Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное

учреждение высшего образования

«Южно-Уральский государственный университет

(национальный исследовательский университет)»

Юридический институт

Кафедра «Судебная и правоохранительная деятельность»

НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА

 «Организованная преступность цифрового мира»

Руководитель работы:

К.ю.н., доцент кафедры

.

Автор работы:

Студент группы Ю-316

Р.И. Шайхитдинов

Челябинск

2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ..............................................................................................................3

ГЛАВА 1 ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ...................................................................5

1.1. История возникновения и развития компьютерных преступлений……………………………………………………………………...5

1.2. Характеристика преступлений, совершаемых в сфере компьютерной информации..............................................................................................................6

ГЛАВА 2 ОСОБЕННОСТИ РАССЛЕДОВАНИЯ И РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ…………9

2.1. Расследование и раскрытие компьютерных преступлений: проблемы и пути совершенствования…………………………………………………………9

2.2. Структура и состояние компьютерной преступности в Российской Федерации..............................................................................................................10

ЗАКЛЮЧЕНИЕ .....................................................................................................12

БИБЛИОГРАФИЧЕСКИЙ СПИСОК .................................................................13

ВВЕДЕНИЕ

Актуальность данной темы носит как практический, так и теоретический характер. Значимость данных вопросов, связанна с формированием и развитием механизмов информационной безопасности в России в различных научных областях, которая сопровождается развитием информационно-коммуникационных технологий и инновациях в промышленности.

Происходящие в мире глобальные изменения ведут к переходу, а именно к новому типу общества - информационному обществу. Основные аспекты реструктуризации информационного общества заключаются в создании, обработке, хранении и использовании информации, которые в настоящее время меняются во многих отношениях.

Информация обрабатывается, хранится и используется в различных областях человеческой деятельности.

Компьютеризация ознаменовала современную эру научного прогресса. Но несмотря на неоспоримые положительные факты этого явления, в частности, имеются недостатки. Это происходит, потому, что внедрение новых технологий, способствует возникновению новых видов преступлений, которые касаются в свою очередь информационного поля.

По своему механизму, метод исполнения таких преступлений имеет свои особенности, например, данный вид характеризуется высокой скрытостью лица, совершающего преступление и низкой раскрываемостью преступлений.

 Основная проблема данной темы заключается в том, что несмотря на большое количество исследований в этой области, многие вопросы до сих пор не решены или решены полностью. Кроме того, постоянно появляются новые разработки, это происходит за счет развития технологий, и это способствует изменению способа совершения киберпреступления.

Внедряются новые методы обеспечения секретности. Для выявления незаконной деятельности и лиц, ее совершающих, внедряются новые методы сокрытия и обнаружения.

Такая ситуация приводит к тому, что ученые постоянно занимаются проблемами выявления и расследования киберпреступлений и необходимостью приобщения тех, кто работает в этой сфере, к информационным технологиям.

Предметом нашего исследования являются социальные отношения, связанные с легальным и безопасным использованием компьютера, информация и информационных ресурсов.

Исследование сосредоточено на преступлениях, связанных с киберпреступностью как криминальная проблема и ее криминализация.

Поэтому предметом исследования являются следующие элементы: природа, структура и динамика киберпреступности, а также методы и особенности расследования киберпреступлений и меры по их предотвращению.

Целью данного исследования является предоставление комплексного криминологического изучения природы, тенденций и основных характеристик преступности в сфере информационных технологий.

Задачи исследования:

- Анализ правовых норм для установления правонарушений, которые подлежат Уголовной ответственности, касающиеся сферы информационных технологий.

- Изучение проблем квалификации киберпреступлений.

- Выявление основных причин и обстоятельств, приведших к совершению преступлений в сфере информационных технологий.

- Изучение характеристик и проблем, связанных с выявлением и расследованием киберпреступлений.

ГЛАВА 1 ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1. История возникновения и развития компьютерных преступлений

20 век стал эрой телекоммуникаций, включая телеграф, телефон, радио и кино и телевидения. За последние несколько десятилетий произошли стремительные изменения. Наступление цифровой эпохи сопровождается развитием компьютерных технологий и их активным использованием во всех сферах жизни общества.

