Министерство внутренних дел Российской Федерации

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

Кафедра уголовного права

ДИПЛОМНАЯ РАБОТА

на тему «Преступления в сфере цифровой информации: понятие, виды и юридический анализ составов преступлений»

Выполнил: слушатель 5 курса 192 уч.гр.,
специальность 40.05.01
Правовое обеспечение национальной безопасности,
2019 года набора
Кузнецова Валерия Владимировна

Руководитель:
Начальник кафедры уголовного права
КЮИ МВД России,
кандидат педагогических наук, доцент
полковник полиции
Куликов Роман Сергеевич

Рецензент:
Начальник ОП №13 «Азино-2»
УМВД России по г. Казани
полковник полиции
Харисов Нагим Ахтямович

Дата защиты: "____" _____20___г. Оценка _____

Казань 2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 3
ГЛАВА 1. ПОНЯТИЕ И ПРИЗНАКИ ИНФОРМАЦИОННЫХ ПРЕСТУПЛЕНИЙ, ОБЩАЯ ХАРАКТЕРИСТИКА СОСТАВОВ ИНФОРМАЦИОННЫХ ПРЕСТУПЛЕНИЙ, СОДЕРЖАЩИХСЯ В УК РФ…..7
§ 1. Понятие информации и компьютерной информации в уголовном праве 7
§ 2. Понятие и признаки информационных преступлений 13
§ 3. Общая характеристика составов информационных преступлений, содержащихся в УК РФ 25

ГЛАВА 2. ВИДЫ ИНФОРМАЦИОННЫХ ПРЕСТУПЛЕНИЙ 33
§ 1. Информационные преступления, предметом которых является информации 33
§ 2. Информационные преступления, способом совершения которых является информационное воздействие 38

ГЛАВА 3. ПРАВОВОЕ РЕГУЛИРОВАНИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В РОССИИ И ЗА РУБЕЖОМ 41
§ 1. Понятие компьютерных преступлений, их место среди информационных преступлений 41
§ 2. Виды компьютерных преступлений 47

ЗАКЛЮЧЕНИЕ 69
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ 72
ПРИЛОЖЕНИЯ 81

ВВЕДЕНИЕ

Актуальность темы. Постоянное совершенствование информационных технологий и стремительное распространение электронно-вычислительных систем почти в каждой области жизнедеятельности граждан сформировали большие проблемы, связанные с нормативным регулированием общественных отношений, которые, в свою очередь, связаны непосредственно с компьютеризацией общества в целом. В связи с этим, формируется такая отрасль права как компьютерное право, которое рассматривает все возможные методы и способы совершения преступлений в сфере цифровой информации.

В качестве объекта данных преступлений могут выступать непосредственно компьютеры, ноутбуки и другие устройства, а также то, что находится на самом техническом средстве, например, программное обеспечение, база данных и др.

Достаточно распространенным преступлением считается преступление, связанное с неправомерным доступом к компьютерной информации. Данные преступные деяния посягают на охраняемые законом сведения, совершающиеся с целью обнаружения нужной информации, чтобы в дальнейшем ее применять в корыстных целях. Преступления в сфере цифровой информации с годом набирают все большее значение в силу того, что людей, использующих цифровые устройства, становится все больше, как и информации, располагаемой на их личных устройствах.

Юридические отличительные признаки преступных деяний в области цифровой информации исследованы недостаточно. Так, многие авторы изучают подобную проблематику, и, в том числе, занимаются изучением объекта, предмета и способов совершения подобного рода преступных деяний. Немаловажным будет отметить то, что некоторые правоведы определенным образом рассматривают и критикуют главу 28 Уголовного кодекса Российской

Федерации (далее – УК РФ),[1] которое раскрывают те преступные деяния, связанные с использованием компьютерной информации.

Но даже если не акцентировать внимание на теоретических мнениях, то можно заметить, что и на практике слишком сложно бороться с преступлениями в области цифровой информации, в связи с тем, что преступники на постоянной основе оказываются на шаг впереди государственных органов, по причине того, что у действующих сотрудников нет соответствующих познаний в этой области. Вследствие чего образуется плохое представление возможных действий преступников.

На основе вышеупомянутого, подчеркивается большая актуальность подобной проблемы тем, что совершаемые преступные деяния в области цифровой информации происходят в тех странах, где цифровые технологии находятся уже на высоком уровне развития. В связи с этим появляется потребность в создании соответствующих правовых положений для борьбы с цифровыми преступлениями. Нормативные акты, регламентирующие гражданскую ответственность, где рассматривается возмещение ущерба, не способны как-либо помешать совершению преступлений в области цифровых технологий.

Говоря непосредственно о статистике, которая связана с совершением различных преступлений в области цифровой информации, то стоит отметить, что число ИТ-преступлений в России за 2023 год выросло на 29,7% в сравнении с 2022-м[2]. Такую статистику официальный представитель Министерства внутренних дел (МВД) РФ Ирина Волк привела 8 февраля 2024 года.

По ее словам, каждое третье преступление в России по итогам 2023 года совершено с использованием информационно-телекоммуникационных технологий. Раскрываемость таких уголовно наказуемых деяний в 2023 году увеличилась на 21%, рассказала Волк[3].

---

[1] Уголовный кодекс Российской Федерации: Федеральный закон №63-ФЗ: принят Гос. Думой 13.06.1996: по состоянию на 10.06.2024г. - Справ. - правовая система «КонсультантПлюс»

[2] https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России

[3] https://www.tadviser.ru/index.php/Компания:Министерство_внутренних_дел_РФ_(МВД)

В рамках данной работы изучено понятие и признаки информационных преступлений, а также была рассмотрена общая характеристика составов информационных преступлений, содержащихся в УК РФ. Вместе с этим были изучены виды информационных преступлений, а также их правовое регулирование в России и за рубежом.

Цель дипломной работы – исследовать и оценить правовые нормы, характеризующие такое понятие как «компьютерное преступление», а также рассмотреть уголовно-правовую структуру неправомерного доступа к цифровой информации. Исходя из поставленной цели, имеется ряд **задач**:

1. Сформулировать понятие информации и компьютерной информации в уголовном праве;
2. Рассмотреть понятие и признаки информационных преступлений;
3. Дать общую характеристику составов информационных преступлений, содержащихся в УК РФ;
4. Рассмотреть информационные преступления, предметом которых является информация;
5. Рассмотреть информационные преступления, способом совершения которых является информационное воздействие;
6. Уточнить понятие компьютерных преступлений и провести анализ их места среди информационных преступлений;
7. Рассмотреть виды компьютерных преступлений.

Предмет дипломной работы – законодательство, непосредственно связанное с противодействием преступлениям в сфере цифровой информации.

Исследование данной темы производилось с помощью следующих **методов**: общетеоретический, анализ, логический, сравнительно-правовой и др.

Краткая характеристика дипломной работы. Во введении четко определены предмет, объект исследования, а также цели и задачи, осуществляемые во время написания работы.

Первая глава посвящена рассмотрению понятия и признаков информационных преступлений, общей характеристике составов

информационных преступлений, содержащихся в УК РФ. Так, поднимаются вопросы касаемо исторического аспекта развития, выявления и расследования подобных преступлений, а также исследуется вопрос, необходимый для полного всестороннего рассмотрения первой главы, который связан с характеристикой преступления в целом.

Вторая глава посвящена уже непосредственному рассмотрению видов информационных преступлений. Проанализированы главы 17 и 21 УК РФ. Проведен сравнительный анализ информационных преступлений, предметом которых является информация и информационных преступлений, способом совершения которых является информационное воздействие, и всех иных преступлений по главам УК РФ с разнообразными группами информационных преступлений по разделам УК РФ.

Третья глава посвящена вопросам квалификации преступлений в сфере компьютерных преступлений, а также изучению отдельных квалифицирующих признаков и судебной практики по данным делам. Проанализирована общая характеристика преступлений, совершаемых в данной сфере, а также установлены отграничения от смежных составов преступлений.

В заключении сформулированы научно обоснованные выводы. Достоверность выводов подтверждается внушительным списком использованных нормативно-правовых актов и литературы.

Юридическая оценка преступлений в сфере цифровой информации требует полноценного изучения и применения соответствующих статей уголовного законодательства. Также в контексте информационных технологий, вместе с этим важно учитывать особенности цифровой среды, включая сложности, которые связаны, например, с идентификацией лиц, совершивших преступление.

Теоретическая основа построена на базе трудов таких авторов как: Щепетильников В.Н., Копылов, В.А., Батурин Ю.М., Дремлюга Р.И., Г.Н. Борзенкова, Комиссарова В.С., Крылов В.В., Ляпунов Ю., Максимов В., Наумов В., Симкин Л.С., Талимончик В.П., Фролов Д.Б., Старостина Е.В. и др.

Нормативно-правовая основа – Конституция Российской Федерации, Уголовный кодекс Российской Федерации, Федеральный закон «Об информации, информатизации и защите информации», Федеральный закон «О связи», Федеральный закон «Об участии в международном информационном обмене» и др.

Научная новизна заключается в том, что составы преступлений в сфере цифровой информации, которые регламентируются УК РФ, исследуются с учетом новейшего российского информационного и телекоммуникационного законодательства. В данной работе проведен терминологический анализ понятий, которые имеются в российском уголовном законе в процессе описания элементов и признаков таких преступлений. Исследование зарубежного и российского уголовного законодательства поспособствовало сделать выводы о тенденциях и современных направлениях совершенствования норм уголовного права, которые устанавливают уголовную ответственность за преступные деяния в сфере цифровой информации.

Апробация результатов исследования. Результаты исследования и выработанные положения апробированы в ходе следующих научно-представительских мероприятий:

– на Всероссийской научно-практической конференции – финале всероссийского конкурса курсантов и слушателей образовательных организаций МВД России «Теория и практика противодействия преступности уголовно-правовыми средствами» на лучшую научно-исследовательскую работу, прошедшей 30 мая 2024 г. в КЮИ МВД России (г. Казань);

– на Всероссийской научно-практической конференции «Уголовное и уголовно-исполнительное законодательство: вчера, сегодня, завтра», прошедший 6 июня 2024 г. в Нижегородской Академии МВД РФ.

– опубликована статья «Информационные преступления» в сборнике научных статей «Кирсановские чтения. Выпуск X. 2023 год» (стр. 204-207).

– на Всероссийском круглом столе «Противодействие преступности уголовно-правовыми средствами», а также одноименной научно-практической конференции, прошедшей 9 февраля 2024 г. (г. Уфа)

Структура дипломной работы: введение, три главы, разбитые на параграфы, заключение, список литературы.

ГЛАВА 1. ПОНЯТИЕ И ПРИЗНАКИ ИНФОРМАЦИОННЫХ ПРЕСТУПЛЕНИЙ, ОБЩАЯ ХАРАКТЕРИСТИКА СОСТАВОВ ИНФОРМАЦИОННЫХ ПРЕСТУПЛЕНИЙ, СОДЕРЖАЩИХСЯ В УК РФ

§1. Понятие информации, компьютерной информации в уголовном праве

На сегодняшний день компьютерная информация вошла полностью во все сферы жизнедеятельности человека. Сейчас от нее зависит работоспособность и совершенствование во многих сферах жизнедеятельности, например, промышленной сферы, строительной, медицинской и др. Главная роль данной информации заключается в удовлетворении всех нужд населения в общении друг с другом посредством, допустим, различных социальных сетей, мессенджеров. Также важно сказать, что совершенствование систем мобильной или же спутниковой связи, появление сети Интернет повысило значение цифровой информации в образовании всеобщего информационного пространства. Компьютерная информация является основой для возникновения информационных отношений[1].

Термин «компьютерная информация» закрепилось в обыденной жизни каждого гражданина. Сегодня никак нельзя представить жизнь человека без использования данной технологии, так как с помощью нее люди удовлетворяют свои потребности посредством просмотра цифровых видео в интернете, просмотра новостных телеканалов, показываемых по цифровому телевидению и др. Помимо этого, цифровая информация также сильно влияет и на формирование правоотношений в области цифровой коммерции.

С точки зрения А.Ю. Чупровой, цифровая коммерция представляет собой применение интернета для совершения разного рода деловых операций. Традиционным ее видом являются выполняемые в цифровой форме финансовые

[1] Бегишев И. Р. Цифровая информация: понятие и сущность как предмета преступления по российскому уголовному праву / И.Р. Бегишев // Академический юридический журнал - 2021. - № 2. - С. 47-49.

операции и различные договорные сделки одного предприятия или организации с другой организацией или с физическим лицом. Выполняемые в цифровом виде транзакции представляют собой различные деловые операции с применение цифровых технологий. Цифровое общество наряду с многообразными возможностями современных технологий толкует правила совершенствования экономических отношений. С каждый днем цифровая информация становится все более ценным инструментом каждой организации. Во время совершенствования цифровых технологий появляются и разного рода противоправные допуски к личным данным граждан, которые в дальнейшем могу нанести большой вред, в особенности отдельным категориям граждан или же большим предприятиям[1].

Этот вид преступлений появился сравнительно недавно и имеет ряд уникальных особенностей. Так что необходимо обратить внимание на предмет преступления. Это: электронные компьютеры (компьютеры), автоматизированные компьютерные системы (АКС), компьютерные сети, компьютерные носители информации. Компьютер - это комплекс электронных устройств, построенных на базе микропроцессоров и предназначенных для автоматической обработки информации при решении вычислительных и информационных задач. АС - это организационно-технические системы, в которых технология обработки информации реализована с использованием аппаратного и программного обеспечения.

В связи с наличием некоторых особенностей, информация представляет собой важный инструмент, способный оказать большое влияние для совершения различных преступных посягательств. Акцентируя внимание на большом значении цифровой информации, в настоящее время, большую роль играют и перспективы ее уголовно-правовой охраны, а вместе с этим и борьба с ее злоупотреблением. Имеющиеся возможности применения цифровой

---

[1] Шутова А. А. Социальная обусловленность норм об уголовной ответственности за посягательства на экономическую информацию / А.А. Шутова // Вестник Нижегородской правовой академии - 2019. - № 4. - С. 73-78.

информации создают также и новые категории преступлений, которые связаны с непосредственным противоправным завладением и дальнейшим использованием различных сведений. Параллельно с этим, важно сказать о том, что любые информационные средства сформированы на базе кодирования, а также передачи данных.

В. Б. Вехов верно отметил, что отсутствие четкого уголовно-правового определения компьютерной информации, единого понимания ее сущности как предмета преступного посягательства значительно затрудняет выработку общей концепции борьбы с компьютерными преступлениями[1].

Такое положение дел привело к тому, что различные ученые трактуют понятие «компьютерная информация» по-разному. Например, В.А. Мещеряков под ней понимает информацию, представленную в специальном виде[2].

Аналогичную точку зрения высказывает и М.В. Старичков[3], который под компьютерной информацией понимает зафиксированные на материальном носителе сведения, представленные в виде, пригодном для обработки с использованием компьютерных устройств, и предназначенные для использования в таких устройствах. В трудах других представителей уголовно-правовой науки содержатся и иные определения понятия «компьютерная информация». Так, Н.А. Зигура предлагает считать, что компьютерная информация – это сведения, представленные в электронно-цифровой форме на материальном носителе, создаваемые аппаратными и программными средствами фиксации, обработки и передачи информации[4].

В Уголовном Кодексе содержится состоящая из трех статей (272-274) глава «Преступления в сфере компьютерной информации». В соответствии со ст. 272[1]

---

[1] Вехов В.Б. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ // Уголовное право. - 2019. - № 4. - С. 15-22.

[2] Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: Изд-во Воронеж. гос. ун-та. - 2022. - С. 46-54.

[3] Старичков М.В. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института МВД России. - 2020. - № 1. - С. 20-26

[4] Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе России: автореф. дис. … канд. юрид. наук. Челябинск. - 2020. - С. 9-21.

УК под компьютерной информацией понимаются «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

То есть под преступлениями в сфере компьютерной информации следует понимать общественно опасные деяния (предусмотренные главой 28 Раздела IX УК РФ), которые посягают на сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Термин же «компьютерные преступления» несколько шире, чем «преступления в сфере компьютерной информации». Он охватывает и те преступления, где компьютерная техника, программы, компьютерная информация и цифровые каналы связи являются орудиями совершения преступления (понятно, что из разряда компьютерных преступлений мы исключаем такие преступления, в которых компьютерная техника используется лишь как материальная ценность) или объектом посягательства.

К таким преступлениям относятся: мошенничество с применением банковских карт (кардинг), мошенничество с выманиванием персональных данных (фишинг), незаконное пользование услугами связи и иной обман в области услуг связи, промышленный и иной шпионаж, когда объектом являются информационные системы, и т.д.

Однако представляется, что включение в определение компьютерной информации понятия «создаваемые аппаратными и программными средствами фиксации, обработки и передачи информации» является неоправданным. Это связано с тем, что создание компьютерной информации средствами фиксации и передачи информации невозможно, так как они являются только дополнительными элементами любой информационной системы. В связи с этим более уместным было бы говорить об аппаратных средствах создания и обработки информации, т.е. компьютерах, а в общем смысле – об информационно-телекоммуникационных устройствах, которые, как правило, и создают компьютерную информацию.

Так, до момента внесения изменений в Уголовный кодекс Российской Федерации[1] в редакции Федерального закона от 7 декабря 2011 года №420 –ФЗ[2] в России не было представлено официального толкования термина «цифровая информация». До этого в статье 272 УК РФ также не было представлено официального толкования термина цифровой информации, а лишь была речь о непосредственных физических носителях, на которых и хранилась сама информация. Также и в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[3] отсутствует точное определение термина «цифровой информации». В связи с тем, что в Российской Федерации до 2011 года не было точного определения термина цифровой информации, возникали разного рода барьеры, которые мешали эффективному развитию цифровой индустрии.

