Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
ЮРИДИЧЕСКИЙ ИНСТИТУТ
Кафедра «Правоохранительная деятельность и национальная безопасность»

ВЫЯВЛЕНИЕ, ПРЕДУПРЕЖДЕНИЕ И ПРЕСЕЧЕНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГАОУ ВО «ЮУрГУ» (НИУ) – 40.05.01.2016. 514.ВКР

Руководитель работы,
канд. юрид. наук, доцент
доцент кафедры
___Евгений Владимирович Никитин
_____2021 г.

Автор работы,
студент группы Ю-514
_____Роман Данилович Гильманов
_____2021 г.

Нормоконтролер,
___Наталья Владимировна Агаркова
_____2021 г.

Челябинск
2021

АННОТАЦИЯ

Гильманов Р.Д. Выпускная квалификационная работа «Выявление, предупреждение и пресечение преступлений в сфере компьютерной информации как средство обеспечения национальной безопасности Российской Федерации»: ФГАОУ ВО «ЮУрГУ (НИУ)», Ю–514, 70 с., библиогр. список – 59 наим., прил.3.

Объектом работы являются общественные отношения, в результате которых нарушаются уголовно-правовые нормы, предусматривающие уголовную ответственность за преступления в сфере компьютерной информации.

Цель работы – состоит в комплексном анализе уголовно-правовой характеристики и вопросов квалификации преступлений в сфере компьютерной информации.

В работе рассмотрены генезис отечественного законодательства в сфере защиты компьютерной информации, состояние компьютерной преступности в России, было определено современное уголовно-правовое понятие преступлений в сфере компьютерной информации и их виды, рассмотрено международное законодательство и зарубежный опыт уголовно-правового регулирования отношений в сфере компьютерной информации, исследованы особенности выявления преступлений в сфере компьютерной информации, проанализировано предупреждение преступлений, совершаемых с использованием информационно-телекоммуникационных технологий и в сфере компьютерной информации, а так же сформулированы предложения по разрешению данных проблем.

Результаты работы имеют практическую значимость, содержат выводы, практические рекомендации и предложения автора по совершенствованию норм, регулирующих порядок вопросов предотвращения преступлений, совершаемых в сфере компьютерной информации и практики их применения.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы работы. Общество XXI века невозможно представить без применения компьютерных и цифровых технологий практически во всех сферах общественной жизни и производства, что является одним из значимых условий активного, современного, цивилизационного развития общества и государства. Такое влияние информационных технологий вызывает и особый интерес к ним со стороны преступников, что указывает на значимость создания истинно действующего механизмы правовой защиты субъектов информационных киберотношений, необходимость выработки мер, направленных на снижение объема компьютерной преступности.

Значительное количество совершаемых компьютерных преступлений привело к необходимости криминализации отдельных деяний в компьютерной сфере, в результате чего в УК РФ была включена глава 28 «Преступления в сфере компьютерной информации». Динамика компьютерной преступности, применение всё новых и новых технологий и способов совершения преступлений в электронном пространстве свидетельствует о необходимости постоянного проведения исследований в данной области с целью выявления их тенденций и разработки соответствующих, адекватных мер реагирования, в том числе и уголовно-правового характера.

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы[1] в качестве приоритетного направления внутренней политики определяет развитие информационных и коммуникационных технологий, формирование информационного пространства и соответствующей инфраструктуры. Информационные

[1] Указ Президента Российской Федерации «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» от 9 мая 2017 г. № 203 // СЗ РФ. 2017. № 20. Ст. 2901

технологии все глубже проникают в повседневную жизнедеятельность большинства граждан. Отмечается, что в 2019 г. в России на 100 человек приходилось 159,95 мобильных телефонов и из 100 человек 71,29 человека использовали мобильный доступ к сети Интернет.

