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)

40.04.01 Юриспруденция
(код и наименование направления подготовки)

Уголовное право и процесс
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему «Современное состояние криминалистической тактики производства отдельных следственных действий при расследовании преступлений в киберпространстве и основные направления ее совершенствования»

Обучающийся Ю.В. Мягков
(Инициалы. Фамилия) (личная подпись)

Научный руководитель канд. юрид. наук, Л.Н. Кабанова
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2023

Оглавление

Введение

Актуальность темы исследования. Развитие интернет-технологий привело к росту преступности в киберпространстве. Современные цифровые технологии в экономике также влияют на модернизацию так называемого «подпольного мира». Специалисты Генпрокуратуры РФ отметили рост киберпреступности в стране более чем на 75%. Так, в 2022 году количество преступлений, совершенных с использованием интернет-технологий, увеличилось на 75,4% [14].

Составлен рейтинг наиболее распространенных преступлений, где первое место составляют кражи. Всего за 2020 год зарегистрировано 691 тысяча случаев хищения чужого имущества, что составляет 36,7% от общего числа совершенных преступлений [9].

Оценивая киберпреступность в мировых масштабах, можно утверждать о ее локальном и организованном распространении. Так российские разработчики средств информационной безопасности предлагают рассматривать международную киберпреступность, как отрасль экономики и полноценную индустрию. Таким образом, сотрудники следственных органов сталкиваются в практической деятельности с новыми более современными преступлениями, реализуемыми в киберпространстве.

В связи с этим отдельные страны предъявляют к сотрудникам следственных органов, проводящих расследования в области киберпреступности, повышенный уровень требований.

Современная криминалистическая тактики производства отдельных следственных действий при расследовании преступлений в киберпространстве содержит ряд пробелов, которые вызывают дискуссионные вопросы в науке и среди правоприменителей, криминалистов.

В данном исследовании предпринята попытка выработать предложения о направлениях совершенствования криминалистической тактики

расследования отдельных следственных действий преступлений в киберпространстве.

Таким образом, актуальность темы исследования обусловлена вышеперечисленными аспектами, практической и научной значимостью повышения раскрываемости данных преступлений, необходимостью анализа составляющих киберпространства, в котором совершаются данные преступления, и последующей проработки рекомендаций по решению возникающих в ходе расследования проблем.

Объектом исследования является криминалистическая тактика отдельных следственных действий при расследовании киберпреступлений.

Предметом исследования выступают киберпреступления, совершаемые в киберпространстве, что обусловливает учет факторов и особенностей при использовании криминалистической тактики в производстве отдельных следственных действий расследования данных преступлений.

Цель исследования – на основе комплексного анализа теоретического, практического и научного материала, характеризующего понятия и особенности преступлений совершенных в киберпространстве разработать научно обоснованные рекомендации, направленные на совершенствования криминалистической тактики при производстве отдельных следственных действии в расследовании киберпреступлений.

Для достижения поставленной цели магистерской работы необходимо решение следующих задач:

- раскрыть понятие киберпреступности путем анализа научной литературы, на этой основе дать авторское определение понятию киберпреступности;
- рассмотреть систему преступлений в киберпространстве, выделить группу факторов, характеризующих киберпространство;
- дать характеристику отличительных особенностей киберпреступлений совершенных в киберпространстве с учетом выделенных факторов;

- рассмотреть критерии классификации киберпреступлений в криминалистике;
- охарактеризовать тактику производства отдельных следственных действий в расследовании киберпреступлений;
- выделить отличительные особенности криминалистической тактики в расследовании отдельных киберпреступлений;
- охарактеризовать криминалистические проблемы в расследовании отдельных киберпреступлений
- предложить пути совершенствования криминалистической тактики при производстве отдельных следственных действии в расследовании киберпреступлений с целью повышения их раскрываемости.

Степень разработанности. Современные подходы к исследованию киберпреступлений основаны на работах отечественных исследователей таких как: Р.А. Барышев, М.А. Простосердов, И.Н. Теркулова, Т.Л. Тропина, С.Н. Хуторной, Е.С. Шевченко и другие. А также труды зарубежных ученых – Р.С. Мюллера, К.Д. Митника, М. Маккарти.

Теоретическую базу исследования составили научные труды таких ученых, как Р.А. Барышев, М.А. Простосердов, И.Н. Теркулова, Т.Л. Тропина, С.Н. Хуторной, Е.С. Шевченко и др. рассматривающие вопросы понятия, особенностей, отличительных характеристик киберпространства и киберпреступности, тактики производства следственных действий, уголовно-правовых мер борьбы с киберпреступностью. Сведения о расследовании преступлений в сфере компьютерной информации рассматривались в научно-методическом пособии А.Н. Яковлева; полном курсе криминалистики А.Г. Филиппова, Проанализированы научные публикации и статьи таких авторов как: М.Е. Батухтин, Н.А. Морозов, В.И. Павловец, М.П. Перякина, С.В. Унжакова, Н.Э. Шишкина и других.

Теоретическая основа исследования базируется на трудах отечественных учёных в области криминалистики, судебной экспертизы, уголовно-процессуального права, уголовного права, криминологии.

Нормативно-правовую основу исследования составляют Уголовный кодекс Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, иные федеральные законы, касающиеся исследуемой темы и иные нормативные правовые акты.

Методологическая основа исследования в данной магистерской работе составили метод познания и получения научного результата. В процессе проведения исследования использовались общенаучные методы познания: сравнительно-правовой и системный. При проведении исследования использовались приемы анализа, синтеза и обобщения.

Научная новизна исследования подтверждена проведённым на магистерском уровне комплексным изучением и анализом производства и организации применения криминалистической тактики следственных действий при расследовании преступлений в киберпространстве. Проведено обоснование необходимости дальнейших научных исследований в рамках роста преступности и разновидности преступлений в киберпространстве с целью подготовки практических рекомендаций по усовершенствованию тактики производства следственных действий относительно отдельных видов киберпреступлений. Научная новизна работы подтверждена положениями и выводами, выдвигаемыми для публичной защиты магистерской диссертации

Положения, выносимые на защиту:

- в рамках проведенного исследования уточнено определение понятия киберпреступления;
- предложена модель функционирования киберпространства с учетом определяющих факторов, в которой осуществляются киберпреступления;
- на основе анализа методов расследования, сформирован системный подходы к пониманию факторов киберпространства и

киберпреступности, дополнены критерии классификации, ранее не применяемые к данным преступлениям;

- рассмотрен критерий классификации в криминалистике по механизму атаки. Охарактеризован каждый тип атаки, так как ему соответствуют уникальные характеристики, которые требуют соответствующих методов расследования и идентификации;
- дана характеристика целевым аудиториям, на которые направлены действия киберпреступников;
- выделены отличительные особенности криминалистической тактики в расследовании преступлений связанных с несанкционированным доступ к компьютерной и иной информации, а также финансовым мошенничеством.
- предложены требования для должностной инструкции специалиста, осуществляющего расследование киберпреступлений;
- обоснована необходимость внесения изменений в УПК РФ с целью закрепления в перечне видов доказательств, такого вида доказательства, как цифровой след, в ч. 2 ст. 74 УПК РФ. Предложена разработка конкретного механизма получения такого вида доказательства как «форензики»;
- предложены общие рекомендаций по расследованию киберпреступлений;
- обосновано использование ГЧП в расследовании киберпреступлений, либо осуществление отдельных следственных действий с использованием механизма ГЧП, рассмотрена криминалистическая тактика расследования киберпреступлений с использованием ГЧП и без него.

Теоретическая значимость диссертационного исследования заключается в предоставлении возможностей по дальнейшему обогащению науки криминалистики, выражающихся в разработке и формировании направлений усовершенствования проведения следственных действий с учетом

привлечения государственно-частного партнерства, для передачи функций сбора и фиксации доказательств в киберпространстве.

Организационных мероприятий направленных на консолидацию усилий противостояния киберугрозам и киберпреступности, через методическое обеспечение и взаимодействие государственного и частного сектора.

Практическая значимость магистерского диссертационного исследования предопределена его прикладным характером. В работе проведена дискуссия, сформированы обоснованные выводы, основанные на анализе судебно-следственной практики по расследованию киберпреступлений. В результате исследования подходов к характеристике и определению термина киберпространства нами предложен системный подход к его рассмотрению.

Результаты работы могут быть также использованы в научных разработках и в учебном процессе.

Апробация и внедрение результатов исследования. Теоретические положения, выводы, изложенные в теоретическом разделе магистерском диссертационном исследовании, получили отражение в опубликованной научной статье: Мягков Ю.В. «Характеристика определения киберпреступности на современном этапе».

Структура и объем магистерской диссертации обусловлены целями и задачами исследования. Магистерская диссертация состоит из введения, трех глав, включающих восемь параграфов, заключения, списка использованной литературы.

Глава 1 Общая характеристика киберпреступлений на современном этапе

1.1 Понятие киберпреступности

Любой исторический этап существования общества характеризуется своими особенностями. Так общественное развитие в текущий момент времени характеризуется информационным обществом – это «общество, в котором социально-экономическое развитие зависит, прежде всего, от производства, переработки, хранения, распространения информации среди членов общества» [8].

Рассматривая вопрос о появлении нового направления преступности важно учитывать источники его появления. Большинство авторов научных публикаций отслеживающих исторический этап появления и развития киберпреступности, связывают его с появлением интернета, так 29 октября 1969 года всемирная система объединённых компьютерных сетей ARPANET успешно провела сеанс связи между серверами, поэтому данная дата является днем рождения Интернет. А в 1972 году появляется электронная почта [5, с. 163].

Можно утверждать, что современные информационные технологии затрагивают все сферы деятельности человека. Раз общество активно внедряет во все сферы все более новые, усовершенствованные информационные технологии, появляются новые виды и разновидности преступлений в информационном пространстве.

В современном обществе наблюдается развитие в использовании информационных коммуникаций, что приводит к прогрессивному росту преступности в относительно новом направлении, которым и является киберпреступность.

По прогнозам экспертов, эти преступления будут увеличиваться, что характеризует статистические данные, представленные в работе МВД,

количество преступлений в киберпространстве имеет положительную динамику, круг этих преступлений с каждым годом расширяется, и это не предел.

Очевидным становится факт мирового распространения информационных технологий и цифровизации общества. Сегодня преступления в киберпространстве не являются единичными, а носят массовый характер, становясь проблемой не единого государства, а всего общества в целом.

Важно помнить, что киберпреступники постоянно развивают новые методы атак и новые способы совершения преступлений. Поэтому важно уделять внимание повышению квалификации, обмену опытом сотрудников и специалистов, осуществляющих расследование данных преступлений, техническому обеспечению, превентивным мероприятиям и т.д.

Возросшая преступность в киберпространстве негативно влияет на все сферы жизнедеятельности государства, активное развитие данных направлений преступности наносит ущерб не только экономическому сектору, но и функционированию всего государственного аппарата и современного мироустройства в целом [28].

Преступления в киберпространстве реализуются не только отдельными преступниками, а в большинстве случаев организованными группами, так как материальная выгода групп, как показывают данные анализа совершенных преступлений превышает экономический эффект получаемый индивидуально.

Современная преступность эффективно использует в своей деятельности новые возможности, представленные киберпространством, в данной среде теряется реальная личность преступника, что позволяет использовать безграничные программные и территориальные возможности, а самому преступнику оставаться анонимно безнаказанным.

Киберпреступность - это современное явление, которое становится все более распространенным и высокотехнологичным. Киберпреступники могут получать доступ к информации, перехватывать данные, внедрять вредоносное

ПО и т.д. это явление представляет серьезную угрозу безопасности государства, критически важной инфраструктуры, отдельных лиц и общества в целом.

Все большее количество преступлений совершается в киберпространстве путем применения современных информационных технологий, то есть в виртуальной среде, которая не позволяет использовать превентивные мероприятия с целью оперативного предотвращения и пресечения данных преступлений, а также привлечения лиц их совершивших к ответственности.

Прогрессивный рост новых видов преступлений определяется следующими факторами:

- увеличение числа пользователей компьютеров и сети Интернет;
- профессионализмом преступников в информационном пространстве;
- совершенствованием и развитием IT-технологий.

Таким образом информационное общество является предпосылкой роста новых видов преступлений [22, с. 141].

Рассмотрим статистические данные на примере муниципального образования, Российской Федерации и в международном аспекте. По данным работы Отдела МВД России по Миасскому городскому округу за 2020 год выявлен рост преступлений в киберпространстве.

Треть преступлений осуществляется с использованием информационных технологий, (за 2020 год их количественное выражение составило 886 преступлений), прирост составил 5,4%. Мошенничество в общем составе имущественных преступлений увеличилось на 20,9% и составило 619 преступлений.

По данным отчетов за 9 месяцев 2021 года рост данных видов преступлений в относительных показателях составил 33,3%, а в количественном выражении совершено 976 преступлений, число краж с банковского счета составило 229 случаев [27].

Так в целом по стране в количественном выражении за 11 месяцев 2020 года было отмечено 461 тысяча таких преступлений, причем их количество возрастает с каждым днем и в настоящий момент составляет четверть от всех мошенничеств и хищений в России.

Киберпреступность - одно из самых опасных явлений в современном мире. Этот вид преступлений использует различные виды технических средств для совершения преступлений в интернете и других информационных системах.

Оценивая киберпреступность в мировых масштабах, можно утверждать о ее локальном и организованном распространении. Так российские разработчики средств информационной безопасности предлагают рассматривать международную киберпреступность, как отрасль экономики и полноценную индустрию.

Анализируя масштабы киберпреступлений, можно выделить крупные кражи, которые организованы целыми IT-компаниями, а также мелкие, проводимые небольшой группой IT-специалистов. По аналогии ущербы, наносимые крупными компаниями киберпреступников составляют более 1 млрд долл. США в год, а прибыль мелких организаций составляют 30–50 тыс. долл. США.

Так по данным компании Bromium, объем мирового рынка киберпреступлений составляет 1,5 трлн долл. США данные показатели сопоставимы с ВВП Канады или Австралии за 2017 г. Так индивидуальные киберпреступники зарабатывают в год до полумиллиона долларов США путем торговли украденными данными [52].

Подводя итог статистическим данным выявлено значительное влияние на рост преступности цифровизации экономики, этим объясняется рост киберпреступлений.

Таким образом, сотрудники следственных органов сталкиваются в практической деятельности с новыми более современными преступлениями, реализуемыми в киберпространстве.

С ростом данных преступлений возникают активные дискуссии в научной сфере. Так авторы научных публикаций вновь и вновь пытаются раскрыть понятие киберпреступности в рамках различных подходов к его содержанию.

Обратим внимание на то, что в западном обществе проблема киберпреступности возникла намного раньше, чем в Российской Федерации, так первые попытки охарактеризовать киберпреступность реализованы в 1986 году в Париже. Организации экономического сотрудничества и развития, представленная группой экспертов, предложили следующее определение киберпреступности: «любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку и (или) передачу данных» [53].

Как можно заметить, данное определение является ограниченным и не отражает содержание самого преступления, реализованного с помощью информационных технологий, а лишь косвенно указывает на неразрешенное использование и передачу данных.

Следующей попыткой охарактеризовать киберпреступность стал, конгресс Организации Объединенных Наций, который в 2000 году обозначил актуальность новой формулировки понятия киберпреступности «любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети» [34].

Предложенная формулировка носит всеобъемлющий характер путем словосочетания «любое преступление», а отношение к киберпреступлению охарактеризовано компьютерной сетью или системой.

Так как киберпреступления рассматривают транснационально Советом Европы то в 2001 году в Европейской Конвенции по киберпреступлениям, предложена следующая формулировка: «киберпреступления – это правонарушения, направленные против конфиденциальности, целостности и

доступности компьютерных систем, сетей и данных, а также неправомерное использование указанных систем, сетей и данных» [57].

Данный термин рассматривает киберпреступления в составе разновидности компьютерной преступности, в которых компонентом является компьютерная сеть или сеть Интернет.