С точки зрения Угланова, в Российской Федерации отсутствует конкретный понятийный аппарат, способный проанализировать как непосредственную цифровую информацию, так и ее обмен. Данный факт предоставляет возможность использовать разнообразные понятия и вводить в заблуждение государственные органы, за счет чего уходить от ответственности за совершенные противоправные деяния. Рассматривая нормативные документы гораздо полноценней, обнаруживаются некоторые несостыковки в терминах и факт того, что нет конкретных их толкований. Подобная проблема рассматривается и Васильевым В.А., говоря о том, что вечная разработка поправок в Российском законодательстве, порождает также и юридические столкновения противоречивых точек зрений.

---

[1] Уголовный кодекс Российской Федерации: Федеральный закон №63-ФЗ: принят Гос. Думой 13.06.1996: по состоянию на 10.06.2024г. - Справ. - правовая система «КонсультантПлюс».

[2] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон №420-ФЗ: принят Гос. Думой 07.12.2011: по состоянию на 03.07.2016 г. - Справ.-правовая система «КонсультантПлюс».

[3] Об информации, информационных технологиях и о защите информации: Федеральный закон №149-ФЗ: принят Гос. Думой 27 июля 2006 г. № 149-ФЗ: по состоянию на 01.01.2024 г. - Справ.-правовая система «КонсультантПлюс».

Так, заводя речь непосредственно как о цифровой информации, так и о преступлениях, совершаемых в цифровой среде, можно сказать следующее, что лица, работающие в сфере «IT», так называемые «айтишники» хоть и не являются юристами и у них нет больших знаний в уголовном праве, однако они обладают своим понимание понятий «цифровая информация» и «цифровое преступление». Проводя сравнение между IT-специалистами и юристами, складывается следующая картинка:

Цифровая информация:

IT-специалисты определяют цифровую информацию как данные, которые находятся в цифровом формате или другими словами бинарном коде. Это могут быть тексты, изображения, видео, аудио, базы данных и другое.

Юристы же в уголовном праве цифровую информацию определяют как любые данные, которые могут применяться в качестве доказательств или содержать информацию, относимую к совершению преступления.

Цифровое преступление:

IT-специалисты описывают цифровое преступление как любое преступление, которое совершается с использованием компьютера или других цифровых устройств. Это может быть взлом компьютеров, кража данных, кибербуллинг, распространение порнографии и др.

Юристы в уголовном праве цифровое преступление определяют как любое преступление, которое касается компьютерных систем или сетей, либо использует компьютер в качестве инструмента для совершения преступления.

Исходя из этого, можно сказать, что IT-специалисты по большей части обращают внимание на технические аспекты цифровых преступлений, таких как метода взлома, виды вредоносного программного обеспечения и др. А юристы обращают свое внимание на юридическую сторону цифровых преступлений, таких как наличие злого умысла, наличие материального ущерба и др.

Подводя итог по данному параграфу, стоит отметить, что указанные выше авторы-правоведы правы по-своему и можно сделать вывод, что компьютерная информация обладает достаточно большим значением в современном обществе,

затрагивая абсолютно все сферы человеческой жизнедеятельности, а также помогает совершенствовать их. Компьютерная информация не только способствует легкому взаимодействию в сети Интернет, а также и изменяет экономические отношения посредством цифровой коммерции, которая дает новые возможности для предпринимателей и покупателей. Присутствие проблемы правильного определения и регулирования цифровой информации в Российском законодательстве говорит о том, что важно продолжать изучать единую структуру понятий и норм, за счет чего можно будет более эффективно управлять информационными данными.

§2. Понятие и признаки информационных преступлений

Преступления в области компьютерной информации - это социально вредные действия, которые определены в уголовном законодательстве и которые наносят ущерб или угрожают безопасности производства, хранения, использования или распространения информации, или информационных ресурсов.

Проводя анализ всех результатов, полученных в процессе изучения теории и практики, не удалось разработать единого толкования преступления в области цифровой информации. Подобного рода преступления в большинстве случае рассматриваются в качестве цифровых преступлений. Однако стоит отметить, что использование данного определения в отношении данных преступлений имеет место быть лишь с наличием большой доли условности, потому что в список цифровых действий, когда компьютерное устройство считается предметом посягательства, как и действия, когда компьютерные устройства выступают в роли технического средства, применяемые с целью совершения преступления. Такого рода обстоятельства наряду с использованием цифровых

данных для совершения преступления, например, мошенничества, не рассматривается как преступление в сфере цифровой информации. Лишь преступление, которое непосредственно совершается в отношении информационных устройств, допустим, ее похищение, рассматривается как преступление против собственности.

Так, М.А. Ефремова полагает, что компьютерная информация и устройства, на которых она зафиксирована или на которых она обращается, могут выступать средствами совершения преступлений. Из чего следует, что преступления, где компьютерная информация выступает средством совершения преступлений, образуют группу так называемых смежных преступлений и расположены в различных разделах и главах Особенной части УК РФ[1].

После того, как современные информационные технологии были включены в каждую сферу жизнедеятельности человека, они стали считаться составляющей частью, и затрагивают все ресурсы, которые занимаются управлением информацией, в число которых входит: компьютер, телекоммуникационные сети, программное обеспечение и др.

Динамика создания разного рода цифровых технологий с целью совершения преступлений растет с неимоверной скоростью и государство просто не может успеть за их распространением, по причине чего считается актуальным проблема об универсальности положений уголовного законодательства Российской Федерации. Естественно, главными и открытыми для изучения считаются статистические сведения о зарегистрированных преступных деяниях в области цифровой информации, которые говорят о наличии опасных быстроразвивающихся тенденциях.

Уровень зарегистрированных преступных деяний, которые совершались в области цифровой информации, с того момента как начал действовать УК РФ продемонстрировала то, что со временем количество совершаемых преступлений данной категории становится все больше и больше.

---

[1] Ефремова М. А. Уголовно-правовая охрана информационной безопасности. М.: Юрлитинформ. – 2019. - С. 226-237.

Доля киберпреступлений среди всех видов регистрируемых в России преступлений за год увеличилась с 31,8% до 38%. При этом относительно уровня 2023 года их массив возрос на 17,4% (до 240,9 тыс.). Такой информацией 30 мая 2024 года поделились в пресс-службе депутата Государственной Думы РФ Антона Немкина со ссылкой на Генпрокуратуру РФ[1].

Число ИТ-преступлений в России за 2023 год выросло на 29,7% в сравнении с 2022-м. Такую статистику официальный представитель Министерства внутренних дел (МВД) РФ Ирина Волк привела 8 февраля 2024 года.

В 2023 году МВД РФ выявило больше 100 тыс. ИТ-преступников, при этом на 20% увеличилось число раскрытых преступлений. Такой информацией 4 апреля 2024 года поделились в пресс-службе депутата Государственной Думы РФ Антона Немкина со ссылкой на министра МВД РФ Владимира Колокольцева[2].

Данное явление связано с возникновением в Российском законодательстве положений, предусматривающих уголовную ответственность за совершение преступлений в области цифровой информации, образованием отдельных подразделений, которые занимаются киберпреступлениями в области цифровой информации. Хоть государством и были предприняты некоторые меры, преступность в данной области никак не изменилась.

Помимо этого, отмечается, что существует большой уровень совершения скрытых преступления подобного рода преступлений. Весь объем совершенных цифровых преступления составляет не больше преступлений, связанных с игорной деятельностью и др.

Также важно упомянуть о том, что высокая общественная опасность данных преступных деяний имеется в связи с низким уровнем производства дознания и предварительного расследование по подобным преступлениям, в виду того, что у правоохранительных органов нет соответствующего уровня

[1] https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России.
[2] https://ria.ru/20240402/it-1937355272.html.

подготовки для раскрытия преступлений, совершаемых в информационном пространстве.

В данный момент существуют несколько точек зрения относительно понятия преступлений в сфере высоких технологий. Проблема точного определения этого понятия заключается в том, что практически невозможно выделить единый объект и предмет преступного посягательства, так как стремительное развитие информационно-телекоммуникационных технологий порождает новые объекты циркуляции цифровой информации.

З.И. Хисамова, проанализировав действующее законодательство и экономико-правовые реалии, пришла к выводу о том, что целесообразно использовать понятие «преступления, совершаемые в сфере использования информационно-коммуникационных технологий» для описания совокупности всех преступлений в сфере высоких технологий.[1] При этом под преступлениями, совершаемыми в сфере использования информационно-телекоммуникационных технологий, З.И. Хисамова предлагает понимать виновные общественно опасные деяния, причиняющие ущерб общественным отношениям, связанным с безопасностью охраняемой законом информации, соблюдением установленного законом порядка оборота и использования информационно-телекоммуникационных технологий.

Соответственно выделяются два основных вида преступлений в сфере обращения цифровой информации: преступления, предметом которых является цифровая информация, и преступления, способом совершения которых являются цифровые технологии. В настоящее время в уголовно-правовой науке сложилось три основных подхода к определению понятия преступления в сфере обращения цифровой информации. Первая часть исследователей к компьютерным преступлениям относит деяния, в которых компьютер является объектом или орудием совершения преступления. Вторая часть исследователей относит к

[1] Хисамова З. И. Квалификация посягательств, совершенных с использованием электронных средств платежа // Юридическая наука и правоохранительная практика. 2020. № 3 (33). С. 127-134.

компьютерным преступлениям только неправомерные действия в сфере обращения информации, циркулирующей в информационно-телекоммуникационных системах, в том числе неправомерный доступ к компьютерной информации. Третья часть исследователей считает, что под компьютерными преступлениями следует понимать информационные преступления.

Ежедневный рост числа пользователей информационных сетей помогает преступникам совершать еще больше преступлений, так как у новых пользователей просто на просто отсутствуют познания, которые бы помогли не поддаваться на злоумышленные действия. Также в связи с тем, что нет физических границ, преступники способны совершать преступления на территории нашего государства, то есть в России, но при этом располагаться в совершенно ином государстве, например, в Китае. Хоть на данный момент и происходит досконально изучение данной проблематики, но, несмотря на это, использование информационных технологий с целью совершения преступных деяний по-прежнему остается огромной проблемой для правоохранительных органов. Пострадавшими выступают миллионы людей не только в стране, но и по всему миру.

Как сообщает специальное подразделение, раскрывающее цифровые преступления, Управление «К» МВД России, в преступной информационной среде повышается уровень специализации и структуры главных функций, улучшается степень координации и общая площадь территорий, где совершаются цифровые преступления.

Тем самым было сформировано две категории данных преступлений в сфере цифровой информации:

1. Преступления, где в качестве предмета выступает цифровая информация;

2. Преступления, совершаемые с использованием цифровых технологий.

На сегодняшний день в уголовно-правовой науке создали несколько направлений для того, чтобы разработать четкое толкование преступлений в области цифровой информации.

Авторы, которые занимаются первым направлением включают в цифровые преступления те действия, где компьютерные устройства выступают в качестве объекта посягательства. Допустим подобного рода мнения придерживаются такие авторы, как Журавленко Н.И.[1], а также Номоконов В.А.[2].

Правоведы второго направления говорят о том, что цифровыми преступлениями выступают лишь противозаконные действия в сфере оборота цифровых данных в информационных сетях, например, в сети Интернет.

Каждая категория совершаемого преступления, непосредственно связанного с завладением цифровой информации, должна быть определенным образом охарактеризована.

1. **Неправомерный доступ к цифровой информации**. Такая категория преступных деяний имеет прямую связь с доступом к данным за счет нарушения законных прав. В перечень такого рода преступлений относятся разнообразные методы совершения преступлений, в результате которых происходит ознакомление, распространение, ликвидация или другие формы воздействия с цифровыми данными.

Так, Мардер Н.С. думает, что сеть Интернет способствует полной и достоверной передачи сведений, однако период времени для ее передачи может стать достаточно продолжительным и она может потерять свою актуальность. Также в качестве искажения получаемых сведений, может выступать попытка подмены одних сведений другими.

Так, приговором Якутского городского суда Республики Саха (Якутия) от 26 августа 2019 года осуждены Б.И. и Б.Д., которые действуя в составе

---

[1] Журавленко Н. И. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере / Н.И. Журавленко // Общество и право – 2018. - № 3. - С. 67-70.

[2] Номоконов В. А. Киберпреступность: прогнозы и проблемы борьбы / В.А. Номоконов // Библиотека криминалиста. - 2019. - № 5. - С. 150-154.

организованной группы, из корыстной заинтересованности осуществили неправомерный доступ к охраняемой законом компьютерной информации, использовали компьютерные программы, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации и нейтрализации средств защиты компьютерной информации.

Они же совершили мошеннические действия в сфере компьютерной информации, то есть хищение денежных средств в особо крупном размере путем ввода, модификации компьютерной информации и иного вмешательства в функционирование средств хранения, обработки, передачи компьютерной информации и информационно-телекоммуникационных сетей[1].

2. **Создание, использование и распространение вредоносных программ для информационно-телекоммуникационных устройств, их систем и сетей**. К числу способов совершения такого рода преступлений относят следующие виды: совершение преступления посредством доступа к данным с установкой вредоносной программы, а также способ доступа к данным удаленно.

Опираясь на практику, можно привести следующий случай для наглядного представления:

«Суд установил, что для активации операционной системы Windows гр. «В» осуществил запуск с жесткого диска вредоносной компьютерной программы RemoveWAT.exe, тем самым умышленно использовал и распространил ее, что привело к нейтрализации системы защиты операционной системы Windows. Как следует из приведенного приговора, действия В. суд квалифицирует по ч. 2 ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ как распространение и использование компьютерной программы, заведомо

[1] Приговор Якутского городского суда (Республика Саха(Якутия)) от 26 августа 2019 г. по делу № 1-1462/2018. - [Электронный ресурс]. URL: https://sudact.ru/regular/doc/8jIATe7oVfNK/ (дата обращения 10.06.2024).

предназначенной для блокирования компьютерной информации и нейтрализации средств ее защиты»[1].

3. **Нарушение работы информационно-телекоммуникационных устройств, их систем и сетей**. Сюда включаются преступные действия, например, которые непосредственно связаны с нарушением нормальной работоспособности информационно-телекоммуникационного оборудования, их систем и сетей. Допустим, покушение на нарушение, связанное с началом срабатывания системы защиты информационно-телекоммуникационного оборудования, в результате чего случился выход из строя устройств. Подобного рода действия обычно именуются как «отказ в обслуживании» и т.п. Покушение на атаку в виде создания определенной электромагнитной волны также способно создать проблемы в нормальной работоспособности информационно-телекоммуникационного оборудования.

4. **Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации**. Должное благосостояние страны в основном зависит от ее же безопасности. После нанесения ущерба информационной инфраструктуре, идут негативные последствия для ее безопасности, в связи с тем, что критическая информационная инфраструктура представляет собой важную составляющую часть между иными областями государственной системы, далее идут и негативные последствия в иных областях.

Так, сотрудница салона сотовой связи для выполнения плана продаж внесла в автоматизированную систему расчетов данные с где-то раздобытого скана паспорта незнакомого человека. Этим, согласно приговору суда, был нанесен вред критической информационной инфраструктуре РФ, поскольку оператор является субъектом КИИ, а автоматизированная система расчетов – значимым объектом КИИ.

---

[1] Приговор Октябрьского районного суда г. Кирова от 13 июля 2016 г. по уголовному делу № 1–298/2016. Электронный доступ - URL: https://rospravosudie.com/court-oktyabrskij-rajonnyj-sud-g-kirova-kirovskaya-oblast-s/act-532913468/ (дата обращения: 23.02.2024).

Приговор: 1 год и 6 месяцев условно с лишением права заниматься деятельностью, связанной с доступом к критической информационной инфраструктуре Российской Федерации, на срок 2 года.[1]

5. **Завладение информационно-телекоммуникационными устройствами обращения цифровой информации**. В эту категорию входят преступные деяния, непосредственно связанные с хищением чужой собственности, уголовная ответственность за данные преступления устанавливается статьями Уголовного кодекса Российской Федерации.

В качестве собственности тут обычно выступают различные носители цифровой информации, например, флешки, диски, мобильные устройства и др. Когда совершается хищение или же вымогательство и после этого происходит неправомерный доступ к цифровой информации, тогда как раз таки преступления и квалифицируется по статье 272 УК РФ «Неправомерный доступ к компьютерной информации».

Исходя из практического опыта, бывают случаи потери носителя данных, в связи с чем, другие лица могут неправомерно получить доступ к цифровой информации. Так, Евдокимов К.Е. считает, что необходимо ввести некоторые поправки в главу 28 Уголовного кодекса, а именно ввести дополнительную часть статьи 272 УК РФ под названием «Незаконное завладение носителем компьютерной информации с целью осуществления неправомерного доступа к компьютерной информации».

Так, например, ФИО2, находясь на территории г. Армавир Краснодарского края, не позднее 26 декабря 2021 года вступил в преступный сговор с Г.Г.Г., в отношении которого постановлен обвинительный приговор), который, работая в должности специалиста офиса продаж <данные изъяты> согласно трудовому договору № от 21 июня 2021 года и дополнительному соглашению № от 2 июля 2021 года к нему, имея единый умысел, направленный

[1] Приговор Петушинского районного суда (Владимирская область) от 19.09.2021 по делу № 1-146/2021 – [Электронный ресурс]. URL: https://actofact.ru/case-33RS0015-1-146-2021-2021-07-27-2-0/ (дата обращения 10.06.2024).