Внедрение автоматических информационных систем и технологий управления и обработки информации, придание юридической силы актам, осуществляемым с помощью компьютерных программ, создали предпосылки использования этих процессов для совершения преступных актов, а следовательно, и необходимость усиления их защиты, в том числе уголовно-правовыми методами. Опасность преступлений в сфере компьютерной информации состоит в том, что уничтожение, блокирование, модификация информации, важной для действий, связанных с управляющими датчиками сложных компьютерных систем оборонного, производственного, экономического, банковского и другого назначения, способны повлечь гибель людей, причинить вред их здоровью, уничтожить имущество, причинить экономический вред в больших размерах. Учитывая эти обстоятельства, законодатель отнес гл. 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной информации» к разд. IX УК РФ «Преступления против общественной безопасности и общественного порядка».

Цель работы состоит в комплексном анализе уголовно-правовой характеристики и вопросов квалификации преступлений в сфере компьютерной информации.

Для достижения поставленной цели в ходе работы решаются следующие задачи, составляющие ее содержание:

– изучение генезиса отечественного законодательства в сфере защиты компьютерной информации и оценка состояния компьютерной преступности в России;

– рассмотрение современного уголовно-правового понятия преступлений

в сфере компьютерной информации;

– анализ международного законодательства и зарубежного опыта уголовно-правового регулирования отношений в сфере компьютерной информации;

– рассмотрение особенностей выявления преступлений в сфере компьютерной информации;

– изучение предупреждения преступлений, совершаемых с использованием информационно-телекоммуникационных технологий и в сфере компьютерной информации;

– анализ проблем квалификации преступлений в сфере компьютерной информации;

– определение основных направлений совершенствования уголовно-правовых механизмов противодействия преступлениям в сфере компьютерной информации.

Объектом исследования дипломной работы являются общественные отношения, в результате которых нарушаются уголовно-правовые нормы, предусматривающие уголовную ответственность за преступления в сфере компьютерной информации.

Предметом дипломной работы образуют уголовно-правовые нормы, регламентирующие ответственность за преступления в сфере компьютерной информации, а также научные воззрения и судебная практика в рассматриваемой области.

Степень научной разработанности темы. Отдельные вопросы рассматриваемой проблемы подвергались анализу в диссертациях, монографиях, научных публикациях и учебной литературе. Изучению уголовно-правовых аспектов преступлений в сфере компьютерной информации посвятили свои труды С.Н. Гришаев, А.П. Днепров, Д.В. Добровольский, М.А. Зубова, И.И. Исаченко, А.А. Комаров,

А.Н. Копырюлин, А.В. Литвинов, Т.М. Лопатина, А.В. Нарижный, А.Ю. Рыков, О.М. Сафонов, В.Н. Черкасов, А.И. Усов, В.В. Челноков и др.

Методологическую основу исследования составил общенаучный диалектический метод познания общественных явлений. Комплексно применялись следующие общенаучные и частно-научные методы познания: историко-правовой.

Структура работыобусловлена целью, задачами, объектом и предметом исследования. Работа состоит из введения, двух глав, объединяющих семь параграфов, заключения, библиографического списка.

1 РАЗВИТИЕ ИНСТИТУТА ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В ОТЕЧЕСТВЕННОМ И ЗАРУБЕЖНОМ ЗАКОНОДАТЕЛЬСТВЕ

1.1. Генезис отечественного законодательства в сфере защиты компьютерной информации

История развития ответственности за компьютерные преступные деяния является относительно не продолжительной ввиду того, что сама компьютерная техника и информационные технологии стали активно развиваться лишь в 1960-х годах.

По утверждению С.Г. Спириной, первым шагом отечественного законодателя по правовой защите определенной части компьютерной информации стало издание законов от 23 сентября 1992 г. № 3523–1: «О правовой охране программ для электронно-вычислительных машин и баз данных»[1] и от 1 января 1994 г. «О правовой охране топологий интегральных микросхем»[2], регламентирующих порядок установления и правовую защиту авторских прав на программные средства компьютерной техники и топологии интегральных микросхем[3]. До принятия законодательных решений предпринимались шаги по разработке отдельных проектов, предусматривающих ответственность в рассматриваемой области.

В 90-х годах XX века, более точно – в 1991 году, был предложен законодателями текст проекта Закона РСФСР «Об ответственности за правонарушения при работе с информацией». В тексте проекта, как отмечает

---

[1]Закон РФ «О правовой охране программ для электронновычислительных машин и баз данных» от 23 сентября 1992 г. // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. № 42. Ст. 2325 (утратил силу).