Например Ю.Ю. Комлев считает, что: «появление киберпреступности можно отсчитывать с момента появления компьютера…» [15, с. 97], конечно такой подход является абстрактным, так как компьютер – это термин, пришедший в русский язык из иноязычных источников, одно из названий электронной вычислительной машины. Используется в данном смысле в русском литературном языке, научной, научно-популярной литературе [35, с. 229], а в законодательстве Евразийского экономического союза: «компьютер - это устройство, которое выполняет логические операции и обработку данных, может использовать устройства ввода и вывода информации на дисплей и обычно включает в себя центральный процессор для выполнения операций. Если отсутствует центральный процессор, то устройство должно функционировать в качестве «шлюза клиента» к компьютерному серверу, который действует как вычислительный блок обработки» [37].

Таким образом ассоциировать исторически появление компьютеров с киберпреступлениями считаем на наш взгляд не совсем правильно, так как компьютер является только техническим устройством позволяющим хранить и обрабатывать информацию, для совершения киберпреступления его наличия не является достаточным.

Другой исследователь Т.М. Хусяинов охарактеризовал термин следующим образом: «под термином «интернет-преступление» или «киберпреступление» стоит понимать весь спектр преступных действий в сфере информационных технологий…» [45, с. 120]. Такая формулировка представляет обобщенный подход, который не позволяет раскрыть содержание киберпреступления.

М.Е. Батухин, как и предыдущий исследователь Т.М. Хусяинов использует в своей трактовке обобщенный подход: «киберпреступление – это любое преступление в электронной сфере, совершенное при помощи компьютерных средств или виртуальной сети, или против них» [2, с. 28].

Не согласимся с позицией Т.М. Хусяинова о том, что киберпреступления осуществляются в сфере информационных технологий, так как согласно ФЗ 149 от 27.07.2006 г. «информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов» [42]. Поэтому для характеристики термина киберпреступность резонно будет утверждать, что само преступление осуществляется с использованием информационных технологий.

Так Т.Л. Тропина в своем диссертационном исследовании предложила следующее определение киберпреступности: «это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей или компьютерных данных» [38, с. 36]. По нашему мнению, в данной формулировке просматривается схожесть определения с термином, предложенным на конгрессе Организаций Объединенных наций, но важным и правильным является акцент на киберпространство именно оно, как мы считаем, является источником зарождения и развития киберпреступности.

Поэтому киберпространство и киберпреступность взаимосвязанные понятия, так как преступления совершаются в определенной информационной среде.

И.М. Рассолов предложил следующее определение киберпреступности: «как общественно опасное деяние, которое совершается с использованием средств компьютерной техники в отношении информации, обрабатываемой и используемой в Интернет». [32, с. 135].

Авторская формулировка И.М. Рассолова, так же имеет в своем содержании ограничения применительно к обработке информации в сети интернет, так как полученная преступным путем информация в дальнейшем может быть использована в различных направлениях и уже не ограничивается ее применение только в сети Интернет.

Следует обратить внимание на подходы к киберпреступности компаний разработчиков программных продуктов, позволяющих защитить информационное пространство организаций и физических лиц, одной из наиболее распространенных программ защиты является антивирус Касперского. Компания, реализующая данные программные продукты предлагает следующий подход к определению киберпреступности: «Киберпреступность – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство. Большинство кибератак совершается киберпреступниками или хакерами с целью получения финансовой прибыли. Однако целью кибератак может быть и выведение компьютеров или сетей из строя – из личных или политических мотивов» [48].

Онлайн проект «Обзор электронной коммерции» подробно рассматривает тему киберпреступности, так термин киберпреступление: «это преступление, совершенное в киберпространстве, представляющее собой противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ» [12].

Именно это определение, по нашему мнению, является наиболее верным в отражении сути киберпреступности, так как дополняет раннее представленные авторские термины формулировкой «противоправного вмешательства» и «общественно опасных действий».

В связи со множественностью подходов к определению киберпреступности думаем, что можно использовать обобщенный и расширенный подход.

Сегодня киберпреступление или компьютерную преступность рассматривают в различных аспектах используя обобщенное значение, где термин, предложенный в зарубежной литературе, является на наш взгляд наиболее подходящим: «это широкий спектр действий, связанных с использованием информационных технологий в преступных целях» [34].

Для отражения расширенного подхода к термину киберпреступности предложим следующее определение – это общественно опасное деяние, посягающее на информационную безопасность через киберпространство с использованием компьютерных систем, сетей, направленных против собственности, авторских прав, общественной безопасности или нравственности и т.д. [26].

В диссертационном исследовании Е.С. Шевченко предложено криминалистическое определение понятия: «Под киберпреступлением следует понимать 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» [49, с. 8]. Данная формулировка рассматривает криминалистическую составляющую термина киберпреступление.

Подводя итог первому параграфу магистерской диссертации, отметим, что нами рассмотрены исторический аспект появления киберпреступности, охарактеризован прогрессивный рост данных преступлений на основе обобщенных данных следующих ведомств и организаций:

- отдела МВД,
- генеральной прокуратуры,

– агентства информационной безопасности.

Выявлены различия в подходах к определению киберпреступности в науке уголовного права.

Для дальнейшего рассмотрения тематики магистерской диссертации необходимо рассмотреть понятие киберпространства в трактовке различных исследователей, а также предложим рассматривать данное пространство с точки зрения системного подхода к данным преступлениям.

Необходимо выявить отличительные особенности киберпространства и соответствующие критерии классификации преступлений.

1.2 Система преступлений в киберпространстве

Рассматривать киберпреступность невозможно без характеристики его составляющей – это киберпространство.

Само определение состоит из двух составляющих «кибер-» (cyber-) и «пространство» (space) и в Оксфордском словаре первая часть проводится как правители, то есть интерпретируя словосочетание получаем управление пространством [54].

Исторически киберпространство и киберпреступность развиваются совместно, основой их появления и развития является технический прогресс, который определен использованием информационных технологий. Освоение данного сектора отдельными специалистами приводит к возникновению и росту преступности в новом направлении.

О историческом появлений словосочетания кибер и пространство впервые упомянул фантаст Уильям Гибсон 1984 г. в романе «Нейромант» («Neuromancer»), он описал его как масштабное, массовое и виртуальное явление: «Киберпространство. Коллективная галлюцинация... Графическое представление данных, извлекаемых из банков памяти любого компьютера в человеческой системе... Световые линии, расчертившие кажущееся пространство разума», – писал Гибсон [6, с. 273].

В своем произведении автор-фантаст рассматривал влияние на человечество будущего информационных потоков, многие вопросы, поднятые автором в прошлом столетии, становятся актуальными только сейчас, получить однозначный ответ о влиянии информационного мира на мир реальный не получится.

Современная реальность и достигнутый технологический прогресс стимулирует развитее дискуссии вокруг данного термина, который расценивается, как новый мир компьютерных коммуникации (computermediated communication, CMC). Текущая интерпретация «кибер» все чаще упоминается, как связь с сетями электронных коммуникаций и виртуальной реальностью.

В научной сфере появились исследовательские работы, определяющие подход к новому термину «киберпространство». С.Н. Хуторной в диссертации предлагает следующее определение: «киберпространство представляет собой компьютерно-технологическую виртуальную реальность, характеризующуюся соединением гипертекста и гиперреальности, интерактивностью, модификацией пространственно-временных черт, разнонаправленностью пространственно-временных потоков и их многомерностью и дискретностью» [46, с. 7].

Р.А. Барышев предлагает следующее определение: «киберпространство – это одна из множества форм виртуальной реальности, при этом если виртуальная реальность обозначает большой круг явлений от кинематографа и музыкального произведения до зеркального отражения, снов и фантазий, то киберпространство в свою очередь четко очерчивает виртуальную реальность границами взаимодействия человека и компьютера ... – это метафизическая абстракция, применяемая для описания объектов, широко распространённых в компьютерной сети» [1, с. 56].

Обе формулировки определения киберпространства рассматривают его как виртуальную реальность, поэтому ряд авторов такое определение посчитали не точным и предложили другой подход к рассмотрению.

Считаем важным отметить, что из себя представляет виртуальная реальность – это искусственная среда, создаваемая путем воздействия технических и электронных устройств на ощущения человека, через способность имитировать функции объектов реального мира: зрение, слух, осязание [56, с. 45]. Таким образом в киберпространстве отсутствует стимуляция каких-либо искусственных процессов в организме пользователей, в нем функционирует объективный информационный мир.

Другую трактовку термина киберпространства предлагает Д.Е. Добринская, она предполагает равенство формулировок киберпространства с цифровой средой и дает следующее определение в своей публикации: «это пространство функционирования продуктов информационно-коммуникационных технологий, позволяющих создавать чрезвычайно сложные системы взаимодействий агентов с целью получения информации, обмена и управления ею, а также осуществления коммуникаций в условиях множества различных сетей» [7, с. 59]. В данной трактовке автор выделяет агентов и ссылается на чрезвычайно сложные системы взаимодействия, по нашему мнению, вопрос сложности системы является спорным, так как в любой сфере существуют профессиональные и непрофессиональные пользователи.

Для того чтобы сопоставить понятия киберпространства и цифровой среды воспользуемся диссертационным исследованием И.Н. Теркуловой в котором предложена следующая формулировка: «Цифровая среда – искусственная среда, являющаяся непрерывной последовательностью компьютерных и сетевых технологий, организующая отношения между объектами физического мира посредством передачи программ в виде сигналов по сетям и телекоммуникационным каналам» [36, с. 6].

В формулировке данного автора на наш взгляд присутствуют некоторые неточности в фразе непрерывной последовательности и передачи программ, мы предполагаем, что необходимо внести корректировку в данное определение цифровой среды.

А.Е. Войскунский рассматривает киберпространство как «возможностей для бесчисленных способов самовыражения» [3, с. 64].

Профессор В.А. Плешаков, отмечает, что «киберпространство – это новое пространство и социализирующая среда социального сетевого… взаимодействия, обеспечивая выход на новый уровень организации и реализации жизнедеятельности человека XXI века» [31].

В Российской Федерации в 2013 году в Проекте Концепции Стратегии кибербезопасности опубликовано, что: «Киберпространство – это сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов сети Интернет и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)» [16].

Информационное пространство, в этом же документе рассмотрено как: «сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию» [16].

В диссертационном исследовании Шевченко Е.С. предложила следующее определение киберпространства: «это область взаимодействия информационных систем различного уровня, включающих следующие элементы: компьютер, компьютерные системы, сети (как глобальные, так и локальные), компьютерные программы пользователей, а также данные, циркулирующие в перечисленных элементах» [49, с. 8]. Данное определение обезличивает существование самого пространства, так как его существование не возможно без пользователей и создателей (руководителей, управляющих), а в определении автора информационная система функционирует обособлено.

Обобщив авторские и исследовательские подходы остановимся на термине М.А. Простосердова предложенном в диссертации, в которой

киберпространство определено как: «искусственно созданная среда, существование которой ограничено информационно-телекоммуникационной сетью, пользователи которой могут свободно вступать в административные, гражданские, уголовные и другие правоотношения. Киберпространство может появиться в любой информационно-телекоммуникационной сети. Например, в рамках сети «Интернет» можно говорить об «Интернет-пространстве». Следовательно, «Интернет» – это не само «киберпространство», а лишь условие, в котором оно может существовать» [29, с. 22].

Согласно решения Верховного Суда США в 1997 году Интернет определяется как «глобальное объединение компьютерных сетей и информационных ресурсов, не имеющее четко определённого собственника и служащее для интерактивной коммуникации физических и юридических лиц» [51].

Рассмотрим киберпреступления в киберпространстве с точки зрения системного подхода, так как данный подход является основополагающим в современной науке и позволяет выявить скрытые особенности при построении системы.

В научных публикациях рассмотрены различные подходы к определению «система». Несмотря на различия формулировок, все они базируются на первоначальном переводе с греческого слова systema – целое, составленное из частей, соединенное.

Попробуем охарактеризовать понятие системы преступлений, так как данное определение отсутствует в научных публикациях.

В действующем УК РФ в ст. 14 дано следующее определение: «преступление — это виновно совершённое общественно опасное деяние, запрещённое уголовным законом под угрозой наказания» [39].

Предложим авторское определение «системы преступлений», так будем рассматривать в нашем исследовании систему преступлений, как группу определенных факторов, имеющих отличительные особенности

применительно к отдельным составам преступлении, предполагающих действующим законодательством страны определенное наказание.

В рамках магистерской диссертации согласимся с исследованиями Д. Кларка, в которых киберпространство рассматривается в многоуровневом аспекте. Рассмотрим систему преступлений в киберпространстве с учетом группы факторов, представленных различными уровнями.

Первой группой являются физические факторы, к которым относятся аппаратные устройства (датчики, маршрутизаторы, спутники, носители и т.д.).

Вторая группа представлена логическими факторами и включает в себя программное обеспечение (коды, протоколы, скрипты и т.д.).

Третья группа факторов является информационными и представлена информацией в различном состоянии (воспроизводство, трансляция, хранение, передача, обработка и т.д.).

Четвертая группа факторов является социальной, представлена людьми, создающими и использующими киберпространство [52].

Соответственно в этой многоуровневой системе совершаются киберпреступления в киберпространстве, которые представлены общественно опасными деяниями преследуемым по закону.

Представленная система преступлений в киберпространстве характеризуется взаимосвязью всей группы факторов. Данная система позволяет отслеживать взаимосвязь и закономерности влияния тех или иных факторов применительно к составу преступлений, совершаемых в киберпространстве.

Однако важной составляющей системы данного вида преступлений является киберпространство, в котором она функционирует, необходимо более подробно остановится на характеристике самого киберпространства.

Рассмотрим каждую группу факторов более подробно.

Физические факторы представлены на современном этапе разнообразными моделями компьютерных устройств, которые инициируют, маршрутизируют и завершают данные. Они могут включать в себя хосты

(персональные компьютеры, телефоны, серверы), а также сетевое оборудование и т.д. Компьютерная сеть, либо сеть передачи данных, позволяет узлам совместно использовать ресурсы, что позволяет устройствам обмениваться данными с помощью линией передачи данных на кабельных носителях или по беспроводным технологиям. Самая известная компьютерная сеть – это Интернет.

Логические факторы представлены множеством программ позволяющим осуществлять информационное взаимодействие, а также работу технических устройств по сохранению обработке и передачи данных и т.д.

Если рассматривать социальную группу факторов, то важно выделить ее обширность, так как она представлена не только отдельной личностью, а всеми видами социумов, таких как:

- правительство;
- организационные структуры и управленческие структуры всех видов и организационно-правовых форм;
- все категории людей, являющихся пользователями виртуального пространства [33].

Информационная группа факторов определяется удобством использования различных ресурсов в сети, образованной киберпространством.

Президент Российской Федерации В.В. Путин в своем выступлении акцентировал внимание на том, что «Интернет возник как спецпроект ЦРУ США, так и развивается» [33].

Интернет, социальные сети, поисковые машины имеют двойное назначение хотя данная информация массово не распространяется.

Таким образом, предложенная четырехфакторная модель функционирует в киберпространстве. Как нами было отмечено ранее киберпространство, является управляемой системой (пространством), у которой есть собственники и руководящая структура, а информация изначально, как было определено при создании сетей подлежит копированию.

Во втором параграфе магистерской диссертации нами рассмотрено понятие киберпространства с учетом авторских подходов различных исследователей.

Выявлены различия в подходах к определению киберпространства в научных кругах, так даны авторские комментарий к определениям различных исследователей.

В результате проведенного исследования подходов к характеристике и определению термина киберпространства ряд исследователей предлагает многоуровневый подход, нами предложено рассматривать киберпространство с точки зрения системного подхода.

Дано авторское определение системы преступлений, рассмотрена система, представленная группой факторов образующую модель, которая функционирует в киберпространстве в том числе при совершении киберпреступлений.

