суть тактики кибертерроризма в том, что преступление должно стать широко известным населению, шокировать общество и создать атмосферу угрозы совершения террористического акта в любом месте, в любое время.

В качестве примера, можно указать Аабид Хана, который занимался противоправной деятельностью; направлял на вербовку террористов через Интернет-сети. Аабид Хан даже создал электронную экстремистскую энциклопедию и призывал своих соратников к войне с не-мусульманами. Он привлёк в экстремистскую ячейку Хаммаада Мунши, которому не было и 16 лет на момент ареста. На компьютере Мунши следователями были найдены пропагандистские ролики «Аль-Каиды», записи с пропагандой к «убийствам и разрушению», а также инструкция, как именно изготовить напалм, взрывчатку, детонатор и гранаты [61].

На сегодняшний день, ни Уголовный кодекс Российской Федерации, ни Федеральный закон «О противодействии терроризму» не формулирует определение понятия «кибертерроризм» [72]. По своей сути, кибертерроризм является преступным деянием, совершаемым в информационной сфере, вследствие чего данное преступление должно быть квалифицировано по статьям из главы 28 УК РФ [73].

Но, если мы посмотрим с другой стороны, кибертерроризм – это подвид классического терроризма. При этом терроризм – это идеология насилия и практика воздействия на принятие решения органами государственной власти,

органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий [72]. Именно поэтому, как нам представляется, его квалификация должна происходить по соответствующим статьям главы 24 УК РФ.

1.2 Анализ отечественного уголовного законодательства, устанавливающего ответственность за киберпреступления

Согласно классическому представлению о государстве и праве, действие любой правовой нормы должно определяться в трёх плоскостях: в пространстве, во времени и по кругу лиц. Специфика пространства информационных технологий вынуждает пересмотреть данный подход, так как в Интернет-среде понятие «пространство» лишено однозначной географической определённости, понятие «время» не привязано ни к одному часовому поясу, а понятие «круг лиц» включает не физических и юридических лиц, а компьютеры и иные устройства, которые участвуют в сетевом взаимодействии и могут быть идентифицированы по их IP-адресам и другим технологическим деталям [2].

В нашей стране законодательство сферы высокотехнологичных преступлений находится пока на стадии становления [17]. Широкое распространение ИТ-технологий в России и рост количества с ними связанных правонарушений возникли относительно недавно. Формирование нормативной базы было начато ещё в 90-е годы, но и к 1997 году в РФ не была выстроена эффективная система защиты информационных отношений, в связи с тем, что не доставало необходимых правовых механизмов [44].

С целью анализа перспектив дальнейшего развития киберпреступности в Российской Федерации, построим график, показывающий динамику количества официально зарегистрированных преступлений в 2017-2021 годах, представленный на рисунке 1.

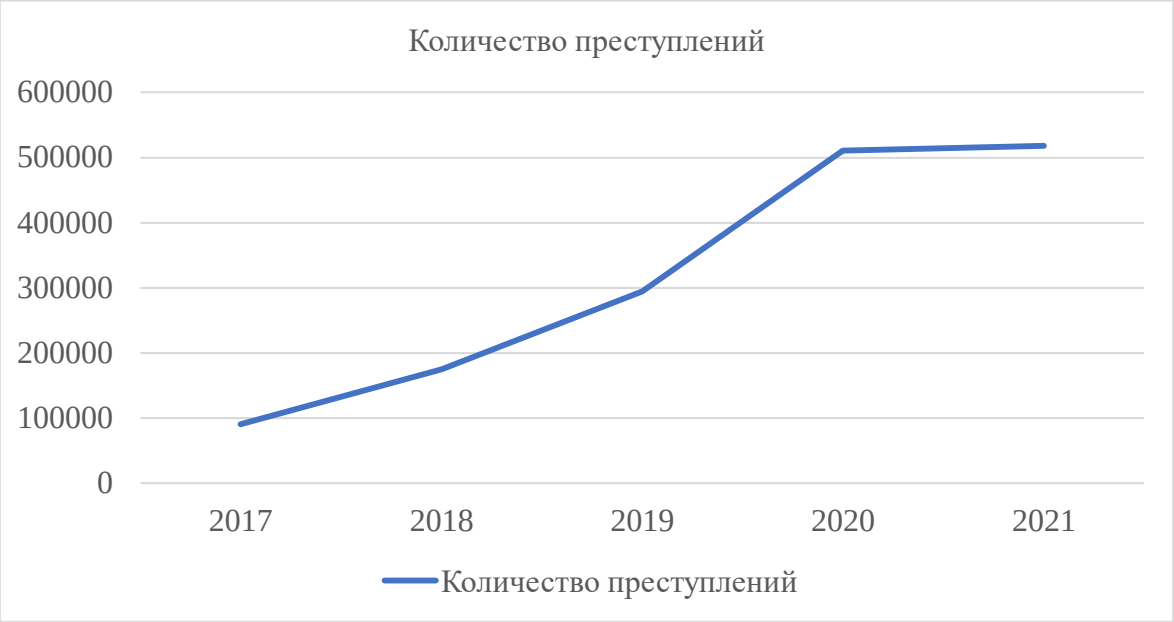

Рисунок 1 – Количество киберпреступлений в 2017-2021 гг.

Опираясь на эти данные, можем сделать вывод, что количество киберпреступлений неуклонно растёт и в перспективе будет только увеличиваться. А это значит, что необходимо усиливать кибербезопасность во всех сферах жизнедеятельности людей, так как цифровые технологии в нашей жизни уже присутствуют повсеместно.

Национальная правовая база в области противодействия киберпреступности, к сожалению, не совершенна в связи с динамичностью развития общественных отношений с использованием интернет – сети, что неоднократно отмечалось учёными и политиками нашей страны [69].

Пока мы все пользуемся инновациями в сфере высоких технологий, за нашей приватной информацией идёт настоящая охота, хакеры изобретают всё более сложные вирусы, а те, кто им противодействуют, наращивают всё более сложную систему защиты. К примеру, «Лаборатория Касперского», сотрудники которой круглосуточно борется за нашу безопасность в виртуальном мире. И пока они пытаются решить эту проблему изнутри, государство с внешней стороны тоже не бездействует [5].

Для эффективной борьбы с киберпреступной детальностью была принята Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 года № 6461, расшифровывающая определение «информационная безопасность Российской Федерации» [66]. Это состояние защищённости личности, общества и государства от внутренних и внешних киберугроз, при этом обеспечиваются реализация конституционных прав и свобод человека и гражданина, респектабельные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства [33].

Главные законодательные акты, касающиеся киберпреступности, изложены в Главе 28 Уголовного кодекса РФ (статьи 272-274 УК РФ). Федеральным законом от 7 декабря 2011 в положения Уголовного кодекса Российской Федерации были внесении изменений (и в отдельные законодательные акты) к ст. 272 УК РФ [74]. Было добавлено примечание, содержащее пояснение, что «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [71].

Статья 272 УК обозначает меры уголоной ответственности за неправомерный доступ к данным компьютера. В зависимости от тяжести совершённого преступления и наличия корыстных мотивов, осуществление данных деяний повлечёт за собой санкции в виде штрафа (в размере от 100 до 300 тыс. рублей), либо доходов преступника за двухлетний период, исправительных работ в течение 12-24 месяцев, ограничения и лишения свободы на срок до 4 лет.

Создание и внедрение вредоносного ПО (программного обеспечения) с целью блокировки, уничтожения или копирования данных, согласно статье 273 УК РФ, влечёт за собой такие виды санкций, как:

– штраф от 100 до 200 тыс. рублей;

– доходы за 18-36 месяцев;
– принудительные работы на срок до 5 лет;
– лишение свободы на аналогичный срок.

Нарушение норм трансляции, обработке, использовании и хранении данных, из-за которых произошло незаконное копирование информации; её блокировка или замена содержания влечёт за собой уголовное наказание в виде штрафа до 500 тыс. рублей, зарплаты осуждённого за 18 месяцев, принудительно-исправительных работ в течении 12-24 месяцев, либо тюремного заключения на соответствующий срок (статья 274 УК РФ).

С 1992 года главным органом, который отвечает за противодействие преступлениям в сфере ИТ-технологий в РФ, является бюро специальных технических мероприятий при МВД РФ.

Управление «К» МВД РФ и специальные отделы «К» при региональных правоохранительных ведомствах занимаются непосредственным выполнением задач этого направления; туда обращаются с заявлением о посягательстве на личную или общественную информационную безопасность [70].

Управление «К», находящееся в составе ГУВД субъекта РФ, занимается обнаружением, предупреждением и раскрытием преступлений в сфере компьютерно-информационных технологий, незаконного оборота РЭС, специальных технических средств и детской порнографии [18].

Задачи управления «К»:

– пресечение нарушения авторских и смежных прав (статья 146 УК РФ, статья 7.12 КоАП РФ);
– выявление незаконного проникновения в компьютерную сеть (статья 272 УК РФ);
– противодействие распространителям вредоносных программ (статья 273 УК РФ);

- выявление нарушений правил эксплуатации ЭВМ (электронно-вычислительных машин), системы ЭВМ или их сети (статья 274 УК РФ);
- выявление использования подложных кредитных карт (статья 159 УК РФ);
- противодействие распространению порнографии посредством Интернета и компакт-дисков (статья 242 УК РФ);
- выявление неправомерного подключения к телефонным линиям (статья 165 УК РФ, статья 13.2 КоАП РФ);
- противодействие незаконному обороту радиоэлектронных и специальных технических средств (ст. 138 УК РФ, ст. 171 УК РФ, ст.ст. 14.1, 14.42 КоАП РФ).

Кроме преступлений в сфере компьютерной информации, среди некоторых статей УК РФ есть конструктивный или квалифицирующий признак совершения киберпреступления «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет» [22].

Конструктивный признак использования высоких технологий при совершении преступления описан только в ст. 137 УК РФ, уже отмеченной статье 159.6 УК РФ, а также в статьях 171.2, 185.3, 258.1, 282 УК РФ [65].

В частности, в ч. 3 ст. 137 УК РФ предусматривается ответственность за незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, которая указывает на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия. При этом аналогичный признак в общем

составе по ч. 1 ст. 137 УК РФ не обнаруживается. Несмотря на то, что законодательно установлено наказание за распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия; в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации [24].

Признаком, увеличивающим общественную опасность содеянного и влекущим ещё более строгое наказание, можно считать совершение преступления с использованием электронных или информационно-телекомуникационных сетей, который содержится всего в тринадцати составах уголовного закона:

- три состава в главе «Преступления против жизни и здоровья» (ст.ст. 110, 110.1, 110.2 УК РФ);
- один состав в главе «Преступления против семьи и несовершеннолетних» (ст. 151.2 УК РФ);
- один состав в главе «Преступления против общественной безопасности» (ст. 205.2 УК РФ);
- пять составов в главе «Преступления против здоровья населения и общественной нравственности» (ст.ст. 228.1, 242, 242.1, 242.2, 245 УК РФ);
- один состав в главе «Экологические преступления» (ст. 258.1 УК РФ);
- два состава в главе «Преступления против основ конституционного строя и безопасности государства» (ст. ст. 280, 280.1 УК РФ) [34].

В УК РФ есть еще несколько составов, которые, по нашему мнению, можно отнести к киберпреступлениям. Так, п. «г» ч. 3 ст. 158 УК РФ содержит особо квалифицированный состав – кража с банковского счета, а в отношении электронных денежных средств, согласно ст. 159.3 УК РФ, устанавливается ответственность за мошенничество с использованием электронных средств платежа, ст. 187 УК РФ в части незаконного оборота электронных средств, электронных носителей информации, технических устройств, компьютерных

программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств. Мы можем соотнести данные составы с киберпреступлениями из-за предмета данного преступного деяния, которым здесь выступают безналичные денежные средства, или же электронные, либо электронные носители информации – всё то, что возникло в результате развития ИТ-технологий и их внедрения в банковский сектор.