на неправомерный доступ к компьютерной информации для её последующего копирования, из корыстных побуждений, согласно которому в соответствии с распределенными между собой преступными ролями, ФИО2 предоставляет имеющиеся у него сведения об абонентах ПАО «МТС» для получения полных сведений о них, а Г.Г.Г.. в свою очередь, используя служебный компьютер и штатное программное обеспечение - информационную систему управления <данные изъяты> доступные ему в связи с его служебным положением и должностными обязанностями, получает информацию об абонентах ПАО «МТС» и копирует ее при помощи принадлежащему ему смартфона марки «Айфон 11» путем фотографирования, после чего пересылает ее с помощью вышеуказанного мобильного телефона ФИО2 за денежное вознаграждение от последнего[1].

6. **Перехват цифровой информации**. В цифровой среде, где происходит оборот электронной информации, в качестве одного из наиболее часто применяемого способа выступает перехват цифровых данных, потому что по сравнению с проводной передачей данных, они могут быть подвержены атаке только в Интернете.

Выделяют следующие беспроводные системы оборота цифровых данных: Bluetooth, Wi-Fi, AirDrop и другие, где цифровые сведения могут передаваться внутри информационной среды. Существенным минусом такого способа передачи данных является просто доступ к перенаправляемой информации для ее копирования, изменения и другим способам ее искажения или перехвата.

Перехват сведений в цифровой среде не может быть произведен без использования определенных технических устройств, которые применяются для получения сведений, обращение которых ограничено. Разновидностью перехвата данных выступает электромагнитный перехват, который происходит в помещениях, где располагаются информационно-телекоммуникационных устройства.

---

[1] Приговор № 1-346/2023 от 26 декабря 2023 г. по делу № 1-346/2023– [Электронный ресурс]. URL: https://sudact.ru/regular/doc/fpHL189SebmH/ (дата обращения 10.06.2024).

Данный способ способствует без какого-либо непосредственного контакта с данными устройствами обращения цифровой информации перехватить образующееся при работоспособности устройств электромагнитное излучение. Допустим, электронно-лучевая трубка экрана монитора излучает определенные электромагнитные волны, в которых как раз располагается цифровая информация. Преступники, используя специальные средства, перехватывают данные с одной аппаратуры на свою, на которой отображается идентичная информация, которая располагается на экране перехваченного цифрового устройства[1].

Так, в один из дней с (дата изъята) по (дата изъята), в период времени с 09 часов 00 минут по 21 час 00 минут, находясь на рабочем месте в офисе продаж АО «Мегафон Ритейл» по адресу: (адрес изъят), ФИО1, являющийся специалистом обслуживания и продаж Кировского филиала АО «Мегафон Ритейл», и в силу своего служебного положения осведомленный о возможности получения сотрудниками АО «Мегафон Ритейл» доступа к абонентским номерам и персональным данным клиентов ПАО «Мегафон», имея корыстную заинтересованность, решил за денежное вознаграждение от неустановленного лица осуществлять неправомерный доступ к служебной компьютерной информации, содержащейся в информационной системе программного обеспечения по обслуживанию клиентов, принадлежащей ПАО «Мегафон», путем копирования абонентских номеров и персональных данных клиентов ПАО «Мегафон» на мобильный телефон марки «Huawei» P20 Lite[2].

7. **Приобретение или сбыт цифровой информации, заведомо добытой преступным путем**. Сильно участились случаи продажи разного рода баз данных, которые говорят о том, что торговля конфиденциальными данными, начала представлять собой определенного рода бизнес. Различными методами

---

[1] Бегишев И. Р. Уголовная ответственность за перехват цифровой информации // Information Security / Информационная безопасность. 2010. № 4. С. 16-19.

[2] Постановление Ленинского районного суда г. Кирова (Кировская область) № 1-168/2020 от 21 февраля 2020 г. по делу № 1-168/2020. – [Электронный ресурс]. URL: https://sudact.ru/regular/doc/Yg7GKxGlWEmV/.

подобной добычи считаются, как правило, хищения и вымогательства цифровых сведений, чтобы в будущем их продать.

8. **Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации**. Стадия вмешательства в цифровые устройства, допустим для внесения изменения в цифровые данные, начинается после стадии обхода или нарушения защитной системы цифровой информации, так как по-другому данные сведения получить невозможно. В связи с этим, имеющиеся на сегодняшний день цифровые технологии находятся под хорошей защитой с целью избежать несанкционированного доступа к цифровым данным.

Указанная выше классификация говорит о том, что различные способы для совершения преступных посягательств в области оборота цифровой информации обладают определенными особенностями. В основном эти действия сопровождаются надежными способами маскировки, в связи с чем появляются существенные проблемы для их обнаружения и дальнейшего расследования преступления. Также следует отметить, что в большинстве случаев преступники применяются разнообразные комбинации способов для получения сведений. В виду постоянного изменения и усложнения логических связей, возникают иные способы для совершения преступления в сфере цифровой информации.

Подводя итог по данному параграфу, можно сказать, что анализ нынешнего состояние преступности в области компьютерной информации демонстрирует то, что, несмотря на усилия органов государства, проблема с информационными преступлениями все еще имеется. Из-за того, что нет точного определение понятия «цифровое преступление» и наличие достаточно сложной классификации подобного рода преступлений ухудшают эффективное противодействие преступлениям. Также не малой проблемой считается слабая подготовка сотрудников и быстроразвивающиеся информационные технологии, которые обгоняют возможности их контролирования.

§ 3. Общая характеристика составов информационных преступлений, содержащихся в УК РФ

Преступные деяние в области цифровой информации первый раз в Российском праве были введены в УК РФ в составе отдельной главы в 1996 году под влиянием более широкого применения электронно-вычислительных машин в жизнедеятельности граждан.

В качестве подобного рода преступлений выступают следующие деяния:

1. Компьютерное мошенничество, которое определяется как ввод, изменение или удаление данных или программ компьютера или иное вмешательство в процессы обработки данных, влияющее на итоги обработки данных, которое причиняет экономический ущерб или приводит к уничтожению собственности другого лица, совершаемое с целью получения незаконным путем экономической выгоды для себя или для другого лица.

2. Компьютерный подлог, то есть ввод, изменение или удаление данных (программ) компьютера либо другое вмешательство в процесс обработки данных, совершенное способом или при условиях, установленных нормами национального законодательства, которыми эти деяния квалифицируются как подлог, и совершены в отношении традиционного объекта правонарушения.

3. Причинение ущерба компьютерным данным или компьютерным программам, то есть незаконное удаление, причинение ущерба или ухудшение качества данных или программ компьютера.

4. Компьютерный саботаж: ввод, изменение или удаление данных или программ компьютера, или создание помех компьютерным системам с целью воспрепятствования работе компьютера или телекоммуникационной системы.

5. Несанкционированный доступ, представляющий неправомочный доступ к системе или компьютерной сети путем нарушения мер охраны.

6. Несанкционированный перехват, то есть неправомерный и осуществленный с применением технических средств перехват сообщений,

направленных в систему или сеть компьютеров, исходящих из системы или сети компьютеров и передаваемых в рамках системы или сети компьютеров.

7. Несанкционированное воспроизведение компьютерной программы, охраняемой авторским правом. Под ним понимается совершенное неправомерно распространение, воспроизведение или передача в общественное пользование компьютерной программы, охраняемой законом.

8. Несанкционированное воспроизведение микросхемы, то есть совершенное неправомерно воспроизведение микросхемы изделия на полупроводниках, если она охраняется законом, либо неправомерное использование или импорт в коммерческих целях микросхемы или изготовленного с ее применением изделия на полупроводниках.

В 1991 году Интерпол разработал определенный кодификатор компьютерных преступлений и способов их совершения.

В 2001 году в городе Минск было заключено следующее Соглашение: «Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации», которое выделяло в качестве уголовно наказуемых такие действия как:

а) осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;

б) создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред или тяжкие последствия;

г) незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб.

Через некоторое время это Соглашение было заменено на «Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий», которое было заключено в городе Душанбе 28.09.2018. В данном документе, который вступил в силу 12 марта 2020 года, содержались главные термины, а также был увеличен список уголовно наказуемых деяний в области информационных технологий, в число которых входят:

а) уничтожение, блокирование, модификация либо копирование информации, нарушение работы информационной (компьютерной) системы путем несанкционированного доступа к охраняемой законом компьютерной информации;

б) создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации компьютерной системы лицом, имеющим к ней доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, если это деяние причинило существенный вред или тяжкие последствия;

г) хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации, либо сопряженное с несанкционированным доступом к охраняемой законом компьютерной информации;

д) распространение с использованием информационно-телекоммуникационной сети «Интернет» или иных каналов электрической связи порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего;

е) изготовление в целях сбыта либо сбыт специальных программных или аппаратных средств получения несанкционированного доступа к защищенной компьютерной системе или сети;

ж) незаконное использование программ для компьютерных систем и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб;

з) распространение с использованием информационно-телекоммуникационной сети «Интернет» или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма.

Так, в период с 01 января 2018 года по 10 января 2018 года у находящегося на территории г. Вологды ФИО1, обладающего достаточными знаниями в области информационных технологий, из соображений любопытства и совершенствования собственных навыков владения компьютерными программами, с целью просмотра видеоизображений с камер наружного видеонаблюдения возник преступный умысел, направленный на использование вредоносной компьютерной программы, заведомо предназначенной для несанкционированного копирования компьютерной информации и нейтрализации средств защиты компьютерной информации[1].

Так, говоря уже непосредственно об определении преступления в сфере компьютерной информации, то это предусмотренные уголовным законом виновные общественно опасные деяния, которые способны причинить вред или создают угрозу причинения вред отношениям в области производства, хранения, использования и распространения цифровой информации.

---

[1] Приговор Вологодского городского суда (Вологодская область) № 1-1094/2020 от 24 сентября 2020 г. по делу № 1-1094/2020 – [Электронный ресурс]. URL: https://sudact.ru/regular/doc/CauwPP3H3Bml/ (дата обращения 10.06.2024 г.).

В качестве родового объекта преступлений в области компьютерной информации выступает общественная безопасность и общественный порядок соответственно разделу, в котором содержится глава 28 УК РФ.

В качестве видового объекта выступают общественные отношения в области обеспечения безопасности компьютерной информации. Безопасность компьютерной информации распространяет свое действие на сведения в компьютерных устройствах и может быть рассмотрена в роли элемента информационной безопасности.

Говоря же о самой компьютерной информации, то в соответствии со статьей 272^1 УК РФ считаются данные, которые представляются в виде электронных сигналов, независимо от средств их хранения, обработки и передачи.

В качестве потерпевшего от подобного рода преступлений выступают лица, являющиеся обладателями данной информации. В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам. Данное лицо имеет право:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Объективная сторона данных преступлений может выражаться как в действиях, так и в бездействиях, однако, по большей части эти преступные деяний совершения путем совершения определенных действий. Но нарушение эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации возможно также и путем бездействия.

Подавляющее число действий, которые регулируются главой 28 УК РФ, сформированы по типу материальных составов и предусматривают наличие описанных в диспозиции статьи деяний, последствий в форме уничтожения, блокирования, изменения или копирования цифровой информации. В большинстве случае местом совершения преступления может признаваться как место совершения деяния, так и место, в котором деяние окончено либо пресечено, либо место наступления общественно опасных последствий.

Важным моментом при определении состава преступления является наличие (отсутствие) специальных мер по защите информации. Другими словами, считается ли доступ незаконным при отсутствии защиты информации или квалифицируется как таковой только с защищенной конфиденциальной информацией? В статье 22 Федерального закона «Об информации, информационных технологиях и защите информации» законодательный орган делает заявление по этому поводу: «Владелец документов ... или уполномоченные им лица ... определяют порядок предоставления информации. Пользователю ... и собственнику ... обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации».

Только такой доступ к секретной информации, уровень защиты которой соответствует ее конфиденциальности, может быть признан незаконным, в противном случае было бы неуместно говорить о незаконности. Статья 272 Уголовного кодекса Российской Федерации посвящена такому виду преступления, как незаконный доступ к компьютерной информации. Он показывает признаки, характерные для объекта, а также для обеих сторон состава преступления - объективного и субъективного. Предметом уголовного

преступления является компьютерная информация, которая находится на машинном носителе и защищена законом.

Субъективная сторона рассматриваемых деяний может характеризоваться как умышленной, так и неосторожной формами вины. Среди мотивов, характерных для всех компьютерных преступлений, преобладают два основных: корысть и «интеллектуальный вызов», то есть стремление продемонстрировать собственный профессионализм.

Субъект преступления общий – вменяемое физическое лицо, достигшее возраста 16 лет, за исключением случаев нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, совершаемых специальным субъектами – лицами, но которых возложены обязанности по соблюдению указанных правил (ст.ст. 274, 274.1 УК РФ).

В качестве примера можно примести следующий случай:

Специалисты управления «К» МВД России вместе с коллегами из Москвы, Свердловской и Оренбургской областей пресекли деятельность межрегиональной группы, создававшей и распространявшей вредоносные компьютерные программы».

«Установлено, что злоумышленники на специализированных ресурсах в интернете, в том числе в теневом сегменте, осуществляли распространение вредоносного программного обеспечения, предназначенного для модернизации персонажей многопользовательских компьютерных игр», - сказала официальный представитель МВД России Ирина Волк.

У тех, кто использовал программу, было преимущество перед другими участниками игры.

Следствие возбудило уголовное дело по ч. 2 ст. 273 УК РФ (создание, использование и распространение вредоносных программ для ЭВМ, повлекшие тяжкие последствия).

«В ходе обысков, проведенных по адресам проживания сообщников, изъяты: компьютерная техника, свыше 100 банковских карт, мобильные телефоны, а также денежные средства в размере свыше 8 млн. рублей, предположительно полученные в результате преступной деятельности», - пояснила Волк.

Специалисты установили одного из участников схемы, проживающего в Санкт-Петербурге. Именно у него приобреталось программное обеспечение. Во время обыска у него изъяли доказательства причастности.

Для 3 фигурантов избрали меру пресечения в виде подписки о невыезде и надлежащем поведении. В настоящее время продолжается предварительное расследование.

Подводя итог, стоит отметить, что введение преступлений в сфере цифровой информации в УК РФ в 1996 году говорит о постоянно растущем значении информационных технологий в жизнедеятельности граждан и важности защиты информационной безопасности. Преступные деяния, которые связаны с цифровой информацией, затрагивают большой перечень деяний, от компьютерного мошенничества до несанкционированного доступа и распространения вредоносных программ, что подчеркивает их разнообразие и сложность. Международное сотрудничество, в том числе соглашения, которые были заключены в пределах Содружества Независимых Государства, говорит о важности объединения усилий в борьбе с данными преступными деяниями.

ГЛАВА 2. ВИДЫ ИНФОРМАЦИОННЫХ ПРЕСТУПЛЕНИЙ

§ 1. Информационные преступления, предметом которых является информация

В качестве информационных преступных деяний, где в роли предмета выступает информация, считаются противозаконные действия, способные нанести ущерб общественным отношениям в области реализации цифровой безопасности человека, социума и страны в целом, воспринимая информацию определенным нематериальным объектом.

Для того чтобы более полно раскрыть сущность составов преступлений данной категории, важно рассмотреть Рисунок 1.

Рисунок 1. Схема составов информационных преступлений

Стоит отметить, что информационные преступления, где в качестве предмета выступает информация, имеются далеко не в каждой главе уголовного законодательства Российской Федерации, так как они располагаются только в 50% всех глав УК РФ.

Больше всего преступлений данного вида, предметом которых выступает информация, регламентируются главой 28 УК РФ – 100% и в главе 19 – 50% УК РФ. Данное явление заставляет лучше рассмотреть преступления, регламентированные главой 19.

Не малое число преступлений в области информационных преступлений в главе 19 УК РФ обуславливаются тем, что некоторые цифровые правомочия населения обладают конституционный характер. В том числе статья 23 Конституции утверждает возможность любого человека на неприкосновенность личной жизни и правомочие на тайну переписки, телефонных переговоров и др.

Рассматривая статью 24 Конституции РФ, можно увидеть, что они определяют то, что собирание, хранение, применение, а также распространение сведений о частной жизни гражданина без него ведома запрещены. Представители государственных органов, в том числе органов местного самоуправления должны предоставлять любому возможность ознакомиться с документами, которые имеют отношение к правам и свободам человека, в случае, когда этого не установлено нормативным актом.

В соответствии с частью 4 статьи 29 Конституции РФ, любой обладает возможностью заниматься поиском, получать, создавать, а также заниматься распространением сведений, но только законным путем.

С точки зрения А.Д. Антонова, основное нормативное правило к каждой статье уголовного закона заключается в должном соблюдении стандартных принципов, которые находятся в основе всей структуры права. В роли нормативного документа, который реализует эти принципы, выступает Конституция, почему это требование и считается принципом конституционной адекватности.

Легко обратить внимание на то, что почти каждое преступное деяние посягает на конституционные правомочия граждан и их законные интересы. Особенно, достоинство личности, ее свобода и неприкосновенность регламентируются нормами Конституции РФ, имеющих непосредственную связь с главой 17 УК РФ, а правомочие на частную собственность имеет тесную связь с главой 21 УК РФ. Но нормативные положения, которые связаны с охраной чести и достоинства рассматриваются законодательством в отдельной главе УК, а составы, которые охраняют информационные права, объединились с иными составами 19 главы УК РФ, без помощи отделения для них конкретной главы, направленной на охрану информационных правомочий. Исходя из этого, можно сказать, что проблема, связанная с выделением данной главы должна быть доработана и более тщательно исследована.