[2]Закон РФ «О правовой охране топологий интегральных микросхем» от 23 сентября 1992 г. // Ведомости Верховного Совета РФ. №42. 1992. Ст. 2328 (утратил силу).

[3] См.: Спирина С.Г. Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации: дис. ... канд. юрид. наук. Краснодар, 2001. С. 73.

А.В. Настоящий, предусматривалось дополнение Уголовного кодекса нормами, определяющими ответственность за деяния в сфере компьютерной информацией[1]. Несмотря на наличие проекта, уголовное законодательство так и не было дополнено нормами, регламентирующими ответственность за совершение преступлений в сфере электронных отношений (с использованием ЭВМ и автоматизированных систем управления). Лишь в УК РФ 1996 года были впервые в истории России включены нормы в сфере компьютерной информации. Но в отличие от ныне действующей редакции главы 28 УК РФ, ранее в УК использовалось указание на ЭВМ.

Толчок к включению в уголовный кодекс норм в сфере компьютерной преступности был определен не только фактом их совершения и постоянным увеличением их числа, но и совершенствованием законодательства в области электронного оборота[2], в том числе принятие в 1995 году закона «Об информации, информатизации и защите информации»[3].

Анализируя историю совершения преступлений с использованием компьютерных технологий О.М. Сафонов выделяет закономерности их развития: «так, если на заре становления киберпреступности основной целью злоумышленника являлось личное обогащение, а компьютер использовался как инструмент хищения, то к 90-м годам XX века основной целью лица,совершающего преступление с использованием компьютерных технологийстал «интеллектуальный вызов», то есть стремление показать своепревосходство в знании компьютерных систем и обходе средств их защиты. Внастоящее время преступления с использованием компьютерных

[1] Настоящий А.В. История появления и развития преступлений в сфере компьютерной информации // Студенческий вестник. 2020. № 7–1. С. 62.

[2]Кочкина Э.Л., Сутурин М.А. Уголовная ответственность за преступления в сфере компьютерной информации: история становления и обзор нормативных документов // Актуальные вопросы совершенствования уголовной политики Российской Федерации: сборник трудов конференции. Ростов-на-Дону: ДГТУ-Принт, 2019. С. 112.

[3] Федеральный закон «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ // Российская газета. 1995. 22 февраля. № 39 (утратил силу).

технологийчасто становятся инструментом незаконного политического давления»[1].

Как первоначально, так и сейчас можно говорить об устаревшей формулировке норм главы 28 УК РФ. Данная точка зрения прослеживается в трудах ряда ученых, в том числе и О.М. Сафонова. Примером устарелого, отсталого формулирования можно было считать использование аббревиатуры «ЭВМ». Лишь в 2011 году, в результате принятия Федерального закона № 420[2], было ликвидировано отжившие себя упоминание ЭВМ в ст. 272 УК РФ, было представлена дефиниция компьютерной информации. Но развитие компьютерных технологий в современном обществе позволяет предполагать возможность дальнейшего совершенствования формулировок и определений.

В XXI веке внесен ряд поправок в части регулирования ответственности за использование компьютерных технологий. Например, значительно скорректированы были нормы самой главы 28 УК РФ, а также других глав УК, в частности, внесены были изменения в ст. 242.1 УК РФ[3], предусматривающие ответственность за изготовление порнографических материалов с изображениями несовершеннолетних с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть «Интернет»). Внесение такого изменения в УК РФ, разработчики проекта обосновывали тем, что до 2012 года в России еще не были установлены повышенные меры уголовной ответственности за оборот

[1] Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. канд. юрид. наук. М., 2015. С. 20.

[2] Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 7 декабря 2011 г. № 420–ФЗ // Собрание законодательства Российской Федерации. 2011. № 50. Ст. 7362.

[3] Федеральный закон «О внесении изменений в УК РФ и отдельные законодательные акты РФ в целях усиления ответственности за преступления сексуального характера, совершенные в отношении несовершеннолетних» от 29 февраля 2012 г. № 14–ФЗ // Собрание законодательства Российской Федерации. 2012. № 10. Ст. 1162.