Для дальнейшего рассмотрения темы исследования в магистерской диссертации необходимо выделить и рассмотреть факторы, определяющие специфику киберпреступлений преступлений, реализуемых в киберпространстве, для этого предложим различные критерии и подходы к классификации киберпреступлений.

1.3 Отличительные особенности и характеристика киберпреступлений

Как нами было обозначено в первом параграфе данной работы наблюдается прогрессивный рост киберпреступлений, по нашему мнению, это обусловлено рядом факторов. В данном исследовании выделим наиболее очевидные и значимые факторы влияющие на рост преступности в киберпространстве.

Перечислим факторы, характеризующие киберпространство и определяющие привлекательность киберпреступлений для преступного мира:

это неосязаемость, мобильность, автономность, массовость, анонимность, латентность, дистанционность.

Одним из первых факторов является неосязаемость киберпространства. Данное пространство не осязаемо, т.е. не является объектом материального мира, отсутствует возможность физического восприятия киберпространства, так же его нельзя соотнести с определенными территориальными границами.

Другим фактором является мобильность. Киберпространство мобильно его состояние изменчиво, действия, реализуемые в данном пространстве подвижны и не привязаны к территориальному и временному пространству.

Следующий фактор — это автономность. Киберпространство нужно рассматривать как отдельный мир, который существует по своим законам, попытки контролировать его на законодательном уровне предпринимает множество стран, но динамика преступлений и прогрессивный рост данного сектора свидетельствует об обратном. То есть на сегодняшний момент, киберпространство является автономной системой и не подчиняется законодательным нормам какой-либо определенной страны, так же отсутствует единый международный подход к контролю данной системы и не отработан механизм взаимодействия между структурами различных стран по оперативному пресечению данного направления преступлений и их расследованию.

Четвертый фактор, характеризующий киберпространство в преступном направлении – это массовость. Киберпространство используется во всех сферах и им охвачено большинство населения мира, что и создает благоприятную среду для роста и развития данного направления преступности. То, что киберпространство является международным, мировым явлением подтверждают данные отчётов о глобализации цифрового рынка, так при населении мира 7,593 миллиардов человек, количество пользователей Интернета в 2018 году составляет 4,021 млрд человек, а социальные сети массово используются как масштабные рекламные компаний в продвижении товаров и услуг [9].

Пятый фактор киберпространства, как преступного сектора – это анонимность, что позволяет преступнику чувствовать себя в безопасности и дает ощущение безнаказанности, так как пользователи могут скрывать свои данные или использовать чужие имена.

Шестой фактор — это латентность киберпреступлений. С учетом современной международной обстановки и состоянием криминалистической тактики расследования данного направления преступности специалисты Национального отделения ФБР США считают, что не выявленные киберпреступления составляют от 85% до 97%. Факторами высокой латентности считают отсутствие обращений от пострадавшей стороны в правоохранительные органы по разным причинам, например юридические лица в большинстве случаев пытаются решить проблемы нанесенные киберпреступниками самостоятельно, а физические лица не обращаются в правоохранительные органы при незначительном ущербе, а также по личным причинам, когда подвергаются шантажу или вымогательству в социальных сетях и т.д. Выявлены факты не регистрации обращений по киберпреступлениям в правоохранительных органах с целью получения положительных отчетов о деятельности следственных органов и снижении статистики нераскрытых преступлений. Таким образом, уровень латентности по киберпреступлениям предположительно является наиболее высоким, с учетом, что сама преступность и способы совершения данных преступлений становится все более инновационной путем разработки и внедрения новых программ. Поэтому предположить реальный масштаб и ущерб от данных преступлении не представляется возможным.

Дистанционность – это отсутствие прямого физического контакта между преступником и потенциальной жертвой киберпреступления. Как нами было описано ранее преступник и объект преступного посягательства (или потерпевший) могут находиться на разных территориях, а в большинстве случаев в разных государствах. Технологические возможности

киберпреступности позволяют в автоматическом режиме осуществлять преступную деятельность одновременно в направлении нескольких объектов.

В ходе расследования киберпреступлении в большинстве случаев с учетом фактора дистанционности потерпевший не всегда моментально узнает, что подвергается в определенный момент преступному воздействию.

На современном этапе с учетом возросшей актуальности к расследованию преступлений в киберпространстве теоретики и практики юридических наук выделяют такие критерии для классификации данных преступлений как средства, способ совершения, цель, объективный признак и субъективная составляющая киберпреступлений, в данном исследовании дополним выделенные ранее критерии территориальным признаком, временным интервалом, характером совершения преступления, составом участников [18].

Рассмотрим различные критерии, по которым можно выделить группы факторов характеризующих систему киберпреступлений и в дальнейшем применять их с целью классификации преступлений в киберпространстве.

Первый критерий территориальный: международные (трансграничные) преступления охватывают несколько стран. В данном контексте место преступление может фиксироваться в нескольких странах начиная от заказчика, место нахождения преступника, место информационной атаки и место хранения полученной информации.

Национальные (региональные, местные) киберпреступления осуществляются на соответствующей территории РФ и подпадают под действие отечественного законодательства.

По временному интервалу такие преступления можно классифицировать на краткосрочные (мгновенные) и продолжительные длящиеся, отличаются они временным интервалом совершения преступления (количеством атак: единичные, многократные) [17, с. 416].

По характеру совершения преступления публично и анонимно.

Уже фактически ежедневно можно увидеть в СМИ информацию о взаимных кибератаках между государствами: «Хакеры Killnet взломали сайт группировки Anonymous, которая ранее атаковала российские государственные интернет-порталы и СМИ». Таким образом такие преступления реализуются публично по итогу их совершения.

Анонимные преступления не имеют прямого контакта межу потерпевшим и преступником, что является одной из наиболее привлекательных составляющих киберпреступлений. В данном случае сфера киберпространства является наиболее приемлемой «средой обитания» различного рода преступников.

По составу участников преступлений в киберпространстве можно выделить индивидуальное или групповое, сегодня известны организованные преступные группы и целые сообщества киберпреступников, как нами было описано ранее, по данным исследований, доходы от киберпреступности в группах значительно превышают заработок от данных преступлений у индивидов.

По спектру преступлений: экономические направленные на финансовое обогащение и информационные направленные на получение, распространение информации, либо организацию сбоя в работе информационных систем.

Средствами таких преступлений являются компьютерная техника, мобильные телефоны и иные информационные носители, имеющие доступ либо временно подключаемых к телекоммуникационным сетям, технологической инфраструктуре.

Наиболее распространенными способами совершения киберпреступлений в киберпространстве являются:

Первый способ – это использование вредоносных программ, для заражения объекта воздействия, которые могут вывести из строя компьютерную технику, как корпоративную, так и индивидуальную. Данный способ совершения преступления позволяет удалять или похищать данные с устройств.

Второй способ – использование DDOS атак осуществляется путем множества запросов с целью повредить или вывести из строя объект воздействия, такие преступления осуществляются преступной группой использующей ботнеты (сеть устройств пользователей, зараженных вредоносными программами), позволяют не только похищать данные, но могут иметь и политические мотивы.

Третий способ – это комбинация вредоносного кода и социальной инженерии, реализуется путем перехода по ссылкам (фишинг), посещение сайтов, предоставления доступа к данным путем прямого контакта по телефону (социальная инженерия) данный способ позволяет получить доступ к информации.

Четвертый способ реализуется путем шифрования сообщений и использованием анонимных профайлов, что позволяет преступникам скрывать следы и осуществлять таким путем шантаж, вымогательство, запугивание и т.д., распространять запрещенный или незаконный контент [13].

По объективному признаку киберпреступления можно разделить следующим образом:

- направленные на определенную личность – физическое лицо, являются самыми распространёнными, по многим причинам и могут быть направлены как на личные данные, так и на финансовую составляющую;
- направленные на юридическое лицо, так как их статус в соответствии с отечественным законодательством в рамках реализации, прав и обязанностей отличается от статуса гражданина, но интересен для киберпреступников и позволяет получить доступ к конфиденциальной информации, технологиям и прочее;
- направленные против государства и государственного устройства, связно с работой правительственных учреждений, банковского сектора, государственных предприятий и служб, региональных и муниципальных администраций, политических партий т.д.

Цель киберпреступлений и субъективную составляющую рассмотрим во второй главе данной магистерской диссертации.

Таким образом, в результате исследования в первой главе можно сделать ряд выводов и обобщений. Так нами рассмотрены теоретические подходы к пониманию определений киберпространства и киберпреступности в научных кругах, выявлены различия в понимании данных терминов, предложено авторское понимание киберпреступности. Предложена модель киберпространства с учетом определяющих факторов в которой осуществляются киберпреступления.

Дано авторское понимание факторов киберпространства и киберпреступности, дополнены критерии классификации, ранее применяемые к данным преступлениям.

Для дальнейшего раскрытия темы магистерской диссертации нам необходимо рассмотреть в следующей главе работы особенности криминалистической тактика следственных действий при расследовании киберпреступлений.

Глава 2 Криминалистическая тактика следственных действий в расследовании киберпреступлений

2.1 Киберпреступления в криминалистике их классификация

В Российской Федерации существуют организаций, которые занимаются борьбой с киберпреступлениями. Например, Министерство внутренних дел России имеет отдел, который специализируется на киберпреступлениях. Также существуют и частные компании, которые предоставляют услуги по защите от киберпреступлений.

Киберпреступления стали серьезной мировой проблемой, поэтому криминалистика играет важную роль в борьбе с ними. Поэтому в данной работе считаем важным рассмотреть различные подходы к классификации киберпреступлений в криминалистике используемые отечественными и зарубежными криминалистами.

Рассмотрим данный вопрос с актуализации значения классификации в криминалистике. Классификация в криминалистике является важным инструментом расследования преступлений и разработки мер по их предотвращению.

Классификация киберпреступлений - это систематизация и распределение преступлений, связанных с компьютерными технологиями и сетевыми технологиями, на основе их характеристик и свойств. Позволяет более точно определять и анализировать киберпреступления, а также разрабатывать меры по их предотвращению и эффективному расследованию, обеспечивая необходимый уровень информационной безопасности для функционирования государства, учреждений и общества.

Существует несколько традиционно используемых в литературе по криминалистике подходов к классификационным признакам. Рассмотрим некоторые из них.

По характеру преступления делятся на умышленные и неосторожные. Умышленные преступления, в свою очередь, разделяются на преступления, совершенные с прямым умыслом и преступления, совершенные с косвенным умыслом.

По месту совершения преступления включает в себя киберпреступления, совершенные через интернет, внутри компьютерных систем, в сетях связи, а также киберпреступления, совершенные с использованием мобильных устройств и других технологий.

По количеству участников преступления делятся на групповые и индивидуальные. Групповые преступления совершаются несколькими лицами, индивидуальные - одним лицом.

По субъекту преступления делятся на преступления, совершенные физическими лицами, и преступления, совершенные юридическими лицами.

По характеру последствий преступления делятся на тяжкие, средней тяжести и легкие, в зависимости от тяжести причиненного вреда.

По степени общественной опасности. Преступления делятся на особо тяжкие, тяжкие, средней тяжести и легкие.

Классификация по типам нарушений включает в себя киберпреступления, связанные с нарушением авторских прав, финансовыми мошенничествами, кражей личных данных, кибершпионажем, кибертерроризмом, кибербуллингом и другие [2].

Классификация по типам объектов нарушений включает в себя киберпреступления, связанные с нарушением прав государства, нарушением прав частных лиц, нарушением прав бизнеса, а также киберпреступления, связанные с нарушением прав на интеллектуальную собственность.

Классификация по типам инструментов и технологий, используемых в преступлениях, включает в себя киберпреступления, связанные с использованием вирусов, троянов, ботнетов, фишинга, скимминга, ддос-атак и других.

Киберпреступления в криминалистике классифицируются по механизму атаки, целевой аудитории и типу предназначения.

Каждый тип атаки имеет уникальные характеристики, которые требуют соответствующих методов расследования и идентификации.

Во-первых, атаки на системы и приложения. Этот тип киберпреступлений направлен на атаку на различные системы и приложения, включая операционные системы, мобильные устройства и программный софт. Часто используются методы фишинга и социальной инженерии для получения доступа к данным пользователей или компаний. Например, в 2019 году был зафиксирован рост числа таких атак на мобильные устройства - на 50% по сравнению с 2018 годом. Одним из самых распространенных механизмов атак является фишинг, когда злоумышленники отправляют письма, которые выглядят как официальные, от банка, социальной сети или государственного учреждения. Цель – заставить получателя открыть вредоносную ссылку или прикрепленный файл, которые содержат вирусы или трояны. Еще одним распространенным видом атак является утилитарный вредоносный код, который позволяет злоумышленникам получать доступ к личной информации пользователя. Они могут использовать его для вымогательства, продажи или публикации в общественном доступе. В последнее время активно использование атак на мобильные устройства, которые стали значительно популярнее для использования онлайн-сервисов [11].

Во-вторых, атаки на блокчейн-технологии. Этот тип киберпреступлений позволяет злоумышленникам получить доступ к цифровым токенам и нарушить целостность блокчейн-сети. Такие атаки могут привести к утрате доверия пользователей и серьезному ущербу компаний, которые используют эту технологию. В 2019 году был зафиксирован рост числа атак на блокчейн-системы на 300% по сравнению с предыдущим годом.

В-третьих, атаки на технологии искусственного интеллекта (ИИ). Это новый вид киберпреступности. Злоумышленники используют искусственный интеллект для улучшения программного обеспечения и создания новых атак.

Это может привести к увеличению числа успешных кибератак и повышению уровня угрозы.

В-четвертых, преднамеренные атаки внутри компаний. Такие атаки могут привести к утечке конфиденциальных данных и нанести серьезный ущерб бизнесу.

Целевая аудитория киберпреступлений является разнообразной и включает в себя как частных пользователей, так и крупные компании, финансовые институты, государственные и научные организации, а также пользователи социальных сетей и мессенджеров.

Атаки киберпреступников могут быть направлены на получение финансовой выгоды, шпионаж, нанесение вреда конкурентам, уклонение от налогов, вымогательство и т.д. Например, в 2020 году был раскрыт крупнейший в мире киберпреступный синдикат, который украл более 100 млн. долларов при помощи вредоносных программ и фишинга [11].

Для злоумышленников наиболее привлекательными являются объекты, содержащие большое количество ценной информации, такой как личные данные пользователей, платежная информация, банковские реквизиты, коммерческие секреты и т.д.

В 2019 году 71% всех кибератак были направлены на малые и средние предприятия. Это связано с тем, что такие компании обычно не имеют достаточных ресурсов для обеспечения эффективной кибербезопасности сотрудников и инфраструктуры. В результате, злоумышленники могут легко получить доступ к конфиденциальным данным, чего они не могут добиться в крупных организациях.

Одним из наиболее распространенных типов киберпреступлений является фишинг, который используется для кражи личных данных пользователей. В 2019 году общее количество атак фишингом увеличилось на 65%, в то время как злоумышленники получили на 14% больше информации в результате этих атак.

Еще один тип киберпреступлений – это рэнсомвэр. За прошедший год количество атак рэнсомвэром увеличилось на 41%, а суммы, требуемые за расшифровку данных, в ряде случаев превышали несколько десятков миллионов долларов.

Другим распространенным типом киберпреступлений являются DoS и DDoS-атаки, которые могут нанести серьезный ущерб компаниям и организациям. В 2019 году было зафиксировано более 4,8 миллиона DDoS-атак.

Рассмотрим виды киберпреступлений:

- кража банковских данных: в 2019 году компания «Capital One» подтвердила утечку личных данных 100 миллионов ее клиентов, в результате которой были украдены имена, адреса, номера социального страхования и другие личные сведения;
- компьютерные вирусы: в 2017 году вирус «WannaCry» атаковал компьютеры в 150 странах мира, блокируя доступ к компьютерным системам и требуя выкупа;
- кража учетных записей: в 2020 году была обнаружена утечка данных пользователей социальной сети «Facebook», в результате чего было скомпрометировано более 500 миллионов учетных записей.