Подобной точки зрения придерживается и ряд других правоведов, в том числе В.А. Копылов, который рассматривает охрану информационных прав и законных интересов личности как отдельное направление нормативного обеспечения цифровой безопасности. Подобное направление, по его мнению, находится под охраной положений уголовного законодательства, которое регламентирует ответственность за такие преступные деяние как:

1. Клевета.

В уголовном праве данное деяние представляет собой распространение заведомо ложной информации о другом лице, которая задевает его честь, достоинство и подрывает репутацию. В качестве объекта выступает честь и достоинство личности, а также деловая репутация физического или юридического лица. Субъект – физическое лицо, достигшее 16 лет, вменяемое. Объективная же сторона заключается в действиях, которые направлены на распространение заведомо ложной информации, которая способна нанести вред чести, достоинству или репутации лица.

Так, 45-летняя жительница Тербунского района пришла в полицию ещё летом прошлого года. Женщина сообщила, что в сети Интернет на одном из

сайтов знакомств опубликованы материалы, порочащие ее честь и достоинство, подрывающие деловую репутацию.

Сотрудниками уголовного розыска в ходе проведенных оперативных мероприятий установлена подозреваемая в совершении преступления. Ею оказалась 50-летняя жильца Тербунского района.

«Полицейские выяснили, что подозреваемая, узнав об измене мужа, решила отомстить сопернице. В соцсетях нашла фотографию женщины, зарегистрировалась от ее имени на сайте знакомств, используя свой личный телефон, и разместила сведения порочащие честь и достоинство женщины. Полицейскими были проведены лингвистические исследование и экспертиза, доказавшие вину подозреваемой», - сообщили в пресс-службе регионального УМВД.

По данному факту возбуждено уголовное дело по признакам преступления, предусмотренного частью 2 статьи 128.1 Уголовного кодекса Российской Федерации «Клевета». Максимальная санкция инкриминируемой статьи предусматривает лишение свободы на срок до двух лет[1].

2. Оскорбление.

Оскорбление представляет собой унижение чести и достоинства другого лица, выраженное в неприличной форме. Оскорбление является административным нарушением, за которое могут наказать штрафом. Однако если кто-то оскорбил, к примеру, сотрудника правоохранительных органов, то это деяние уже квалифицируется как «публичное оскорбление представителя власти», регламентируемое статьей 319 УК РФ.

Так, жительница Алтайского края попала под суд за крепкие выражения в интернет-переписке. Бывшие супруги из Барнаула переписывались друг с другом в одном из популярных мессенджеров. Не сдержавшись, женщина оскорбила интернет-собеседника, применив слова и выражения, которые

---

[1] Жительница Тербунов оклеветала в Интернете соперницу. URL: https://lipetsktime.ru/news/incidents/zhitelnitsa_terbunov_oklevetala_v_internete_sopernitsu/ (дата обращения: 10.06.2024).

унизили его достоинство и честь. Участники предоставили на суде скриншоты своей занимательной переписки, не отрицая факт употребления эмоционально окрашенных выражений. Девушка свою вину признавать отказалась. Она объяснила свой поступок тем, что находилась в плену эмоций. Ее судили по административной статье. Эмоциональная горожанка заплатит штраф в 3 тысячи рублей, уточнили в Объединенной пресс-службе судов Алтайского края.[1]

3. Нарушение неприкосновенности частной жизни.

Данное преступление может относиться к действиям, которые непосредственно нарушают личную жизнь индивида без его согласия. Сюда могу входить разнообразные виды вмешательства, к примеру, незаконное прослушивание, видеонаблюдение, сбор, распространение или использование личной информации без разрешения человека.

4. Отказ в предоставлении гражданину сведений.

Данное преступление имеет место быть, когда государственный служащий или должностное лицо организации, которое обязано предоставить информацию в соответствии с законом, умышленно отказывает в предоставлении данной информации гражданину, который имеет право на получение такой информации.

5. Нарушение авторских и смежных прав.

Данное преступление относится к категории преступлений, которые связаны с незаконным использование интеллектуальной собственности без разрешения правообладателя. Сюда могу входить разнообразные формы интеллектуальной деятельности, такие как литературные, музыкальные и др. Такие преступления могут выражаться в копировании, распространении, публичном исполнении защищенных авторским правом произведений без разрешения автора.

Так, управление «К» МВД возбудило уголовное дело против 26-летнего москвича, который разместил на своей странице в «В контакте» 18 записей

---

[1] Девушку из Барнаула наказали за хамство в мессенджере. URL: https://www.ap22.ru/paper/Devushku-iz-Barnaula-nakazali-rublem-za-hamstvo-v-messendzhere.html

«известной российской музыкальной группы», сообщила пресс-служба управления. Дело возбуждено по ст. 146 УК «Нарушение авторских и смежных прав» (до шести лет лишения свободы) по обращению фирмы грамзаписи «Никитин», которой принадлежат исключительные права на эти записи [1].

6. И др.

Подводя итог данному параграфу, стоит отметить, что информационные преступления, которые непосредственно затрагивают цифровую безопасность человека, общества и государства в целом, представляют собой большую угрозу, так как влияют на конституционные права и свободы граждан. Помимо этого акцентируется внимание на принципе конституционной адекватности, которые отмечает важность соблюдения основных принципов права, регламентируемых Конституцией РФ.

§ 2. Информационные преступления, способом совершения которых является информационное воздействие

Информационными преступлениями, которые совершаются с помощью оказания информационного воздействия, считаются противозаконные действия, опасные для общества, способные нанести ущерб общественным отношениям по организации информационной безопасности личности, социума и страны в целом, где способом совершения преступления является информационное воздействие.

Важно сказать о том, что информационные преступления, которые совершаются посредством оказания информационного воздействия, располагаются в большинстве глав УК РФ. В связи с этим, отмечается явный

[1] Первое уголовное дело против пользователя соцсети за нарушение авторских прав.URL: https://www.vedomosti.ru/technology/articles/2011/01/20/v_kontakte_s_tyurmoj.

отличительный показатель, по сравнению с информационным предметом преступлений, способ совершения преступного деяния в форме определенного информационного воздействия довольно сильно распространен в большинстве главах уголовного законодательства.

Большинство нормативных положений уголовного законодательства, которые регламентируют информационные преступления, совершаемые посредством оказания информационного воздействия, охраняют информационную безопасность личности, общества и государства в целом за счет закрепления этих преступлений в законодательстве.

Также стоит отметить, что общее количество преступления данной категории увеличилось в главе 31 УК РФ в отличие от уголовного законодательства РСФСР 1960 г. с 36% до 48%. Это говорит о том, что происходит повышение объема общего количества преступлений в сфере информации. Говоря о преступных деяниях, направленных против порядка управления, можно отметить снижение количества составов с 15% до 8%, но подобное уменьшение не играет особой роли, потому что если говорит об абсолютных числах, то это выражено только одним составом преступления.

Если проводить сравнительный анализ информационных преступлений, предметом которых является информация, и всех иных преступлений по главам УК РФ и информационных преступлений, способом совершения которых является информационное воздействие, и всех иных преступлений по главам УК РФ с разнообразными группами информационными преступлениями по разделам УК РФ, то выделяются некоторые отличия по данным об информационных преступлениях, где в качестве способа совершения преступления выступает информационное воздействие.

Так, если рассматривать группы информационных преступлений по разделам УК, то здесь наибольшее число информационных преступлений являются преступления с информационным способом совершения (130 составов со способом совершения и 75 преступления, где предметом является информация), тогда как при рассмотрении информационных преступлений,

предметом которых является информация, и всех иных преступлений по главам УК РФ и информационных преступлений, способом совершения которых является информационное воздействие, и всех иных преступлений по главам УК РФ выходит, чуть ли не одинаково число (52 против 48). Данное расхождение можно оправдать тем, что наибольший объем преступлений в сфере информации, где способом их совершения считается информационное воздействие, занимают те посягательства, где информационный способом считается как квалифицирующий признак, когда главное деяние в пределах объективной стороны, регламентируемое частью 1 данной статьи, не имеет информационного значения.

Подводя итог, важно сказать, что информационные преступления, которые совершаются посредством информационного воздействия, представляют собой большую угрозу для информационной безопасности личности, общества и государства в целом. Они достаточно широко распространены в уголовном законодательстве Российской Федерации, что говорит о большом значении и опасности. Со временем число преступлений данной категории сильно увеличилось, что говорит о растущей проблеме в области информационной безопасности. Правовые положения уголовного законодательства активно регламентируют и охраняют от таких преступлений, что говори об их важности и необходимости защиты информационного пространства.

ГЛАВА 3. ПРАВОВОЕ РЕГУЛИРОВАНИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В РОССИИ И ЗА РУБЕЖОМ

§ 1. Понятие компьютерных преступлений, их место среди информационных преступлений

Понятие «компьютерные преступления» сформировалось уже в середине XX века с момента возникновения компьютерных устройств. На данный момент, по причине большого совершенствования цифровых технологий, возрастает и роль наиболее правильного толкования данного термина. Но, стоит сказать, что на сегодняшний день нет единой точки зрения у правоведов и научных работников. Это имеет отношение к понятийным противоречиям, где излагаются предложения о даче наименований компьютерных преступлений в преступления в информационной среде, а также и к противоречиям в отношении объема термина «компьютерные преступления».

Помимо этого, по мнению некоторых ученых, достаточно нередко в литературе по уголовному праву появляются сравнения информационных преступлений с компьютерными, то что, как мы думаем, неправильно, так как они обладают совершенно разными значениями.

Данное явление усложняется еще тем, что компьютерные преступления довольно часто обладают международным значением, в связи с тем, что некоторые данные способны передаваться с устройства на устройства на длинных расстояниях между собой. Данное значение нуждается в единообразии уголовно-нормативных положений с целью противодействия с ними, что отмечалось на организованной в 1999 г. в Санкт-Петербурге международной научной конференции, которая была направлена на поиск решений проблемы компьютерной преступности.

Параллельно с этим, отечественные ученые акцентируют внимание на слабом уровне изучения иностранного практического опыта, связанного с противодействием компьютерным преступлениям, однако в других государствах

данная проблема также выступает достаточной важной и образует для людей и государства в целом достаточно много проблем, которые полноценно изучаются.

Также, отмечается, что ученые в общей структуре принципов криминализации выделяется принцип трансграничной нормативной допустимости и важности. Опираясь на мнение А.Д. Антонова, сейчас этот принцип обладает двойным значением. Если рассматривать его с одной стороны, то Российская Федерация должна привести уголовное законодательство в порядок в соответствии с установленными международными требованиями, связанными с противодействием преступлениям, а если с другой, то каждая готовящаяся правка уголовного законодательства подлежит предварительному анализу и оценке соответствия его установленным требованиям.

Важным нововведением в области противодействия компьютерным преступлениям явилась разработка Европейской Конвенции о киберпреступности[1]. Большинство государств уже примкнули к данной Конвенции и разработали свое законодательство, опираясь на эту Конвенцию. Беря во внимание достаточно большой теоретический уровень готовности Конвенции, считается разумным во время разработки отечественных нормативных документов, которые будут направлены на противодействие преступности в информационной среде и во время изучения этих вопрос придерживаться также и ее нормами и разработками зарубежных ученых в этой сфере.

Подобный подход способен сформировать рабочие нормативные инструменты по противодействию киберпреступлениям в стране, а также и за рубежом. Данная точка зрения поддерживается несколькими учеными и вместе с этим нашла поддержку на государственном уровне. Так, в пункте 7 Доктрины информационной безопасности России, рассматривается такая задача, как координация деятельности сотрудников правоохранительных органов

[1] Конвенция о преступности в сфере компьютерной информации ETS N 185 от 23 ноября 2001 г. - Справ.-правовая система «КонсультантПлюс» (дата обращения: 10.04.2024).

государств, которые находятся в мировом сообществе, связанным с борьбой с киберпреступлениями.

В конце 1980-х годов, ученый Зибер, являющийся одним из лучших в области изучения преступлений в сфере информации, обратил внимание на то, что с каждым годом является очевидным тот факт, что компьютерные преступления помимо того, что считаются новейшей формой совершения преступлений, а также и вбирают в себя большое количество новых явлений, в том числе новые виды преступных деяний, которые совершаются за счет применения информационных технологий. Через некоторое время, Зибер сказал, что ответить на вопрос, как же нужно противодействовать данным преступлениям, никак нельзя без тщательного исследования главных норм, которые касаются парадигмы цифрового общества, где нематериальные предметы обретают все большее значение и бросают вызов обычным нормативным системам, который совершенствовались, опираясь на материальные вещи.

Начиная с середины 1980-х годов, Совет Европы изложил собственное толкование компьютерному преступлению, отличающееся на тот момент особой гибкостью[1]. Толкование было следующим: «это любое противозаконное, неэтическое или неуправомоченное поведение в отношении автоматизированной обработки и передачи данных». Исходя из данного толкования, можно назвать следующие признаки:

1. Противоправность;
2. Неэтичность;
3. Неуправомоченность;
4. Совершение преступления в отношении автоматизированной обработки и передачи данных.

[1] Майкл Бойл, Жан-Клод Вюльерм. Краткое пособие по проведению допросов в ходе следствия. Практическое руководство. Общеевропейские принципы и стандарты работы полиции. Совет Европы. 2020. Электронный ресурс - URL: https://rm.coe.int/guide-to-investigative-interviewingrussian/1680934b21 (дата обращения 10.04.2024).

В голландском уголовном праве, как отмечает проф. Х.Касперсен, учёные придерживаются мнения, что, скорее всего, невозможно дать удовлетворительное понятие компьютерного преступления, которое, будучи сформулировано в общих словах, потеряет самоочевидную ценность или, наоборот, будет слишком узким, если его сформулировать с помощью специальных терминов. Голландский консультативный комитет по компьютерным преступлениям, который занимался поправками к УК и УПК в 1987 г., не дал своего определения компьютерного преступления, однако представил типологию преступлений в данной области, из которой следует, что под компьютерными преступлениями он подразумевает любое поведение с уголовно наказуемым умыслом, которое: причиняет вред определённым интересам, связанным с автоматической обработкой данных. Эти интересы были обозначены как доступность данных, их целостность и конфиденциальность доступа к средствам (оборудованию) и данным.

Следует отметить, что криминалисты Нидерландов до сих пор придерживается рекомендаций комитета, сформулировавшего понятие компьютерных преступлений, и, по словам специалиста в области компьютерных преступлений проф. П. Виманса, компьютерные преступления, закреплённые в действующем УК Голландии, преследуют цель защиты трёх вышеупомянутых интересов.

Таким образом, можно сделать вывод, что под компьютерными преступлениями в рассмотренных зарубежных правовых системах понимается достаточно широкий круг деяний, связанных с электронной передачей данных, и что до сих пор не существует общего универсального определения, которое охватывало бы все категории компьютерных преступлений. Существующие определения являются во многом утилитарными, сформулированными для конкретных исследовательских целей. Для более детального анализа компьютерных преступлений необходимо обращаться к рассмотрению их отдельных видов.

§ 2. Виды компьютерных преступлений.

Анализ преступлений за неправомерный доступ к охраняемой законом цифровой информации, регламентируемых статьей 272 УК РФ

Объект данного преступления - общественные отношения, обеспечивающие правомерный доступ, создание, обработку, преобразование, использование компьютерной информации самим создателем, потребление ее иными пользователями, а также правильное функционирование ЭВМ, системы ЭВМ или их сети. Данное преступление, совершенное лицом с использованием своего служебного положения, предусмотренное ч. 2 ст. 272 УК РФ, посягает еще и на второй непосредственный объект - общественные отношения, обеспечивающие интересы службы (ч. 2 ст. 272 УК РФ).

Предметом преступления является информация ограниченного доступа, т.е. сведения (сообщения, данные) независимо от формы их представления, содержащиеся на машинном носителе, в ЭВМ, системе ЭВМ или их сети.

В объективную сторону преступления, связанного с неправомерным доступом к охраняемой законом цифровой информации, входит несколько особенностей, а именно:

1. Неправомерный доступ к охраняемой законом цифровой информации;
2. Негативные последствия, выражающиеся в ликвидации, ограничении или каком-либо изменении информации;
3. Определенная взаимосвязь у неправомерного доступа и последствий.

Доступ к информации представляет собой четкое ознакомление со сведениями, их изменение, ограничение в доступе ликвидация и другие действия, которые могут быть реализованы посредством применения компьютера. Противоправным доступом считается ознакомление со сведениями, их изменение, ограничение в доступе ликвидация и другие действия, которые могут быть совершаться без разрешения владельца сведений.

Неправомерный доступ происходит тогда, когда осуществляется вмешательство в цифровую систему посредством использования технических устройств, которые помогают обойти все защитные барьеры. Также данный доступ можно организовать за счет традиционного доступа к компьютеру или техническим носителям информации, на которые у лица нет разрешения для использования, допустим, посредством включения компьютера, когда собственник компьютера отсутствует, и он не давал разрешение на его включение.

С целью использования статьи 272 УК РФ мало присутствия непосредственного факта совершения проникновения в компьютер, допустим, для того, что узнать какая есть на нем информация. Важной особенностью, в случае отсутствия которой отсутствует и состав преступления, считается совершения конкретного действия или появления последствий, которые регламентируются законодательством. Другими словами, структура объективной стороны считает помимо ознакомления и обязательную ее противоправную ликвидацию, ограничение в доступе, изменении и др.

Ликвидация информации представляет собой полное уничтожение компьютерных сведений, придача им такого состояния, где информацию уже никак не будет восстановить. Без разницы, была стерты все сведения или только определенная часть, все равно наступает ответственность, установленная уголовным законодательством.