С помощью использования высоких технологий совершаются не только вышерассмотренные преступления. Незаконное приобретение или сбыт оружия возможен, к примеру, в том числе посредством Интернет-сети, однако в ст. 222 УК РФ, данный квалифицирующий признак не нашёл своего отражения, как в ст. 228.1 УК РФ относительно наркотических средств, психотропных веществ или их аналогов. Несмотря на законодательные запреты, незаконная розничная продажа алкогольной и спиртосодержащей продукции продолжает осуществляться с помощью Интернета [1].

1.3 Виды киберпреступлений и методы кибератак

Рассмотрим основные группы субъектов киберпреступлений по подгруппам. В таблице 2 представлена соответствующая классификация.

Таблица 2 Группы субъектов киберпреступлений

Основные типы	Подтипы групп
Группы, как субъекты киберпреступлений	Традиционно организованные киберпреступные группы
	Идеологически и политически мотивированные киберпреступные группы
	Группы, использующие информационные технологии для преступлений
	Группы, использующие технологии для мобилизации и действий
Группы, как объекты киберпреступлений (жертвы)	Возраст
	Раса
	Пол
	Сексуальная ориентация
	Религия
	Инвалидность

В настоящее время среди ученых нет однозначного мнения, какие именно общественно опасные деяния следует относить к киберпреступлениям. Например, в Конвенции Совета Европы «О преступности в сфере компьютерной информации» содержится информация, что компьютерные преступления направлены «против конфиденциальности, целостности и доступности компьютерных данных и систем» [33].

Богданова Т.Н. считает, что компьютерные преступления – это «общественно опасные деяния, в которых компьютерная информация является объектом преступного посягательства» [9].

В таблице 2 представлена классификация групп киберпреступников, и то, каким образом происходит разделение на отдельные группы жертв киберпреступлений, но стоит заметить, что в данной таблице мы разделяем жертв киберпреступности на группы, как отдельных граждан, иная классификация по объекту киберпреступления будет рассмотрена нами в таблице 3.

Таблица 3 Группы объектов киберпреступлений и виды угроз

Объекты киберугроз	Виды киберугроз
Государство	Кибератаки на государственные системы управления (электронное правительство, сайты государственных структур)
	Экономическая блокада (масштабное отключение платёжных систем, систем бронирования)
	Аппаратные кибератаки на персональные компьютеры и критически важную инфраструктуру государственных предприятий
Бизнес	Атаки хакеров на сайты компаний
	Воздействие на системы интернет-банкинга
	Воздействие на информационную инфраструктуру
	Блокировка систем онлайн-торговли и геоинформационных систем
Граждане	Утечка и обнародование приватной частной информации
	Мошенничество
	Сбор персональных данных и кибератаки на персональные компьютеры и мобильные устройства граждан
	Распространение опасного контента

Теперь рассмотрим виды и основания классификации объектов киберугроз: бизнес-структуры, государство, граждане. Это основные объекты киберпреступлений, им наносят неоценимый ущерб – как отдельным правоотношениям, так и экономике в целом. По отношению к девяти из представленных в таблице 3 объектах, могут быть совершены виды кибератак, рассмотренные нами далее в данном параграфе.

Рассмотрим каждый вид в отдельности несколько поподробнее. На рисунке 2 представлены наиболее актуальные в современном обществе виды киберугроз.

Рисунок 2 – Основные виды киберпреступлений

Во-первых, электронное и компьютерное мошенничество, а также кража денег с банковских счетов и карт. Финансовая сфера является одной из самых привлекательных для киберпреступников, при этом малозащищённой. Значительная часть денежной массы приняла безналичный характер с

развитием современных методов коммуникации, что упростило преступникам варианты осуществления хищения денежных средств со счетов банков и со счетов пластиковых карт обычных граждан.

Во-вторых, атаки хакеров, распространение вирусов, взлом и хищение баз данных. Проблемами предупреждения данных видов угроз является непрогнозируемость потенциальных проблем, использование аналогичного ПО в различных устройствах, что увеличивает шансы нахождения преступниками технических уязвимостей; а также недостаточное количество квалифицированных кадров в области кибербезопасности [75].

В-третьих, неправомерное вторжение в приватную жизнь (хищение частных персональных данных) получает всё большее распространение из года в год. Люди по всему миру используют современные гаджеты, из которых можно узнать о местоположении пользователя, и даже более приватную, конфиденциальную информацию. Указанный вид преступления довольно популярен и среди вымогателей, и среди отделов маркетинга предприятий и организаций. С помощью отслеживания личной информации потенциального потребителя, можно выстроить анализ его предпочтений, сформировать целевую рекламу и занести эту информацию в свои базы данных [25].

В-четвертых, неправомерное присвоение интеллектуальной собственности тоже является распространённым видом киберпреступности, потому что с развитием ИТ-технологий, некоторые создатели интеллектуальной собственности, не могут использовать экономические плоды своей собственной работы, и это существенно подрывает стимул к вкладыванию инвестиций в развитие своего продукта. Создатель интеллектуальной собственности в этом случае находится в невыгодном положении по отношению к тому, кто просто скопировал его наработки, так как создатель вкладывал в разработку собственные идеи, деньги и своё время [78].

Таким образом, тактика и искусство борьбы с киберпреступлениями за последние годы существенно изменились, и это требует от правительств

государств пересмотра прежних военных доктрин, переоценки в области военного искусства. Сетецентрическая война и кибервойна, как принципиально новые виды ведения войн против государств, требуют особого подхода и противодействия [11].

Основным моментом необратимых изменений в сфере кибервойн стало применение программного обеспечениям «черв» под именем «Stuxnet» [6]. Паршин С. А. указывает на следующие сведения: «… в сентябре 2010 г. сообщения о зараженных иранских промышленных предприятиях, прежде всего в ядерной сфере, стали главной новостью всех основных СМИ. Чуть позже аналогичные системы в России и Казахстане также испытали значительные трудности вследствие воздействия данной программы. Данный случай, по мнению большинства членов мирового экспертного сообщества, перевел нашу цивилизацию в новую эру, в которой кибервойны и применение кибероружия, нацеленного на разрушение критической инфраструктуры, больше не относятся к абстрактной категории. При этом вирус «Stuxnet» был признан экспертами в области кибервойн как первое реальное кибероружие [43, С. 99-100].

В-пятых, незаконный оборот наркотиков. В марте 2021 года Всемирная организация здравоохранения (ВОЗ) предупредила людей о недопустимости продажи поддельных вакцин против Covid-19, особенно в даркнете. Мошеннические услуги, такие как поддельные вакцины, могут использовать неудовлетворенный мировой спрос на вакцины против Covid-19 в преступных целях [4].

Наибольшую опасность сейчас приобретает такой вид компьютерных преступлений, как кибертерроризм. В этот вид киберпреступлений можно отнести такие деяния, как распространение информации о различных террористических актах в сети. Цель кибертерроризма – выведение из строя программного обеспечения какой-либо крупной корпорации или организации, нарушение системы сетей электросвязи отдельной линии или даже целого города, получение доступа к личным персональным данным, равно как и к

военным секретным данным. Всё это находится в пределах интересов киберпреступников. Помимо того, данное деяние может быть совершено с целью политически мотивированных атак на государственную секретную информацию [45].

На рисунке 3 представлены методы кибератак, рассмотрим их более подробно. Типы используемых методов и уровни сложности кибератак варьируются в зависимости от категории.

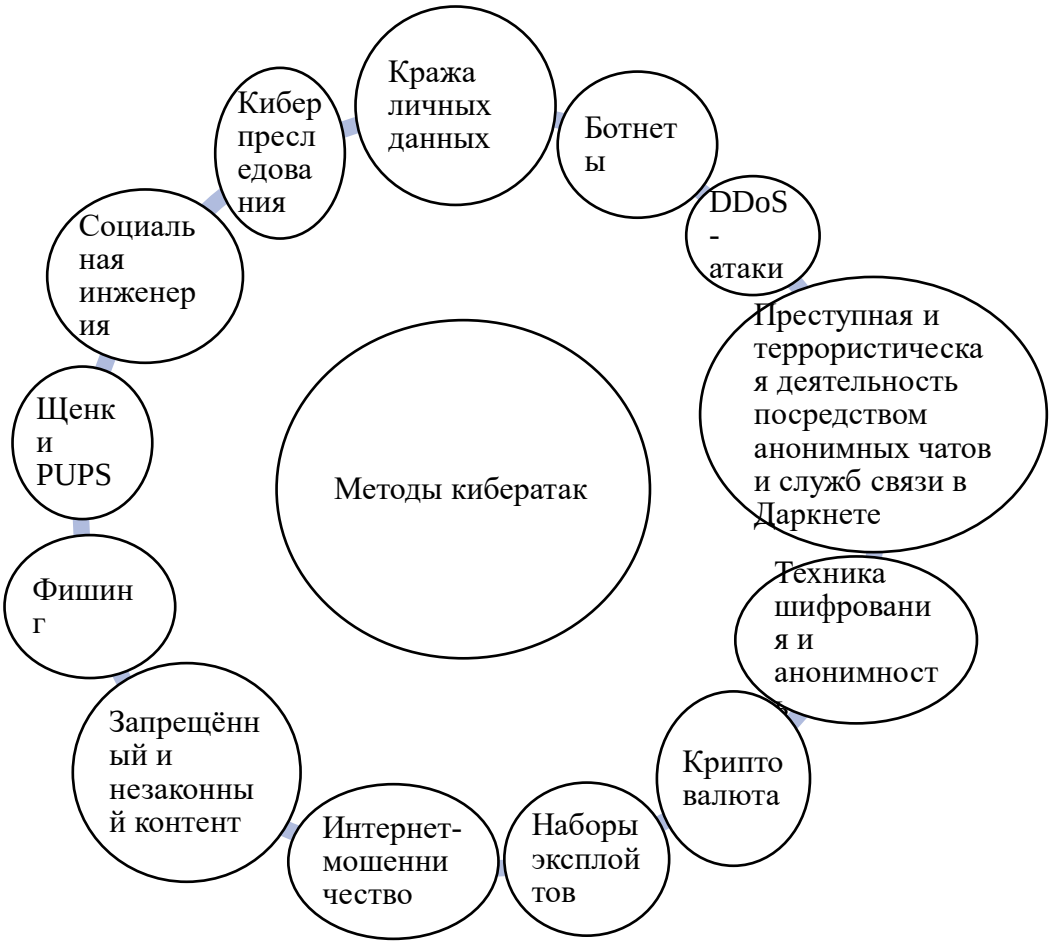

Рисунок 3 – Методы кибератак

Так, например, DDoS-атаки используются, чтобы сделать онлайн-сервис недоступным и отключить сеть, перегрузив сайт трафиком из различных источников. Большие сети зараженных устройств, известные как ботнеты, создаются путем размещения вредоносных программ на компьютерах пользователей. Затем хакер взламывает систему, когда сеть не работает.

Ботнеты используются в сети из скомпрометированных компьютеров, которые контролируются извне удаленными хакерами. Затем удаленные хакеры рассылают спам или атакуют другие компьютеры через эти ботнеты. Ботнеты также могут использоваться в качестве вредоносных программ и выполнять вредоносные задачи.

Кража личных данных – это киберпреступление происходит, когда преступник получает доступ к личной информации пользователя для кражи средств, доступа к конфиденциальной информации или участия в мошенничестве с налогами или медицинским страхованием. Они также могут открыть учетную запись телефона/интернета на ваше имя, использовать ваше имя для планирования преступной деятельности и требовать государственных пособий от вашего имени. Они могут сделать это, узнав пароли пользователей путем взлома, получения личной информации из социальных сетей или отправки фишинговых писем.

Киберпреследование – этот метод киберпреступления включает онлайн-преследование, когда пользователь подвергается множеству онлайн-сообщений и электронных писем [57]. Обычно кибersталкеры используют социальные сети, веб-сайты и поисковые системы, чтобы запугать пользователя и внушить страх. Обычно кибersталкер знает свою жертву и заставляет человека бояться или беспокоиться за свою безопасность.

Социальная инженерия предполагает, что преступники вступают в прямой контакт с вами, как правило, по телефону или электронной почте. Они хотят завоевать ваше доверие и обычно изображают из себя агента по обслуживанию клиентов, чтобы вы предоставили необходимую информацию. Обычно это пароль, компания, в которой вы работаете, или банковская информация. Киберпреступники узнают о вас всё, что могут, в Интернете, а затем попытаются добавить вас в друзья в социальных сетях. Получив доступ к учетной записи, они могут продавать вашу информацию или защищать учетные записи от вашего имени.