детской порнографии с использованием сети Интернет и других информационно-телекоммуникационных сетей общего пользования[1].

Предлагалось внести в Уголовный кодекс Российской Федерации следующие изменения: в квалифицированных составах статей 135, 242, 242.1 Уголовного кодекса Российской Федерации установить повышенную уголовную ответственность за массовые, публичные формы растления детей, в том числе с использованием информационно-телекоммуникационных сетей общего пользования.

Предлагаемые изменения социально, криминологически и юридически обоснованы и соответствуют международным стандартам в сфере защиты детей от преступности. В результате принятия Федерального закона от 29 февраля 2012 г. № 14-ФЗ ст. 242.1 УК РФ была изложена в новой редакции и теперь предусматривает квалифицированный состав за изготовление и оборот материалов и предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть «Интернет») (п. «г» ч. 2 ст. 242.1 УК РФ).

До внесения соответствующих изменений УК РФ предусматривал ответственность граждан Российской Федерации, иностранных граждан и лиц без гражданства за нарушение законодательства о безопасности критической информационной инфраструктуры. В 2016 году Правительством РФ было предложено выделить составы таких посягательств в отдельную статью[2]. В ней предлагалось предусмотреть ответственность за создание и

[1] Пояснительная записка «К проекту Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации в целях усиления ответственности за преступления сексуального характера, совершенные в отношении несовершеннолетних» Режим доступа: https://www.lawmix.ru/lawprojects/4804?page=2 (дата обращения: 05.12.2020).

[2] Досье на проект федерального закона № 47591–7 «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» (внесен

(или) распространение компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру; неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в критической информационной инфраструктуре; нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре. Предлагаемая норма должна была содержать квалифицирующие признаки (совершение деяния группой лиц, по предварительному сговору или организованной группой лиц или лицом с использованием служебного положения). С учетом этих признаков санкции за указанные деяния предусматривают наказания в виде штрафа, принудительных работ, лишения свободы (с лишением права занимать определенные должности или заниматься определенной деятельностью). В итоге в 2017 году УК РФ был дополнен статьей 274.1[1].

Значительным явлением в совершенствовании уголовно-правовых норм в области ответственности за компьютерные преступления следует признать дополнение УК РФ специальными составами мошенничества, совершаемыми при непосредственном использовании платежных систем (ст. 159.3 УК РФ) и компьютерной информации (ст. 159.6 УК РФ).

Федеральным законом от 29 ноября 2012 г. № 207-ФЗ[2] Уголовный кодекс дополнен нормой об ответственности за мошенничество в сфере компьютерной информации. В пояснительной записке к проекту авторы законопроекта так обосновали предложения о дополнении уголовного закона

06.12.2016 Правительством РФ) Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71456958/ (дата обращения: 05.12.2020).

[1] Федеральный закон «О внесении изменений в УК РФ и статью 151 УПК в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 194–ФЗ// Собрание законодательства Российской Федерации. 2017. № 31. Ст. 4743.

[2] Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 29 ноября 2012 г. № 207-ФЗ // Собрание законодательства Российской Федерации. 2012. № 49. Ст. 6752.

указанной нормой: «Предлагается также выделить в самостоятельный состав преступления мошенничество в сфере компьютерной информации (статья 159.6 законопроекта), когда хищение или приобретение права на чужое имущество сопряжено с преодолением компьютерной защиты имущества (имущественных прав) и осуществляется путем ввода, удаления, модификации или блокирования компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Подобные преступления совершаются не путем обмана или злоупотребления доверием конкретного субъекта, а путем получения доступа к компьютерной системе и совершения вышеуказанных действий, которые в результате приводят к хищению чужого имущества или приобретению права на чужое имущество»[1]. В настоящее время мошенничество в сфере компьютерной информации рассматривается как новая форма хищения.