Из-за характера киберпреступлений, их часто не удается раскрыть и привлечь злоумышленников к ответственности. Но благодаря развитию технологий и более серьезному отношению к кибербезопасности, возможности раскрыть преступные действия в Интернете становятся все больше.

Для борьбы с киберпреступлениями необходимо правильно классифицировать тип атаки и принимать соответствующие меры по защите от нее. Кроме того, необходимо строго соблюдать правила безопасности, чтобы не стать жертвой киберпреступников.

Зарубежная криминалистика также имеет множество классификаций киберпреступлений, похожих на те, что используются в России. Существует некоторое разнообразие в терминологии и подходах.

Например, классификация киберпреступлений может основываться на месте совершения преступления, типах нарушений, типах объектов, которые были нарушены, а также на типах инструментов, используемых при совершении преступления.

Некоторые зарубежные исследователи также используют другие критерии классификации, такие как масштаб преступления, характер жертвы и так далее.

Классификация киберпреступлений в зарубежной криминалистике позволяет более точно определять и анализировать различные типы киберпреступлений, что помогает в разработке мер по их предотвращению и борьбе с ними.

Среди авторов, которые изучают киберпреступления и их классификацию, можно выделить: Кевин Митник (Kevin Mitnick) - известный американский хакер и специалист в области кибербезопасности. Он является автором книги «Искусство обмана: Хакерские приемы социальной инженерии» и уделяет много внимания классификации киберпреступлений.

Рассмотрим классификацию киберпреступлений, предложенную Кевином Митником, он разделил все киберпретупления на шесть категорий.

Первая категория киберпреступлений, описанная Митником, – это фишинг. Фишинг - это мошенническая практика, которая использует ложные электронные письма и веб-сайты, чтобы обмануть пользователей и получить доступ к их личным данным, таким как пароли и финансовая информация.

Вторая категория – это вирусы и черви. Вирусы и черви - это злонамеренные программы, которые распространяются через компьютерные сети и могут нанести серьезный ущерб компьютерной системе, включая уничтожение данных и кражу информации.

Третья категория киберпреступлений - это кража личной информации. Кража личной информации - это преступление, которое включает в себя несанкционированный доступ к личным данным, таким как социальные страховые номера, адреса, номера телефонов и финансовые данные.

Четвертая категория – это DDoS-атаки. DDoS-атаки - это атаки на компьютерные сети, которые используются для перегрузки сетевых ресурсов и приводят к отказу в обслуживании.

Пятая категория – это кибершпионаж. Кибершпионаж – это преступление, которое включает в себя несанкционированный доступ к конфиденциальной информации, такой как секреты компаний, политические секреты и другая чувствительная информация.

Шестая категория – это кибертерроризм. Кибертерроризм - это использование компьютерных технологий для создания угрозы национальной безопасности, включая атаки на критическую инфраструктуру и другие важные объекты. Классификация киберпреступлений, которую предложил Кевин Митник является важный инструмент для понимания различных типов киберпреступлений, которые могут угрожать компьютерной безопасности. Разработка и использование эффективных методов защиты от киберпреступлений является важной задачей для обеспечения безопасности в сети [23].

Роберт Мюллер (Robert Mueller) - бывший директор Федерального бюро расследований (ФБР) США, известный американский юрист, специалист в области кибербезопасности, который рассматривает киберпреступления, как один из главных вызовов для национальной безопасности. Мюллер выработал свою систему классификации киберпреступлений, которая помогает организациям и правоохранительным органам понимать действия киберпреступников и осуществлять борьбу с различными видами киберпреступлений. Она состоит из четырех основных категорий, каждая из которых определяет конкретный вид киберпреступлений. Классификация киберпреступлений Р.С. Мюллера является важным инструментом для

разработки стратегий борьбы с киберпреступностью и предотвращения преступлений в киберпространстве. Она также помогает правоохранительным органам и компаниям разрабатывать более эффективные методы защиты от киберугроз [24].

Первая категория предложенная Р.Муллером включает в себя взлом с использованием методов «фишинга» (Phishing), «социальной инженерии» (Social Engineering), «спуфинга» (Spoofing) и «наклонной атаки» (Spear Phishing). Эта категория взлома, который происходит путем использования социальной инженерии с целью получения предоставляемой цели критической информации. Некоторые методы, используемые злоумышленниками для реализации этих атак, могут включать в себя поддельные веб-сайты, электронную почту и социальные сети. Эта категория может включать в себя мошенничество на распределенной логистике, совершение преступлений с использованием взломанной инфраструктуры и администрации.

Вторая категория представлена кибершпионажем (Cyber Espionage) и кражей интеллектуальной собственности. Включает в себя нарушения, которые имеют цель получение конфиденциальной информации наряду с повышением конкурентных преимуществ. Эта категория может включать в себя хищение прав на интеллектуальную собственность, вредоносные программы и шпионские программы, а также утечку данных.

Третья категория представлена кибератаками на критическую инфраструктуру. Включает в себя нарушение, связанное с нарушением критической инфраструктуры. Это могут быть атаки на энергосистемы, телекоммуникационные системы и системы транспорта и многие другие. Цель таких атак может быть нарушение работы системы и создание хаоса на территории, на которой расположена критическая инфраструктура.

Четвертая категория включает в себя ботнеты, краудфандинг и мошенничество в офлайн. Представляет собой множество нарушений, таких как мошенничество с использованием мошеннических веб-сайтов,

жульничество в социальных сетях и на биржах, кибератаки на финансовые институты и другие. Эта категория также включает в себя организованные преступления, связанные с киберпреступностью, и мировой проект военной безопасности.

Классификация киберпреступлений Роберта Мюллера является ценным инструментом для повышения бдительности в отношении технологических угроз. Она предоставляет правоохранительным органам и организациям возможности распознавать угрозы своей инфраструктуре и улучшать защиту своей информации от атак. Необходимо понимать, что киберпреступность постоянно развивается и классификация Роберта Муллера должна быть пересмотрена и дополнена в соответствии с новыми видами угроз в онлайн-пространстве. Роберт Мюллер также выделяет несколько общих признаков киберпреступлений, включая использование компьютерных сетей и технологий для совершения преступлений, использование интернета для коммуникации и координации преступной деятельности, а также использование анонимности и шифрования для скрытия следов преступления [25].

Классификацию киберпреступлений в криминалистике так же рассматривает и автор книги «Киберпреступность: понимание и борьба с ней» Майкл Маккарти (Michael McGuire). Он предложил систематизацию киберпреступлений на основе их особенностей и свойств. Криминалистическая классификация киберпреступлений Майкла Маккарти – это одна из первых и наиболее известных классификаций разработанная в 1995 году американским криминологом. Она включает в себя четыре категории киберпреступлений:

- компьютерные преступления: это нарушения, связанные с взломом, изменением и уничтожением данных, кражей или копированием информации, публикацией нелегальных или вредоносных программ и другими преступлениями, связанными с использованием компьютеров и сетей;

- компьютерные преступления, направленные на имущество: в эту категорию входят кражи или подделки клиентских данных, взломы банковских счетов, мошенничество и другие преступления, которые причиняют ущерб компаниям и организациям;
- компьютерные преступления, направленные на личность: сюда относятся кибербуллинг, кибердомогательство, онлайн-нападения на личность, распространение порнографических материалов, нарушения авторских прав и другие преступления, которые могут нанести ущерб психическому и эмоциональному здоровью человека;
- компьютерные преступления, связанные с национальной безопасностью: в эту категорию входят кибернападения на правительственные сайты, хакерские атаки на крупные корпорации, саботажные действия и другие преступления, которые могут нанести ущерб стране и ее экономической стабильности.

Такая классификация киберпреступлений помогает судебным экспертам оценить характер и масштаб преступления, установить причину и мотив преступления, а также принять меры по защите от подобных атак в будущем. Учитывая быстрое развитие киберпреступлений и новые виды их совершения, классификация Маккарти может потребовать дополнительной корректировки и усовершенствования.

М.Маккарти предлагает так же другой критерий классификации киберпреступлений на основе типов нарушений, которые они совершают, а также на основе целей их совершения. Он выделяет несколько основных типов киберпреступлений:

Кража личных данных – это киберпреступление, которое включает в себя незаконный доступ к личной информации, такой как пароли, номера социального страхования, финансовые данные и т.д. [34].

Фишинг – это киберпреступление, которое включает в себя обман пользователя, чтобы получить доступ к его личным данным или финансовым ресурсам.

Вирусы и черви – это киберпреступления, которые связаны с созданием и распространением вредоносных программ, которые могут нанести ущерб компьютерной системе или украсть личные данные.

Кибершпионаж – это киберпреступление, которое связано с несанкционированным доступом к конфиденциальной информации, такой как тайные государственные документы или коммерческие секреты.

В данном параграфе магистерской диссертации рассмотрены криминалистические подходы к классификации киберпреступлений на основе выделенных критериев: по характеру преступлений; по месту совершения; по количеству участников; по характеру последствий и т.д.

Рассмотрен критерий классификации в криминалистике по механизму атаки. Охарактеризован каждый тип атаки, так как ему соответствуют уникальные характеристики, которые требуют соответствующих методов расследования и идентификации. Дана характеристика целевым аудиториям, на которые направлены действия киберпреступников.

Рассмотрены категорий киберпреступлений, предложенные Кевином Митником, Роберт Мюллером и Майклом Маккарти.

2.2. Тактика производства отдельных следственных действий в расследовании киберпреступлений

Следственная ситуация – это комплексная оценка состояния уголовного дела, которое включает в себя всю доступную информацию о преступлении и подозреваемых, тактико-психологические и тактико-управленческие особенности расследования, а также организационные аспекты работы сотрудников правоохранительных органов».

Познавательный аспект рассмотрения следственной ситуации заключается в определении всех возможных версий преступления, выявлении улик и свидетельских показаний, анализе мотивов подозреваемых и многом другом.

Информационный аспект связан с оценкой имеющихся данных и их релевантности, а также с организацией процесса расследования и принятием решений в этой связи.

Знание и учет следственной ситуации позволяют эффективнее проводить расследование и принимать обоснованные решения. Интересно отметить, что расследование любого преступления в большей или меньшей степени связано с теми же общими элементами. Их правильное определение помогает следователям лучше понять суть происходящего и детализировать следственную ситуацию. Типичная следственная ситуация может быть описана в виде последовательности действий, которые выполняются в ходе расследования. Например, первым этапом может быть сбор данных о преступлении, затем – о личности преступника, далее – о месте и обстановке преступления и т.д.

В свою очередь, конкретная следственная ситуация имеет свои особенности, которые зависят от конкретного дела. Это может быть, например, наличие свидетелей, определенных свидетельских показаний или физических улик.

При расследовании уголовных дел возникают как общие, так и частные следственные ситуации.

Тактика производства отдельных следственных действий является важной частью расследования киберпреступлений. В обобщенном виде тактику производства следственных действий при расследовании киберпреступлений можно представить следующим образом [45].

Первым шагом в расследовании киберпреступлений является сбор информации. Следователи должны собрать как можно больше информации о преступлении, включая данные о жертвах, месте и времени совершения преступления, методах и инструментах, используемых для совершения преступления. Эта информация может быть получена из многих источников, включая жертв, свидетелей, компьютерные журналы и другие электронные данные.

Одним из основных следственных действий в расследовании киберпреступлений является анализ информации. Следователи должны анализировать собранную информацию, чтобы определить, какие действия были совершены, какие уязвимости были использованы, и какие данные были украдены или повреждены. Этот анализ может помочь следователям определить, кто может быть ответственен за преступление.

Другим важным следственным действием является изъятие доказательств. Следователи должны изъять все возможные доказательства, включая компьютеры, телефоны, флешки и другие электронные устройства, которые могут содержать информацию о преступлении. Информация с данных устройств должна быть проанализирована, чтобы определить, как совершалось преступление, какие цели преследовались и т.д.

Еще одним важным следственным действием является проведение допроса. Следователи должны провести допрос потерпевших, свидетелей и других лиц, которые могут иметь информацию о преступлении. Эти сведения могут помочь следователям получить дополнительные доказательства.

Тактика производства отдельных следственных действий является важной частью расследования киберпреступлений. Следователи должны собирать информацию, анализировать данные, проводить допрос и изымать доказательства, чтобы определить, кто может быть ответственен за преступление.

Для начального этапа расследования преступлений в сфере компьютерной информации наиболее типичны следующие ситуации:

Когда собственник или обладатель компьютерной информации самостоятельно выявил факт преступления и обнаружил лицо, его совершившее. В таких случаях проводятся:

- задержание подозреваемого,
- допрос подозреваемого,
- обыск по месту работы (службы) и жительства подозреваемых,
- осмотр места происшествия,

– осмотр изъятых носителей информации,
– допрос свидетелей,
– назначение судебных экспертиз,
– следственный эксперимент.

Если собственник или обладатель компьютерной информации самостоятельно выявил факт преступления, но преступник неизвестен.

Проводятся следующие действия:

– допрос заявителя,
– признание собственника или правообладателя потерпевшим,
– осмотр места происшествия,
– поручение органу, осуществляющему оперативно-розыскную деятельность, о поиске преступников и фактов, имеющих значение для дела,
– допрос свидетелей,
– анализ обстановки и выдвижение версий по каждому обстоятельству, подлежащему установлению,
– назначение экспертиз,
– установление субъекта преступления и его задержание [44].

Первым источником информации о преступлении может быть потерпевший. Обычно в таких случаях на место происшествия направляется следователь, который устанавливает обстоятельства преступления, допрашивает свидетелей и потерпевшего. Если виновник неизвестен, то полиция может начать поиск свидетелей и следов на месте происшествия.

Но иногда полиция получает информацию о преступлении из другого источника или находит следы на месте происшествия самостоятельно. В этом случае расследование может быть начато без участия потерпевшего. Важно, чтобы были получены следы преступления и собраны доказательства.

Для установления фактов и обстоятельств совершения преступления используются различные процессуальные действия. Это могут быть обыски, производство экспертизы, допросы свидетелей и другие. Благодаря этим

действиям дознаватели, следователи могут установить общую картину происшествия и найти виновного в преступлении.

Рассмотрим особенности проведения экспертизы при расследовании киберпреступлений.

На данный момент не существует единого подхода к названию и определению пределов компетенции экспертов. Как правило, они могут быть названы как эксперты по информационной безопасности, аналитики по программному обеспечению, инженеры по тестированию и др.

Несмотря на разные названия, компетенция этих экспертов сводится к тому, что они умеют проводить тестирование и анализ программного и аппаратного обеспечения, выявлять уязвимости таким образом, получить информацию о преступлении.

В первую очередь, это компьютерная экспертиза информационных систем и компьютерных средств. Эта экспертиза проводится с целью выявления следов, связанных с проникновением в компьютерную систему, хакерскими атаками, кражей информации и другими видами преступлений. Эксперты анализируют журналы безопасности, каналы связи и другие объекты, связанные с работой информационной системы.

Другой важный вид компьютерной экспертизы – судебная экспертиза цифровых доказательств. Эта экспертиза проводится для установления подлинности электронных документов и сообщений, а также выявления возможных искажений или подделок. Анализируются метаданные, открытые и закрытые ключи шифрования, а также другие характеристики, связанные с цифровым контентом.

Кроме того, существуют методы компьютерной экспертизы для установления причастности к преступлениям. Эксперты анализируют компьютеры, телефоны, планшеты и другие электронные устройства, связанные с подозреваемыми. В результате экспертизы выявляются следы использования запрещенных программ и связей с соучастниками преступных групп.

Одним из новых видов компьютерной экспертизы является использование специализированных систем для автоматического распознавания лиц. Этот вид экспертизы позволяет установить, кто находился в определенном месте в конкретное время при помощи камер наблюдения.