«Щенки PUPS» или потенциально – нежелательные программы менее опасный метод, чем другие, но является разновидностью вредоносных программ. Они удаляют необходимое программное обеспечение в вашей системе, включая поисковые системы и предварительно загруженные приложения. Они могут включать шпионское или рекламное ПО, поэтому рекомендуется установить антивирусное программное обеспечение, чтобы избежать вредоносной загрузки [36].

Фишинг – в этом типе кибератаки хакеры отправляют пользователям вредоносные вложения электронной почты или URL-адреса для получения доступа к их учетным записям или компьютеру. Киберпреступники становятся более авторитетными, и многие из этих электронных писем уже не будут помечаться, как спам. Пользователей обманом отправляют по электронной почте, якобы им нужно сменить пароль или обновить свою платёжную информацию и это даёт преступникам доступ [30].

Фишинг всегда был широко распространен, а в последние годы стал самой серьезной угрозой кибербезопасности. Для борьбы с фишинговыми атаками компании, занимающиеся информационной безопасностью, на протяжении многих лет продолжали разрабатывать новые методы, такие как аппаратная аутентификация и обновленные подходы к обучению и повышению осведомленности, ориентированным на безопасность, однако фишинг по-прежнему эффективен и сегодня.

Ещё более остро эта проблема обозначилась из-за Covid-19. Киберпреступники использовали информацию о пандемии для нагнетания страха и обмана людей, чтобы предоставить им доступ к конфиденциальной информации.

Ещё один распространившийся способ фишинга был следующим: получатели электронной почты были вынуждены переходить по ссылкам, которые предлагают медицинские организации. Мошенники звонили людям, и их номера выглядели так, как будто они исходят от CDC и просили пожертвования. Дополнительно, злоумышленники использовали электронные

письма с ссылками и файлами для загрузки вредоносных программ, которые позволяют им красть информацию у жертв [15].

Рабочая группа по анализу угроз Google сообщила, что они заблокировали 18 миллионов электронных писем на тему Covid-19, которые содержали фишинговые ссылки и загрузки вредоносных программ в день (журнал Security Magazine, 2020 г.). И это далеко не все письма, многим удалось избежать сетей кибербезопасности.

Запрещенный и незаконный контент, в котором участвуют преступники, обменивающие и распространяющие неприемлемый контент, который можно считать крайне неприятным и оскорбительным. Оскорбительный контент может включать, помимо прочего, сексуальные действия между взрослыми, видео с интенсивным насилием и видео криминальной деятельности. Незаконный контент включает материалы, пропагандирующие террористические акты, и материалы, связанные с эксплуатацией детей. Этот тип контента существует как в повседневном Интернете, так и в темной сети, анонимной сети.

Интернет-мошенничество, обычно они представлены в виде рекламы или спам-писем, которые включают обещания вознаграждения или предложения нереальных сумм денег. Онлайн-мошенничество включает в себя заманчивые предложения, которые «слишком хороши, чтобы быть правдой», и при нажатии на которые вредоносное ПО может вмешаться и скомпрометировать информацию.

Наборы эксплойтов – ошибка в коде программы, чтобы получить контроль над компьютером пользователя. Это готовые инструменты, которые преступники могут купить в Интернете и использовать против любого, у кого есть компьютер. Наборы эксплойтов регулярно обновляются, как и обычное программное обеспечение, и доступны на хакерских форумах даркнета.

Преступная и террористическая деятельность в даркнете. Анонимные чаты и службы связи в даркнете делают его идеальной платформой для

планирования и координации опасных преступных и террористических действий.

Техника шифрования и анонимность. Это одна из самых больших проблем, с которыми сталкиваются власти: тёмная сеть полностью анонимна, что затрудняет получение достаточной информации, которая может помочь в борьбе с киберпреступлениями и отслеживании преступников, которые используют это пространство [83].

Большинство финансовых транзакций в даркнете выполняются в криптовалютах, что обеспечивает дополнительную анонимность. Технология криптовалюты, называемая блокчейном, представляет собой цифровой реестр транзакций, распределенных по сети, в котором блоки криптографически защищены [52]. Он записывает информацию таким образом, что сделать изменение или взлом системы затруднительным или невозможным. Биткойн-транзакции способствовали всевозможным незаконным действиям киберпреступников и террористов в даркнете, и это чрезвычайно усложнило правоохранительным органам отслеживание денежных потоков для сбора доказательств преступления. Регулирование криптовалют возможно только в отношении их законного использования, в то время как большая их часть все еще может использоваться в незаконных целях. Темная сеть – это сложная среда, имеющая как преимущества, так и недостатки в зависимости от того, использует ли ее пользователь [23].

Даркнет помогает защитить право на свободу информации и конфиденциальность в Интернете и поэтому часто используется журналистами и другими активистами по всему миру для безопасного и надежного общения. В то же время злоумышленники злоупотребляют им, что приводит к ряду преступлений.

Даркнет часто появляются в новостях. Важно понимать различные термины, связанные с этим понятием. Несмотря на то, что он прост в использовании, его сложность в кибермире сбивает с толку, и его трудно отследить или контролировать. Легкая доступность темных веб-форумов,

посвященных свободному обмену технологиями, обеспечивающими конфиденциальность, программным обеспечением для вторжений и вредоносным кодом, означает, что глобальные правоохранительные органы постоянно участвуют в этом [4].

Всемирная паутина (www) содержит множество соединений веб-страниц в сети компьютеров, подключенных через Интернет. Интернет-сеть состоит из «поверхностной» сети и «глубокой» сети. Поверхностная сеть – это та часть, к которой могут получить доступ обычные пользователи Интернета, используя стандартные поисковые системы, такие как Google, Yahoo и т. д. Но она может получить только около 4% результатов поиска, в то время как большинство результатов скрыто. Содержимое даркнета зашифровано, и для доступа к этим страницам требуются определенные браузеры, такие как TOR (The Onion Ring), FreeNet, Invisible Internet Project (I2P), TAILS (The Amnesic Incognito Live System), браузер Whonix [5].

TOR был разработан сотрудниками военно-морской исследовательской лаборатории США для защиты коммуникаций американской разведки в Интернете. Это называется так, потому что трафик из браузера создал несколько слоев, прежде чем достичь целевого сайта. TOR также используется в законных целях, таких как безопасная и конфиденциальная связь, связанная с заболеваниями, помогающая сотрудникам правоохранительных органов выслеживать преступников и помогающая специалистам по кибербезопасности безопасно проводить тестирование безопасности в своих сетях. Он также обеспечивает доступ к веб-сайтам социальных сетей в странах, где они запрещены. Использование браузера «Tor» не является преступной деятельностью, хотя разведывательные подразделения отслеживают загрузки «Tor», чтобы предсказать любую возможную преступную деятельность [26].

Даркнет превратился в место незаконных транзакций, представляющих угрозу для киберпространства во многих измерениях. Поскольку анонимайзеры в тёмной сети затрудняют отслеживание веб-шаблонов, таких

как история просмотров, местоположение и т. д., преступники используют их не по назначению, чтобы скрыть свою личность и осуществлять незаконную деятельность.

Рынок даркнета «Шелковый путь» был первым современным рынком даркнета, известным продажей незаконных наркотиков. Это выяснилось в 2013 году. Но с тех пор пользователи по всему миру искали на тёмном онлайн-рынке анонимный доступ к оружию, данным кредитных карт, вредоносным программам, распределенному отказу в обслуживании (DDoS), украденным данным и т. д.

Правоохранительным органам необходимо проявить «изощренный» подход к защите преимуществ этого пространства, а также к устранению незаконной деятельности в нем.

В 88% кибератак в 2021 году киберпреступники пользовались методами социальной инженерии. При использовании социальной инженерии злоумышленники пытаются эксплуатировать актуальные темы и социально значимые события. Например, популярными темами фишинга в 2021 году стали пандемия COVID-19, премьеры фильмов и сериалов, инвестиции и корпоративные рассылки, представленные на рисунке 4.

Особой популярностью у киберпреступников в 2021 году пользовалась тема инвестиций. Этот интерес продиктован притоком непрофессиональных инвесторов. Только за прошедший год к торгам на Московской бирже присоединились более 6 млн человек. По данным Банка России, в III квартале 2021 года доля кибератак с использованием методов социальной инженерии на клиентов финансовых организаций выросла на 163,5% в сравнении с показателями III квартала 2020 года. Уже в начале 2022 года российские граждане были вынуждены столкнуться с фишинговыми атаками, где злоумышленники пообещали помочь сохранить и преумножить денежные накопления в том случае, если Россию отключат от системы международных переводов SWIFT или предлагали заработать на арбитражной торговле,

предлагая начинающим инвесторам приобрести быстро дорожающие активы [10].

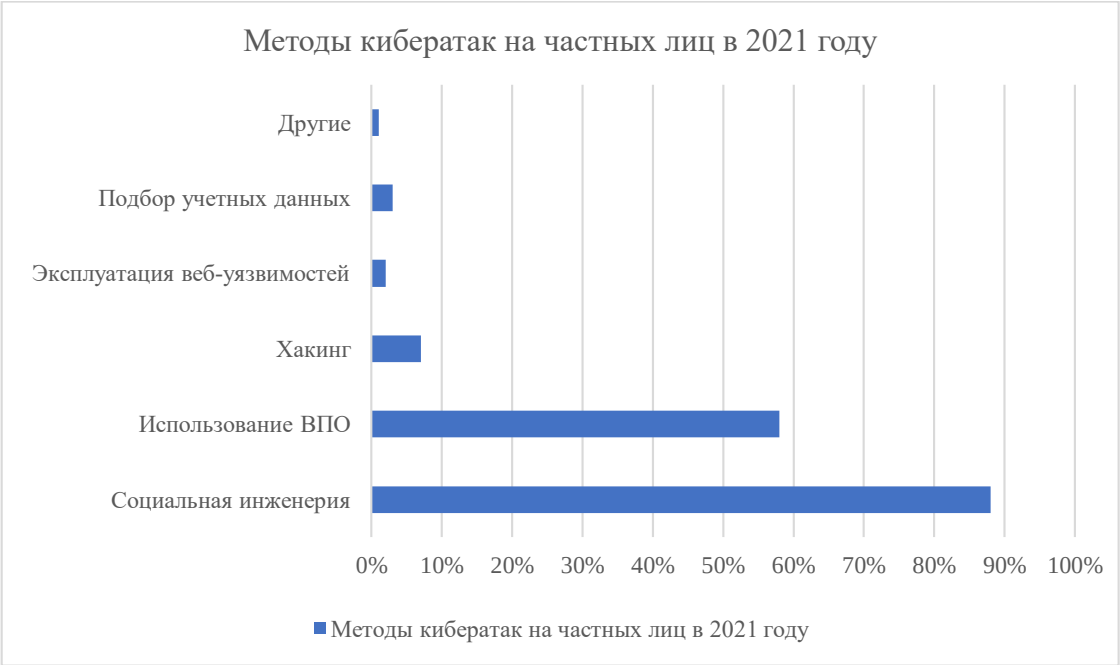

Рисунок 4 – Методы кибератак в 2021 году

Основные причины модифицирования киберпреступности в теневой бизнес представлены на рисунке 5.

Рисунок 5 – Причины модифицирования киберпреступности в теневой бизнес

Когда мы говорим о незначительном риске наказуемости в сфере киберпреступлений, мы подразумеваем, что киберпреступность не имеет геополитических разграничений, а это говорит о том, что органам власти в разы тяжелее найти киберпреступника, а международные расследования и кооперация совместных усилий с другими государствами потребуют больших затрат.

Растущая лояльность общества к киберпреступникам может быть объяснена тем, что киберпреступник часто рассматривается обществом в качестве лица, которое выступает за свободу слова, бесплатное ПО (программное обеспечение), интернет блага, поэтому владельцы бизнеса всё чаще задумываются о ведении теневого бизнеса через интернет, в том числе для обеспечения его защиты через теневые киберструктуры.