Важно учесть то, что ликвидация информации и ее удаление, это разные понятия. Ликвидация представляет собой такое состояние, когда восстановить сведения уже не представляется возможным. В случае же удаления информации, ее еще можно восстановить посредством использования определенных средств операционной системы. В связи с этим, когда происходит умышленное удаление преступником данных, однако сведения были восстановлены, деяние преступника в случае присутствия прямого умысла уничтожить данные полностью, необходимо квалифицировать как покушение на уничтожение информации. Когда же происходит неосторожное удаление данных на

компьютере, однако их можно восстановить, тогда состава преступления нет, потому что утери данных не было.

Ограничение доступа к информации представляет собой определенные действия, в результате совершения которых пропадает возможность получить или применить данные для определенной цели с полною сохранностью самих сведений. Ответственность наступает в том случае, когда было образовано ограничение как временное, так и постоянное.

Изменение данных представляет собой всякое введение модификаций, которые не считаются совершенствованием информации. Когда определенная программа для компьютера работает в штатном режиме, тогда внедрять изменения в программы компьютера не допустимо. Также, допустим, когда лицо обходит защитную систему программы, которая располагается на компьютере, а потом саму программу копирует и тиражирует, тогда данное деяние нужно квалифицировать по статье 272 УК РФ, а также по статье 146 УК РФ.

От изменения или модификации данных необходимо отличать от декомпилирования данных. Так, декомпилирование представляет собой техническое действие, которое вводить определенные изменения объективного кода в начальный текст для исследования и последующего кодирования программы для компьютера. Объективный код представляет собой начальный текст, который компилируется в набор машиночитаемых знаков. Начальный текст представляет собой описанный посредством программных языков алгоритм анализа информации.

Декомпилирование является правомочным, когда соблюдаются несколько требований:

1. Сведений, которые нужны для взаимодействия, до этого не находилась в отрытом доступе для преступника;

2. Данное деяние совершалось в отношении составляющих частей декомпилированной программы для компьютера, считающиеся важными для взаимодействия;

3. Данные, которые были получены посредством декомпилирования, могут применяться только для организации взаимодействия независимо созданной программы для компьютера с иными программами, а также не подлежит передаче, помимо случаев, когда это важно для взаимодействия с иным программами.

Копирование представляет собой повторение сведений в цифровой форме. Российское законодательство позволяет создание копии программы компьютера тогда, когда данная копия будет направлена для архивных целей и для осуществления замены экземпляра в случаях, когда подлинник программы компьютера, например, был потерян. Также данная копия не применяется для других целей и ликвидируется, когда последующее ее применения данных программ перестают быть правомерными.

На технической основе, цифровую информацию можно копировать бесконечно. Так, копирование происходит посредством записывания данных на другое устройство или на материальный носитель цифровой информации с применением специальных программ. Считается, что распечатка информации, которая была получена преступным путем, не создает признаков копирования цифровой информации, так как копированием считается создание копии объекта, другими словами, копии программы, данных в цифровой форме.

Чтобы был состав преступления, важно чтобы копирование данных происходило за счет применения программ компьютера.

Также стоит акцентировать внимание на том, что процесс работы вредоносных программ действует на принципе перехвата цифровых пекетов, их исследовании с целью изъять конфиденциальные данные для дальнейшего раскодирования похищенной информации. В информационной области в качестве одного из самых серьезных преступных посягательств, связанных с получением компьютерных данных считается именно перехват цифровых данных, потому что по сравнению с системами, которые подключены различными проводами, используемыми для отправки сведений, подвергаются хакерским атакам только в информационной сети.

Так, информационное пространство применяется для совершения преступления, в связи с широким его развитием. Важно сказать о том, что рассматривая спутниковую и другие формы беспроводной связи, где в качестве объекта преступлений считается компьютерная информация, данные направляются за счет работы электромагнитных сигналов, даже не смотря форму ее передачи. Говоря о самих электромагнитных сигналах, то отмечается, что в качестве таковых выступают радиосигналы.

Исходя из способа совершения преступного деяния в информационной сфере, не представляется возможным его совершить без использования определенных устройств, которые нужны для тайного обнаружения данных, оборот которых запрещен. Достаточно серьезным положительным моментом при поиске сведений за счет перехвата для преступника считается то, что подобное действие не может оставить после себя каких-либо следов преступления, по причине чего данное преступление в большинстве случаев является скрытым.

Для того чтобы совершить подобного рода преступление, лица делают следующее:

1. Изучение сети, которая будет подвержена атаке, посредством поиска соответствующего электромагнитного сигнала;
2. Непосредственный перехват компьютерных данных в информационной среде;
3. Применение определенного устройства для расшифровки данных и дальнейшее ее преобразование в тот вид, который будет наиболее подходить для ее восприятия.

Одной из форм перехвата, считается электромагнитный перехват, который происходит в зданиях, где располагаются цифровые устройства. Данная форма совершения преступления способствует выполнению противоправных действий без непосредственного взаимодействия с этими устройствами обнаружить электромагнитный источник, который формируется во время работы данных устройств. Допустим, монитор компьютерного устройства выдает определенные

электромагнитные сигналы, которые могут содержать в себе различные данные. Лица, совершающие такие преступления, за счет перехвата определенными устройствами электромагнитных сигналов, отсылают их на компьютерное устройство, полностью копирующее картинку, которая показывается на компьютерном устройстве жертвы.

Субъективная сторона преступления. Неправомерный доступ к защищаемой государством цифровой информации происходит лишь умышленно, однако не исключается то, что противоправное деяние, не говори о том, что данное преступление совершается лишь умышленно, потому что законодательством уголовная ответственность наступает не за неправомерный доступ, а именно за действия, после которые привели к неправомерному доступу. В связи с этим вид форма виновности определяется исходя из наступивших последствий в форме ликвидации, ограничения к информации доступа или изменения.

На основе того, что статья 272 УК РФ намеренно не рассматривается, что подобное преступное деяние совершается исключительно по неосторожности, беря во внимание правки части 2 статьи 24 УК РФ, считается, что данное преступления совершается и умышленно и по неосторожности. Допустим, когда преступник намеренно добился неправомерного доступа к цифровой информации и после этого по неосторожности были внесения изменения данных, тогда в действиях преступника имеются все признаки состава совершения преступления.

Субъектом данного преступления выступает любое вменяемое физическое лицо, которое на момент совершения преступления достигло 16 лет.

В качестве квалифицирующего признака выступает наступление последствий, которые выражаются в нанесении крупного вреда и мотивом совершения преступления является корысть. Крупным ущербов в данном преступлении считается вред, сумма которого является больше 1 миллиона рублей. Корысть заключается в непосредственном желании преступника получить определенную материальную выгоду.

В качестве квалифицирующих признаков, которые регламентируются частью 3 статьей 272, считается совершение преступления в группе лиц по предварительному сговору, организованной группой или лицом с применения своего служебного положения. Для того, что признать совершение преступления группой лиц по предварительному сговору, важно выявить, что лица, участвующие в совершении преступления полностью или частично совершали действия, которые упоминаются в содержании данной статьи, а именно способствовали получению неправомерного доступа к сведениям и др.

Деяние лиц преступной группы будет квалифицироваться по части 3 статьи 272 УК РФ, не смотря на то, выполнялась объективная сторона или же нет. Чтобы за совершением преступления следовало назначение уголовного наказания, достаточно доказать факт совершения преступления в группе лиц по предварительному сговору, когда поле совершения преступных действий произошло уничтожение, ограничение доступа или изменения цифровой информации.

Использование служебного положения предусматривает осуществление доступа к цифровой информации, противоправно используя правомочия, которыми было наделено лицо только для выполнения своих служебных функций. Также преступник пользуется правомочиям против законных интересов владельца информации. Стоит отметить, что законодательство не уточняет имеющееся статусное положение лица, которое злоупотребляет полномочиями для получения доступа к данным, после чего происходит ликвидация, ограничение в доступе или изменения цифровой информации. Считается, что подобным лицом может выступает абсолютно любое лицо, которое за счет владения необходимыми полномочиями может получить доступ к данным против воли владельца цифровых сведений.

Квалифицирующим признаком, в соответствии с частью 4 статьи 272 УК РФ, выступает наступление тяжких последствий или же непосредственная угроза их наступления. Считается, что виновность в отношении подобных последствий бывает умышленной и неосторожной, а также то, что тяжесть

совершения преступления нужно устанавливать относительно к каждой отдельной ситуации.

Угроза наступления тяжких последствия представляет собой то, что впоследствии совершения преступником противоправных действия, появились определенные обстоятельства, в результате наступления которых возможны последствия в форме получения крупного материального ущерба и др.

В качестве примера можно привести следующий случай из судебной практики:

«Так, ФИО1 в 2013 году, обладая познаниями и навыками компьютерного программирования, используя личные средства компьютерной техники, в том числе ЭВМ с подключенными носителями информации №, проживая по адресу: <...>, посредством программирования на языке «...», удовлетворяя свой интерес к познаниям в области информационной безопасности, желая получать доход от деятельности в данной сфере, создал компьютерную программу «...», предназначенную для проверки состояния учетных записей ... которую продолжал модифицировать с использованием указанной компьютерной техники до 11.08.2016 года, в том числе, по новому месту проживания со второй половины 2014 года по адресу: <...>.

Компьютерная программа «...», согласно замыслу ФИО1, функционирует в следующем порядке: пользователю данной компьютерной программы необходимо загрузить в нее текстовый файл, содержащий .... Далее, компьютерная программа осуществляет подключение к ..., после чего осуществляет несанкционированный, то есть нелегитимный, без ведома и разрешения легального пользователя, доступ к компьютерной информации - учетной записи пользователя, то есть к хранимой в компьютерной системе совокупности данных о пользователе, необходимой для его идентификации и предоставления доступа к его личным данным, чем производит модификацию компьютерной информации о данном доступе, и далее, при успешной авторизации (идентификации пользователя), несанкционированно копирует информацию о состоянии счета учетной записи в текстовый файл, после чего

пользователь данной компьютерной программы получает возможность ознакомиться с полученными данными на своем ПЭВМ и распоряжаться ими. Данная компьютерная программа имеет единственное предназначение - копирование компьютерной информации пользователей электронной почты, зарегистрированных в электронной платежной системе «....», с последующим формированием базы данных с указанной информацией.

После создания указанной компьютерной программы, в тот же период времени у ФИО1 возник умысел на получение денежных средств от продажи данной компьютерной программы посредством распространения ее в телекоммуникационной сети Интернет неограниченному кругу лиц.»

Анализ преступлений за создание, использование и распространение вредоносных компьютерных программ, регламентируемых статьей 273 УК РФ.

Образовавшийся практический опыт, который поспособствовал возникновению ряда мнений у правоведов относительно того, какие именно противоправные деяния считаются противоречащие статьи 273 УК РФ. Проблема, связанная с признанием вредоносных программ полностью передан следственным и судебным органом группе специалистов. Так, наибольшее число преступлений расследуются в условиях признания обвиняемыми их обвинения без единого обжалования со стороны защиты. От того, что Верховный Суд РФ не представляет собственного объяснения судебным органам о судебной практике использования правовых положений, связанных с ответственностью за преступные деяния в информационном пространстве только оказывает поддержку одностороннего подхода для решения данного вопроса относительно наличия состава преступного посягательства в деянии лица, подозреваемого в совершении преступления.

Вместе с этим, различными правоведами обращается внимание на возникновении у практикующих экспертов и научных деятелей юридических мнений, которые могут достаточно сильно повлиять на изменение

сформировавшейся судебной практики и реализовать соответствующее применение нормативных положений уголовного законодательства.

Стоит отметить, что содержание статьи 273 УК РФ представляет собой довольно легкую норму. У сотрудников государственных органов не возникает больших вопросов касательно доказывания факта разработки и применения программ и возникших последствий их функционирования в форме нарушения первоначальной целостности цифровых данных.

Важным элементом в уголовных делах выступают заключения экспертов, которые рассматривают изучаемые программы в качестве вредоносных. В связи с тем, что проблема, связанная с отнесением вирусных программ на стыке технического и нормативного аспектов, она создает все больше и больше обсуждений в процессуальном споре со стороны защиты и со стороны обвинения.

Основной объект преступления - общественные отношения, обеспечивающие безопасность в сфере компьютерной информации.

Объективной стороной преступления этой категории является непосредственное создание, применение и распространение цифровых программных обеспечений или иных цифровых данных, первоначально предназначенных для уничтожения, изменения или совершения иных преступных действий.

Исходя из вышесказанного, можно сказать, что в качестве нормативных особенностей вредоносных программ в уголовном законодательстве считается следующее:

1. Преднамеренная разработка программы с целью достижения противоправного результата. Естественно, возникшая у создателя программы ошибка в получившемся коде, которая способна нарушить целостность цифровых данных их владельца, не считается правовым поводом для отнесения программы к категории вредоносных.

2. Противоправный характер функционирования вредоносной программы, обуславливающийся отсутствие информирования пользователя о том, что

программа была запущена, и ее функционирование без предварительного соглашения на это владельца данных.

У данного вида преступления состав считается формальным.

В случае, когда при любой попытке какой-либо манипуляции с цифровой информацией, присутствует тяжкий вред или же угроза его наступления, то данное преступное деяние должно квалифицироваться по части 3 статьи 273 УК РФ.

Компьютерная программа – это объективное представление набора информации, которая применяется для надлежащего функционирования устройства с целью достижения необходимого результата, включая подготовительные материалы, собранные при разработке программного обеспечения для компьютерного устройства. Другие цифровые данные в силу своих характеристик тоже применяются с целью совершения противозаконных действий, включающих в себя уничтожение, перехват или внесение каких-либо изменение в них. Поэтому важно сказать о том, что сейчас очень просто и быстро разрабатываются новые и более совершенные вредоносные программы.

Непосредственное создание подобных программ заключаются в том, что нарушить нормальную работоспособность компьютерных устройств. Так, к примеру, лицо может разработать определенную программу, перенести ее каким-либо образом на другое цифровое устройство и это устройство будет заражено данной программой, после чего зараженное устройство будет нуждаться в немедленной переустановке всей системы. Стоит отметить, что создание подобного рода программ уже считается оконченным преступлением с того момента, когда начался их оборот.

Вместе с этим важно сказать о том, что создаются также специальные программы, которые способны полностью обойти систему защиты данных или вовсе сломать ее как навсегда, так и на определенный промежуток времени.

Существует достаточно большое число программ, в том числе и вредоносных, однако запрещенными являются лишь программы, способные

уничтожить, заблокировать или модифицировать данные на компьютерном или другом устройства.

Одним из подвидов таких противозаконных программ выступают логические бомбы и компьютерные вирусы. Так, компьютерные вирусы могут создавать точную копию себя же бесконечное количество раз, внести определенные изменения в программное обеспечение цифрового устройства, после чего это устройство будет нуждаться в полной переустановке. Также они могут залезать даже в глобальные цифровые сети, что является существенным отличием от логических бомб, так как в какое программное обеспечение они залезли, там они и останутся.

Считается, что под вредоносностью программы принято воспринимать нормативную особенность объективной стороны совершенного преступления, регламентируемого статьей 273 УК РФ, который должен быть доказан. Обнаружение таких особенностей обуславливается изучением цифрового кода компетентным для этого экспертом на базе его особых знаний в цифровой сфере.

Вместе с этим выделяются некоторые ограничения в деятельности специалиста только вопросов обнаружения признаков вредоносности разработанной программы. Нормативное толкование этих признаков и отнесения подобных программ к вредоносным относится только к полномочиями следственных и судебных органов. Альтернативное преподнесение закона привело бы к тому, что роль осуществления правосудия исполняли бы специалисты.

Допустим, тщательно изучив программу проверки надежности Интернет-ресурса к внешнему воздействию, которое способно вызвать большую нагрузку компьютерного устройства, специалист скорей всего после обнаружения признаков отсутствия сообщения о работе программы и запроса на ее исполнение, отнесет программу к категории «вредоносная». Также, когда есть согласие сотрудника, который имел доступ к конфиденциальным сведениями пользователя, на мониторинг его активности, говорит о санкционированном характере работы внешне незаметной программы, способная осуществлять

копирование данных пользователя, а также блокировать доступ к конфиденциальной информации и др.

Нормативная логика данного примера относится и к случаю разрешенного владельцем тестирования Интернет-ресурса к хакерским атакам за счет функционирования вредоносной программы.

Определение того, что имеется несанкционированный характер функционирования программы, возможно лишь следственным способом, особенно за счет организации допроса, проведения оценки документов и организации других процессуальных действий.

Данные примеры открыто показывают то, что вредоносность программы должна определяться именно за счет организации следствия, опираясь на результаты экспертных исследований, направленных на изучение принципа работы программы.

Субъективная сторона – прямой умысел, потому что лицо осознает тот факт, что оно разрабатывает, применяет и распространяет запрещенную законом программу и хочет этого.

Субъект преступления общий - вменяемое лицо, достигшее шестнадцати лет.

Существуют разные манипуляции с вредоносными программами, однако вне зависимости от того, что именно лицо делает, оно будет считаться уголовно наказуемым.

Помимо этого, отмечается, что цель и мотив данных преступлений не играют никакой роли, за исключением, если только назначения уголовного наказания.

Сейчас же официальные данные по расследования уголовных дед по статье 273 УК РФ по большей части составляют факты, которые именуются как «патчи», «кейгены» и др., направленные на цифровой взлом лицензионных программ посредством применения вредоносных программ. Обычно, эта норма вменяется вместе со статьей 146 УК РФ в делах, связанных с противоправной установкой программы.