В результате изложенного следует, что развитие института ответственности за компьютерные преступления имеет относительно не продолжительный период. Первые нормы, определяющие уголовную ответственность за преступления в рассматриваемой сфере, были включены в отечественное уголовное законодательство в конце XX века. Несмотря на вносимые в УК РФ дополнения, кардинального изменения уголовного законодательства не происходит, по-прежнему законодательство «отстаёт» от развития технологии информационных систем и от развития отношений в кибепространстве. Преступления, совершаемые в области компьютерной информации и в киберпространстве, представляют собой достаточно распространенное противозаконное явление, при этом, число данных деяний в ближайшем будущем будет увеличиваться. Такая тенденция обусловлена

[1]Постановление Пленума Верховного Суда РФ «О внесении в Государственную Думу Федерального Собрания Российской Федерации проекта Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» от 5 апреля 2012 г. № 6 // СПС «КонсультантПлюс».

активным развитием компьютерных технологий и программного обеспечения, что предопределяет необходимость разработки рекомендаций по правильной квалификации деяний, совершаемых в сфере компьютерной информации.

1.2 Современное уголовно-правовое понятие преступлений в сфере компьютерной информации

Впервые термин компьютерной преступности начал употребляться в США, а затем и в других странах с начала 60-х годов XX века, когда были зарегистрированы первые противоправные посягательства с использованием тогда еще называемых ЭВМ. Первоначальная попытка разработки легальной дефиниции компьютерного преступления имела место на полях Организации экономического сотрудничества и развития. Так, В.С Комиссаров предлагает «преступлениями в сфере компьютерной информации» признавать «умышленные общественно опасные деяния (действие или бездействие), причиняющие вред либо создающие угрозу причинения вреда общественным отношениям, регламентирующим безопасное производство, хранение, использование или распространение информации и информационных ресурсов либо их защиту»[1].

По убеждению Д.В. Добровольского факт наличия преступлений в сфере компьютерной информации можно представить как определенный способ регулирования, методов управления в целях уменьшения причиняемого вреда, категория оцениваемая с точки зрения государства как негативное явление современной действительности и обладающее основными признаками профессиональной преступности, а в правовой области представляющее собой обширное, массовое виновное нарушение уголовных норм, совокупность всех фактически деяний совершенных

[1] Комиссаров В. С. Преступления в сфере компьютерной безопасности; понятие и ответственность // Юридический мир. 1998. № 2. С. 22.

вменяемыми физическими лицами, достигшими возраста шестнадцати лет, преступлений в области информационных технологий[1].

23 ноября 2011 г. в Будапеште была подписана Конвенция Совета Европы о преступности в сфере компьютерной информации ETS № 18514[2]. Она была подписана государствами-членами Совета Европы, а также США и Японией. В настоящий момент Россия не подписала Конвенцию. Тем не менее, Конвенция содержит важные положения и проводит классификацию киберпреступлений, выделяя их виды в 5 групп.

Первая группа: преступления, которые посягают на конфиденциальность, целостность и недоступность компьютерных данных и систем. Примером можно назвать, например: несанкционированный доступ в базы данных и в систему.

Вторая группа: преступления, связанные с использованием компьютера как средства совершения противозаконных действий. К этой группе можно отнести компьютерное мошенничество.

Третья группа: преступления, связанные с содержанием информации, размещаемой в сети Интернет. В частности с размещением в сети детской порнографии.

Четвертая группа: преступления, связанные с нарушением авторского права и смежных прав. Однако установление таких правонарушенийКонвенцией отнесено к компетенции национальных законодательств государств.

Пятая группа: преступления, связанные с распространением расистских и ксенофобских материалов в сети Интернет.

Анализируя уголовные дела по преступлениям в сфере компьютерной

---

[1] Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: Уголовно-правовые и криминологические проблемы: автореферат дис. ... канд. юрид. наук. М., 2006. С. 8.

[2]Counsil of Europe. Convention on Cybercrime, Budapest. // Электрон. дан. – 2017. – URL: https://www.coe.int/en/web/conventions/full-list/- /conventions/treaty/185/ (датаобращения 20.05.2021).