В данном случае, угрозой будут считаться уже государственные структуры.

И, наконец, третей причиной развития киберпреступности в качестве теневого бизнеса является простота совершения киберпреступлений. В сети интернет можно найти множество алгоритмов и подробных объяснений по киберпреступлениям [27].

Названные принципы нуждаются в закреплении на законодательном уровне для совершенствования актуальных нормативных правовых актов.

В результате исследования в первой главе, мы можем сделать ряд выводов и рекомендаций по улучшению в сфере противодействия киберугрозам, в том числе правового регулирования:

- в XXI веке киберугрозы – одни из наиболее опасных посягательств на общественную и личную безопасность. Со сменой обычного оружия на информационные технологии, меняется представление о безопасности граждан [16].
- на основе анализа нормативно-правового законодательства Российской Федерации в сфере киберпреступлений, мы можем сделать вывод о том, что в России процесс дальнейшего

формирования и усовершенствования законодательства в сфере киберзащиты должен быть основан на принципах международного сотрудничества; профилактики киберпреступлений; анализе международного опыта для прогнозирования выявления новых видов преступлений; взаимодействии законодателя со специалистами в области кибербезопасности для совместного формирования актуальной правовой базы [62].

- сотрудничество между государственными и частными организациями может помочь в решении новых и возникающих технологических проблем «темной» сети, предоставляя такие решения, как новые инструменты шифрования и т.д. Правоохранительные органы должны активно использовать сложные технологии, такие как искусственный интеллект, машинное обучение и так далее. Уточнённое регулирование объема персональных данных, собираемых различными компаниями, и их автоматическое удаление по истечении установленного периода может в значительной степени повысить эффективность киберсистем для защиты данных и предотвращения подобных инцидентов в будущем. Проблемы трансграничного характера даркнета можно решить путем обмена данными между различными секторами, агентствами и организациями. В этом отношении большое значение имеет международное сотрудничество в форме многосторонних обменов через форумы и совместные мероприятия по повышению потенциала [19].

Таким образом, результаты исследований и научные материалы представителей учёного сообщества, доказывают, что проблема киберпреступности в современном мире является одной из наиболее актуальных.

Среди учёных продолжаются дискуссии по поводу правильной терминологии и набора отличительных признаков и классификации подобных преступлений [36].

Однако, большая часть учёных сходится в том, что «киберпреступность» более широким понятием, чем «компьютерная преступность» и включает в себя множество возможных способов совершения преступлений в информационном пространстве с помощью современных высокотехнологичных средств [58].

Из вышесказанного делаем вывод, что киберпреступность – это совокупность преступных действий, совершённых в киберпространстве с помощью компьютерных систем (сетей), а также иных средств доступа, в рамках компьютерных сетей (систем), направленных против данных людей, организаций, государств [36].

Глава 2 Криминалистический анализ отдельных видов киберпреступлений

2.1 Общий криминалистический анализ преступлений, совершённых с помощью компьютерных сетей

Криминалистическая характеристика киберпреступлений является совокупностью самого характерного, криминалистически значимого массива информации о признаках и свойствах данного вида преступлений, который способен служить основанием для выдвижения версии о событии киберпреступления и личности преступника; позволяет дать правильную оценку ситуации по раскрытию и расследованию кибердеяний; предусматривает применение соответствующих методов, приёмов и средств [14].

Криминалистически значимые элементы анализа киберпреступлений, следующие:

- способ совершения преступления;
- особенности следовой информации;
- особенности места и обстановки совершения преступления (время совершения преступления, детали и др.);
- личностная характеристика преступника;
- особенности непосредственного предмета преступного посягательства.

Элементы криминалистического анализа преступлений изучены и описаны, в частности, И. Зуевым [28, с. 120]. Однако, нужно учитывать специфику киберпреступлений, отличия от всех остальных.

Наличие сети и компьютерных средств при совершении киберпреступлений не требует упоминания, это очевидно. Следует акцентировать внимание на иных, более подробных элементах.

Итогом изучения учёными уголовных дел в области компьютерной информации, стал тот факта, что лишь в 10% уголовных дел по

киберпреступлениям, личность преступника можно назвать специалистом высокого уровня – хакером. А в остальных 90% дел преступником является просто компьютерный пользователь, владеющий специфической информацией по причине занимаемой им должности. Но если в США в 80-х годах XX века из каждой 1000 киберпреступлений только 7 осуществлялись хакерами, то на сегодняшний день, по данным Национального центра криминальной информации США, хакеры совершают уже около 20 % исследуемых правонарушений. Обоснованно будет предположить, что и в дальнейшем продолжится повышение количества киберпреступлений, совершённых подготовленными специалистами [11].

Мы поддерживаем позицию Е. Козлова, характеризующего вторую группы правонарушителей и предлагающего именовать их лицами, страдающими новой разновидностью психической неполноценности (информационные болезни или компьютерные фобии) [31]. Тогда в процессе расследования есть необходимость назначить судебно-психиатрическую экспертизу на предмет установления вменяемости преступника во время совершения им преступных деяний.

Отличительной особенностью личности киберпреступника выступает желание остаться инкогнито. Вследствие чего, преступники непосредственно пользуются никнеймами, под которыми происходят противоправные деяния, или программами, обеспечивающими анонимность пользователя.

Можно выделить три главные группы потерпевших от киберпреступлений: собственники компьютерной системы; клиенты, пользующиеся их услугами; все иные лица. Надо заметить, что потерпевшая сторона из первой группы, обычно неохотно идёт в правоохранительные органы по факту совершения преступления.

Жертвами киберпреступлений чаще всего становятся юридические лица, что объясняется тем, что процесс компьютеризации широко охватывает, в первую очередь, юридических лиц (фирмы, организации, учреждения), а в значительно меньшей степени – физических лиц.

Способ совершения преступления стоит отнести к наиболее важным и информативным элементам для практики криминалистической характеристики всех видов киберпреступничества; мошенничества и кражи в том числе.

Что касается исследования орудия совершения преступления, нам, в первую очередь, нужно выяснить, является ли компьютерная информация и предметом преступления, и средством его совершения. Так, А.В. Сорокин полагает, что признание компьютерной информации средством преступления «...означало бы слишком расширить рамки понятия «компьютерное преступление» и затруднить работу как законодателю, так и правоприменителю» [57]. Точка зрения М.В. Богомолова нам представляется наиболее обоснованной; он утверждает, что «...средством в техническом и юридическом смысле информация будет только в совокупности с компьютером» [9].

Что касается сокрытия следов преступления, то нужно отметить, что указанный элемент тоже подходит больше преступлениям, которые осуществляются группой лиц по предварительному сговору или организованной группой. При анализе киберпреступных деяний в научных кругах возникла дискуссия о возможности вычленения наряду с материальными и идеальными следами, виртуальных следов.

Виртуальные следы – это следы совершения любых действий (включения, создания, открытия, активации, внесения изменений, удаления) в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей.

В. Мещеряков под виртуальными следами понимает «любое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации. Данные следы занимают условно промежуточную позицию между материальными и идеальными следами» [41].

Фиксацию виртуальных следов следует осуществлять в определённом порядке:

- описание следственного действия в протоколе. В протоколе также подлежат упоминанию некоторые сведения: кому принадлежит устройство; в памяти какого именно устройства были обнаружены виртуальные следы; имеет ли устройство выход в Интернет, иные телекоммуникационные или локальные сети; какая оперативная система функционирует в этих устройствах; в каких файлах были обнаружены следы вмешательства и что именно; когда файл был создан, изменён, когда открывался последний раз [29].
- фотография экрана, содержащая информацию о свойствах исследуемых файлов, журналов администрирования, служб безопасности и т.д. Подвидом этого варианта фиксации можно назвать «снимок экрана» (клавиша «Print screen» на клавиатуре) с его дальнейшей распечаткой;
- изъятие устройств для изучения всех виртуальных следов на объекте.

Согласно ст. 177 УПК РФ, обнаружение, фиксация и изъятие виртуальных следов киберпреступной деятельности усложняются временными и техническими трудностями, поэтому они относятся к особым следственным действиям, направленным на получение виртуальной информации. В течении расследования преступления необходимо распознавание и фиксация не материальных объектов, а кибернетического пространства, образуемого средствами вычислительной сети, доступным сегментом локальной вычислительной сети, глобальной сети Интернет и цифровыми носителями компьютерной информации [31].

К средствам и приёмам стандартного характера для обнаружения виртуальных следов мы относим:

- специальные программы: например, из файла данных, записанного в формате «jpg» (формат хранения изображений) по определённому алгоритму, создаётся изображение;

- программно-аппаратные средства для осуществления криминалистического анализа компьютерных носителей информации «EnCase Forensic Edition»: это программное обеспечение для сбора и анализа компьютерных данных, работающее в среде Windows и предназначенное для криминалистического исследования компьютерных носителей информации;
- технические средства: как например, Мобильный комплекс по сбору и анализу цифровых данных «UFED»; Мобильный подавитель работы сотовых телефонов «Мозаика+» и другие.

При проведении следственных действий, осуществляемых для получения виртуальной информации, проведение выемки и обыска имеет свои отличительные особенности [47].

Общие основания и порядок проведения обыска и выемки указаны в ст.ст. 182 и 183 УПК РФ. Согласно статье 182 УПК РФ, причиной (основанием) для производства обыска является наличие достаточных данных для предположения, что в каком-либо месте или у какого-либо лица могут находиться орудия, оборудование или иные средства для совершения преступления; предметы, документы и ценности, имеющие значение для уголовного дела [10].

Следователь имеет право в соответствии со статьёй 181 УПК произвести следственный эксперимент с целью установления достоверности фактов и получения новых доказательств путём воспроизведения действий, а также обстановки или иных обстоятельств определённого события. При этом, осуществляется проверка возможности восприятия каких-либо фактов, совершения определённых действий, наступления какого-либо события, а также выявляется последовательность произошедшего события и механизм образования так называемых «виртуальных следов».

На сегодняшний день, главной проблемой в криминалистическом анализе киберпреступности является определение места происшествия. Если

совершено одно преступление, к примеру, неправомерный доступ к компьютерной информации, может быть несколько мест происшествия:

- рабочее место (рабочая станция) в качестве места для обработки информации, ставшей предметом посягательства киберпреступника;
- место для постоянного хранения или резервирования информации – сервер либо стример;
- место использования технических средств для неправомерного доступа к компьютерной информации, находящейся в ином месте. Место использования может совпадать с рабочим местом, но находиться вне организации (например, при стороннем взломе путём внешнего удалённого сетевого доступа);
- место подготовки преступления (разработка вирусов, программы взлома, подбор паролей) или место использования информации (копирование, распространение, искажение), полученной в результате незаконного доступа к данным, содержащимся на устройстве.

Характерной особенностью обстановки совершения преступлений в сети Интернет является наличие собственных, присущих только этим киберпреступлениям факторов, которые способствуют перемене обстановки в момент их совершения: программные средства, блокирующие движение файлов, модификация информации и т.п.

Установление места совершения преступной деятельности относительно киберпреступлений осложняется удалённостью друг от друга жертвы и преступника; это обеспечивает латентный характер преступления и расчёт преступников на безнаказанность.

При проведении расследования киберпреступных деяний назначаются различные судебные экспертизы.

В настоящее время выделены следующие виды компьютерно-технической экспертизы:

- программно-компьютерная экспертиза;

– компьютерно-сетевая экспертиза;
– информационно-компьютерная экспертиза;
– аппаратно-компьютерная экспертиза.

У каждого из этих видов компьютерно-технической экспертизы есть свои отличительные особенности. Например, изучение аппаратных средств компьютерной системы, как материальных носителей информации, проводится в рамках аппаратно-компьютерной экспертизы. К объектам данной экспертизы относят ПК (персональные компьютеры), периферийные устройства, сетевые аппаратные средства и различные комплектующие.

Программно-компьютерная экспертиза исследует программное обеспечение компьютерной системы.

Информационно-компьютерная осуществляет поиск, анализ, обнаружение и оценку информации, подготовленной пользователем или же созданной специальными программами для организации информационных процессов в компьютерной системе.