В последние десятилетия компьютерные технологии стремительно развиваются и быстро завоевывают позиции во всех сферах жизни общества. информации всех видов.

Информация предоставляется в виде компьютерных данных, что облегчает работу с ней.

Локальные информационные сети и Интернет. Они создают единое информационное пространство и позволяют мгновенно обмениваться информацией.

Внедрение информационных технологий позволило автоматизировать различные производственные процессы. Это позволяет улучшить ситуацию на различных предприятиях.

В 21 веке коммуникационные устройства, смартфоны и планшеты, стали обычным явлением. Компьютеры, которые дорого и громоздко ремонтировать, стали заменяться более практичными моделями технических устройств, которые могут позволить себе большая часть населения планеты.

Так, с развитием компьютерных технологий появился новый вид преступлений - киберпреступность.

Родиной термина «компьютерная преступность» считается США, где в 60-х годах прошлого века подобное словосочетание впервые появилось в СМИ в связи с выявлением первых преступлений, совершенных с использованием 7 ЭВМ, в 1969 г. Альфонсе Конфессоре, получив незаконно доступ к информации в электронно-вычислительной сети, совершил налоговое преступление, ущерб от которого составил $620000, а в 1970 году, также путем незаконного доступа к информации "Секюрити пасификбэнк" с одного из счетов банка было незаконно списано $10,2 миллиона[[1]](#footnote-1).

Для России первое киберпреступление было совершено в 1991 году, когда 125 500 долларов были похищены из Внешэкономбанка в СССР, сотрудником образовательного компьютерного центра.

В связи с появлением новых угроз было предпринято несколько попыток на законодательном уровне. Неоднократно предпринимались попытки регламентировать ответственность в отношении киберпреступности.

1 января 1997 г. вступил в силу новый Уголовный кодекс Российской Федерации, в котором появилась Глава 28 «Преступления в сфере компьютерной информации», объединяющая ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ» и ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети», который с рядом изменений действует и по настоящее время[[2]](#footnote-2).

 Дальнейшее развитие информационных технологий, появление и активное внедрение сети Интернет, массовая компьютеризация привели к бурному развитию компьютерной преступности, как на уровне отдельных государств, в том числе, России, так и на международном уровне[[3]](#footnote-3).

1.2. Характеристика преступлений, совершаемых в сфере компьютерной информации

Согласно с определением «компьютерного преступления», предложенным авторами В.А. Дуленко, Р.Р. Мамлеевым, В.А. Пестриковым, сказано, что компьютерное преступление как уголовно-правовое понятие – это предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства[[4]](#footnote-4).

С учетом представленных позиций вышеуказанных авторов, на сегодняшний день в действующей редакции Уголовного кодекса РФ под компьютерной информацией понимаются «сведения (сообщения, данные), представленные в форме электрических сигналов независимо от средств их хранения, обработки и передачи»[[5]](#footnote-5).

По данным количество несанкционированных операций в сфере информационных технологий в мире растет год за годом. Прогнозируют, что затраты, связанные с киберпреступностью, будут **расти ежегодно на 15% в течение следующих пяти лет**. Они приходят к такому выводу, оценивая исторические финансовые показатели кибератак и будущую среду угроз.

Согласно предоставленным данным Cyber Polygon: «в 2021 году доминирующими были классические атаки – фишинговые сайты на тему коронавируса, оформление якобы подлинных документов о вакцинации, мошеннические операции с услугами, реклама проектов, приносящих мгновенных доход. Такие злонамеренные действия составили более 85 % атак. Примерно 10 % атак, зафиксированных в 2021 году, пришлись на программы-вымогатели, которые были нацелены на корпорации. Наиболее известный пример – атака на Colonial Pipeline, из-за чего оказалась парализованной гигантская сеть заправок в США. И меньше всего атак было, не более 5 %, таргетированного характера, чрезвычайно хорошо организованные, направленные на государственные структуры разных стран. Они до сих пор полностью не расследованы. В компании Ростелеком-Солар предоставили свою статистику. Согласно ей фишинг в 2021 году был самым известным методом, используемым преступниками низкой квалификации. Таких атак было зафиксировано не менее 60 %. Хакеры более высокого уровня подготовки эксплуатировали веб-уязвимости государственных органов власти. Таких атак было в 2021 году 50 %».