информации и изучая работы отечественных ученых в сфере киберпреступлений, возможно выделение более 20 основных способов совершения компьютерных преступлений и еще большего числа их разновидностей. Такое количество способов совершения преступлений в рассматриваемой сфере постоянно растет в связи с развитием компьютерной техники, коммуникационных сетей, а также разнообразием модификаций средств (аппаратных и программно-аппаратных) совершения киберпреступлений.

Согласно ныне действующему уголовному законодательству компьютерные преступления представляют собой преступные деяния, которые совершаются в области информационных процессов, в связи с чем посягают на сферу информационной безопасности, в качестве предмета которых выступает информация, а также компьютерные средства[1]. Ежегодно осуждается более ста человек за совершение преступлений, квалифицируемых по статьям главы 28 УК РФ, только в 2019 году было осуждено 165 лиц[2] (см. приложение 1). Отметим, что по ст. 274 УК РФ не вынесено ни одного приговора. В действительности подобные общественно опасные деяния встречаются довольно часто и то, что действия виновных не охватываются нормами об уголовной ответственности за нарушение 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, свидетельствует о наличии проблемы в правоприменении ст. 274 УК РФ, требующей правового решения. По ст. 274.1 УК РФ вынесено только четыре обвинительных приговора в 2019 году.

[1]Строчкина А.И. Информация как предмет преступления в сфере компьютерной информации // Актуальные проблемы правоприменения и управления на современном этапе развития общества: сборник трудов конференции. Ставрополь: Фабула, 2020. С. 239.
[2] Судебный департамент при Верховном Суде Российской Федерации. Режим доступа: http://www.cdep.ru (дата обращения: 05.12.2020).

Данное обстоятельство, как представляется связано с тем, что только в 2017 году ст. 274.1 УК РФ была введена в УК РФ.

В данном случае показателен следующий пример из судебной практики:

Уголовное дело № 1-55/2016 возбуждено 11 марта 2016 года в г. Новокуйбышевске. Из обвинительного заключения следует, что Тимофеев, работавший в ОАО “ВымпелКом” с 28.02.2014, в период времени с 03.05.2014 года по 07.06.2014 года осуществлял неправомерный доступ к охраняемой законом компьютерной информации, содержащей персональные данные клиентов ОАО «ВымпелКом» и их лицевых счетов, путём отключения запрета на услугу «Мобильная коммерция», установленной компетентной службой ОАО «ВымпелКом», повлекшие модификацию компьютерной информации, которая была в распоряжении собственника и законного пользователя, из корыстной заинтересованности, у Тимофеева появилась возможность пользоваться лицевыми счетами более 50 абонентских номеров.

Неправомерный доступ Тимофеев осуществлял находясь на своём рабочем месте, в офисе продаж и обслуживания ОАО «ВымпелКом», расположенном в ТЦ «Сити-Парк» по адресу: г.Новокуйбышевск, пр. Победы, д. 1 «ж» ТЦ «Сити-Парк», используя своё служебное положение, под своими индивидуальными логином «ACTrofimov» и паролем, который является конфиденциальным осуществил доступ в компьютерную программу АБС «Ensemble», которая используется сотрудниками ОАО «ВымпелКом». После чего, Тимофеев, действуя умышленно, совершил неправомерный доступ в модуль «CSM», который используется для внесения изменений в список услуг и проведения абонентских операций с номерами клиентов, где не имея соответствующего заявления клиента, с целью последующего завладения денежными средствами, находящимися на лицевых счетах абонентов ОАО «ВымпелКом», выбрал абонентский номер для проведения

модификации ICCID номера сим-карты, путём внесения изменений в программу АБС «Ensemble», содержащую сведения об индивидуальных ICCID номерах сим-карт абонентов ОАО «ВымпелКом», в результате чего у него появилась возможность распоряжаться лицевым счётом абонента.

Преступные действия подсудимого Тимофеева правильно квалифицированы по ч. 3 ст. 272 УК РФ — неправомерный доступ к охраняемой законом компьютерной информации, повлекший модификацию компьютерной информации, совершенное лицом с использованием своего служебного положения[1].