Компьютерно-сетевая экспертиза решает аппаратные, программные и информационные аспекты выявления фактов и обстоятельств по имеющемуся делу.

Недавно образовался новый вид экспертизы в рамках компьютерно-технической экспертизы – это экспертиза устройств сотовой связи. Сюда мы относим следующие объекты исследования: мобильные телефоны, планшеты, смартфоны, sim-карты, комплектующие и другие устройства.

В настоящее время, к сожалению, не существует единого для всех подхода ни к названию компьютерно-технической экспертизы, ни к конкретным компетенциям экспертов.

Так, в качестве примера, Министерство юстиции РФ и Министерство внутренних дел Российской Федерации подобные экспертизы формально называют в своих ведомственных документах по-разному.

В Министерстве юстиции Российской Федерации указанный вопрос регламентирован приказом от 27.12.2012 г. № 237 «Об утверждении Перечня

родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России» [54]. В данном документе для указания обозначенной экспертизы используется термин «компьютерно-техническая экспертиза» [67]. На основании данного термина определена и соответствующая экспертная специальность: 21.1 «Исследование информационных компьютерных средств», в компетенцию экспертов которой относят разрешение вопросов в отношении аппаратной части цифровых устройств, а также вопросы по программному обеспечению и данным, имеющимся на носителях информации подобных устройств.

В МВД России компьютерно-техническая экспертиза регламентирована совсем иным приказом от 29 июня 2005 года № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» [55]. В этом документе приводится перечень видов судебных экспертиз, которые используются в экспертно-криминалистических подразделениях органов внутренних дел РФ. Для обозначения описываемого рода экспертизы, тут был использован термин «компьютерная экспертиза».

При проведении эксперимента следователю требуется присутствие понятых (понятые с навыками работы на компьютере и в сети); переводчика (в случае необходимости); педагога (в случае, когда возраст участника эксперимента не достиг 14 лет). В зависимости от решения следователя, в следственном действии может принять участие обвиняемый, потерпевший, свидетель и специалист [87].

В том случае, когда в следственных действиях участвует несовершеннолетний, необходимо руководствоваться положениями статьи 191 УПК РФ, участие специалиста в этом случае обязательно. В случае возникновения вопросов, он во время следственного эксперимента сможет

дать пояснения следователю о происходящем. Когда подозреваемый захочет ввести следователя в заблуждение (ввиду недостаточных знаний следователя в области компьютерных технологий), специалист сможет это распознать и предупредить об этом следователя.

Согласно данным, опубликованным Всесторонним исследованием проблем киберпреступности Управления Организации Объединенных Наций по наркотикам и преступлениям (далее – УНП ООН) [3] в среднем по всему миру в правоохранительные органы обращается лишь 1 % жертв преступных посягательств в области ИТ-технологий, среди международных исследований частного сектора приведена статистика об обращении лишь 20 % лиц, которые жертвами киберпреступлений. Бездействие потерпевших объясняется чаще всего безосновательным предположением о низкой вероятности раскрытия преступления. Помимо этого, часто в случае обращения в судебные органы потерпевшие не в состоянии предоставить минимально необходимый рнабор данных и электронных доказательств для создания картины расследования (точки доступа к данным, параметры входа в сеть, учетные данные и пр.), что обуславливается всё ещё низким уровнем просвещённости населения в области информационно-коммуникационных технологий, например, в странах с низким показателем индекса человеческого развития. Крупные компании и корпорации к тому же не хотят сообщать в правоохранительные органы о совершённых в отношении них преступлениях в связи с действующей репутационной политикой [11].

2.2 Криминалистическая характеристика киберпреступлений в сфере мошенничества, кражи, кибертерроризма и экстремизма

В представленном параграфе подробно рассмотрим характеристик отельных видов преступлений, начнем с анализа криминалистической характеристики мошенничества и кражи в сфере компьютерной информации.

В.В. Коломинов упоминает, что: «...основная черта механизма мошенничества в сфере компьютерной информации является наличие в распоряжении субъекта преступной деятельности компьютерных средств, а также обязательное их подключение к компьютерной сети» [32] На наш взгляд, это очевидно.

Анализ личности преступника в рамках криминалистической характеристики киберпреступлений, таких как, кражи и мошенничества, требует углубленного рассмотрения.

Практика исследования уголовных дел, связанных с мошенничеством в сфере ИТ-технологий и указывает на то, что в сорока пяти процентах случаев в составе преступных групп среди пособников числятся лица из финансовых учреждений, выполняющие поручения по предоставлению информации.

Анализ следственной и судебной практики демонстрирует данные, что в 96% случаях, как в краже, так и в мошенничестве субъектом киберпреступления является лицо мужского пола, в возрасте от 18 до 40 лет.

Если рассматривать киберпреступление с точки зрения количественного состава, то примерно в семидесяти процентах случаев имеет место быть осуществление преступления группой лиц, в том числе, и организованными преступными группами. Эта статистика продиктована тем, что при совершении мошенничества и кражи с использованием цифровых технологий применяются самые высокотехнологичные способы совершения преступления, и, кроме того, ввиду полной организованности таких деяний в преступных группах обеспечивается распределение полномочий по подготовке, реализации и сокрытию преступления [16].

Таким образом, много исследований и данных мы можем получить о мошенничестве, краже в компьютерной сети, это говорит об определённом эмпирическом опыте, однако, с точки зрения уголовно-правового регулирования данного преступления нельзя утверждать об эффективности в структуре закрепленных составов в УК РФ.

В п. 20. Пленума Верховного суда «О судебной практике по делам о мошенничестве, присвоении и растрате» от 30 ноября 2017 г. № 48 предложена следующая квалификация мошенничества, предусмотренного ст. 159.6 (Мошенничество в сфере компьютерной информации), по смыслу пункта «... вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него [48].

Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ».

Исходя из всего вышеисследуемого, нельзя не согласиться с мнением Коломинова В.В., утверждающего, что: «Следует констатировать, что все элементы механизма мошенничества в сфере киберпреступности оказывают взаимообратное воздействие друг на друга. Это связано с тем, что профессиональная квалификация субъектов кибермошенничества обуславливает выбор способа его совершения, а также орудий и средств, используемых в этих целях. Чем выше квалификация субъектов преступной деятельности, тем более изощренные приемы и средства применяются в ходе ее совершения» [32]. Это же относится и к краже в цифровой среде.

Кроме низкого уровня раскрываемости киберпреступлений, существуют также вопросы по скорости реагирования на активность кибермошенников. Так, в ходе Прямой линии с Владимиром Путиным в 2021 г. президент поделился, что на блокировку мошеннических фишинговых сайтов в настоящий момент потребуется до трёх дней, хотя ранее на подобные операции могло уйти несколько недель или даже месяцев [59].

Из анализа практики применения мы можем привести криминалистическую характеристику киберэкстремистов. Что касается кибертерроризма, обстоятельства абсолютно иные из-за высокой степени анонимности данных киберпреступников. Не исключается совершение кибертеррора санкционированного государством, что придаёт высокий уровень латентности данному виду преступления [12].

В таком случае, можем говорить о диверсионных действиях в большей степени, нежели о терроризме. Однако, криминалистическая характеристика кибертеррора и кибердиверсии довольно затруднительна, как из-за отсутствия доступа к материалам судебной практики, так и теоретических положений в криминалистической науке.

Если опираться на исследование, проведённое компанией «Ростелеком-Солар», можно с уверенностью утверждать, что примерно 90% ИТ-систем государственных органов в РФ способны взломать даже неопытные киберхулиганы. Вывод был осуществлён на основе анализа сведений, полученных из 40 государственных организаций [26].

2.3 Объективные и субъективные признаки составов преступлений в сфере компьютерной информации

Оценивая объективнее признаки составов преступлений в сфере компьютерной информации обратим особое внимание последствиям как конструктивному признаку объективной стороны.

Выявление материальных последствий киберпреступлений имеет свои особенности. Требуется учитывать тот факт, что конкретно случилось в результате произошедшего киберпреступного деяния, какие именно убытки понесли владельцы и пользователи; сколько затрачено на ремонт машин, ликвидацию вируса, восстановление программ; как могут быть определены размеры упущенной материальной выгоды [63].

Моральные последствия характеризуются посягательством на честь и достоинство лица, а, также при любом нарушении прав человека, в случае, когда виновный своими действиями выражает неуважение к законным интересам лица, чьи права он нарушает. Можем сделать вывод, что при совершении компьютерного преступления субъект, кроме материального вреда, причиняет ещё и моральный вред.

Отличительной чертой морального вреда от любого другого выступает возможность его возмещения по гражданскому иску. Размер морального вреда не имеет ограничения по российскому законодательству, потому что права человека определяются, как явления нематериальные, их нельзя посчитать и измерить, а значит нет возможности определения объема нарушенной чести или достоинства. Политические последствия имеют место быть в тех случаях, когда виновное лицо посягнуло или на установленный в государстве строй, или же на права граждан, что может привести к политическим последствиям глобального характера.

«Статья 272 УК РФ предусматривает ответственность за неправомерный доступ к компьютерной информации, если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы вычислительных систем» [65].

Статья 272 УК РФ прописывает характеристики объекта, объективную сторону и субъект данного преступления. Опираясь на диспозицию указанной статьи, мы можем выделить обязательные признаки объективной стороны преступления, такие как копирование информации, приведшее её к блокировке, модификации или уничтожению. Наличие причинно-

следственной связи между неправомерными действиями в отношении защищаемой информации и наступившими последствиями непременно имеет место быть.

«Преступление, предусмотренное ст. 272 считается оконченным с момента наступления общественно опасных последствий. Причины совершения данного преступления могут быть любыми: корыстные мотивы, проверка собственного профессионализма, месть и др. Объектом преступного посягательства являются общественные отношения, связанные с безопасностью использования компьютерной информации» [22, с. 8].

Объективная сторона преступления может характеризоваться использованием специальных технических или программных средств, действующих учетных данных пользователей, хищения цифровых носителей информации (при условии организации охраны этих носителей). В качестве предмета преступного посягательства выступает компьютерная информация [21].

Объективную сторону преступления, предусмотренного ст. 273 УК РФ (Ответственность за создание различного вредоносного ПО), составляют такие неправомерные действия:

- создание программ для ЭВМ (электронно-вычислительных машин); которые ведут к общественно опасным последствиям;
- внесение изменений в существующие программы для ЭВМ, заведомо приводящие к общественно опасным последствиям;
- использование подобных программ или машинных носителей с этими программами;
- распространение подобных программ или машинных носителей с этими программами;

«При этом следует обратить внимание на то, что, согласно буквы и смысла закона, состав преступления, предусмотренный ч. 1. ст. 273 УК, сконструирован как формальный. Следовательно, для признания преступления оконченным не требуется реального наступления вредных

последствий в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Достаточно установить сам факт совершения общественно опасного деяния, если оно создавало реальную угрозу наступления альтернативно перечисленных выше вредных последствий. В том случае, когда виновный умышленно создает вредоносную программу для ЭВМ или вносит изменения в существующую программу, доводя ее до качества вредоносной, а равно использует либо распространяет такие программы или машинные носители с такими программами и при этом не совершает неправомерного доступа к охраняемой законом компьютерной информации, то его действия подлежат квалификации по ст. 273 УК» [20].

Выход из строя одной из компьютерных систем может оказаться трагичным, в связи с чем законодатель уделил особое внимание безопасности ЭВМ, систем ЭВМ или их сетей и установил уголовную ответственность за нарушение правил эксплуатации данных машин в ст. 274 УК РФ.

Объективная сторона данного преступления состоит в нарушении правил эксплуатации ЭВМ и квалифицируется:

- общественно опасным деянием, нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети;
- возникновением общественно опасных последствий (в виде уничтожения, блокирования, либо модификации компьютерной информации, причинившей существенный вред или повлекшей по неосторожности тяжкие последствия);
- наличием причинной взаимосвязи между действием и наступившими последствиями.

В описываемом случае лицо вполне осознаёт, что его действия носят неправомерный характер, предвидит или прогнозирует наступление общественно опасных последствий и при этом допускает их наступление.