Поэтому вопрос кибербезопасности имеет первостепенное значение для потребителей и предприятий. Уровень квалификации киберпреступников растет. Число краж личных данных растет, и пользователям и предприятиям необходимо продолжать внедрять передовые технологии безопасности в дополнение к существующим мерам защиты, чтобы снизить риски.

ГЛАВА 2 ОСОБЕННОСТИ РАССЛЕДОВАНИЯ И РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

2.1. Расследование и раскрытие компьютерных преступлений: проблемы и пути совершенствования

В сегодняшней динамичной среде предприятия и физические лица постоянно сталкиваются со соответствующими проблемами. Проблемы, стоящие перед обществом, многочисленны и разнообразны, но часто они проистекают из стремления создать лучшую, более эффективную окружающую среду.

Разработка лучших и более эффективных способов жизни часто является вопросом. Это абсолютно верно в некоторых случаях. Некоторые сферы нашей жизни становятся все более и более распространенными. Это также относится к электронным устройствам и компьютерным приложениям.

Информационные технологии содержат социальные риски, связанные с незаконной деятельностью, несанкционированное уничтожение, модификация, искажение и подделка информации, а также иное незаконное вмешательство в работу информационных систем, влекущее за собой самые серьезные и необратимые последствия.

Для успешного расследования преступления необходимо учитывать такие составляющие личности подозреваемого лица, как пол, возраст, социальное происхождение, уровень образования, род занятий, семейное положение, социальный статус, уровень материальной обеспеченности, место жительства, а также места проведения досуга и возможная принадлежность к определенной субкультуре[[6]](#footnote-6).

Обнаруживая и расследуя следы незаконной деятельности преступников.

 Т.е. специализированных на телекоммуникациях и компьютерных преступлениях, как минимум в области электроники и информационных технологий.

Необходимо заключения квалифицированного эксперта, обладающего познаниями в данной сфере деятельности для того, чтобы вынести обвинение и возбудить уголовное дело.

2.2. Структура и состояние компьютерной преступности в Российской Федерации

По данным ЦБ: «количество несанкционированных операций в РФ растет год за годом. В 92% случаев причиной является использование электронного средства платежа без согласия владельца, а в сегменте юридических лиц большинство случаев (54%) приходится на воздействие вредоносного кода.»

В 2015 году количество несанкционированных преступлений составило 260 992, в 2016 году количество преступлений увеличилось на 6 345, а 2017 год стал рекордным число преступлений составило 317 178.

Рост киберпреступности является естественным следствием цифровизации современного мира. Важно отметить, что процесс цифровизации все еще находится в зачаточном состоянии, а киберпреступность стала глобальной индустрией. Поскольку процессы и взаимодействия становятся все более цифровыми, киберпреступность растет экспоненциально. По оценкам IDC, через семь лет - к 2025 году - объем уязвимых данных будет составлять около половины всех существующих данных, по сравнению с четвертью в 2015 году.

При этом необходимо отметить серьезные проблемы не только в выявлении преступлений в сфере компьютерной информации, но и в деятельности органов дознания и предварительного следствия при расследовании данной категории дел. Например, статистика расследованных уголовных дел, возбужденных по признакам преступлений, предусмотренных ст. 273 УК РФ, показывает: «что по реабилитирующим основаниям прекращены: в 2009 г. – 50, в 2010 г. – 35, в 2011 г. – 78, в 2012 г. – 163 уголовных дела; «приостановлены за не розыском лица либо в случае не установления лица, совершившего преступление»: в 2010 г. – 58, в 2011 г. – 75, в 2012 г. – 108, в 2013 г. – 106, в 2014 г. – 119, в 2015 г. – 193 уголовных дела. Также в 2010 году из находившихся в производстве по ст. 273 УК РФ 1 066 уголовных дел в суд направлено 914, в 2011 году из 754 уголовных дел в суд направлено 558, в 2012 году из 953 уголовных дел в суд направлено только 664, в 2013 году из 860 уголовных дел в суд направлено 575, в 2014 году из 665 уголовных дел в суд направлено 344, в 2015 году из 974 уголовных дел в суд направлено 369.»