Каждый вид компьютерной экспертизы требует специфических знаний и навыков. Эксперты детально исследуют каждый объект для того, чтобы получить максимально полную информацию о происходившем преступлении.

Компьютерные эксперты являются неотъемлемой частью правоохранительных органов и быстро приспосабливаются к новым вызовам. При проведении судебной компьютерно-технической экспертизы (СКТЭ) очень важно определить вид экспертизы и задачу. Взаимодействие между следователем и экспертом, в том числе информационное, должно быть установлено на достаточно высоком уровне. Мнение ученых состоит в том, что необходимо определить род экспертизы, а конкретный вид будет уточнен экспертом. Важно понимать, какие действия необходимо произвести при проведении такой экспертизы и какая информация может быть извлечена из компьютерных данных [44].

Экспертные задачи могут быть идентификационными или диагностическими. Важно выбирать вопросы в соответствии с технической направленностью задачи. Вопросы не должны касаться правовых вопросов или стоимости объекта исследования. При составлении перечня вопросов необходимо согласование со специалистом. От правильного подхода зависит точность результата СКТЭ.

Сбор сравнительных образцов также необходим для проведения точного сравнительного анализа, что в свою очередь позволяет сделать более объективные выводы.

Судебно-компьютерная и техническая экспертиза (СКТЭ) - комплекс мероприятий, направленных на изучение и сбор информации, связанной с использованием компьютерной техники и средств вычислительной техники в различных сферах деятельности.

Перед проведением СКТЭ специалисты должны составить список вопросов, на которые должен ответить эксперт.

Обратимся к опыту Кевина Митника который предложил следующий криминалистический подход: «Считает, что для того, чтобы поймать киберпреступника, необходимо понять, как он работает и как работает его мышление».

Согласно криминалистическому подходу Кевина Митника, расследование киберпреступности должно включать следующие шаги:

- сбор данных: вся информация о преступлении, включая информацию о компьютерах, сетях и других устройствах. Сбор исходного кода, файлов, получение доступа к устройствам, на которых совершено преступление, и т. д.;
- анализ данных: на этом этапе происходит анализ собранных данных, включая выделение ценных данных и определение пути доступа преступника к системе, сбор и анализ цифровых следов.
- идентификация устанавливается личность преступника, место жительства и другая информация.
- арест – на этом этапе происходит задержание преступника и предъявление ему обвинения в совершении киберпреступления [23].

Данный подход предлагает собирать максимальное количество информации о преступнике, которая может быть скрыта за множеством аккаунтов и ников. Биография, местоположение, окружение, структура мышления, хобби, интересы – все это может иметь большое значение при определении личности киберпреступника.

Применение криминалистического подхода в расследовании киберпреступлений включает также установление мотива преступления. Мотивы могут варьироваться от желания получить выгоду до желания навредить кому-то. Определение мотива может помочь следователям сосредоточиться на персонах, которые могут иметь причины для совершения подобных действий.

В целом, криминалистический подход, пропагандируемый К. Митником, признан одним из самых эффективных в кибербезопасности. Это связано с тем, что он позволяет лучше понять намерения и действия злоумышленников, а следовательно, более эффективно бороться с киберпреступностью.

Важно отметить, что в настоящее время преступления, связанные с нарушением компьютерных систем, становятся все более распространенными. Благодаря компетенции следователей и осведомленности пользователей о правилах безопасности в интернете, можно бороться с подобными преступлениями.

Кроме того, стоит отметить, что способы совершения таких преступлений постоянно усложняются. Для борьбы с ними необходимо постоянно следить за их изменением, изучать литературу и обмениваться опытом в этой области. Ведь только так можно создать эффективную защиту от компьютерных преступлений и предотвратить их совершение в будущем.

В данном параграфе магистерской работы нами рассмотрены общие и частные подходы к тактике проведения следственных действий, охарактеризованы особенности проведения экспертизы при расследованиях киберпреступлений. Представлен криминалистический подход Кевина Митника в расследовании преступлений в киберпространстве. В следующем параграфе работы выделим отличительные особенности криминалистической тактики.

2.3 Отличительные особенности криминалистической тактики в расследовании отдельных киберпреступлений

Криминалистическая тактика в расследовании киберпреступлений имеет несколько отличительных особенностей, которые связаны с тем, что киберпреступления происходят в онлайн-среде.

Расследование преступлений в сфере компьютерной информации может поставить перед следователем фактически непреодолимые преграды.

В главе 25 УПК РФ сгруппированы следующие следственные действия [40]:

- обыск,
- выемка,
- личный обыск,
- наложение ареста на почтово-телеграфные отправления,
- контроль и запись переговоров,
- получение информации о соединениях между абонентами и (или) абонентскими устройствами.

По содержанию данных следственных действии можно предположить, что они объединены в отдельную главу УПК РФ по критерию поиска материальных или нематериальных объектов (информации).

Первые меры при расследовании киберпреступлений принимаются правоохранительными органами с привлечением IT-специалистов, работающими в сфере кибербезопасности. Их задача - сохранить цифровые доказательства, полученные на месте преступления, либо на устройстве, чтобы они могли быть использованы в дальнейшем при проведении расследования.

Как нами было рассмотрено в третьем параграфе работы, основные особенности расследования определяют, именно факторы киберсреды в которой происходят данные преступления. Мы выявили и обозначили следующую группу факторов, которые оказывают непосредственное влияние на криминалистическую тактику расследования:

- неосязаемость пространства, в котором совершаются киберпреступления;
- мобильность преступлений в онлайн - среде и отсутствие привязки ко времени и местоположению;

- автономность киберпространства, не подвластна правовым нормам отдельных государств, отсутствует глобальный подход к пресечению данных преступлений;
- массовое применение онлайн - технологий;
- отдаленность взаимодействия между преступником и потенциальной жертвой;
- анонимность преступления, поскольку потенциальная жертва не располагает информацией и возможностью подтвердить совершение киберпреступления определенным лицом или группой лиц.

Исходя из этих факторов, также можно выделить следующие особенности: как правило, в киберпреступлениях отсутствуют свидетели, что исключает проведение следующих следственных действий, таких как допрос свидетелей киберпреступлений. Следы преступления являются виртуальными и имеют свои особенности.

Криминалистическая характеристика преступления - это совокупность особенностей, характеризующих преступление как юридический, социальный и психологический факт, и определяющих его связь с обществом, личностью преступника и объектом преступления. Она играет важную роль в исследовании и расследовании преступлений, а существующее относительное единство ученых в ее определении дает возможность более точно и объективно анализировать преступления. Для успешного раскрытия и расследования преступлений необходимо учитывать все детали преступления.

С развитием технологий и дальнейшей интеграцией информационных систем возникает необходимость в анализе виртуальных следов. Извлечение и анализ виртуальных следов должны осуществляться с использованием современного программного и аппаратного обеспечения [30 с. 98].

Профессор В.П. Леонтьев разделил виртуальные следы на две категории: локальные и сетевые.

Локальные следы - это часть компьютера или устройства, которые использовались при совершении преступления, например, файлы кэша, файлы cookie или история браузера.

Сетевые следы, с другой стороны, создаются в результате использования Интернета или другой сети, например, электронной почты или записей чата [20]. Кроме того, виртуальные следы могут быть скрыты или зашифрованы, чтобы затруднить их обнаружение и анализ. Поэтому специалисты по кибербезопасности должны быть профессионалами высокого уровня, чтобы обнаруживать и проводить анализ таких данных.

Для классификации следов необходимо провести анализ структуры носителя, на котором возможно присутствие следов. Специалисты используют разнообразные методики, такие как техники восстановления и сбора информации, анализ файловой системы, метаданных и т.д. Проведя анализ, возможно выявление следов определенных видов преступлений, которые будут использоваться в дальнейшем расследовании [47].

Несанкционированный доступ к компьютерной информации является одним из видов преступлений. При проведении расследования данного вида преступлений следователю следует обратить внимание на очевидные обстоятельства, указывающие на такое преступление. К таким обстоятельствам относятся использование чужого логина и пароля для доступа к конфиденциальной информации, внедрение вредоносного ПО в систему, модификация или уничтожение данных, а также незаконное копирование информации [42].

Одной из основных особенностей расследования преступлений, связанных с компьютерной информацией, является необходимость доказать направленность действий преступника на охраняемую законом информацию. Это означает, что при расследовании подобных преступлений необходимо установить, что действия преступника были направлены именно на получение, изменение или уничтожение конкретной информации [43]. Кроме того, при

расследовании подобных преступлений необходимо установить наличие причинно-следственной связи.

Для того, чтобы привлечь преступника к уголовной ответственности за такие преступления, как нарушение правил эксплуатации компьютерной системы, необходимо также установить наличие существенного вреда, причиненного неправомерными действиями. Это означает, что правоохранительные органы должны установить, что действия преступника причинили существенный вред охраняемой информации или привели к нарушению функционирования компьютерной системы.

Важно учитывать все особенности расследования таких преступлений, чтобы обеспечить эффективное пресечение таких преступлений и защиту охраняемой компьютерной информации. При расследовании необходимо учитывать такие важные обстоятельства, как личность преступника и потерпевшего, материальные следы и обстановку совершения преступления.

В ходе расследования могут возникнуть различные ситуации, которые потребуют назначения экспертиз и сбора материалов, проведение осмотров и обыска.

Необходимость производства обыска может возникнуть в случае хищения данных, кражи личной информации, создания и распространения вирусов и других преступлений, возможных с использованием сетей интернет и телекоммуникаций.

Далее следует произвести изъятие всех возможных носителей информации, включая компьютеры, мобильные телефоны, флэш-накопители и другие устройства. Важно также не только изъять данные, но и защитить их от уничтожения или изменения.

Для успешного проведения обыска следователю необходимо ознакомиться с техническими способами хранения и передачи информации, а также иметь техническую поддержку со стороны экспертов-информатиков, следует учитывать возможность удаленного управления компьютерами и другими устройствами. Если они имеются, необходимо отключить удаленный

доступ и заблокировать их. Такие меры позволят обезопасить хранящиеся на компьютере или устройствах данные и предотвратить их утечку. Важно понимать, что информация, полученная как результат работы с информационными носителями, должна быть надлежащим образом зафиксирована и сохранена, чтобы она могла быть использована в дальнейшем при рассмотрении дела. Для этого используются специальные программные обеспечения и решения для создания копий жестких дисков и других носителей информации [55].

Тактика проведения обыска заключается в сохранении целостности доказательств, обеспечении соблюдения процессуальных правил и требований.

Каждый компьютер имеет свой уникальный IP-адрес, который могут использовать злоумышленники для скрытия своих действий.

Специалисты-эксперты должны иметь высокую квалификацию и обширные знания в сфере информационных технологий для эффективного проведения следственных действий и возможности восстановления уничтоженных или скрытых данных. При осмотре устройств определяется операционная система, фиксируются выполненные операции, и проводится анализ установленных программ, также снимается изображение с экрана.

Далее, проводится поиск информации на компьютере, которая может иметь значение для расследуемого преступления. Поиск может быть осуществлен как с помощью специализированного программного обеспечения, так и вручную посредством просмотра содержимого дисков [44].

По окончании осмотра и изъятия каждого устройства, необходимо составить протокол следственного действия, в котором должны быть указаны дата, время, место, обстоятельства и условия осмотра (обыска), а также результаты изъятия и наличие на устройствах информации, имеющей криминальную природу.

Также необходимо составить опись всех изъятых устройств, в которой указаны их марки, модели, серийные номера, название производителя, а также

их состояние, включая наличие повреждений. Эти документы служат основанием для дальнейшего расследования. Важно, чтобы процедуры осмотра и изъятия проводились в соответствии с установленными правилами и процедурами [50].

Компьютерное мошенничество - это преступление, связанное с использованием современных технологий для обмана и причинения вреда другим людям или организациям. Она основана на незаконном присвоении чужой собственности, которое может быть осуществлено путем взлома персональных данных, подмены финансовых транзакций, создания поддельных веб-сайтов или программ [14].

Компьютерное мошенничество может привести к серьезным экономическим и правовым последствиям для потерпевших, включая финансовые потери, утечку конфиденциальной информации и нарушение прав человека. Перспективы предотвращения подобных преступлений должны включать в себя обучение населения основам кибербезопасности, а также совершенствование системы выявления и пресечения преступлений в Интернете.

Общемировой проблемой является работа колл-центров, в которых целые организованные группы, осуществляют преступные действия, по разработанным схемам, путем обмана населения. Наибольшее распространение получили телефонные мошенники. Злоумышленники используют базы телефонных номеров, чтобы звонить и вымогать деньги у доверчивых людей.

Так глава Центрального Банка России отметила, что проблема мошенничества остается актуальной и требует внимания со стороны всех государственных органов и граждан.

Мошенники в колл-центрах используют - психологическое давление и уговоры. Первые роли занимаются звонками, которые направлены на привлечение внимания и установление контакта с жертвой. Вторые роли

занимаются более агрессивными действиями и специализируются на принуждении жертв взять кредит или перечислить деньги мошенникам [4].

Фишинг – один из способов киберхищения. Хакеры отправляют электронные письма, подделывая имена крупных компаний, банков или государственных учреждений, и просят получателей перейти по ссылке [19].

При переходе на сайт, который выглядит как оригинальный, жертва оказывается на странице, где злоумышленники могут заполучить личные данные, пароли и номера банковских карт [48].

Такие преступления могут расследоваться долгий период времени, поскольку дознавателю необходимо:

- получить показания потерпевшего, сотрудников отдела информационной безопасности банка, сотрудников интернет-провайдера;
- поручить проведение оперативно-розыскных мероприятий, направленных на установление лица, совершившего хищение;
- получить ответы банка о перечислении денежных средств со счета потерпевшего, снятии денежных средств с банкомата;
- получить ответы Бюро специальных технических мероприятий (подразделения МВД России) об установлении информации учетных записей в социальных сетях, электронной почтовой службы, информации об администрировании этих данных;
- при установлении личности хакера – произвести его задержание, решить вопрос об избрании меры пресечения, допросить в качестве подозреваемого, произвести обыск, изъять компьютерную технику, которая послужит объектом исследования компьютерно-технической экспертизы и пр.

В связи со сложностью расследования и большим количеством данных преступлений, наблюдается тенденция отказа следователей и дознавателей возбуждать уголовные дела и вынуждает выносить незаконные постановления об отказе в их возбуждении. «В таком случае потерпевшему необходимо

обжаловать этот документ вышестоящим надзирающим лицам, что, однако, может повлечь за собой передачу материала доследственной проверки то одному следственному подразделению, то другому» [14].

Много жертв попадаются на уловки мошенников, потому что они могут быть очень убедительными и использовать социальную инженерию, чтобы заполучить доверие. Например, они могут убедительно выдавать себя за сотрудников банка, полиции или другой организации. Они также могут обещать ложные выгоды или предложить выгодные условия, чтобы заинтересовать жертв.

Злоумышленники, владеющие психоанализом и знанием первоначальной информации о потенциальной жертве, могут убедить в необходимости выполнить определенную операцию и получить финансовую выгоду. Используя IP-телефонию и виртуальные номера, они могут звонить из любого региона или страны, так что жертва не подозревает о мошенничестве.

Наиболее распространенным способом мошенничества является воздействие злоумышленников через личную информацию и получение доступа к финансовым ресурсам, как правило, в таких преступлениях используются навязчивые телефонные звонки. Мошенники активно используют телефонные номера для разнообразных мошеннических схем. Их легко приобрести за небольшую сумму денег на Интернет-сервисах, которые предоставляют подобные услуги [4].

Также можно заменить номер на одной трубке в процессе переговоров и использовать голосовые тембры, чтобы обмануть доверчивую жертву.

Многие мошенники пользуются базами потенциальных жертв, которые можно купить на Даркнете за несколько долларов. Они могут обращаться к людям, обладающим значительными доходами или более финансово устойчивым, чтобы получить крупное денежное вознаграждение, для этого убеждают перевести деньги на определенный счёт. К сожалению, в информационном мире, личная информация подвергается постоянной угрозе, ее часто используют без нашего разрешения, либо получают незаконным

образом путем взлома государственных программ, данных телефонных операторов и т.д. Как оказалось, стоимость персональных данных зависит от различных факторов, таких как их количество, качество и актуальность [4].