Поводом для того, чтобы признать программу вирусной, необходимо заключение эксперта. В качестве обоснования, происходит акцентирование внимания на том, что происходит вывод из строя защитной системы компьютерного устройства, в связи с чем, программа будет считаться вредоносной. Этот подход важно считать неправильным. Ведь, как говорилось до этого, специалист не имеет право принимать решение о вредоносности изучаемой программы. Компетенция эксперта ограничивается изучение алгоритма программы и обнаружения признаков ее вредоносности, то есть:

I. Преднамеренное назначение программы для получения противоправного результата;

II. Отсутствие добровольного согласия на функционирование программы, а также предварительного введения в курс касательно того, что будет работать программа.

Если с наличием первого признака вредоносности «активатора/патча/кейгена» всё более-менее очевидно, так как данные программы изначально создаются для «взлома» программного обеспечения, то признак «несанкционированности» в подавляющем большинстве случаев на деле отсутствует.

Как правило, алгоритм работы «активатора/патча/кейгена» или иной программы-взломщика всегда сопровождается сообщением о том, в какую программу будут внесены изменения. Не редко пользователю самому предлагается выбрать объект воздействия (взламываемую программу), переместить взломщика в каталог с взламываемой программой, произвести замену файлов в ручном режиме и т.п. Кроме того, исполнение программы-взломщика всегда связано с прямым волеизъявлением пользователя, который должен её запустить, инсталлировать, отдать команду на выполнение, иными словами санкционировать её работу для получения конечного результата в виде генерации ключа активации или изменения функциональности взламываемой программы. Здесь следует закономерный вывод, что воздействие на компьютерную информацию (лицензионный софт) программой-взломщиком

осуществляется только с согласия пользователя или по его прямому волеизъявлению, что исключает возможность отнесения программы-взломщика к вредоносному программному обеспечению в понимании действующей редакции уголовного закона.

Случаи использования подобных взломщиков должны рассматриваться в плоскости нарушения авторских (лицензионных) прав на программное обеспечение по статье 146 УК РФ. Использование программы-взломщика должно оцениваться как орудие совершения правонарушения. Дополнительная квалификация правонарушений с использованием «активаторов/патчей/ кейгенов» по статье 273 УК РФ в подобных случаях не соответствует основам уголовного законодательства.

Анализ преступлений за нарушение правил эксплуатации средств, используемых для хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, регламентируемых статьей 274 УК РФ.

Основными способами осуществления незаконных действий, ответственность за которые наступает по ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», являются использование вредоносных компьютерных программ с целью доступа к охраняемой законом компьютерной информации и хищения чужих денежных средств (64,5 %), а также распространение вредоносных компьютерных программ (25,5 %). Несколько приговоров посвящены использованию вредоносных компьютерных программ, работающих на мобильных информационно-телекоммуникационных устройствах (2 %).

В качестве примера можно привести дело, рассмотренное Октябрьским районным судом г. Тамбова. Из материалов дела № 1–331/10 следует, что, работая в сети Интернет, гр. Б. скопировал из указанной сети на свой персональный компьютер модифицированную программу Radmin с возможностью скрытой установки, позволяющую администрировать подключенными в единую сеть электронно-вычислительными машинами.

Согласно заключению эксперта, в компьютере гр. Б. найден файл со сценариями скрытой негласной установки серверной части программы Radmin, заведомо приводящей к модификации компьютерной информации.[1]

Данная категория преступления предусматривает собой невыполнение или же ненадлежащее выполнение установленных требований, связанных с использованием компьютерных устройств, которые определяются правовыми документами на уровне государства, непосредственными организациями, которые являются обладателями компьютерных устройств.

Эта статья считается бланкетной, в связи с чем, для более точного толкования объективной стороны совершаемого деяния важно определить определенный правовой документ, положения которого гражданин нарушил. Здесь говорит об обнаружении нарушения требований, которые непосредственно вводят запрет на совершение конкретных действий или которые наоборот обязывают лицо соответствовать им.

В случае невыполнения именно рекомендательных положений, тогда лицо, которое их нарушило, в соответствии с законодательством не может быть привлечено к уголовному ответственности.

В качестве объекта данной категории преступления выступают отношения, связанные с осуществлением безопасности цифровых устройств и средств их обеспечения и которые близко связанные с ними процесс создания, сбора, фиксации и других функций взаимодействия с цифровыми данными.

Предметом данного преступления выступают требования, связанные с пользованием компьютерами, их системы или сети.

Эта статья считается бланкетной и отсылает к определенным инструкциям и нормам, которые определяют четкий порядок работы с компьютерными устройствами в организации. Подобные положения определяются уполномоченным на это лицом. Как правило, требования по эксплуатации

---

[1] Приговор Октябрьского районного суда г. Тамбова от 9 июля 2010 г. по уголовному делу № 1-331/2010. Электронный ресурс - URL: http://sud23.tmb.sudrf.ru/modules.php?name=information&id=1242 (дата обращения: 10.04.2024).

компьютерных устройств обуславливаются определенными техническими правовыми документами.

Вместе с этим они представляются в паспортах качества, технических описаниях и инструкциях по эксплуатации, передаваемых пользователю. Во время приобретения вещественных средств компьютерных устройств. Прилагающие инструкции представляются в письменной форме, а также на машинных устройствах.

В последнем случае они легко подстраиваются под программу, способную предоставить к ним доступ в любой момент. Нарушение требования по эксплуатации компьютерных устройств делятся на физические, например, несоответствующая установка средств, ненадлежащее подключение компьютера к источнику подачи питания, а также интеллектуальные, например, неправильный ввод данных и др.

Говоря о данной норме, в качестве сети выступает та сеть, на которую можно распространить действие определенных требований. Федеральный закон «О связи»[1] относит к сетям электросвязи следующее:

1. Взаимоувязанная сеть связи. Она представляет собой систему технологически соединенных сетей электросвязи в пределах России, оснащенный общим централизованным управлением;

2. Сеть связи общего пользования. Представляет собой неотъемлемую часть взаимоувязанной сети связи России, являющаяся публичной для любого человека или организации, где не может быть вынесено отказа в предоставлении услуг;

3. Ведомственные сети связи. Представляют собой сети электросвязи различных министерств и других органов государственной власти, которые также могу выйти на сеть общего пользования;

4. Локально-производственные сети связи. Представляют собой связи федеральных органов исполнительной власти и организаций, которые

[1] О связи: Федеральный закон №126-ФЗ: принят Гос. Думой 07.07.2003 г.: по состоянию на 04.08.2023 г. - Справ.-правовая система «КонсультантПлюс».

образуются с целью управления локально-производственной деятельностью и технологическими процессами, которые не обладают выходом на сеть связи общего пользования;

5. Выделенные связи. Это связи физических лиц или организаций, которые не обладают выходом на сеть общего пользования. Конечно, в случае присутствия определенных правовых документов, которые предусматривают требования по эксплуатации данными сетями, за их нарушением будет следовать ответственность, установленная Российским законодательством.

По причине этого, акцентируется внимание на том факте, что в глобальных сетях, например, Интернет, нет единых требований по его использованию, и их заменяют так называемые «кодексы поведения», не соблюдение которых в связи с содержанием статьи 274 УК РФ не могут считаться соответствующим поводом для назначения уголовного наказания.

Объективная же сторона данного деяния заключается в действиях, которые непосредственно нарушают правила по эксплуатации компьютерных устройств, системы или их сетей, после совершения которых, произошло уничтожение, изменение цифровых данных с учетом того, что после совершения противоправного деяния был причинен существенный ущерб.

Эти действия могут нарушать:

– правила эксплуатации аппаратных средств ЭВМ, системы ЭВМ или сети ЭВМ;

– правила эксплуатации программных средств, предназначенных для функционирования ЭВМ, системы ЭВМ, сети ЭВМ.

Преступное деяние будет являться оконченным только после того, когда наступили негативные последствия, регламентируемые статьей 274 УК РФ, другими словами, перехват или изменение цифровой информации. Деяния, которые имеют прямую связь с этим, нужно рассматривать тогда, когда присутствует угроза безопасности цифровым данным, располагающихся на компьютерном устройстве и наносится ущерб программному обеспечению самого компьютера. Общий характер нанесенного вреда пострадавшему

определяется в зависимости от определенных фактов и событий, беря во внимание то, что уровень нанесенного вреда должен быть менее серьезным, по сравнению с тяжкими последствиями.

По мнению А.В. Сизова, причинение крупного имущественного ущерба не следует рассматривать в качестве тяжких последствий. Он считает, что если имущественный ущерб нанесен вследствие дезорганизации информационной системы посредством преступных действий, направленных на компьютерную информацию то данный ущерб будет входить в понятие существенного вреда, предусмотренного ч. 1 ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»[1].

Субъективная сторона преступление этой категории имеет смешанную форму виновности, так преступление можно совершать умышленно для того, чтобы нарушить требования по эксплуатации компьютерного устройства или же по неосторожности, например, сотрудник, решил установить программу на устройство без тщательной и всесторонней проверки файла.

Часть 2 статьи 274 УК РФ регламентирует квалифицирующий признак, который предусматривает причинение тяжких последствий в виду неосторожности. Поэтому считается некорректным только экспертам ограничивать состав совершенного преступления.

Преступные посягательства в цифровой среде, которые направлены на нарушение отношений, связанных с реализацией правомочий на цифровые ресурсы, компьютерные устройства и другие, не регламентируются отдельным нормативным актом.

Опираясь на практический опыт, то можно сказать, что подобные преступления в зависимости от определенных событий рассматриваются на основании огромного спектра положений Уголовного кодекса Российской

[1] Сизов А. В. Квалификация нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети // Информационное право. – 2020. - № 4. - С. 28-37.

Федерации и от зависимости от общего числа совершенных в настоящее время преступлений.

Допустим, когда в процессе совершения цифрового преступления происходит сбор, хищение или хранение данных, составляющих государственную тайну, с целью последующей их отправке зарубежной кампании или ее представителю, тогда такие действия могут рассматриваться по совокупности преступлений в том числа за подобное нарушение, связанное с разглашение государственной тайны.

Нередко невозможно определить источник их возникновения среди людей, которые никак не связаны с данными организациями, из-за огромного количества третьих лиц между владельцами цифровой информации и их распространителями. Также стоит отметить, что их продажа или другая форма распространения влечет за собой растущую опасность для общества, так как конфиденциальные данные могут применяться с плохой целью в отношении отдельных граждан.

Поэтому необходимо сказать, что преступления, связанные с незаконной покупкой, передаче, продажей и др., цифровых данных в виде общей базы данных, которая содержит данные конфиденциального характера, подлежат уголовной ответственности и подлежат уголовной ответственности, а эти сведения будут ограничены в свободном обороте.

Настоящее законодательство Российской Федерации схожие меры распространяются и на оружия, что может стать образцом соответствующего нормативного регулирования, которое касается купли-продажи подростков детей или детской информаций, содержащей элементы порнографии.

Логично, возрастает уровень опасности, которую эти действия представляют для общества в связи с распространением детской порнографии через свободно доступные компьютерные сети, без полного соблюдения требований статьи 242 УК РФ. Для этого потребуется дополнить данную норму новым разделом или включить отдельную норму в Уголовный Кодекс Российской Федерации.

Подобный подход представляется необходимым также и в других случаях. Помимо отмеченных недостатков уголовно-правовой защиты по нормам УК РФ в области цифровой информации, необходимо сказать, что происходит сужение ее границ. Благодаря статье 21 ФЗ «Об информации, информатизации и защите информации», все письменные сведения должны находиться под должной защитой, так как любые манипуляции с ними также могут причинить вред и ее владельцу.

По причине этого присутствие в настоящем отраслевом законодательстве определенных ограничений исключительно на противоправное использование, во-первых, для сведений, являющихся государственной тайной, во-вторых для конфиденциальных данных и вместе с этим включение в статью 272 УК РФ признака «охраняемая законом цифровая информация» по сути, исключает значительный объем цифровых данных.

Вместе с этим положения статьи 272 УК РФ также связаны с реализацией защиты интересов государства и бизнеса. Но на основании норм части 1 статьи 2 УК РФ в такой же мере должны обеспечивать защиту законных правомочий человека, граждан, имущества и др.

Для того, чтобы в полностью выполнить конкретные задачи, установленные уголовным законодательством, важно убрать термин «охраняемой законом» в целях обеспечения уголовно-правовой защиты абсолютной разной цифровой информации.

Итак, подводя итог, можно сказать, что преступные деяния в области цифровой информации, в большей части связаны с удаленным взломом компьютерных устройств, что представляет собой отличную возможность для лиц достигать своих противоправных целей безнаказанно. Реальная возможность доказать совершение противоправных действий падает до 0. Естественно, имеются и достаточно известные дела знает вся планета, однако по причине наличия цифровой и нормативной безграмотности граждан, дела, которые связаны со взломом информационных технологий, в большинстве случаев вообще не заводятся.

Также стоит сказать, что каждое цифровое преступление стоит разделить на две основные группы, а именно:

1. Преступления, которые непосредственно связаны с вмешательством в нормальную работу цифровых устройств;

2. Преступления, при совершении которых применяются компьютерные устройства.

В действующем уголовном праве уголовно-правовая защита рассматривается первый раз.

ЗАКЛЮЧЕНИЕ

Детально разобравшись в теме «Преступления в сфере цифровой информации: понятие, виды и юридический анализ составов преступлений», можно подвести следующие итоги.

Первое. После того, когда произошло зарождение человеческого общества, люди в нем все больше и больше нуждаются во взаимодействии между собой. Изначальное общение между людьми происходило за счет показа различных жестов или знаков, и только после этого возникло голосовое общение, а также возникла письменность. В 20 веке возникли такие технологии как радио, кино, компьютерные средства и другое. Вместе со всем этим, различными учеными достигались разные достижения в науке, которые в последующем стали применяться для совершения преступных деяний. Как только информация стала обладать большим значением в жизни каждого человека, повысилось значение и цифровой информации как одной из видов формирования и передачи информации.

Но введение в каждую область человеческой жизнедеятельности цифровых технологий имеет достаточно большое значение в сфере технологического вооружения преступности. Анонимность лиц, которые совершают преступления, а также их способность из любой точки мира получить доступ к засекреченным данным, тем самым привлекает человека совершать противоправные деяния. Цифровые махинации, обычно, считаются необнаруженными, в связи с совершение уличных преступлений.

Второе. Начиная с 1990-х годов, в законодательстве появились нормативные положения в области применения цифровой информации, однако оно не всегда было последовательное. В том числе, противоречие понятий разнообразных законов, допустим, отсутствие соответствия термина информации, которое использовалось в ФЗ «Об информации, информатизации и защите информации» и Уголовном законе. К тому же, в настоящее время с

каждый днем стремительно появляются все больше и больше преступлений, которые в основном отличаются друг от друга. Это в большей степени связано динамичным развитием различных цифровых технологий и модернизацией искусственного интеллекта, поэтому терминов, которые могли бы найти свое отражение в законодательстве, не так разнообразно.

Отсутствие последовательности имеется и в Уголовном законе, к примеру, во время нарушения требований по использованию компьютерных технологий или их системы, где говорится о некоторых последствиях в форме уничтожения, блокирования или изменения данных. Однако не сказано о нарушении работоспособности компьютеров или их системы, но это, как и в двух других составах, регламентируемых Уголовным законом, способно причинить определенный вред.

Помимо этого, важно акцентировать внимание на непоследовательном подходе к созданию квалифицирующего признака о неосторожном причинении тяжких последствий. Данный признак указан в таких статьях как 273, а также 274 УК РФ, что не стоит считать правильным, потому что неосторожное причинение тяжких последствий в одинаковой степени может стать последствием всех трех противоправных действий.

Третье. Считается важным внедрить большой объем изменений в имеющееся законодательство и разработать новые правовые акты, в которые будет уже включено правовое регулирование в цифровых правоотношениях, действующее на всей территории Российской Федерации.

Так, исходя из имеющихся слабых сторон Российского законодательства, необходимо прибегнуть таким действиям как:

1. Начать в качестве предмета преступления, которое непосредственно покушается на информацию, находящуюся в информационной среде, считать не компьютерную информацию, а цифровую. В примечании 1 к статье 272 УК РФ необходимо привести толкование термина «цифровая информация», а не «компьютерная информация».

2. С целью четкого упорядочивания понятийного аппарата уголовного законодательства, опираясь на термины, которые рассматриваются в нормативном документе, которые регулирует отношения, возникающие при осуществлении правомочий на поиск, получение, передачу и других действия во время использования информационных технологий необходимо применять более широкий по содержанию термин «информационно-телекоммуникационные устройства, их системы и сети» в положениях Особенной части УК РФ вместо предусмотренного в статье 274 УК РФ понятия, которое указывает на объекты обращения цифровой информации в форме «средств хранения, обработки или передачи компьютерной информации и ИТКС».

3. Поскольку ИТКС «Интернет» содержит интернет-ресурсы, размещающие информацию о способах совершения преступлений в сфере компьютерной информации, а также объявления о предоставлении незаконных услуг в этой сфере, предлагается в порядке предупреждения этих преступлений ввести механизм внесудебного ограничения доступа на территории Российской Федерации к такой информации, дополнив п. 1 ч. 5 ст. 15.1 «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации" следующим пунктом:

е) информации о способах совершения преступлений в сфере цифровой информации, а также объявлений по предоставлению незаконных услуг в этой сфере.