 Таким образом, в цифровом мире взаимодействие происходит не между людьми, не между компаниями и компаниями, не между устройствами и процессами, а между их цифровыми проекциями. Цифровизация способствует распространению таких проекций. Укрепление инструментов и методов идентификации и аутентификации приобретает все большее значение.

Для удовлетворения этой потребности будут разработаны новые технологии, методы и средства идентификации и аутентификации. Они однозначно удобны, портативны и имеют много преимуществ перед традиционными методами. Однако они также имеют недостатки в плане безопасности и не получили широкого распространения. Однако новые технологии расширяют рынок идентификации и аутентификации, играют важную роль в развитии рынка ИТ-безопасности и позволяют разрабатывать экономически эффективные процессы ИТ-безопасности.

ЗАКЛЮЧЕНИЕ

Роль и значение компьютерной информации как одного из важнейших средств создания заключается в использовании и передачи информации. Это означает, что, с ростом важности компьютерной информации возросла и потребность в специалистах более высокого уровня.

Это должно быть защищено техническими, организационными и, в частности, правовыми средствами. Проведена реорганизация информационных технологий в компаниях, учреждениях и организациях.

Анализ материала, представленного в данной работе, позволил сделать следующие выводы: требуются значительные дополнения и изменения в законодательство Российской Федерации. Кроме того, существует необходимость принятия новых законов для создания правовой базы в области информации.

Причины неэффективности мер, разработанных для борьбы с киберпреступностью, заключаются в отсутствии комплексных мер, их непоследовательности и длительном времени существования киберпреступлений.

Отсутствие комплексных мер, их непоследовательность и фрагментарность, а также длительный инкубационный период киберпреступности являются одними из причин неэффективности превентивных мер.

Повышение осведомленности для защиты законных интересов, а также Использование и развитие ИТ, модернизация и развитие ИТ, техническое оснащение и профессиональное развитие.

Улучшение технического оснащения и профессиональных навыков сотрудников полиции для эффективного выявления этих преступлений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Уголовный кодекс Российской Федерации от 13.06.1996 №63 – ФЗ (ред. от 23.04.2018) // СЗ.1996. № 25.

2. Ворошилова Т.В. Социальная и психологическая характеристика личности компьютерного преступника: практ. пособие. М.: ВНИИ МВД России. 2009. С. 5.

3. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2001. С. 496.

4. Дуленко В.А., Мамлеев Р.Р., Пестриков В.А. Преступления в сфере высоких технологий: учеб. пособие / В.А. Дуленко, Р.Р. Мамлеев, В.А. Пестриков. М.: ЦОКР МВД России, 2010. С. 67

5. Сычев Ю.Н. Основы информационной безопасности : учебно-практическое пособие / Ю.Н. Сычев. Изд. центр ЕАОИ, 2007. С. 300.

1. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2001. С. 496. [↑](#footnote-ref-1)
2. Уголовный кодекс Российской Федерации от 13.06.1996 №63 – ФЗ (ред. от 23.04.2018) // СЗ.1996. № 25. Ст. 2954 [↑](#footnote-ref-2)
3. Сычев Ю.Н. Основы информационной безопасности : учебно-практическое пособие / Ю.Н. Сычев. Изд. центр ЕАОИ, 2007. С. 300. [↑](#footnote-ref-3)
4. Дуленко В.А., Мамлеев Р.Р., Пестриков В.А. Преступления в сфере высоких технологий: учеб. пособие / В.А. Дуленко, Р.Р. Мамлеев, В.А. Пестриков. М.: ЦОКР МВД России, 2010. С. 67 [↑](#footnote-ref-4)
5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 27.12.2018) // Собрание законодательства РФ. - 17.06.1996. - № 25. [↑](#footnote-ref-5)
6. Ворошилова Т.В. Социальная и психологическая характеристика личности компьютерного преступника: практ. пособие. М.: ВНИИ МВД России. 2009. С. 5. [↑](#footnote-ref-6)