Базы клиентов сайтов бесплатных объявлений могут быть куплены по довольно низкой цене, в то время как банковские документы с информацией о нашей финансовой ситуации или имуществе могут стоить очень дорого.

Получение баз данных для мошенников считается большой удачей, позволяющей сэкономить время и деньги. В основном, молодые люди возрастом от 18 до 25 лет, работающие в колл-центрах, не задаются вопросом о моральности своей работы, так как это быстрый способ заработать деньги без образования и опыта. В Украине мошенники не теряют времени и нанимают людей для проведения крупных афер. Некоторые из них даже стараются совмещать свою работу в мошеннической конторе с обычной, но после первой успешной аферы больше не могут вернуться к прежней работе.

Одна из таких аферисток, заработавших 170 тысяч евро, уже не желает возвращаться к обычному производству, зная, что она может заработать гораздо больше [4].

Следователи областного управления МВД Челябинской области озвучили статистические данные о раскрываемости преступлений связанных с кибермошенничеством, она составляет 20 %. За 2021 год кибермошенники похитили у жителей Челябинской области 1 млрд. 200 млн. рублей.

Полиция Южного Урала обнародовала данные статистики мошенничества в онлайн-среде.

За первое полугодие 2022 года зафиксированы следующие способы совершения преступлений:

- 958 случаев звонков от лжесотрудников банков;
- 189 случаев, когда гражданам сообщали, что их родственник стал виновником ДТП;
- 287 происшествий в работе на биржах;

– 1130 фактов обмана во время покупки товаров на сайтах бесплатных объявлений и в социальных сетях.

Обманутые киберпреступниками люди обращаются в отделение полиции. Полицейские нечасто прибегают к помощи специальной техники во время расследования таких дел. Мошенников задерживают сотрудники розыска, а не мощная аппаратура. Основными жертвами мошенников 27% составляют граждане от 31 до 40 лет, следующая группа 19 % - это люди от 41 до 59 лет. 17 % составляют граждане от 21 года до 30 лет [41].

Как прокомментировал раскрываемость преступлений связанных с кибермошенничеством заместитель начальника полиции по оперативной работе ГУ МВД России по Челябинской области Сергей Федерягин — «Без сотрудника сыска преступники не будут пойманы, техника тут не поможет. Сама техника - это сопутствующий инструмент работы. Необязательно иметь едва ли не компьютерный центр, нам достаточно сделать запросы в некоторые компании и определить провайдера. Если мы ловим киберпреступника, то главная наша задача – раскрыть не только это конкретное преступление. Мы берем его телефон, изымаем компьютер, отправляем все на экспертизу. Мы изучаем, связывался ли мошенник с кем-нибудь еще. Если задержанный совершал подобные преступления, то мы за это цепляемся и дальше расследуем».

Несмотря на то, что полиция проводит рейды на мошеннические конторы, судьба их владельцев остается неизвестной. Некоторые из них, вероятно, скрываются за границей.

Уровень раскрытия подобных преступлений довольно низкий, в городе Миассе Челябинской области в среднем ежедневно фиксируется пять преступлений связанных с кибермошенничеством, раскрывается одно. Главная проблема в борьбе с киберпреступностью – это закрытые интернет-площадки, зарегистрированные в других странах [41].

Даже после раскрытия преступления, не все украденные денежные средства, возможно, вернуть, так как преступники переводят сбережения в

виртуальную валюту. По информации полиции, за последние пять лет число преступлений с использованием IT увеличилось в три раза, до 522 тысяч случаев в 2022 году. При этом следствие не имеет права без суда приостановить операции по счетам.

Поэтому актуальным становится возможность замораживать расходные операции на счетах, подозреваемых в кибермошенничествах на срок до десяти дней без решения суда, путем внесения дополнений в УПК РФ статью 115, предусматривающей возможность «в случаях, не терпящих отлагательства, при наличии оснований полагать, что счета (вклады, депозиты) использовались или предназначались для использования в преступной деятельности, принимать решение о приостановлении расходных операций с денежными средствами, электронными денежными средствами по указанным счетам (вкладам, депозитам) на срок до десяти суток» [21].

В целом, борьба с компьютерным мошенничеством должна стать неотъемлемой частью глобальной стратегии борьбы с преступностью в наши дни. Только от совместных усилий со стороны правительств, международных организаций и общественности можно ожидать успехов в этой сложной и важной задаче.

«Вся сложность работы заключается в том, что преступления совершаются посредством интернет-связи, то есть на различных закрытых площадках. Поэтому идет техническая работа. Мы выясняем, кто, откуда, где и на кого зарегистрирован данный телефон или сайт. Интернет-пространство не всегда находится в границах нашего государства. Как правило, некоторые социальные сети зарегистрированы и находятся в других странах и нам не отвечают на наши запросы о том, кому принадлежит тот или иной IP-адрес», — комментирует С. Федерягин.

Относительно технической оснащенности, требуется постоянное усовершенствование программного обеспечения и внедрение новых программ и устройств в отделы полиции для оперативной борьбы с все более разнообразными способами совершения кибермошенничества. Такие цели

требуют современное оборудование и программного обеспечения, которое позволит проводить мониторинг крипто - транзакций и раскрытия нелегальных операций, программы аналитики и мониторинга для выявления мошенников и обнаружения взломов, фишинга и т.д., которые широко используются зарубежом.

Сейчас органы правопорядка и представители других организаций, должны проводить работу по информированию общественности о новых видах мошенничества. Поэтому необходимость конкретизации в составах мошенничества и ужесточения наказания за эти преступления вполне оправдана.

Обобщим итоги написания второй главы магистерской диссертации, так нами рассмотрена классификация киберпреступлений в криминалистике с использованием различных критериев. Рассмотрены авторские подходы к классификации Роберта Мюллера, Майкла Маккарти и Кевина Митника. Дана общая характеристика проведения следственных действий. Рассмотрены общие подходы к тактике следственных действий при расследовании киберпреступлений. Выделены отличительные особенности криминалистической тактики в расследовании преступлений связанных с несанкционированным доступ к компьютерной и иной информации, а также финансовым мошенничеством. Для дальнейшего раскрытия темы магистерской диссертации нам необходимо рассмотреть в следующей главе работы пути совершенствования криминалистической тактики при производстве отдельных следственных действий в расследовании киберпреступлений.

Глава 3 Пути совершенствования криминалистической тактики при производстве отдельных следственных действии в расследовании киберпреступлений

3.1 Криминалистические проблемы расследования отдельных киберпреступлений

Первая проблема - это недостаточное количество квалифицированных специалистов. Расследование киберпреступлений требует специальных знаний, как от следственных органов, так и от сотрудников, проводящих экспертизу, поэтому правоохранительным органам нужны высококвалифицированные специалисты.

Прежде всего, следователи должны обладать определенными навыками и умениями в области IT-технологий. Они должны знать, как использовать специализированные программы для сбора данных о действиях преступников и защиты от вирусов и хакерских атак.

Это позволит им обеспечить конфиденциальность и сохранность полученной информации. Кроме того, следователи должны привлекать специалистов по кибербезопасности для выявления и предотвращения возможных утечек информации. Именно эти ИТ-специалисты (эксперты) могут помочь выявить сложные способы обхода мер безопасности, что значительно повышает эффективность расследования.

Еще одной проблемой при расследовании киберпреступлений является разнообразие технических средств и устройств, а также программного обеспечения, что вызывает трудности при проведении расследования и требует обработки большого объема данных, а это затрудняет их анализ и увеличивает время обработки.

Киберпреступники используют различные технологии и методы для сокрытия своей деятельности, что усложняет работу правоохранительных органов.

При этом одним из самых серьезных препятствий при расследовании является анонимность пользователей в сети и использование темного интернета (Даркнет). Он часто ассоциируется с незаконными действиями, такими как торговля наркотиками, контрабанда оружия, продажа личных данных и т.д. В темной паутине есть и легальные сервисы, например, зона свободной прессы, где журналисты и борцы за права человека могут безопасно общаться.

Использование темной паутины может быть опасным. Во-первых, легко стать жертвой мошенничества или атаки злоумышленников. Во-вторых, случайные действия в Даркнете могут являться незаконными или криминальными. В-третьих, некоторые пользователи темной паутины могут преследовать свои собственные интересы, угрожая жизни и здоровью других людей.

В общем, темная паутина – это сложная и опасная среда, которая требует осторожного использования. Нужно быть технически и программно оснащенным, чтобы использовать сведения Даркнета для расследований киберпреступлений.

Атрибуция – это процесс определения того, кто ответственен за киберпреступление. Однако данная задача становится все более сложной из-за использования киберпреступниками инструментов, которые повышают анонимность и дают возможность скрыть свой истинный IP-адрес, что затрудняет расследование.

На данный момент в Информационном центре электронной приватности доступна информация об инструментах, повышающих анонимность, включая онлайн-сервисы и программное обеспечение.

Таким образом, органы правопорядка должны постоянно обновлять свои методы и технологии для противодействия киберпреступлениям и обеспечения безопасности в интернете.

В мире киберпреступлений все более сложно установить авторство преступлений. Это объясняется тем, что злоумышленники используют

зараженные компьютеры и устройства, которые принадлежат невинным людям, чтобы совершить атаку. В результате, трудно установить, кто конкретно совершал киберпреступление.

Такие преступления могут расследоваться долгий период времени, поскольку дознавателю необходимо в ходе расследования направить множество запросов, для выявления всех составляющих киберпреступления и обработать большой массив информации, как нами было отмечено ранее, имеет место отказ в возбуждении уголовного дела.

При расследовании уголовных дел, связанных с использованием информационно-коммуникационных технологий, тактика осмотра места преступления очень важна, в предыдущем параграфе работы подробно рассмотрена криминалистическая тактика проведения следственных действий при расследовании киберпреступлений, таких как обыск и выемка. Изъятие всей компьютерной техники и последующая компьютерная экспертиза занимают много времени и ресурсов.

Это усложняет работу следователей занимающихся расследованием киберпреступлений, а так же увеличивает продолжительность проведения расследования уголовного дела.

Отсутствие единой международной системы сотрудничества является наиболее актуальной проблемой в борьбе с киберпреступлениями и в практики их расследования. Так Российская Федерация столкнулась с проблемой, актуальной в целом для национальной безопасности и с которой сталкиваются правоохранительные органы - это отсутствие единой международной системы сотрудничества.

Запад воспринимает Россию как угрозу своему лидерству в мире и использует многочисленные методы киберпространственной войны, включая ложную информацию о событиях в России. Российскую Федерацию используют, как источник финансирования, организуя поддержку и развитие киберпреступности на территории Украины, так многочисленным

кибератакам подвергаются критическая инфраструктура на территории России [10].

Вице-премьер России Дмитрий Чернышенко предупредил о резком увеличении количества кибератак на Россию на 65% по сравнению с прошлым годом. Он отметил, что атаки направлены на поиск уязвимостей в системах для дальнейшего проникновения. В январе 2023 года Вице-премьер сообщал о том, что за 2022 год было отражено около 50000 кибератак на российские интернет-ресурсы. В 2021 году был зафиксирован высокий уровень киберугроз в финансовом секторе, что является существенной угрозой для экономики [48].

Каждый день мошенники похищают десятки миллионов рублей у российских граждан, представляясь как должностные лица. Мошенническая схема нацелена на принуждение людей переводить деньги на видимо «безопасный» счет, обещая защиту от проблем с банковскими счетами. На Finopolis сообщили о рекордной похищенной сумме в России – 150 млн. рублей за один случай в 2022 году. Похитители позвонили из Украины, так как в городе Днепр, Львов распространено явление колл-центров [4].

Для решения данной проблемы необходимо позволить сотрудникам, проводящим расследование киберпреступлении блокировать счета подозреваемых, в совершении киберпреступлений, без решения суда.

Следующей проблемой в расследовании киберпреступлений является - отсутствие единой системы классификации киберпреступлений и системы виртуальных доказательств.

Фиксируются случаи большой латентности данных преступлений, а так же следственные органы пытаются убедить пострадавшего отказаться от подачи заявления, таким образом, отказывают в возбуждении дела, чтобы не портить показатели по раскрываемости. В большинстве случаев расследование преступления не возможно, так как место преступления в

классическом понимании этого термина и отлаженные механизмы реагирования отсутствуют.

В данном параграфе магистерской диссертации путем обобщения ранее изложенного материала, выделены проблемы криминалистической тактики при производстве отдельных следственных действий в расследовании киберпреступлений.

Так одной из наиболее существенных проблем озвученной теоретиками и практиками юридических наук, а также высказываемой в ходе научных конференций является квалификация специалистов участвующих в расследовании киберпреступлений.

Другой проблемой, является технический аспект данных преступлений, который образует наличие разнообразных технических средств и устройств, а так же программного обеспечения, задействованного в совершении преступления, что вызывает сложности в проведении расследования и требует обработки большого объема данных.

Поэтому требуется постоянное усовершенствование программного обеспечения и внедрение новых программ и устройств в отделы полиции для оперативной борьбы с все более разнообразными способами совершения киберпреступлений. Оборудование и программное обеспечение, должно позволять проводить мониторинг крипто – транзакций, раскрывать нелегальные операций, обнаруживать взломы и фишинг, с этой целью важно перенимать зарубежный опыт.

Определенные недоработки есть в нормативно – правовом регулировании, связанные с процессом доказывания по уголовным делам в сфере киберпреступлений. На наш взгляд информация о киберпреступлении, выступает и как орудие совершения преступления, и как его предмет, имеет значение и как доказательство, улика, свидетельствующая о том, что преступник совершил то или иное противоправное деяние.

Информация, интересующая следствие, которая изымается из рабочего компьютерного устройства или сети, динамична, идентифицировать ее можно

лишь по ее цифровому следу, который может быть получен различными способами. Обычно информация о киберпреступлении изымается на носитель (флэш-накопитель, диск), но может изыматься и в виде цифрового следа.

Таким образом, расширение перечня видов доказательств для использования цифрового следа в УПК РФ, а также установление порядка их процессуального изъятия и закрепления является необходимостью в современном мире. Ведь цифровой след становится все более распространенным элементом в судебном процессе и имеет большую значимость при вынесении решения суда по конкретному уголовному делу.

Существует целая прикладная наука - форензика, которая призвана исследовать цифровые доказательства и изучать раскрытие, расследование преступлений, связанных с компьютерной информацией, а также обнаружение, закрепление, изъятие, сохранение этих цифровых следов преступления.

Думается, что именно методология данной науки способна разработать соответствующий порядок работы с цифровыми следами совершения преступлений.

Еще одной проблемой является возможность анонимного использования устройств за счет различных технологии и методов сокрытия, что усложняет работу правоохранительных органов.

Отсутствие единой международной системы сотрудничества является наиболее актуальной проблемой в борьбе с киберпреступлениями и в практики их расследования

Следующей криминалистической проблемой в расследовании киберпреступлений является - отсутствие единой системы классификации киберпреступлений и системы виртуальных доказательств, что затрудняет их расследование и последующее преследование виновных, а так же назначение наказания.

В следующем параграфе магистерской работы рассмотрим возможные пути решения вышеперечисленных проблем в криминалистической тактике расследования отдельных киберпреступлений.

3.2 Возможные направления повышения раскрываемости киберпреступлений

Как было указано выше, профессиональные навыки и способности играют важную роль в работе следователя. Для повышения раскрываемости киберпреступлений к сотрудникам следственных органов должны предъявляется соответствующие профессиональные требования, они должны обладать соответствующими навыками и способностями.