Помимо этого, также считается целесообразным разработать ряд программ, связанных с поощрением для различных организаций и специалистов, которые сильно взаимодействуют с органами государственной власти в области кибербезопасности и способствуют предотвращению и пресечению кибератак.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I.Законы, нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: (принята всенародным голосованием 12 декабря 1993 г.) // Российская газета. - 1993. - №237; Собрание законодательства РФ. - 2014. - №31. - Ст. 4398.

2. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон №174-ФЗ: принятый Гос. Думой 18.12.2001 - Справ.-правовая система «КонсультантПлюс».

3. Уголовный кодекс Российской Федерации: Федеральный закон № 63-ФЗ: принят Гос. Думой 13.06.1996: по состоянию на 10.06.2024г. - Справ. - правовая система «КонсультантПлюс»

4. Об информации, информационных технологиях и о защите информации: Федеральный закон №149-ФЗ: принят Гос. Думой 27 июля 2006 г. № 149-ФЗ: по состоянию на 01.01.2024 г. - Справ.-правовая система «КонсультантПлюс».

5. О связи: Федеральный закон №126-ФЗ: принят Гос. Думой 07.07.2003 г.: по состоянию на 04.08.2023 г. - Справ.-правовая система «КонсультантПлюс».

6. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон №420-ФЗ: принят Гос. Думой 07.12.2011: по состоянию на 03.07.2016 г. - Справ.-правовая система «КонсультантПлюс»

7. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. N 37 // Справ.-правовая система «КонсультантПлюс».

8. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 №646 - Справ.-правовая система «КонсультантПлюс».

9. Конвенция о преступности в сфере компьютерной информации ETS N 185 от 23 ноября 2001 г.: по состоянию на 15 февраля 2023 г. // Справ.-правовая система «КонсультантПлюс».

10. Соглашения о сотрудничестве государств - участников Содружества Независимых Государств по борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 года: по состоянию на 23 марта 2023 г. // Справ.-правовая система «КонсультантПлюс».

11. Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации: Приказ МВД России от 29.12.2022 N 1110 // Справ.-правовая система «КонсультантПлюс».

II.Монографии, учебники, учебные пособия

1. Кушниренко С. П. Цифровая информация как самостоятельный объект криминалистического исследования / С. П. Кушниренко - М.: ЮрИнфоР. - 2020. – 43с.

2. Противодействие расследованию преступлений и меры по его преодолению : учебник для вузов / Б. Я. Гаврилов [и др.] ; под общей редакцией Б. Я. Гаврилова, В. П. Лаврова. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 156-166 с.

3. Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: Изд-во Воронеж. гос. ун-та. - 2022. - С. 46-54.

10. Способы получения доказательств и информации в связи с

обнаружением (возможностью обнаружения) электронных носителей : [Текст] : учебное пособие / В. Ф. Васюков [и др.] ; под общей редакцией Б. Я. Гаврилова. - Москва : Проспект. - 2021. – 159 с.

11. Гутник, С. И. Преступные посягательства в отношении персональных данных : монография / С. И. Гутник ; под редакцией Н. В. Щедрина . - Москва : Проспект. - 2021. - 176 с.

12. Юрченко, И. А. Преступления против информационной безопасности : учебное пособие / И. А. Юрченко. - Москва : Проспект. - 2021. - 208 с.

13. Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе / В. Ю. Агибалов. – М.: Юрлитинформ. - 2022. – 182 с.

14. Летелкин Н. В. К вопросу об определении понятия преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) // Уголовное право: стратегия развития в XXI веке: Материалы XV Международной научно-практической конференции. Ст. М.: Проспект - 2020. – 237с.

15. Майкл Бойл, Жан-Клод Вюльерм. Краткое пособие по проведению допросов в ходе следствия. Практическое руководство. Общеевропейские принципы и стандарты работы полиции. Совет Европы. 2019 // [Электронный ресурс] URL: https://rm.coe.int/guide-to-investigative-interviewingrussian/1680934b21 (дата обращения: 10.04.2024).

16. Международное уголовное право: учебное пособие / А. И. Розенцвайг. – Самара: Издательство Самарского университета. - 2020. – 160 с.

17. Овчинский, В. С. Основы борьбы с киберпреступностью и кибертерроризмом : хрестоматия / сост. В.С. Овчинский. — Москва : Норма : ИНФРА-М, 2024. – 528 с.

18. Зигура Н. А. Компьютерная информация как вид доказательств в уголовном процессе России: автореф. дис. … канд. юрид. наук. Челябинск. - 2020. - С. 9-21.

19. Овчинский, В. С. Криминология цифрового мира : учебник для

магистратуры / В. С. Овчинский. — Москва : Норма : ИНФРА-М, 2024. — 352 с.

20. Афанасьева О. Р., Гончарова М. В., Шиян В. И. Криминология: учебник и практикум для вузов. М.: Юрайт. - 2023. - 340 с.

21. Ефремова М. А. Уголовно-правовая охрана информационной безопасности. М.: Юрлитинформ. – 2019. - С. 226-237.

22. Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: дис. …канд. юрид. наук / А. А. Балашова – М.: Проспект - 2020. – 216 с.

23. Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы: монография / А. Л. Осипенко. – Омск. - 2022. – 135с.

III.Статьи, научные публикации

24. Бегишев И. Р. Цифровая информация: понятие и сущность как предмета преступления по российскому уголовному праву / И.Р. Бегишев // Академический юридический журнал - 2021. - № 2. - С. 47-49.

25. Вехов В. Б. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ // Уголовное право. - 2019. - № 4. - С. 15-22.

26. Хисамова З. И. Квалификация посягательств, совершенных с использованием электронных средств платежа // Юридическая наука и правоохранительная практика. - 2020. - № 3 (33). - С. 127-134.

27. Бегишев И. Р. Уголовная ответственность за перехват цифровой информации / И. Р. Бегишев // Информационная безопасность. - 2020. - № 4. - С. 16-19.

28. Старичков М. В. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института МВД России. - 2020. - № 1. - С. 20-26.

29. Кузнецов Д. А., Манохина О. В. Компьютерная преступность // Бюллетень медицинских интернет-конференций. - 2021. - № 12. - С. 1484–1485.

30. Хабриева Т. Я. Право в условиях цифровой реальности / Т. Я. Хабриева, Н. Н. Черногор // Журнал российского права. – 2022. – № 1. – С. 85 – 102

31. Вехов В. Б. Особенности организации и тактика осмотра места происшествия при расследовании преступлений в сфере компьютерной информации // Российский следователь. - 2021. – № 7. – С. 122-125.

32. Косынкин А. А. Некоторые аспекты преодоления противодействия расследованию преступлений в сфере компьютерной информации на стадии предварительного расследования / А. А. Косынкин // Российский следователь. – 2022. – № 2. – С. 76-79.

33. Шапошников А. А. Криминологическая характеристика киберпреступника. / А. А. Шапошников // Вестник юридического факультета Южного федерального университета. – 2023. - №19. – С. 29-32.

34. Раскина, Т. В. О некоторых аспектах организации противодействия преступлениям, совершаемым в сфере информационно-коммуникационных технологий в Российской Федерации / Т. В. Раскина. – Текст: непосредственный // Вестник Университета прокуратуры Российской Федерации. – 2023. – № 2. – С. 61–69.

35. Янгаева М. О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России. - 2021. – №42. - С. 133–138.

36. Вдовин Е. А. Проблема противодействия распространению идей экстремизма и терроризма в сети Интернет / Е. А. Вдовин // Молодой ученый. 2019. - № 16. - С. 79-81.

37. Большаков М. С. Основные ошибки осмотра места происшествия и

пути их преодоления следователями органов внутренних дел / М.С. Большаков // Преступность в сфере информационно-телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. Воронежский институт МВД РФ. Воронеж. - 2020. - № 1 (6). - С. 12-14.

38. Галкина У. В. Участие специалиста, как обязательное условие производства отдельных следственных действий при расследовании преступлений в сфере компьютерной информации / У. В. Галкина // Криминологический журнал. - № 4. - 2020. – С. 89 – 95.

39. Меняйло Д. В., Крупенникова К. К., Меняйло Л. Н. Трансформация экстремизма в условиях цифровизации общества / Д. В., Меняйло, К. К., Крупенникова, Л. Н. Меняйло // Право и государство: теория и практика. - 2023. - № 11. - С. 417-419.

40. Сизов А. В. Квалификация нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети // Информационное право. – 2024 - № 4. С. 28-35.

41. Номоконов В. А. Киберпреступность: прогнозы и проблемы борьбы / В. А. Номоконов // Библиотека криминалиста. – 2023 - № 5. - С. 150-154.

42. Пинкевич Т. В., Зубалова О. А. Современное состояние экстремизма и терроризма в условиях развития цифровых технологий / Т. В. Пинкевич, О. А. Зубалова // ЮП. - 2023. - № 3. - С. 64-68.

43. Фельдман, В. Е. Противодействие совершению бесконтактных преступлений с использованием цифровых технологий / Фельдман, В. Е. –Текст: непосредственный // Вестник УрФО. Безопасность в информационной сфере. – 2020. – № 2. – С. 18–28.

44. Уголовно-правовая модель защиты телекоммуникаций от преступных посягательств: проблемы теории и практики: Специальность 5.1.4. Уголовно-правовые науки (юридические науки): диссертация на соискание ученой степени доктора юридических наук / Пучков Денис Валентинович; Уральский государственный юридический университет имени В. Ф. Яковлева. – Екатеринбург. - 2022. - 51 с.

45. Особенности методики расследования мошенничества в сфере компьютерной информации: Специальность 5.1.4. Уголовно-правовые науки (юридические науки): диссертация на соискание ученой степени кандидата юридических наук / Харина Елена Алексеевна. - Красноярский государственный аграрный университет. – Краснодар. - 2024. - 33 с.

46. Методика расследования незаконного оборота огнестрельного оружия с использованием информационно-телекоммуникационных сетей, в том числе сети «интернет»: Специальность 5.1.4. Уголовно-правовые науки (юридические науки): диссертация на соискание ученой степени кандидата юридических наук / Столбова Наталья Алексеевна. - Восточно-сибирский институт министерства внутренних дел российской федерации. – Иркутск. - 2024. - 243 с.

47. Введенская О.Ю. Особенности предварительного и первоначального этапов расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий: диссертация ... кандидата юридических наук - Краснодар, 2022. - 201 с.

IV. Эмпирические материалы

48. Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) Департамента информационной безопасности Банка России. Обзор несанкционированных переводов денежных средств за 2019 год;

49. Данные Судебного департамента при Верховном Суде Российской Федерации, полученные на сайте www.cdep.ru.

50. Приговор Якутского городского суда (Республика Саха(Якутия)) от 26 августа 2019 г. по делу № 1-1462/2018. - [Электронный ресурс]. URL: https://sudact.ru/regular/doc/8jIATe7oVfNK/ (дата обращения 10.06.2024)

51. Приговор Октябрьского районного суда г. Кирова от 13 июля 2016 г.

по уголовному делу № 1–298/2016. Электронный доступ: URL: https://rospravosudie.com/court-oktyabrskij-rajonnyj-sud-g-kirova-kirovskaya-oblast-s/act-532913468/ (дата обращения: 23.02.2024).

52. Приговор Октябрьского районного суда г. Тамбова от 9 июля 2010 г. по уголовному делу № 1-331/2010. Электронный ресурс - URL: http://sud23.tmb.sudrf.ru/modules.php? name=information&id=1242 (дата обращения: 10.04.2024).

53. Приговор Вологодского городского суда (Вологодская область) № 1-1094/2020 от 24 сентября 2020 г. по делу № 1-1094/2020 – [Электронный ресурс]. URL: https://sudact.ru/regular/doc/CauwPP3H3Bml/ (дата обращения 10.06.2024 г.).

54. Постановление Ленинского районного суда г. Кирова (Кировская область) № 1-168/2020 от 21 февраля 2020 г. по делу № 1-168/2020. – [Электронный ресурс]. URL: https://sudact.ru/regular/doc/Yg7GKxGlWEmV/

55. Приговор Петушинского районного суда (Владимирская область) от 19.09.2021 по делу № 1-146/2021 – [Электронный ресурс]. URL: https://actofact.ru/case-33RS0015-1-146-2021-2021-07-27-2-0/ (дата обращения 10.06.2024).

56. Серию преступлений в сфере компьютерной безопасности пресекли в России. Режим доступа: https://riamo.ru/news/proisshestviya/seriyu-prestuplenij-v-sfere-kompyuternoj-bezopasnosti-presekli-v-rossii-xl/.

V.Справочная литература

57. Рост числа киберпреступлений в 11 раз за 5 лет, до свыше 510,4 тыс. случаев – Генпрокуратура. Электронный доступ: URL: https://www.tadviser.ru/index.php/ Статья: Число_киберпреступлений_в_России (дата обращения: 19.05.2024).См.: Статистика и аналитика // Официальный сайт МВД России. – URL: https://mvd.ru/Deljatelnost/statistics (дата обращения:

10.04.2024).

58. Новости России: сайт. URL: http://news-russia.info/2017/05/12/ v-micro soft-nazvali-skolko-kompyuterov-v-mire-rabotayut-na/ (дата обращения: 17.12.2023).

59. Состояние преступности в России за январь – декабрь 2022 года // Отчет МВД России от 20.01.2023. [Электронный ресурс] // URL: chrome-extension://mhjfbmdgcfjbbpaeojofohoefgiehjai/index.html (дата обращения: 10.04.2024 г.).

60. Организация Объединенных Наций: вебсайт ООН. URL: http:/ /www.un.org/ru/documents/decl_conv/declarations/crime91.shtml (дата обращения: 10.04.2024).

61. Майкл Бойл, Жан-Клод Вюльерм. Краткое пособие по проведению допросов в ходе следствия. Практическое руководство. Общеевропейские принципы и стандарты работы полиции. Совет Европы. 2020. Электронный ресурс - URL: https://rm.coe.int/guide-to-investigative-interviewingrussian/1680934b21 (дата обращения 10.04.2024).

62. Число киберпреступлений в России. Электронный ресурс - URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России24 545918 (дата обращения: 10.04.2024).

ПРИЛОЖЕНИЯ

Приложение 1.

Считается важным внедрить большой объем изменений в имеющееся законодательство и разработать новые правовые акты, в которые будет уже включено правовое регулирование в цифровых правоотношениях, действующее на всей территории Российской Федерации.

Так, исходя из имеющихся слабых сторон Российского законодательства, необходимо прибегнуть таким действиям как:

1. Начать в качестве предмета преступления, которое непосредственно покушается на информацию, находящуюся в информационной среде, считать не компьютерную информацию, а цифровую. В примечании 1 к статье 272 УК РФ необходимо привести толкование термина «цифровая информация», а не «компьютерная информация».

2. С целью четкого упорядочивания понятийного аппарата уголовного законодательства, опираясь на термины, которые рассматриваются в нормативном документе, которые регулирует отношения, возникающие при осуществлении правомочий на поиск, получение, передачу и других действия во время использования информационных технологий необходимо применять более широкий по содержанию термин «информационно-телекоммуникационные устройства, их системы и сети» в положениях Особенной части УК РФ вместо предусмотренного в статье 274 УК РФ понятия, которое указывает на объекты обращения цифровой информации в форме «средств хранения, обработки или передачи компьютерной информации и ИТКС».

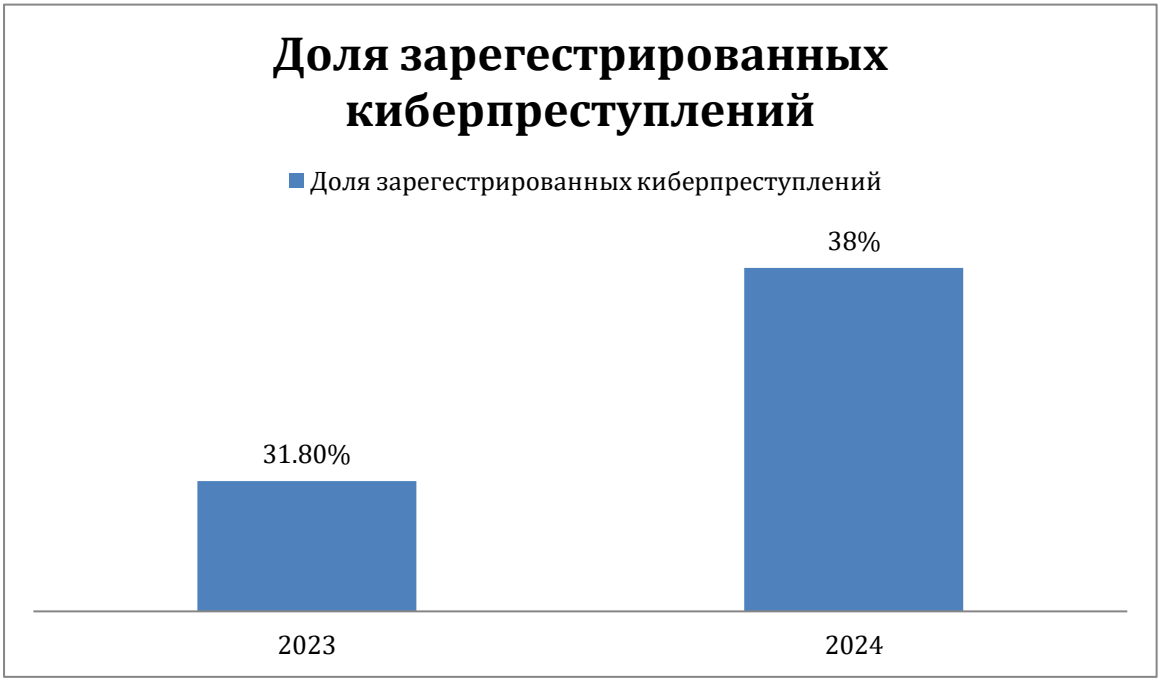
4. Поскольку ИТКС «Интернет» содержит интернет-ресурсы, размещающие информацию о способах совершения преступлений в сфере компьютерной информации, а также объявления о предоставлении незаконных услуг в этой сфере, предлагается в порядке предупреждения этих преступлений ввести механизм внесудебного ограничения доступа на территории Российской Федерации к такой информации, дополнив п. 1 ч. 5 ст. 15.1 «Единый реестр

доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации" следующим пунктом:

е) информации о способах совершения преступлений в сфере цифровой информации, а также объявлений по предоставлению незаконных услуг в этой сфере.