«Неправомерный доступ к компьютерной информации – умышленное деяние, поскольку в диспозиции ст.272 УК не указано обратное» [24].

«По общему правилу, ответственность за совершение преступлений, предусмотренных статьей 272 УК РФ наступает с 16 лет, однако часть вторая ст. 272 предусматривает наличие специального субъекта, совершившего данное преступление» [65].

При анализе данного состава преступления обратимся к ч. 2 ст. 72 УК РФ, согласно которой деяние признаётся совершённым по неосторожности, только в том случае, когда это оговорено соответствующей нормой УК РФ. Это подтверждает мою точку зрения, что преступления, предусмотренные ст. 273 УК РФ совершаются только в виде прямого умысла.

Для объективной стороны ч. 1 ст. 273 требуется наличие двух признаков: наличие вредоносного ПО или изменений в программе, несанкционированность последствий.

Субъектом преступления может быть любой гражданин, который достиг шестнадцати лет. Субъективная сторона части 1 ст. 274 данной статьи характеризуется наличием умысла, направленного на нарушение правил эксплуатации ЭВМ. В случае наступления тяжких последствий ответственность по части 2 ст. 274 наступает только в случае неосторожных действий.

Умышленное нарушение правил эксплуатации ЭВМ, систем ЭВМ и их сети влечет уголовную ответственность в соответствии с наступившими последствиями и нарушение правил эксплуатации в данном случае становится способом совершения преступления.

Субъект данного преступления – специальный, это лицо в силу должностных обязанностей имеющее доступ к ЭВМ, системе ЭВМ и их сети и обязанное соблюдать установленные для них правила эксплуатации.

2.4 Проблемы правового регулирования киберпреступности, примеры киберпреступлений и судебной практики в этой сфере

Особенность раскрытия киберпреступного деяния с использованием мессенджера «Telegram» заключается в том, что возможность технической части данного мессенджера допускает использование неограниченного количества технических устройств, работающих от одного личного кабинета. С целью установления соучастников преступной деятельности, возможно осуществление контроля за перепиской участника преступной деятельности или ведение переписки между соучастниками и оперативными сотрудниками от лица установленного участника киберпреступной деятельности.

Учитывая положения ст. 138 УК РФ и разъяснение Верховного Суда РФ в части использования доступов к содержанию переписки, сообщений, переговоров - доступ заключается в ознакомлении с текстом и материалами переписки, сообщений, в прослушивании телефонных переговоров, голосовых сообщений, их копировании, записи с помощью различных технических устройств и так далее. Данные действия могут осуществляться лишь с согласия хозяина личного кабинета [49].

В качестве примера из судебной практики РФ по киберпреступлениям, рассмотрим опыт оперативных сотрудников УНК ГУ МВД России по Свердловской области в деле расследования сбыта наркотических средств, совершённого Л. в составе группы неустановленных лиц [51].

В конце 2021 г. был задержан Л., при досмотре у которого было изъято 20 свертков с наркотическим веществом – производное N-метилэфедрона в крупном размере, а также сотовый телефон «Honor» чёрного цвета. В ходе оперативной работы, задержанный предоставил оперативным сотрудникам доступ к его сотовому телефону и личному кабинету в мессенджере «Telegram».

Учитывая время между моментом задержания лица и оперативной работы с ним, применили легенду об отсутствии заряда телефона Л. на период

паузы в их переписке. Таким образом, переписка могла была продолжена с пользователем «Каспер»; с его аккаунта Л. получал адреса «мастер-кладов» (оптовая закладка с уже сформированными свёртками наркотических средств, далее «МК») и отправлял самостоятельно фотографии и описание тайников-закладок, сделанных Л., с наркотическими средствами для конечного покупателя. С целью сохранения данных, оперативниками было задействовано другое устройство с возможностью выхода в интернет и установленным приложением «Telegram» с личным кабинетом Л.

Возможность проведения дальнейших оперативно-розыскных мероприятий была дана именно это перепиской, в результате чего оперативные сотрудники получили информацию о местонахождении «МК».

В ходе наблюдения был задержан гражданин К., которому поручили формирование «тайников-закладок» с наркотическими средствами, используя свёртки, находящиеся в известном «МК». К. был задержан и привлечён к ответственности за покушение на сбыт наркотических средств в особо крупном размере. Таким образом, путём использования информации о необходимости распространения «МК», была реализована возможность разоблачения иных лиц в преступной деятельности.

Во время расследования деятельности экстремистской организации (ст. 282.2 УК РФ), которая совершена дистанционным способом, данная информация позволяет установить факт склонения, вербовки или иного вовлечения лица в деятельность экстремистской организации или участия в его деятельности.

Так, Д., с помощью сотового телефона с доступом в Интернет, через свою страницу в социальной сети «ВКонтакте», склонял определённых лиц и прочих неустановленных участников «конференции», к участию в деятельности экстремистской организации «Misanthropic division»; популяризировал украинские национально-радикализованные вооруженные формирования «Азов», «Правый сектор», «Misanthropic division»; пробуждал у участников переписки желание вступить в ряды запрещённых

экстремистских организаций [51]. Всё это путём восхваления и одобрения деятельности запрещённой экстремистской организации «Misanthropic division», а также уговоров, демонстрации графических изображений и текстов экстремисткой направленности,

Стоит отметить, что наибольшую ценность в атаках на организации, и на частных лиц представляют учётные данные, которые могут быть проданы на теневом рынке позже или же использоваться для развития атаки внутри корпоративной сети. Охота на такую информацию ведётся регулярная.

Так, в середине марта специалисты PT Expert Security Center (PT ESC) зафиксировали фишинговую рассылку на российские организации, отправленную якобы от Госуслуг, представленную на рисунке 6, сделанную с сбор доменных учетных записей. В теле письма содержалась ведущая на поддельную страницу ссылка, которая формировалась интересным образом: злоумышленники использовали всего лишь несколько доменов, однако, чтобы ссылка была похожа на домен компании, вставляли в третий уровень домен атакуемой компании.

Структура ссылки выглядела следующим образом: mail – домен компании – фишинговый домен – ru.

Отметим и крупные атаки на агропромышленность, которые произошли в I квартале в России: например, в марте один из крупнейших производителей и дистрибьютеров мясной продукции «Мираторг» подвергся атаке шифровальщика BitLocker, а в Ростовской области в результате атаки был временно остановлен завод «Тавр». Крупные атаки были вызваны не только шифровальщиками. В феврале злоумышленники попытались испортить 40 тонн продукции в агрохолдинге «Селятино»: получившие несанкционированный доступ к системам преступники изменили ключевые параметры, отвечающие за температурный режим хранения замороженной продукции.

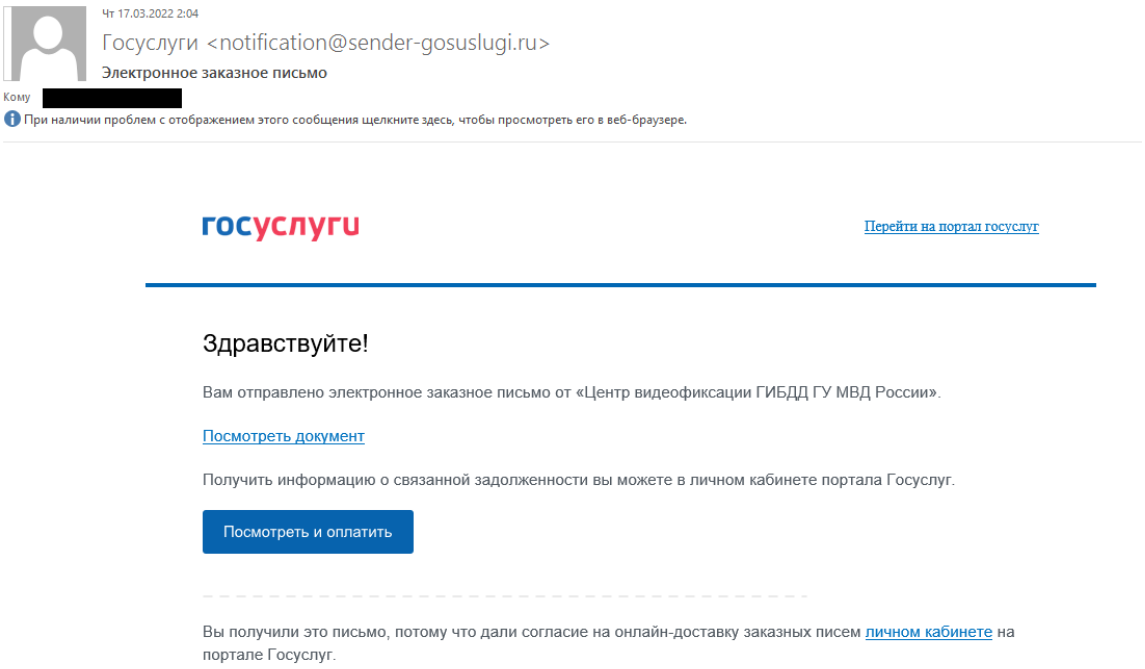

Рисунок 6 – Фишинговая рассылка, имитирующая рассылку от сайта Госуслуг

Из самых актуальных примеров кибератак (30.09-06.10.2022 гг.) в блоге компании Антифишинг (Антифишинг-дайджест № 293, с 30.09.22 по 06.10.22) указана следующая: была зафиксирована целевая атака на российские организации, в ходе которой злоумышленники разослали несколько сотен вредоносных писем, якобы касающихся темы частичной мобилизации [46].

Схема действий преступников:

– в поддельных письмах говорилось, что, из-за неполучения повестки с указанным номером, человека призывают в срочном порядке явиться в назначенное место и время. Более подробная информация якобы указывалась в повестке в формате PDF, которую необходимо скачать по ссылке;
– письмо выглядело правдоподобно: с содержанием ссылок на статьи УК РФ, геральдику и стилистику соответствующего ведомства. В тексте злоумышленники угрожали возможными штрафами и уголовной ответственностью;
– ссылка выводит на архив с исполняемым скриптом с расширением WSF. Если открыть файл, он для отвода глаз скачает и отобразит в

браузере PDF-документ, имитирующий отсканированную повестку, но параллельно создаст файл AnalysisLinkManager.exe во временной папке и запустит его;

– данное вредоносное ПО и техники схожи с активностью группы XDSpy; с версиями прошлых лет совпадают исходный код вредоносного WSF-скрипта и способы запуска, а также частично названия файлов.

Цели XDSpy – это шпионаж, кража документов и других файлов, а также данных для доступа к корпоративным почтовым ящикам.

В заключение, хотелось бы отметить, что ведущие мировые специалисты в IT-сфере разделяют мнение, что в ближайшем будущем сохранится тенденция к дальнейшему росту количества преступлений, которые совершаются в сфере информационно-коммуникационных технологий, поэтому крайне важно разрабатывать новые и усовершенствовать уже имеющиеся методы противодействия киберпреступности. Не стоит также забывать, что с целью обеспечения эффективности подобного противостояния, противодействия и исследования киберпреступности в целом, необходимы высококвалифицированные подготовленные кадры. На это обращал внимание и Генеральный прокурор Российской Федерации, к примеру, одной из главных задач усовершенствования системы профилактики и раннего обнаружения преступления, совершаемого с помощью IT-технологий и компьютерной информации, была выделена такая: «учитывая специфику их выявления, стремительное распространение криминального использования виртуальных активов, компьютерных атак на критическую информационную инфраструктуру государства необходимо внедрять специализацию сотрудников, осуществлять их профессиональный отбор, добиваться устойчивого повышения раскрываемости преступлений».

По моему мнению для того, чтобы решить эту комплексную, сложную и многогранную проблему требуется масштабная и долгосрочная взаимосвязанная работа государственных и правоохранительных органов,

коммерческих и некоммерческих организаций, научного сообщества, а также активные кооперативные решения с международными партнёрами. Для эффективного противостояния виртуальным преступникам нам требуется многоуровневая институциональная система по киберзащите, которая сможет защитить как простых граждан, так и государственные институты.