Поэтому для решения основной проблемы в расследовании киберпреступлений, такой как квалификация сотрудников следственных органов и уровень их профессионализма, на наш взгляд должен решаться предъявлением требований к компетенциям и знаниям сотрудников, возможно через оформления соответствующей должностной инструкции, которая должна быть закреплена в методических указаниях соответствующих органов МВД.

Мы в рамках данной магистерской работы предлагаем следующие характеристики для должностной инструкции данных сотрудников.

Основное требование к специалисту – это знание кибербезопасности и киберпреступности - это первый и самый важный аспект, которому должен соответствовать следователь, расследующий киберпреступления.

Этот аспект включает в себя знание международного и национального законодательства, связанного с киберпреступностью, политику по обеспечению безопасности в сети Интернет, технологические изменения и новшества в сфере IT, а также их возможные влияния на кибербезопасность и т.д.

Другое требование - это опыт работы в данной области, что позволит решать различные проблемы и принимать решения, касающиеся кибербезопасности.

Навыки, которыми должен владеть следователь, осуществляющий расследование киберпреступлений. Их можно разделить на три главные категории:

- навыки сбора, анализа и интерпретации электронных данных. Это может включать в себя использование различных устройств, таких как компьютеры, мобильные телефоны, системы видеонаблюдения и так далее, а также программного обеспечения для сбора и анализа данных;
- навыки работы со специальными программами и различными устройствами, такие навыки и знания хакерских инструментов и систем мониторинга, позволяют следователю при сборе доказательств киберпреступлений и восстановлении данных;
- важный навык, это способность предоставлять доказательства и подготавливать отчеты, которые могут быть использованы в судебном заседании или административном расследовании.

Способности – это смогут обеспечить успешную работу следователя по делам о киберпреступности. Они включают:

- аналитические способности, которые помогут идентифицировать и оценить киберугрозы и риски;
- способность к общению, которая позволит следователю легко выстраивать коммуникации с другими членами команды или представителями других организаций;
- способности к обучению и наставлению других членов команды в области кибербезопасности и киберпреступности.

Помимо выше перечисленных составляющих к квалификации сотрудников следственных органов в области киберпреступлений необходимо предъявлять требования постоянного повышения квалификации и обмена

опытом, возможно всероссийские, региональные конференции и совещания в онлайн формате.

Таким образом, наличие квалифицированных специалистов и эффективное сотрудничество между регионами, другими странами являются важными условиями для эффективной борьбы с киберпреступностью и повышении раскрываемости данных преступлений.

Следующим шагом для повышения раскрываемости киберпреступлений является признание в нормативно-правовых документах информационной (кибер) войны. Западные страны не скрывают своей враждебной политики относительно Российской Федерации.

НАТО считает киберпространство пятой сферой боевых действий, что свидетельствует о серьезности угрозы, которую представляет киберпреступность для государств и национальной безопасности.

НАТО проявляет значительную активность, сотрудничая с Европейским союзом, чтобы защитить свои государства от кибератак.

Следует отметить также создание механизмов ГЧП на национальном уровне, которые позволяют бороться с киберпреступностью. К примеру, NCFTA в США, JC3 в Японии и проект 2Centre в Европе объединяют специалистов из государственных органов, научных кругов и частного сектора в области кибербезопасности [38].

Это требует соответствующего финансирования, организационных и технических мероприятий. Также в некоторых странах создаются специализированные единицы по борьбе с киберпреступлениями, которые включают в себя представителей различных специализированных ведомств.

В России существует Национальный центр кибербезопасности, который объединяет представителей ФСБ, МВД, Минкомсвязи и других ведомств. Нами видится необходимым широкомасштабное привлечение ГЧП (Государственно-частного партнерства) в данный сектор, выделение структуры военной полиции для расследования случаев нарушения военной юстиции и киберпреступлений, связанных с национальной безопасностью.

Нами видится возможность применение и реализация данных проектов в Российской Федерации, расширения данных направлений и актуализация данного аспекта в правовом, политическом, военном и прочее.

Частный сектор играет важную роль в борьбе с киберпреступностью. Большинство государственных учреждений и правоохранительных органов не обладают достаточными ресурсами для того, чтобы гарантировать расследование и предотвращение преступления, обеспечение безопасности.

Частные компании предоставляют услуги по обеспечению кибербезопасности, которые включают в себя анализ угроз, мониторинг сетей и защиту конфиденциальной информации.

Следующим направлением является правовое ограничение в использовании темной паутины, использование Интернет-Даркнет должно быть ограничено и регулируемо. Правительство должно разработать законы и строгие процедуры для контроля торговли на темной паутине, а полиция должна работать на предотвращение противоправной деятельности.

Другим направлением повышающим раскрываемость уголовных дел при расследовании киберпреступлений и упрощающим проведение следственных действий является использование соответствующих программ, которые позволяют быстро извлекать информацию. То есть необходимы более эффективные методы изъятия информации. Возможно, следует использовать специальные программы для извлечения электронной почты или другой информации, что значительно сократит время на проведение экспертизы и изъятие информации с запоминающих устройств, что позволит ускорить расследование уголовного дела.

В предыдущих параграфах магистерской диссертации нами были рассмотрена тактика расследования киберпреступлений следователями, обозначены такие моменты получения доказательств, как направления множество запросов, обработка огромного массива технической информации, привлечения экспертов или технических специалистов, для извлечения или сохранения данных и т.д.

Поэтому видится возможным привлечении частных компаний в сферу расследования данных преступлений, что позволит разгрузить следственные отделы от не раскрытых дел, высвободить сотрудников от огромной технической работы, обработки массива информации, а сам процесс расследования будет выглядеть следующим образом:

- обратиться к высококвалифицированным техническим специалистам, в услуги которых входит проведение «киберрасследования», с целью составления справки и фиксирования цифровых доказательств (компания осуществляющая данные функции в рамках ГЧП);
- составить заявление о преступлении с описанием обстоятельств произошедшего, при этом оформить его «уголовно-процессуальным» языком с отражением существа подозрения и квалификацией содеянного;
- подготовить правовую позицию доверителя и составить проект его объяснений, в котором подробно отразить описание обстоятельств содеянного, где также отразить комплекс процессуальных действий, которые необходимо провести для возбуждения дела;
- приобщить к заявлению справку о результатах расследования и иные цифровые доказательства, содержащие сведения, о совершенном преступлении представленные компанией в рамках ГЧП.

На наш взгляд, данный вид сотрудничества имеет ряд преимуществ.

Во-первых, частные компании, работающие в сфере IT- технологий и программирования имеют дорогостоящее оборудование для расследования таких преступлений.

Во-вторых, имеют высококвалифицированные кадры, которые успешно осуществляют деятельность в темной стороне Интернета – Даркнет.

В третьих компании участвующие в ГЧП помимо самозащиты, могут осуществлять обслуживание систем безопасности в критических отраслях, и применять ответные меры в случае совершения киберпреступлений

направленных на их системы и данные. В таких случаях необходимо обращаться к специалистам, которые могут оперативно разобраться в ситуации и сделать все необходимое для восстановления деятельности.

Но при этом взаимодействие в рамках ГЧП не должно приводить к нарушению прав на конфиденциальность и репутацию людей. В современном мире кибербезопасность играет огромную роль. Каждый день миллионы людей пользуются интернетом, отправляют сообщения, хранят личную информацию в онлайн хранилищах. И в этой связи, защита своих систем и данных от кибератак и киберпреступлений является важной задачей. Поэтому без развития информационной (кибер) безопасности существование государства ставится под угрозу.

Таким образом, координация между правоохранительными органами, частными компаниями и учеными нацелена на предотвращение киберпреступности и должна явиться неотъемлемой частью стратегии защиты информационной инфраструктуры и повышения раскрываемости данных преступлений.

Киберугрозы национальной безопасности являются актуальной проблемой, с которой сталкиваются многие государства в современном мире. Россия не является исключением.

Необходимо включение цифрового следа в перечень видов доказательств, предусмотренных УПК РФ, что позволит правоохранительным органам более эффективно собирать доказательную базу и применять ее в судебном процессе. Необходимо так же установление порядка процессуального изъятия цифровых следов.

Особенностью цифрового следа является его динамичность и возможность изменения. Поэтому, наравне с надлежащим извлечением цифрового следа, важно установить и методы закрепления полученных доказательств при использовании их в судебном процессе.

УПК РФ закрепляет перечень видов доказательств, который является исчерпывающим. Вместе с тем, такой вид доказательства, как цифровой след,

в ч. 2 ст. 74 УПК РФ не предусмотрен, соответственно не разработан конкретный механизм получения такого вида доказательства и порядок работы с ним, в то время как при расследовании преступлений, совершенных с использованием компьютерных технологий, информация, получаемая с таких цифровых следов, является наиболее значимой, поскольку она обладает таким признаком, как высокая скорость трансформации.

Данная проблема, несомненно, нуждается в разрешении. Помимо разработок соответствующих криминалистических и уголовно-процессуальных методик, касающихся вопросов доказывания по уголовным делам рассматриваемой категории, необходимо внести некоторые изменения и в сам УПК РФ.

Внесение дополнений в УПК РФ статью 115, предусматривающей возможность блокировки расходных операции на счетах, подозреваемых в кибермошенничестве, на срок до десяти дней без решения суда. «В случаях, не терпящих отлагательства, при наличии оснований полагать, что счета (вклады, депозиты) использовались или предназначались для использования в преступной деятельности, принимать решение о приостановлении расходных операций с денежными средствами, электронными денежными средствами по указанным счетам (вкладам, депозитам) на срок до десяти суток». В течение десяти суток, на которые приостановлены расходные операции, следователь с согласия прокурора должен направить в суд ходатайство о наложении ареста на денежные средства, находящиеся на счетах либо вынести постановление об отмене постановления о приостановлении операций по соответствующим счетам. Такие изменения позволят предотвратить отток денежных средств полученных преступным путем из страны. А также возместить похищенные средства пострадавшим от действий мошенников.

В магистерской диссертации охарактеризована тактика расследования киберпреступлений следователями, выделены негативные моменты в раскрываемости таких преступлений и затягивании процесса расследования, такие как направление и обработка множества запросов, обработка огромного

массива технической информации, привлечения экспертов или технических специалистов, для извлечения или сохранения данных и т.д. В связи с обозначенными сложностями, предложено привлечение частных (профессиональных) компаний в сферу расследования данных преступлений, что позволит сократить этапы расследования, обеспечит более быструю обработку и получение доказательственной базы, так как профессиональные IT- специалисты уже владеют теми навыками, которые мы только начинаем внедрять к сотрудникам следственных органов в области расследования киберпреступлений. При этом важно отметить, что IT-компании имеют в своем распоряжении необходимые технические средства и программное обеспечение, позволяющее более оперативно выполнять данные задачи.

С учетом всех факторов в расследовании данных преступлении и с учетом особенностей киберпространства, в котором они осуществляются, на наш взгляд наиболее перспективным является механизм ГЧП для решения проблем раскрываемости и латентности данных преступлений.

Так криминалистическая тактика проведения расследований в киберпространстве будет содержать этапы соответствующие юридическому профилю, что не потребует использования высокотехнологического программного обеспечения и технических средств.

Общие рекомендаций для следователей осуществляющих расследование киберпреступлений:

- собрать как можно больше информации о данных карт (банковских счетов), с которых осуществлены операции, связанные с киберпреступлениями, проанализировать операции, включая данные о времени и месте использования карты, суммы транзакций, места расположения банкоматов и терминалов платежных систем;
- проанализировать все собранные данные и искать связи между разными операциями и местами использования карты;
- установить контакты с банками и системами платежей, чтобы получить дополнительную информацию о картах и транзакциях;

- использовать технологии и инструменты для обработки больших объемов данных, такие как анализ данных (Data Mining) и анализ социальных графов (Social Network Analysis), чтобы выявить скрытые связи и подозрительные схемы;
- осуществлять взаимодействие со специалистами по кибербезопасности, чтобы лучше понимать технические и правовые аспекты преступлений;
- вести оперативную работу по выявлению подозреваемых и привлечению их к ответственности;
- работать в сотрудничестве с другими правоохранительными органами, такими как Федеральная служба безопасности, для обмена информацией и координации действий.

Если при киберпреступлениях используется мобильная связь или переписка по социальным сетям с потенциальной жертвой киберпреступления, то важно определить местоположение преступника, сделать это можно несколькими способами, если это не скрытый номер или номер с искажённой информацией:

- запрос у оператора связи.

Сотрудники правоохранительных органов могут запросить у оператора связи информацию о местоположении абонента, который звонил с мобильного телефона. В ответ они получат геоданные, которые определяют местоположение мобильного устройства и его хозяина в момент, когда был осуществлен звонок.

- использование баз данных.

Есть базы данных, которые содержат информацию об IP-адресах, приставленных к мобильным номерам, которые позволяют определить местоположение того, кто звонил. Эти данные часто не достаточно точные, и в действительности могут не соответствовать реальному местоположению.

- слежение и отслеживание.

Если мошенник звонит с определенного места, например, с телефона или компьютера, IP-адрес которого известен, правоохранительные органы могут провести оперативное слежение и отслеживание, чтобы выяснить, где находится преступник и с кем он взаимодействует.

Но важно учитывать, что определение местоположения не всегда является точным и может быть затруднено, если мошенник использует специальное программное обеспечение для скрытия своего IP-адреса или местоположения.

Если мошенник скрывает свой IP-адрес и местоположение, то необходимо определить его точное местоположение может быть сложно или невозможно. Существует несколько методов, которые можно использовать при сокрытиях данных о месте положения киберпреступников:

Также необходимо исследовать все доступные данные: сообщения, электронную почту и другие данные, чтобы обнаружить любую информацию, которая может помочь установить местоположение мошенника.

Необходимо внедрение в следственную практику специализированного программного обеспечения для отслеживания. По опыту зарубежных стран, используются множество программ и технологий. Некоторые из них включают в себя: платформы для обнаружения мошенничества, фильтры-антифрод, системы обхода блокировок, аналитика и мониторинг, блокчейн-технологии. Это только некоторые из инструментов, которые используются для борьбы с мошенничеством в западных странах, которыми должны быть обеспечены и обучены сотрудники следственных органов в РФ осуществляющих расследования киберпреступлений.

Заключение

В ходе проведенного исследования с целью совершенствования криминалистической тактики при производстве отдельных следственных действии в расследовании киберпреступлений на основе комплексного анализа теоретического, практического и научного материала, характеризующего понятия и особенности преступлений совершенных в киберпространсте предпринята попытка по разработке рекомендаций, направленных на решение поставленных задач.

В магистерской диссертации рассмотрен исторический аспект появления киберпреступности, охарактеризован прогрессивный рост данных преступлений на основе обобщенных данных. Выявлены различия в подходах к определению киберпреступности в научных кругах, даны авторские комментарий к определениям различных исследователей, предложено авторское понимание термина киберпреступлений.

Предложена авторская четырехфакторная модель функционирования киберпространства. Рассмотрено понятие киберпространства с учетом авторских подходов различных исследователей. Выявлены различия в подходах к определению киберпространства в уголовно-правовой доктрине.

В результате проведенного исследования подходов к характеристике и определению термина киберпространства ряд исследователей предлагает многоуровневый подход, нами предложено рассматривать киберпространство с точки зрения системного подхода.

Выделены и рассмотрены факторы, определяющие специфику киберпреступлений преступлений, предложены и обобщены различные критерии и подходы к классификации киберпреступлений.

В магистерской диссертации реализована попытка выделить факторы, привлекающие в данную сферу киберпространства преступную деятельность, предпринята попытка по уточнению факторов, оказывающих влияние на

прогрессивный рост киберпреступлений. Дополнены критерии классификации преступлений в киберпространстве.

При решении поставленных задач, рассмотрены криминалистические подходы к классификации киберпреступлений. Рассмотрен критерий классификации в криминалистике по механизму атаки. Охарактеризован каждый тип атаки, так как ему соответствуют уникальные характеристики, которые требуют соответствующих методов расследования и идентификации. Дана характеристика целевым аудиториям, на которые направлены действия киберпреступников. Рассмотрены категории киберпреступлений, предложенные Кевином Митником, Роберт Мюллером и Майклом Маккарти.