Помимо этого, также считается целесообразным разработать ряд программ, связанных с поощрением для различных организаций и специалистов, которые сильно взаимодействуют с органами государственной власти в области кибербезопасности и способствуют предотвращению и пресечению кибератак.

Приложение 2.



Кафедра уголовного права

УТВЕРЖДАЮ
Начальник кафедры
уголовного права
к.п.н., доцент
полковник полиции
_____ Р.С. Куликов
«29» 05 2023 г.

ПЛАН-ГРАФИК
выполнения дипломной работы

Тема: Преступления в сфере цифровой информации: понятие, виды и юридический анализ составов преступлений

Курсант (слушатель): Кузнецова Валерия Владимировна Учебная группа № 192
(фамилия, имя, отчество)

Специальность 40.05.01 – Правовое обеспечение национальной безопасности

Форма обучения Очная Год набора 2019

№ п/п	Характер работы (главы, параграфы и их содержание)	Примерный объем выполнения (в %)	Срок выполнения	Отметка руководителя о выполнении
1	Разработка план-графика выполнения дипломной работы и согласование его у научного руководителя, предоставление для утверждения начальником кафедры	2,5 %	до 30.06.2023	выполнено
2	Сбор и анализ эмпирического материала по теме дипломной работы	5%	до 20.07.2023	выполнено

3	Подготовка параграфа 1 главы 1 «Понятие информации и компьютерной информации в уголовном праве»	10 %	до 15.09.2023	выполнено
4	Подготовка параграфа 2 главы 1 «Понятие и признаки информационных преступлений»	10%	до 02.10.2023	выполнено
5	Подготовка параграфа 3 главы 1 «Общая характеристика составов информационных преступлений, содержащихся в УК РФ»	10%	До 15.10.2023	выполнено
6	Устранение замечаний научного руководителя	2,5%	до 20.10.2023	выполнено
7	Подготовка параграфа 1 главы 2 «Информационные преступления, предметом которых является информация»	10%	до 10.11.2023	выполнено
8	Подготовка параграфа 2 главы 2 «Информационные преступления, способом совершения которых является информационное воздействие»	5 %	до 01.12.2023	выполнено
9	Подготовка параграфа 1 главы 3 «Понятие компьютерных преступлений, их место среди информационных преступлений»	5 %	до 20.12.2023	выполнено
10	Устранение замечаний научного руководителя	2,5%	до 01.01.2024	выполнено
11	Подготовка параграфа 2 главы 3 «Виды компьютерных преступлений»	10%	до 10.01.2024	выполнено
12	Подготовка введения и заключения, подготовка	10%	до 15.02.2024	выполнено

	списка литературы, оформление приложений			
13	Устранение замечаний научного руководителя	5%	до 01.03.2024	выполнено
14	Подготовка введения и заключения, подготовка списка литературы, оформление приложений	2,5 %	до 01.04.2024	выполнено
15	Представление для изучения рукописи дипломной работы научному руководителю	2,5 %	до 19.04.2024	выполнено
16	Редактирование, проверка работы по системе «Антиплагиат»	2,5 %	до 06.05.2024	выполнено
17	Оформление документации, представление дипломной работы на кафедру	2,5%	до 30.05.2024	выполнено

Подпись выпускника _____

«__» _____ 20__г.

СОГЛАСОВАНО
Руководитель:
Начальник кафедры уголовного права,
Кандидат педагогических наук, доцент
Казанского юридического института МВД России
полковник полиции
_____ Р.С. Куликов

АВТОРСКАЯ СПРАВКА

Автор:

Кузнецова В.В. - слушатель 192 учебной группы факультете подготовки специалистов по программам высшего образования КЮИ МВД России.

Научный руководитель – начальник кафедры полковник полиции Куликов Р.С.

Настоящим сообщаю, что при подготовке к опубликованию дипломной работы «Преступления в сфере цифровой информации: понятие, виды и юридический анализ составов преступлений»:

- не использовались литературные источники и документы, имеющие пометку «Для служебного пользования», и гриф секретности «секретно», «совершенно секретно», а также служебные материалы других организаций;

- не содержаться сведения, составляющие в соответствии с Законом РФ от 21 июля 1993 г. №5485-1 «О государственной тайне», Указом Президента РФ от 30 ноября 1995 г. №1203 «Об утверждении перечня сведений, отнесенных к государственной тайне», а также Перечня сведений, подлежащий засекречиванию, Министерства внутренних дел Российской Федерации утвержденного приказом МВД России от 10 сентября 2018 г. №580дсп, государственную тайну;

- не содержатся сведения, которые представляли бы собой конфиденциальную информацию, в то числе персональные данные физических лиц, которые в соответствии с Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных» ограничены или запрещены к открытому опубликованию.

Материалы дипломной работы рассмотрены на заседании кафедры уголовного права КЮИ МВД России (протокол №20 от 6.06.2024 г.) и рекомендованы к открытому опубликованию в электронно-информационной образовательной среде института.

Начальник кафедры уголовного права КЮИ МВД России
полковник полиции Р.С. Куликов
«6» 06 2024 г.
Автор:_____Кузнецова В.В.

РАЗРЕШЕНИЕ

на размещение дипломной работы в электронно-библиотечной системе

Я, Кузнецова Валерия Владимировна
(фамилия, имя, отчество)

обучающийся (-аяся) 192 учебного взвода (группы), очной
очной / заочной

формы обучения Казанского юридического института МВД России (далее – Институт) по специальности 40.05.01 Правовое обеспечение национальной безопасности.
код, наименование специальности

разрешаю разместить выполненную мной дипломную работу на тему Преступления в сфере цифровой информации: понятие, виды и юридический анализ мотивов преступления
наименование темы

в полном
полном / неполном

объеме в электронно-библиотечной системе Института, для доступа любого пользователя указанной системы к ее тексту. Изъятию из текста дипломной работы подлежат следующие элементы: _____
_____.
элементы, не подлежащие размещению в ЭБС

Подтверждаю, что дипломная работа выполнена мной лично. Все прямые заимствований из печатных и электронных источников имеют соответствующие ссылки.

Подпись: _____

Дата: _____

АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

Казанский юридический институт МВД России

СПРАВКА

о результатах проверки текстового документа
на наличие заимствований

ПРОВЕРКА ВЫПОЛНЕНА В СИСТЕМЕ АНТИПЛАГИАТ.ВУЗ

Автор работы: Кузнецова Валерия Владимировна
Самоцитирование рассчитано для: Кузнецова Валерия Владимировна
Название работы: Преступления в сфере цифровой информации: понятие, виды и юридический анализ составов преступления
Тип работы: Дипломная работа
Подразделение:

РЕЗУЛЬТАТЫ

■ **ОТЧЕТ О ПРОВЕРКЕ КОРРЕКТИРОВАЛСЯ:** НИЖЕ ПРЕДСТАВЛЕНЫ РЕЗУЛЬТАТЫ ПРОВЕРКИ ДО КОРРЕКТИРОВКИ

СОВПАДЕНИЯ	35.38%	СОВПАДЕНИЯ	35.38%
ОРИГИНАЛЬНОСТЬ	55.39%	ОРИГИНАЛЬНОСТЬ	55.39%
ЦИТИРОВАНИЯ	9.23%	ЦИТИРОВАНИЯ	9.23%
САМОЦИТИРОВАНИЯ	0%	САМОЦИТИРОВАНИЯ	0%

ДАТА ПОСЛЕДНЕЙ ПРОВЕРКИ: 10.06.2024

ДАТА И ВРЕМЯ КОРРЕКТИРОВКИ: 10.06.2024 08:33

Структура документа: Проверенные разделы: библиография с 63-69, титульный лист с 1, содержание с 2, основная часть с 3-62
Модули поиска: Модуль поиска "КЮИ МВД РФ"; Медицина; Перефразирования по Интернету; Издательство Wiley; Диссертации НББ; Переводные заимствования по Интернету (EnRu); СМИ России и СНГ; СПС ГАРАНТ: нормативно-правовая документация; Переводные заимствования по eLIBRARY.RU (EnRu); Переводные заимствования (RuEn); Сводная коллекция ЭБС; Сводная коллекция вузов МВД; ИПС Адилет; Патенты СССР, РФ, СНГ; Переводные заимствования издательства Wiley (RuEn); eLIBRARY.RU; СПС ГАРАНТ: аналитика; Перефразирования по СПС ГАРАНТ: аналитика; Цитирование; Сводная коллекция РГБ; Перефразирования по eLIBRARY.RU; Кольцо вузов; Интернет Плюс; Шаблонные фразы; Библиография

Работу проверил: Куликов Роман Сергеевич
ФИО проверяющего

Дата подписи: 10.06.2024

Подпись проверяющего

Чтобы убедиться в подлинности справки, используйте QR-код, который содержит ссылку на отчет

Ответ на вопрос, является ли обнаруженное заимствование корректным, система оставляет на усмотрение проверяющего. Предоставленная информация не подлежит использованию в коммерческих целях.

С результатами проверки ознакомлена Кузнецова 10.06.2024

Отзыв о работе

слушателя 192 учебной группы, очной формы обучения, 2019 года набора, по специальности 40.05.01 – Правовое обеспечение национальной безопасности Кузнецовой Валерии Владимировны в период подготовки дипломной работы на тему: «Преступления в сфере цифровой информации: понятие, виды и юридический анализ составов преступлений»

Тема дипломной работы выбрана из списка тем, предложенных кафедрой. Кузнецова В.В. проявила заинтересованность в выборе темы дипломной работы, так как она понятна автору и чрезвычайно актуальна в настоящее время. Поэтому Кузнецова В.В. обосновала заинтересованность в выбранной теме актуальностью, наличием эмпирического материала по теме исследования, а также личными мотивами.

Результаты исследования и выработанные положения дипломной работы автором апробированы в ходе следующих научно-представительских мероприятий: на Всероссийском круглом столе «Противодействие преступности в современном мире», проведенном 9 февраля 2024 г. Уфимским юридическим институтом МВД России (г. Уфа); на Всероссийской научно-практической конференции – финале всероссийского конкурса курсантов и слушателей образовательных организаций МВД России «Теория и практика противодействия преступности уголовно-правовыми средствами», проведенной 30 мая 2024 г. Казанским юридическим институтом МВД России (г. Казань); на Всероссийской научно-практической конференции «Уголовное и уголовно-исполнительное законодательство: вчера, сегодня, завтра», проведенной 6 июня 2024 г. Нижегородской академией МВД России (г. Нижний Новгород); опубликована статья «Преступления в сфере цифровой информации: понятие, виды и юридический анализ составов преступлений» в сборнике научных статей «Кирсановские чтения. Выпуск X. 2023 год». г. Казань (стр. 204-207).

Содержание работы соответствует заданию.

Кузнецова В.В. продемонстрировала навыки и умения в формулировании цели и постановке задач, которые соответствуют теме работы, отражают актуальность выбранной темы исследования.

Структура работы логична, построена таким образом, что позволяет раскрыть наиболее актуальные вопросы темы. Работа состоит из введения, трех глав, объединяющих 7 параграфов, заключения и списка использованной литературы.

Кузнецова В.В. выполнила работу в установленные сроки. Совместно с научным руководителем составила план дипломной работы, осуществила поиск источников, материалов судебно-следственной практики. В процессе подготовки работы автор постоянно осуществлял взаимодействие с научным руководителем. Все замечания относительно теста работы, устраняла в кратчайшие сроки.

Кузнецова В.В. продемонстрировала способность и умения пользования научной литературой, в том числе профессиональной, навыки к поиску, обобщению и анализу материалов практики. Автор проявил эрудицию, показал хорошую теоретическую подготовку по дисциплинам уголовно-правового цикла, а также ранее изученным предметам, имеющим связь с уголовным правом и темой дипломной работы.

Автор показал способность формулировать собственную точку зрения, навыки и умения работы с законодательными актами, а также обобщению и анализу эмпирического материала по тематике дипломной работы. В работе отразились умение и навыки Кузнецовой В.В. оперировать научно-юридическими терминами и категориями, применять их в процессе написания работы, а также в работе с материалами следственно-судебной практики, способность и умения к проведению анализа статистических данных и их применения в исследовании.

Кузнецова продемонстрировала способность к самостоятельному формулированию обоснованных и достоверных выводов и результатов исследования.

Работы выполнена самостоятельно. Так, проверка текста в системе «Антиплагиат.вуз» показала, что оригинальность текста составляет – 55,39%, цитирования – 9,23 %, заимствования – 35,38 %, что соответствует требованиям, предъявляемым к оригинальности текста работы.

Дипломная работа Кузнецовой Валерии Владимировны на тему: «Преступления в сфере цифровой информации: понятие, виды и юридический анализ составов преступлений» может быть допущена к защите и заслуживает высокой положительной отметки, а её автор присвоения квалификации, соответствующей специальности обучения.

Научный руководитель:
Начальник кафедры уголовного права
Казанского юридического института
МВД России
кандидат педагогических наук, доцент
полковник полиции
«10» июня 2024 г.

Подпись Куликова Р.С.
УДОСТОВЕРЯЕТСЯ
ОД и РКЮИ МВД России

_____Р.С. Куликов

С отзывом ознакомлена
«10» июня 2024 г.

_____ В.В. Кузнецова

РЕЦЕНЗИЯ

на дипломную работу

обучающейся 192 учебного взвода очной формы обучения, 2019 года набора, по специальности 40.05.01. – Правовое обеспечение национальной безопасности ФПС по ПВО Кузнецовой Валерии Владимировны на тему «Преступления в сфере цифровой информации: понятие, виды и юридический анализ преступлений»

Содержание рецензии

Преступления в сфере цифровой информации являются одним из актуальных направлений в деятельности сотрудников ОВД. Исследования в данной дипломной работе выполнены на актуальную тему, поскольку в настоящее время деяния, совершаемые в сфере цифровой информации, носят разносторонний характер. В связи с этим появляется потребность в создании соответствующих правовых положений для борьбы с цифровыми преступлениями. Достаточно распространенным преступлением считается преступление, связанное с неправомерным доступом к компьютерной информации. Данные преступные деяния посягают на охраняемые законом сведения, совершающиеся с целью обнаружения нужной информации, чтобы в дальнейшем ее применять в корыстных целях. Преступления в сфере цифровой информации с годом набирают все большее значение в силу того, что людей, использующих цифровые устройства, становится все больше, как и информации, располагаемой на их личных устройствах.

Дипломная работа состоит из введения, трех глав, объединяющих 7 параграфов, заключения и списка использованной литературы. Структура работы логична, соответствует заявленной структуре в плане-графике выполнения выпускной квалификационной работы.

Во введении четко определены предмет, объект исследования, а также цели и задачи, осуществляемые во время написания работы.

Первая глава посвящена рассмотрению понятия и признаков информационных преступлений, общей характеристике составов информационных преступлений, содержащихся в УК РФ. Так, поднимаются вопросы касаемо исторического аспекта развития, выявления и расследования подобных преступлений, а также исследуется вопрос, необходимый для полного всестороннего рассмотрения первой главы, который связан с характеристикой преступления в целом.

Вторая глава посвящена уже непосредственному рассмотрению видов информационных преступлений. Проанализированы главы 17 и 21 Уголовного Кодекса РФ. Проведен сравнительный анализ информационных преступлений, предметом которых является информация и информационных преступлений,

способом совершения которых является информационное воздействие, и всех иных преступлений по главам УК РФ с разнообразными группами информационных преступлений по разделам УК РФ.

Третья глава посвящена вопросам квалификации преступлений в сфере компьютерных преступлений, а также изучению отдельных квалифицирующих признаков и судебной практики по данным делам. Проанализирована общая характеристика преступлений, совершаемых в данной сфере, а также установлены отграничения от смежных составов преступлений.

В заключении сформулированы научно обоснованные выводы. Достоверность выводов подтверждается внушительным списком использованных нормативно-правовых актов и литературы. Работа сама по себе имеет исследовательский характер, хорошо изложенную теоретическую часть, логичное и последовательное изложение материала с соответствующими выводами и обоснованными предложениями.

Автором был проанализирован достаточный объем теоретического материала, нормативно-правовой базы: для написания работы использованы труд отечественных авторов, проблема раскрыта всесторонне. Прослеживается тщательная и глубокая проработка вопроса. Также стоит отметить стиль написания работы, который является научным, но при этом понятным и доступным для понимания.

Выбранная проблематика раскрыта полностью, цель достигнута, задачи решены, выводы правильны и обоснованы.

Дипломная работа соответствует установленным требованиям.

С учетом вышеизложенного и результатов выступления при её защите, полагал бы необходимым оценить работу дипломную работу В.В. Кузнецовой по теме: «Преступления в сфере цифровой информации: понятие, виды и юридический анализ преступления» оценить на оценку отлично.

Рецензент:
Начальник ОП №13 «Азино-2»
УМВД России по г. Казань
полковник полиции Н.Г. Харисов

«24» июня 2024 г.

С рецензией ознакомлена В.В. Кузнецова

«24» июня 2024 г.