Проведя криминалистический анализ отдельных видов киберпреступлений, мы пришли к выводу о серьёзной угрозе киберпреступности для социума по причине её транснационального и организованного характера. Вследствие вышеуказанного, ни одно государство в мире на сегодня не способно эффективно противостоять этой угрозе в одиночку, а значит потребность активизации международного сотрудничества сейчас может считаться первостепенной.

Расследование киберпреступлений связано с проблемами обнаружения доказательной базы для выдвижения обвинений. Сопряжено это обычно с некоторыми сложностями, как технологического характера и отсутствия чётких стандартов в области экспертизы, так и с проблемой запутывания следов и сокрытия информации, которые в информационной среде становятся ещё более неуловимыми в процессе следственного процесса.

Эффективность получения доказательств преступлений, совершённых в сети Интернет, напрямую зависит от тактической и технической компетенции следователя. Грамотная организация взаимосвязи и работы со специалистами, оперативными работниками, правильная фиксация следственных мероприятий обеспечивают высокое качество раскрытия и расследования любых преступлений, в том числе и в сфере компьютерной информации.

Для того, чтобы противодействовать киберпреступности успешно, государственным структурам и коммерческим организациям необходимо рассматривать кибербезопасность, как одну из ключевых компонентов их деятельности.

Для решения приведённых во второй главе проблем, учёные и представители профессиональных сообществ дают следующие рекомендации:

– повышение уровня мониторинга киберпреступлений;
– разработка программы повышения квалификации следователей (дознавателей) по расследованию киберпреступных деяний;
– повышение технических возможностей тех экспертов, которые специализируются в области исследования компьютерных технологий;

Также, считаю важным повышение уровня информированности у населения и активизацию просветительской деятельности.

Отдельные виды преступлений должны быть взяты под особый контроль с учетом сохранения репутационной политики (расследования в отношении крупных корпораций).

Решением проблемы недостаточного уровня квалификации сотрудников, привлечённых к раскрытию преступлений в сфере информационных технологий станет разработка образовательных программ с обязательным изучением как основ информационной безопасности на правовом и организационном уровнях, так и специфики киберпреступлений на техническом уровне – физическом, аппаратном, программном и криптографическом [53]. Отдельного исследования при подготовке специалистов требует компьютерная криминалистика (форензика); важно всесторонне изучить методы сбора цифровых доказательств, фреймворки для криминалистической характеристики и анализа проведения оперативных расследований на удалённых конечных точках; проводить грамотный анализ сетевого взаимодействия, способов извлечения информации с изучаемых жестких дисков, цифровых устройств и тому подобных элементов [23].

Недостаточным должен считаться уровень оснащения подразделений, расследующих киберпреступления, современными техническими средствами, такими как:

– средства выемки электронных доказательств и аппаратного обеспечения;

– средства восстановления данных по «виртуальным отпечаткам» в памяти жёстких дисков, обработки и расшифровки данных, создания электронных образов и хэш-кодов;
– средства экспертизы оборудования и уничтожения информации в удалённом формате.

Подводя итог, следует согласиться с мнением Поляков В.В., котрый полагает, что: «В отдельных случаях потерпевшие оказывают противодействие расследованию преступления, выражавшееся в уничтожении следов преступления и предоставлении только части требуемых документов. Объяснение такого поведения заключается в том, что для многих потерпевших, например, кредитных организаций, разглашение информации о низкой защищенности конфиденциальной информации может привести к причинению серьезного ущерба деловой репутации. Другой причиной может является страх перед тщательным расследованием, которое способно выявить все возможные внутренние махинации и нарушения или спровоцировать вопрос о профессиональной непригодности должностных лиц» [45, с. 49].

Нет сомнений в том, что ситуация с данным видом преступлений в скором времени изменится. Ведь на современном этапе в России повсеместно и очень активно внедряется электронный документооборот, электронные торги, онлайн заявки на оказание услуг. Всё это вкупе влечёт за собой, с одной стороны, ускорение процессов подачи заявлений, а с другой – переносит их в менее защищенную реальность – виртуальную; это усиливает риски утечки информации из компьютера в базы злоумышленников.

По результатам исследования во второй главе можно сделать ряд выводов и обобщений.

Во-первых, для киберпреступлений в большинстве своём характерны корыстные и политические мотивы преступления. Цели киберпреступлений тоже различны, но, в основном, на практике встречаются цели незаконного обогащения и дестабилизации каких-либо, в том числе, и государственных структур. Таким образом, со становлением и развитием информационных

технологий возникают риски роста киберпреступности. Мотив и цель киберпреступлений – это важные криминологические характеристики, особенности которых положительно влияют на практику по раскрываемости и профилактике данного вида преступлений [85].

Во-вторых, раскрываемость и расследование киберпреступлений остаётся действительно сложной задачей для следователей. Причины этого следующие: отсутствие единой для всех госструктур судебной практики и следственной практики по уголовным делам в сфере киберпреступлений; недостаточное количество специалистов с высокой квалификацией в системе следствия (в области IT-технологий и специализирующихся на расследовании данного вида преступлений); сложность и высокие затраты на проведение компьютерной экспертизы и др.

В-третьих, на сегодняшний день, когда проблема кибермошенничества достаточно распространены, важно, для начала, замедлить, а в дальнейшем полностью остановить фиксируемые высокие темпы прироста новых случаев киберпреступлений.

В-четвертых, из анализа криминалистической характеристики киберпреступных деяний, мы выявили следующие признаки: кибертерроризм носит групповой характер; наиболее высокая степень компьютерных цифровых знаний обнаруживается именно у кибертеррористов; исходя из анализа судебной практики осуществлённых кибератак, отнесённых к террористическим, можно отметить, что кибертеррористы, в противовес обычным террористам, предпочитают работать инкогнито. В лучшем случае, общественность может выяснить название группировки или вымышленные имена (никнеймы) исполнителей кибертеррakта [13].

Заключение

Результаты предоставленного анализа официальной статистики показали, что в России в последние годы происходит взрывной рост киберпреступлений, особенно усилившийся в период пандемии COVID-19. Стоит отметить тот факт, что предпосылки зарождения и развития киберпреступности формировались в России в течение последних двадцати лет.

С одной стороны, это цифровизация различных сторон жизнедеятельности россиян, примером может выступать высокий интерес к банковским картам и счетам, безналичным способам оплаты; онлайн-досуг и активное использование соцсетей.

С другой стороны, низкий уровень цифровых компетенций граждан страны сохраняется по сей день.

Наконец, низкая квалификация правоохранительных органов, несовершенство antifraud-инфраструктуры, сложности в оперативном пресечении киберпреступной деятельности и эффективном расследования инцидентов в цифровой среде.

Исходя из криминалистической характеристики киберпреступлений хотелось бы выделить трансграничность исследуемых преступлений, которая накладывает свой отпечаток. Место нахождения преступника и жертвы при осуществлении преступлений, как экстремистского, так и террористического характера в информационной среде характеризуется дистанцированностью друг от друга. Помимо этого, момент совершения киберпреступного деяния и момент его обнаружения не единовременны. То есть преступник может совершить уголовно наказуемое деяние, а его восприятие жертвой может произойти лишь спустя определенный промежуток времени. Вследствие чего, такие элементы, как место и время совершения преступления в данном случае фактически нивелируются.

Таким образом, при раскрытии и анализе данных преступлений необходимо акцентировать внимание на следующих аспектах:

- непосредственно на кибер-следах.
- на мерах, которые направлены на сокрытие следов преступления и противодействие по его раскрытию.

Подводя итог, хотелось бы отметить, что достаточно лёгкой жертвой киберпреступников являются предприятия малого и среднего бизнеса (МСБ), в силу малого бюджета, отсутствия высококвалифицированных кадров и пробелов в познаниях сотрудников.

Кроме того, банковские учреждения, независимо от времени и достижений техники, остаются привлекательной целью для быстрого получения богатства.

Хакеры пользуются слабыми местами в программном обеспечении популярных социальных сетей и серверов, различных государственных служб и учреждений. Социальные сети в особенной степени привлекательны для преступника из-за популярности у большого числа людей, безосновательного к ним доверия в плане безопасности. Доступ к указанным сетям даёт возможность получения огромных объемов конфиденциальной информации в собственное пользование, среди которой могут находиться массивы данных для последующего онлайн мошенничества, шантажа, перепродажи информации заинтересованным лицам.

Мы можем наблюдать в последние годы, как виды преступлений в сфере информационных технологий меняются в качественном отношении и непрерывно эволюционируют, становятся более высокоорганизованными и изощрёнными, добавляются новые виды этих преступных деяний. Кроме того, возрастает техническая оснащённость киберпреступников, что связано со стремительным развитием в области информационных технологий; появляются всё новые способы совершения этих противоправных деяний, что, в свою очередь, вынуждает нас на принятие незамедлительных и эффективных мер по противодействию киберпреступлениям, развитие компьютерной

криминалистики (форензики) и своевременное изменение программы обучения специалистов по расследованию и раскрытию преступлений в области инфокоммуникационных технологий, в особенности, в сети «Интернет».

В рамках данного дипломного исследования, цель достигнута, обозначенные во введении задачи, по моему мнению, решены, а именно:

- определены понятие, состояние и криминалистическая классификация преступлений в сфере ИТ-технологий;
- проанализирована динамика развития киберпреступности в Российской Федерации в 2017-2021 годах, опираясь на статистику Министерства внутренних дел о количестве зарегистрированных киберпреступлений в эти годы в РФ;
- охарактеризованы уголовно-правовые нормы по регулированию отношений в сфере киберпространства;
- исследованы становление и развитие правоотношений в сфере компьютерной информации и криминализации киберпреступлений;
- определены объективные и субъективные признаки киберпреступных деяний;
- выявлены причины сложностей квалификации киберпреступлений;
- сформулированы и обоснованы основные факторы, ставшие причиной ухудшения ситуации с киберпреступностью в РФ, усугубившейся за последние 5 лет.

Список используемой литературы и используемых источников

1. Азизов Р.Ф. Развитие уголовного законодательства в сфере борьбы с киберпреступлениями в Азербайджанской республике // Вестник СПб. 2015. № 1. С. 123-129.
2. Анисимова А.С. Анализ правотворческой политики зарубежных стран в сфере регулирования Интернет-отношений // Вестн. Саратовской гос. юрид. акад. 2014. № 5 (100). С. 38-44.
3. Антонян Е.А. Блокчейн-технологии в противодействии кибертерроризму // Актуальные проблемы российского права. 2021. № 6 (103). С. 167-177.
4. Батраченко Е.К. Анализ рынка антивирусного программного обеспечения // World science: problems and innovations: сб. междунар. конф. Пенза, 25 дек. 2017 г. Пенза., 2017. С. 78-82.
5. Безкоровайный М.М. Кибербезопасность подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1 (2). С. 22-27.
6. Белоус А.И. Программные и аппаратные трояны – способы внедрения и методы противодействия: Первая техническая энциклопедия: в 2 кн. // Техносфера. 2021. 1318 с.
7. Белоусов А.С. Некоторые аспекты расследования компьютерных преступлений // Информационные технологии и безопасность: сб. материалов междунар. конф. Киев., 2003. С. 13-22.
8. Бессонов С.А. История и зарубежный опыт правовой регламентации компьютерной преступности // Территория науки. 2013. № 2. С. 231-237.
9. Богданова Т.Н. К вопросу об определении понятия «Преступления в сфере компьютерной информации» // Вестник Челябинского государственного университета. 2012. № 37 (291). С. 64-67.
10. Бутузов В.М. Документирование преступлений в сфере использования электронновычислительных машин (компьютеров), систем и

компьютерных сетей и сетей электросвязи при проведении доследственной проверки : наук. практ. пособ. Вид. дом «Аванпост-Прим». 2010. 55 с.

11. Бутусова Л.И. К вопросу о киберпреступности в международном праве // Вестник экономической безопасности. 2016. № 2. С. 48-52.

12. Варфоломеев А.А. Кибердиверсия и кибертерроризм: пределы возможностей негосударственных субъектов на современном этапе. // Военная мысль. 2012. № 12. С. 3-11.

13. Васильев М.В. Кибертерроризм как элемент гибридной войны // Современные исследования в сфере социальных и гуманитарных наук сборник результатов научных исследований. 2018. С. 554-569.