В данной магистерской работе представлены общие и частные подходы к тактике проведения следственных действий, охарактеризованы особенности проведения экспертизы при расследованиях киберпреступлений. Представлен криминалистический подход Кевина Митника в расследовании преступлений в киберпространстве.

Дана общая характеристика проведения следственных действий, таких как обыск, выемка и проведение экспертизы. Рассмотрены общие подходы к тактике следственных действий при расследовании киберпреступлений.

Выделены отличительные особенности криминалистической тактики в расследовании преступлений связанных с несанкционированным доступ к компьютерной и иной информации, а так же финансовым мошенничеством.

Путем обобщения ранее изложенного материала, выделены проблемы криминалистической тактики при производстве отдельных следственных действий в расследовании киберпреступлений.

Так одной из наиболее существенных проблем является квалификация специалистов участвующих в расследовании киберпреступлений. Другой проблемой, подробно рассмотренной в данной работе, является технический аспект данных преступлений, который вызывает сложности в проведении расследования и требует обработки большого объема данных. Фактор анонимного использования устройств за счет различных технологии и методов

сокрытии – данное обстоятельство усложняет работу правоохранительных органов.

Отсутствие единой международной системы сотрудничества является наиболее актуальной проблемой в борьбе с киберпреступлениями и в практики их расследования, а так же отсутствие единой системы классификации киберпреступлений и системы виртуальных доказательств, что затрудняет их расследование и последующее преследование виновных, а так же назначение наказания.

В заключительной части работы предложены возможные пути совершенствования криминалистической тактики расследования киберпреступлений, на основе возможных направлений в решении обозначенных проблем.

Так следователю необходимо иметь не только теоретическую базу, но и практический опыт в области расследования киберпреступлений. Для выполнения таких требований он должен владеть соответствующими комплексными знаниями, навыками и способностями, чтобы качественно и эффективно проводить расследование в области киберпреступности.

Необходимы умения работать с программным обеспечением, извлечением и обеспечением защиты доказательств, информации в различных системах.

Добыть электронные доказательства – это необходимое условие для проведения расследования, дальнейшего предотвращения данных киберугроз, так как сведения о способах совершения данных преступлений позволяют реализовывать превентивные мероприятия, например путем информирования общественности о способах кибермошенничества и т.д.

Высокий уровень профессионализма сотрудников следственных органов, осуществляющих расследования киберпреступлений позволит повышать уровень раскрываемости данных преступлений.

При расследовании киберпреступлений следователь должен изучить широкий спектр технических и правовых аспектов, таких как:

- основы компьютерных сетей, протоколов и технологий;
- средства и методы кибератак. Следователь должен знать, как работают основные средства и методы, используемые преступниками при кибератаках, например, вирусы, трояны, фишинг и другие социально-инженерные атаки.
- основные виды киберпреступлений. Следователь должен знать, какие виды киберпреступлений существуют, например, кража данных, мошенничество, кибершпионаж, хакерские атаки и другие.
- средства и методы кибербезопасности. Следователь должен изучить основные средства и методы кибербезопасности, используемые для защиты данных и информационных систем, например, брандмауэры, антивирусные программы, системы обнаружения вторжений.
- правовые аспекты киберпреступлений. Следователь должен иметь представление о соответствующих законах и нормах, регулирующих киберпреступления, уголовные и гражданские последствия таких преступлений.

В целом следователь должен осведомлен о современных методов и средств кибербезопасности и иметь достаточные технические знания для того, чтобы эффективно расследовать киберпреступления.

Но не только квалификация сотрудников является важным фактором в борьбе с киберпреступностью. Также важно, чтобы законодательство соответствовало быстро меняющейся технологической ситуации, что позволит правоохранительным органам разрабатывать и внедрять методические указания, способы и правила, проведения необходимых следственных действий для расследования и пресечения киберпреступлений.

Так, следует ввести в перечень видов доказательств (статья 74 УПК РФ) новый вид доказательства – цифровой след, предусмотрев также порядок его процессуального изъятия и закрепления.

Даны общие рекомендации для следователей осуществляющих расследование киберпреступлений, в том числе при сокрытии преступником места нахождения, или IP-адреса.

Описано программное обеспечение, используемое западными странами в борьбе с киберпреступлениями.

Акцентировано внимание на разработку правового ограничения использования «темной паутины» (Интернет–Даркнет), данные меры позволят значительно сократить преступность в киберпространстве, если использование данного ресурса будет уголовно наказуемо.

С точки зрения совершенствования законодательства, в том числе уголовно-правовых средств борьбы требуется разработка комплекса поправок в УК РФ и строгие процедуры для контроля торговли и использования «темной паутины».

Рекомендовано создания целевых групп, которые будут ответственны за конкретные виды киберпреступлений. Например, группа, которая занимается «электронными преступлениями» или группа, которая борется с атаками на системы финансовых расчетов и т.д.

Список используемой литературы и используемых источников

1. Барышев Р.А. Киберпространство и проблема отчуждения: дис. … канд. фил. наук. Красноярск, 2009. 131 с.

2. Батухтин М.Е. Киберпреступления: причины, виды, формы, последствия, направления противодействия // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе Материалы Международной научной конференции адъюнктов, аспирантов, курсантов и студентов. Том Часть 3. 2018. С. 28-31.

3. Войскунский А.Е. Метафоры интернета // Вопросы философии. 2001. № 11. С. 64-79. [Электронный ресурс]. URL: http://www.relarn.ru/human/cyberspace.html (дата обращения: 18.11.2022).

4. Глава МВД рассказал о мошенниках в колл-центрах в Херсонской области 28 мая 2023 [Электронный ресурс] // URL: https://sevastopol.su/news/glava-mvd-rasskazal-o-moshennikah-v-koll-centrah-v-hersonskoy-oblasti (дата обращения 29.05.2023).

5. Грачев А.В. В сборнике «Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи» // Материалы внутривузовской конференции. 2015. С. 162-175.

6. Гибсон У. Нейромант / пер. с англ. под ред. А. Черткова. - М. : АСТ. 2000. 317 с.

7. Добринская Д.Е. Киберпространство: территория современной жизни // Вестник Московского университета. 2018. Т. 24. № 1 С. 52-70.

8. Дэвис Э. Техногнозис: миф, магия и мистицизм в информационную эпоху / Э. Дэвис. - Екатеринбург, 2008. 480 с.

9. Интернет 2017-2018 в мире и в России: статистика и тренды [Электронный ресурс] URL: https://www.web-canape.ru/business/internet-2017-2018-v-mire-i-v-rossii-statistika-i-trendy (дата обращения 09.12.2022)

10. Информационная война против России в условиях осуществления специальной военной операции [Электронный ресурс] // URL:

http://ruspolitology.ru/ekspertnaya-deyatelnost/13040/ (дата обращения: 26.05.2023).

11. Киберпреступность в цифрах [Электронный ресурс] // URL: https:// www.aktiv-company.ru/analitics/articles/cybercryme.html (дата обращения 18.11.2022).

12. Киберпреступность – определение, классификация киберпреступлений. [Электронный ресурс] // URL: https://elcomrevue.ru/blog/cybercrime/kibeoprestupnost-chto-eto (дата обращения: 18.11.2022).

13. Киберпреступления: понятие, виды и методы защиты (sys-team-admin.ru) [Электронный ресурс] // URL: https: sys-team-admin.ru/stati/bezopasnost/170-kiberprestupnost-ponyatie-vidy-i-metody-zashchity.html (дата обращения 08.12.2022).

14. Киберпреступлений становится все больше, однако их раскрываемость уменьшается [Электронный ресурс] // URL: https://www.advgazeta.ru/obzory-i-analitika/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/(дата обращения 26.05.2023).

15. Комлев Ю.Ю. Интеграция криминологических знаний, расширенная методологическая триангуляция и «big data» в социологическом изучении преступности // Вестник экономики, права и социологии. 2019. № 3 С. 97-104.

16. Концепция Стратегии кибербезопасности Российской Федерации. [Электронный ресурс] // URL: http://www.council. gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 18.11.2022).

17. Коробеев А.И., Дремлюга Р.И. и др. Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации // Всероссийский криминологический журнал. 2019 Т. 13 № 3 С. 416-425.

18. Кузнецов П.С. Проблемы расследования преступлений в сфере компьютерной информации // Молодой ученый. 2020. № 15 (305). С. 210-212.

19. Куява Т.Ю. Киберпреступность: проблемы уголовно-правовой оценки и организации противодействия // Молодой ученый. 2016 № 29 (133). С. 255-257.

20. Леонтьев В.П. Большая энциклопедия компьютера и Интернета / В.П. Леонтьев. - М., 2006. 264 с.

21. МВД предложило без суда блокировать расходы со счетов кибермошенников [Электронный ресурс] // URL: https://ria.ru/20230620/kibermoshenniki-1879262118.html (дата обращения: 10.10.2023).

22. Морозов Н.А. Борьба с компьютерной преступностью в Японии // Общество и право. 2014. № 2 (48). С.141-145.

23. Митник К.Д. Искусство обмана / пер. с англ.: А.А. Груздев, А.В. Семенов. – Москва : ДМК Пресс, 2006. 124 с.

24. Мюллер Р.С. Отчетный документ № 2, опубликованный Международной организацией полиции (INTERPOL), разработан на основе рекомендаций, вынесенных на конференции по киберпреступности в Лондоне. [Электронный ресурс] // URL: https://dev.abcdef.wiki/wiki/Mueller_Report#Book_editions (дата обращения: 01.03.2023)

25. Мюллер Р.С. Отчетный документ № 3, опубликованный Международной организацией полиции (INTERPOL), разработан на основе рекомендаций, вынесенных на конференции по киберпреступности в Лондоне. Электронный ресурс] // URL: https://dev.abcdef.wiki/wiki/Mueller_Report#Book_editions (дата обращения: 03.01.2023).

26. Мягков Ю.В. Характеристика определения киберпреступности на современном этапе. В сборнике: Всероссийский форум молодых ученых. 2023. 2023. С. 428-437 [Электронный ресурс]. URL: http://elibrary.ru/item.asp?id=50467167 (дата обращения:06.04.2023).

27. Отчет начальника Отдела МВД России по г. Миассу по вопросу: «Об итогах оперативно-служебной деятельности Отдела МВД России по городу Миассу за 2020-21 год» [Электронный ресурс] // URL: https:// 74.мвд.рф/document/19759866(дата обращения 18.11.2022).

28. Павловец В.И. России нужны не биороботы, а креативный средний класс: о направлениях эффективного реформирования экономики и образования // Альманах современной науки и образования. 2013 г. № 1 (68). С. 102-105.

29. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. … канд. юрид. наук: 12.00.08. Москва, 2016. 229 с.

30. Противодействие правонарушениям, совершаемым с использованием информационных технологий: сборник статей по материалам научно-практической конференции (III школы семинара молодых ученых-юристов), г. Москва, 11 ноября 2020 г. М. : МФЮА, 2021. 224 с.

31. Плешаков В.А. Про мозаичную культуру и сознание человека в эпоху киберсоциализации // Электронный научно-публицистический журнал «Homo Cyberus». 2016. №1. [Электронный ресурс] http://journal.homocyberus.ru/o_mozaichnoy_kulture (дата обращения 18.11.2022).

32. Рассолов И.М. Право и «Интернет»: теоретические проблемы / И.М. Рассолов. 2-е изд., перераб. и доп. - М., Норма. 2009. 210 с.

33. Составляющие киберпространства [Электронный ресурс] // URL: https:// www.osp.ru/news/articles/2016/26/13049892 (дата обращения 25.11.2022).

34. Справочный документ для семинара-практикума по использованию компьютерной сети «Десятый конгресс» Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями» [Электронный ресурс] // URL: https://mgimo.ru/upload/iblock/ddf/ddf0bdf94430720ca8e8957af028690f.pdf

35. Толковый словарь по вычислительным системам [Текст] / Под ред. В. Иллингуорта и др.: Пер. с англ. А.К. Белоцкого и др.; Под ред. Е.К. Масловского. - М.: Машиностроение, 1990. - 560 с.

36. Теркулова И.Н. Цифровая среда как педагогическое условие позитивной социализации обучающихся во франкоговорящих странах (Франция, Канада): дис. канд. пед. наук: 13.00.01. Новосибирск, 2019. 230 с.

37. Технический регламент Евразийского экономического союза «О требованиях к энергетической эффективности энергопотребляющих устройств». ТР ЕАЭС 048/2019 Приложение 17 [Электронный ресурс] // URL: https://docs.cntd.ru/document/564066302 (дата обращения 20.11.2022).

38. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. канд. юрид. наук: 12.00.08. Владивосток, 2005. 234 с.

39. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 14.07.2022, с изм. от 18.07.2022) // СЗ РФ. 1996. № 25. Ст. 2954.

40. Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ: принят Гос. Думой 22 ноября 2001 г.: одобрен Советом Федерации 5 декабря 2001 г.: (ред. от 21.11.2022) // Консультант плюс: справочно-правовая система.

41. Украдены сотни миллионов: как челябинские следователи раскрывают интернет-мошенничества [Электронный ресурс] URL: https://eanews.ru/news/ukradenny-sotni-millionov-kak-chelyabinskiye-sledovateli-raskryvayut-internet-moshennichestva_22-08-2022 (дата обращения:06.04.2023).

42. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (ред. От 14.07.2022г.) [Электронный ресурс] // Консультант плюс: справочно-правовая система.

43. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ // Консультант плюс: справочно-правовая система.

44. Филиппов А.Г. Криминалистика. Полный курс: учебник для бакалавров / А.Г.Филиппов [и др.]; под общей редакцией А.Г.Филиппова. 5-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2020. 855 с.

45. Хусяинов Т.М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве // Уголовный закон Российской Федерации: Проблемы правоприменения и перспективы совершенствования материалы всероссийского круглого стола. Том Выпуск 6. 2015 С. 120-125.

46. Хуторной С.Н. Киберпространство и становление сетевого общества: дис. канд. фил. наук. Воронеж. 2013. 166 с.

47. Что такое киберпреступность? Кибербезопасность и предотвращение киберпреступлений. [Электронный ресурс] // URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения 18.11.2022).

48. Число кибератак на информационные системы России выросло на 65% [Электронный ресурс] // URL: https://www.vedomosti.ru/technology/news/2023/03/03/965181-chislo-kiberatak (дата обращения 25.05.2023).

49. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: автореферат дис. … канд. юрид. наук. Москва, 2016. 29 с.

50. Шишкина Н.Э., Перякина Процессуальные и криминалистические аспекты изъятия электронных носителей информации в свете защиты прав участников уголовного судопроизводства // Сибирский юридический вестник. 2019. № 3 (86). С. 81-85.

51. «Ciec.org». Reno vs. ACLU, 117 S.Ct. 2329 (1997) (casebook at 932-53 // URL:http//ciec.org/SC_appeal/opinion.shtml. (дата обращения 25.05.2023).

52. Clark D. Characterizing cyberspace: past, present and future, MIT/CSAIL Working Paper, 12 March 2010 // URL:https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace (дата обращения 25.05.2023).

53. OECD, Computer – Relates Crime: Analysis of Legal Policy. Paris, 1986. 450 p.

54. Oxford dictionary of English. Oxford, 2010. 75 p.

55. Rush H., Smith C., Kraemer-Mbula E., Tang P. Crime online: Cybercrime and illegal innovation (research report: July 2009) // ResearchGate: site. 2020. URL: https: researchgate.net/publication/28550926. P. 64-75.

56. Holmes D. Communication theory: media, technology, society. L., 2005. P. 44-45.

57. Tackling the Challenges of Cyber Security / ETSI White Paper No. 18. December 2016 URL: https: //www.etsi.org/ images/files/ETSIWhitePapers/etsi_wp18_CyberSecurity_Ed1_FINAL.pdf.