14. Гликерман, А.П. Криминалистическая характеристика мошенничества на примере судебной практики Забайкальского края // Молодой ученый. 2020. № 15 (305). С. 183-188. [Электронный ресурс] URL : https://moluch.ru/archive/305/68634/ (дата обращения: 07.10.2022).

15. Глотина И.М. Киберпреступность как теневой бизнес // Вестн. Челябинского гос. ун-та. 2016. № 6 (388). С. 51-57.

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

17. Грачев А.В. История возникновения киберпреступлений // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи: сб. материалов внутривузовской конф. Магнитогорск, 09-12 окт. 2015 г. Магнитогорск. 2015. С. 162-175.

18. Давыдов В.О. Информационное обеспечение раскрытия и расследования преступлений экстремистской направленности, совершенных с использованием компьютерных сетей: дис... канд. юрид. наук. Тула, 2013. 264 с.

19. Дворецкий М.Ю. Проблемы толкования терминов при квалификации преступлений по ст. 272 уголовного кодекса РФ // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2013. № 12 (128). С. 527532.

20. Дементьева М.А. Киберпреступления в банковской сфере РФ: способы выявления и противодействия / М.А. Дементьева [и др.] // Экономические отношения. 2021. № 2. С. 109-120.

21. Добрынин Ю.В. Классификация преступлений, совершаемых в сфере компьютерной информации [Электронный ресурс] // Право и Интернет. URL: https://www.russianlaw.net/law/computer_crime/a158/ (дата обращения: 02.02.2020).

22. Долгиева М.М. Квалификация преступлений, совершаемых в сфере компьютерной информации в отношении криптовалюты // Современное право. 2018. № 2. С. 103-108.

23. Долгиева М.М. Операции с криптовалютами: актуальные проблемы теории и практики применения уголовного законодательства // Актуальные проблемы российского права. 2021. № 4 (101). С. 128-139.

24. Ефремова М.А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения // Право и кибербезопасность. 2014. N 2. С. 33-38.

25. Зверянская Л.П. Исторический анализ этапов развития киберпреступности и особенности современных киберпреступлений // Концепт. 2016. № 15. С. 881-885 // КонсультантПлюс. 2022.

26. Зигмунт О.А. Кибер-и Интернет-преступность в Германии и России: возможности сравнительного исследования // Юридическая наука и правоохранительная практика. 2015. № 4 (34). С. 180-188.

27. Зуев В.С. IT-справочник для следователя М. : Юрлитинформ, 2021. 232 с.

28. Зуев Е.И. Криминалистика: актуальные проблемы М., 1988. 120 с.

29. Интернет-портал Российской газеты // Рубрика: Происшествия. [Электронный ресурс]. URL: https://rg.ru/ (дата обращения: 11.10.2022).

30. Картавченко В.В., Лисун Е.А. Использование высоких технологий в качестве способа совершения преступления // Проблемы и перспективы развития современной юриспруденции: сборник научных трудов по итогам Международной научно-практической конференции. Воронеж, 2015. С. 91.

31. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М., Горячая линия, Телеком. 2012. С. 13.

32. Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно теоретическая основа и прикладные аспекты первоначального этапа: дисс. ...канд. юрид. наук. Иркутск, 2017. 211 с.

33. Конвенция о преступности в сфере компьютерной информации (ETS № 185) [рус., англ.] (Заключена в г. Будапеште 23.11.2001) из информационного банка «Международное право» // СПС КонсультантПлюс. 2022.

34. Конституция Российской Федерации: принята всенар. Голосованием 12 дек. 1993 г.// КонсультантПлюс. 2022.

35. Кочкина Э.Л. Определение понятия «киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3. С. 162-169.

36. Крылов Д.О. К вопросу о терминологии в сфере киберпреступности (на материале английского языка) [Электронный ресурс] // Международный студенческий научный вестник. 2017. № 1. С. 1-6. URL: http://www.eduherald.ru/ru/article/view?id=16836 (дата обращения 12.12. 2021).

37. Кушниренко С.П. Методика расследования преступлений в сфере высоких технологий: конспект лекций. СПб: Изд-во юрид. ин-т Генеральной прокуратуры РФ. 2007. 64 с.

38. Лебедев М.В. Комментарий к уголовному кодексу РФ. Научно-практический комментарий. М., Юрайт-М. 2004. 560 с.

39. Ляпунов Ю. Максимов В. Ответственность за компьютерные преступления // Законность,1997. № 1. С. 8-14.

40. Мавринская Т.В. Психологические особенности киберпреступников // Инновационное развитие. 2018. № 4 (21). С. 156-158.

41. Макушев Д.И. К вопросу об определении понятия «киберпреступность» [Электронный ресурс] // «ExLegis: правовые исследования». 2016. № 1. С. 30-34. URL: http://exlegis.ru. (дата обращения: 06.10.2022).

42. Морозов И.Л. Информационная безопасность политической системы // Полис. Политические исследования. 2002. № 5. С. 134-145.

43. Паршин С.А. Современные американские подходы к проблеме кибертерроризма // Вестник М. гос. ун-та. 2011. № 3. С. 81-105.

44. Положение Федеральной службы безопасности Российской Федерации от 09 фев. 2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» // Российская газета. 19 февраля 2005 г. № 55.

45. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского гос. унта. 2013. С. 114-116.

46. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: дис. … канд. юрид. наук. Барнаул. 2008. 247 с.

47. Постановление Пленума Верховного Суда Рос. Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» // КонсультантПлюс. 2022.

48. Постановление Пленума Верховного Суда Рос. Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // КонсультантПлюс. 2022.

49. Постановление Пленума от 09 фев. 2012 г. № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» // КонсультантПлюс. 2022.

50. Постановление Правительства Российской Федерации от 08 фев. 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры РФ, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры РФ и их значений» // КонсультантПлюс. 2022.

51. Приговор Невинномысского городского суда Ставропольского края по уголовному делу №1-330/2016. [Электронный ресурс]. URL: https://rospravosudie. com/court-nevinnomysskij-gorodskoj-sudstavropolskij-kraj-s/act-467039955/ (дата обращения: 09.10.2022).

52. Приказ Генпрокуратуры России от 14 сентября 2017 г. N 627 «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года» // Законность. 2017. № 12. С. 67-87.

53. Приказ Министерства информационных технологий и связи Российской Федерации от 16 янв. 2008 г. № 6 «Об утверждении требований к сетям электросвязи для проведения оперативно-розыскных мероприятий» // КонсультантПлюс. 2022.

54. Приказ Федеральной службы безопасности Рос. Федерации от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам» // КонсультантПлюс. 2022.

55. Приказ Федеральной службы безопасности Российской Федерации от 24 июля 2018 г. № 367 // КонсультантПлюс. 2022.

56. Проект Концепции стратегии кибербезопасности Российской Федерации [Электронный ресурс]: постановление правительства Рос. Федерации от 29 нояб. 2013 г. // КонсультантПлюс. 2022.

57. Скляров С.В. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации // Всероссийский криминологический журнал. 2016. Т. 10, № 2. С. 322-333.

58. Состояние преступности // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports (дата обращения: 01.09.2022).

59. Степанов О.А. Актуальные проблемы противодействия кибертерроризму. М. : Изд-во Акад. Ген. пр-ры, 2014 г. 100 с.

60. Стёпин Д.С. Информационное воздействие террористической и экстремисткой агитации и пропаганды в сети Интернет // Криминологические проблемы регионов Крайнего Севера России / под ред. проф. А.И. Долговой. - М. : Российская криминологическая ассоциация, 2015. С. 182-184.

61. Стёпин Д.С. Особенности осуществления террористической агитациии пропаганды с использованием интернет-ресурсов (на примере форума «КавказЧат») // Проблемы теории и практики борьбы с экстремизмом и терроризмом: материалы научно-практической конференции. М. : Российская криминологическая ассоциация; Ставрополь : Изд-во СКФУ, 2015. С. 25-32.

62. Талипова Л.Р. Международно-правовая регламентация киберпреступности. // Гуманитарные, социально-экономические и общественные науки. 2016. № 4. С. 121-123.

63. Тимофеев А.В. Выявление и раскрытие киберпреступлений в кредитно-финансовой сфере // Вестник Санкт-Петербургского университета МВД России. 2016. № 3 (71). С. 137–140.

64. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дисс. … канд. юрид. наук. Владивосток, 2005. 234 с.

65. Уголовный кодекс Российской Федерации [Электронный ресурс] : федер. закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ: (ред. от 30 дек. 2020 г.) // КонсультантПлюс. 2022.

66. Указ Президента Рос. Федерации от 28 июля 1993 г. № 966 «О концепции правовой информатизации России» // Российские вести. 13 июля 1993 г. № 132. С. 67-89.

67. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» //

Официальный интернетпортал правовой информации [Электронный ресурс] URL: http://www.pravo.gov.ru, 06.12.2016.

68. Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Официальный интернет-портал правовой информации [Электронный ресурс] URL: http://www.pravo.gov.ru, 10.10.2022 г.

69. Указ Президента РФ от 30.11.2016 N 640 «Об утверждении Концепции внешней политики Российской Федерации» // Официальный интернет-портал правовой информации [Электронный ресурс] URL: http://www.pravo.gov.ru, 01.10.2022.

70. Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации» // Официальный интернет-портал правовой информации [Электронный ресурс] URL: http://www.pravo.gov.ru, 31.09.2022.

71. Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» [Электронный ресурс]. URL: http:/ www.consultant.ru (дата обращения: 10.10.2022 г.)

72. Федеральный закон Российской Федерации «О противодействии терроризму» от 06 марта 2006 г. № 35-ФЗ: (ред. от 08 дек. 2020 г.) // КонсультантПлюс. 2022.

73. Федеральный закон Российской Федерации от 07 июля 2003 г. №126-ФЗ (от 8 дек. 2020 г.) «О связи» // КонсультантПлюс. 2022.

74. Федеральный закон Российской Федерации от 25 июля 2002 г. № 114-ФЗ (ред. от 08 дек. 2020 г.) «О противодействии экстремистской деятельности» // КонсультантПлюс. 2022.

75. Федеральный закон Российской Федерации от 26 июля 2017 г. № 187-ФЗ (ред. от 26 июля 2017 г.) «О безопасности критической

информационной инфраструктуры Российской Федерации» // КонсультантПлюс. 2022.

76. Федеральный закон Российской Федерации от 27 июля 2006 № 149-ФЗ (ред. от 08 июня 2020 г.) «Об информации, информационных технологиях и о защите информации» // КонсультантПлюс. 2022.

77. Федотов М.А. Конституционные ответы на вызовы киберпространства // Lex Russica. 2016. № 3 (112). С. 164-182.

78. Халиуллин А.И. Подходы к определению компьютерной преступности // Контуры глобальных трансформаций: политика, экономика, право. 2011. № 6. С. 16-23.

79. Хрусталев А.О. Понятие киберпреступности // Аллея науки. 2018. № 5(21). С. 147–150.

80. Чайковский Н.С., Кухенная М.А. Статистика киберпреступности в Российской Федерации // Оценка социально-экономического развития: опыт и перспективы: сб. материалов междунар. конф. Донецк, 04-05 апр. 2021 г. Донецк. С. 399-401.

81. Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2012. № 1. С. 9-22.

82. Чернякова А.В. Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации // Юридическая наука и правоохранительная практика. 2018. № 4(46). С. 168-179.

83. Чжэн И. Сотрудничество РФ и КНР в борьбе с кибертерроризмом // Вестн. М. гос. обл. ун-та. 2018. № 2. С. 204-214.

84. Чуфаровский Ю.В. Психология оперативно-розыскной деятельности. 2-е изд., доп. М., 2001. С. 208.

85. Шапошников А.А. Криминологическая характеристика личности киберпреступника // Вестник Юридического факультета южного федерального университета. 2018. № 3-4. С. 58-63.

86. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дисс. … канд. юрид. наук. Владивосток, 2007. 270 с.

87. Шибаев Д.В. Содержание понятия «Преступление в сфере компьютерной информации» // Российский журнал правовых исследований. 2018. № 4 (17). С. 131-140.