Обратим внимание на мнение К.А. Шмалевой, согласно которому к компьютерным преступлениям также могут относиться: преступления, которые затрагивают область компьютерной информации, а также общеуголовные преступные деяния, которые совершаются с использованием механизмов и возможностей компьютерных технологий; сетевые компьютерные преступления и, наконец, трансграничные киберпреступления[2].Учитывая фактор задействования в механизме совершения преступного деяния сети Интернет, И.Д. Смирнов совершенно справедливо выделяет среди преступлений в области компьютерной и цифровой информации, которые совершаются:

– внутри локальной сети;
– с использованием глобальной, общедоступной Интернет-сети[3].

Систематизацию преступлений в сфере компьютерной информации можно осуществлять по различным основаниям, и любая систематизация будет в дальнейшем совершенствоваться ввиду того, что уголовный закон

[1]Приговор № 1-55/2016 от 25 марта 2016 г. по делу № 1-55/2016 // Режим доступа: novokuibyshevsky.sam.sudrf.ru/ (дата обращения: 03.04.2021 г.)
[2]Шмалева К.А. Преступления в сфере компьютерной информации // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации: сборник статей. Пенза: Наука и Просвещение, 2020. С. 109.
[3] Смирнов И.Д. Уголовно-правовое противодействие преступлениям, затрагивающим сферу компьютерной информации, совершенным с использованием сети Интернет // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений: сборник трудов конференции. Воронеж: Изд-во Воронежского института МВД РФ, 2017. С. 142.

постоянно претерпевает изменения, посвященные использованию информационно-телекоммуникационных технологий при совершении различного рода общественных посягательств. Государство признает рост количества преступлений, совершенных с применением информационно-телекоммуникационных технологий, в результате чего наблюдается активное совершенствование уголовно-правовых норм в данной области путем добавления норм, предусматривающих ответственность за совершение преступного деяния с использованием цифровой информации, передаваемой по информационно-телекоммуникационным сетям, включая Интернет-каналы.

Представляется необходимым глубокий анализ всех статьей Особенной части УК РФ с целью выявление тех составов, в которых назрела насущная потребность в дополнении их таким квалифицирующим признаком, как использование для совершения преступления компьютерных технологий и информационных ресурсов.

В результате вышеизложенного представляется возможным преступления в сфере компьютерной информации определить в качестве совершаемых в сфере информационных процессов и посягающих на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

Рассмотрим состав преступления. Общим объектом компьютерных преступлений являются общественные отношения в области гарантированности информационной безопасности[1]. Непосредственными объектами преступного деяния могут рассматриваться базы и банки определенных компьютерных систем или сетей, в том числе их отдельные файловые составляющие. В качестве непосредственного объекта в компьютерной сфере выступают, и компьютерные технологии, и

[1]Самигуллина З.Ф. К вопросу о рассмотрении понятия «информация» как объект уголовно-правовой защиты // Аллея науки. 2019. № 2. С. 631.

программное обеспечение, включая множество средств защиты компьютерной и киберинформации.

Предметом преступного деяния, предусмотренного ст. 274.1 УК РФ, являются критическая информационная структура России; информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, сети электросвязи, относящиеся к критической информационной структуре Российской Федерации. Нередко объектами посягательства становятся компьютерные сети государственных учреждений и ведомств, Сбербанка, Центробанка и т. д. До двух третей этих негативных проявлений связано с незаконным проникновением в информационные базы данных и внесением в них соответствующих изменений, производимым, как правило, извне путем так называемого удаленного доступа.

Объективную сторону преступления, предусмотренного ст. 272 УК РФ, составляет неправомерный доступ к охраняемой законом компьютерной информации. Как отмечает А.М. Доронин : «выражение объективной стороны преступления, связанного с неправомерным доступом к компьютерной информации, заключается в неправомерном подходе к охраняемой законом киберинформации, расположенной на электронном носителе или в сети, если в результате такого доступа киберинформация уничтожена, блокирована, модифицирована или произошло неправомерное ее копирование, или нарушена работа компьютерного устройства или отдельного компонента сети»[1].

Значимым признаком неправомерного доступа к компьютерной информации является само общественно опасное деяние, выражающееся в активных действиях субъекта преступления. Как представляется иметь доступ к киберинформации путем бездействия – невозможно.

Неправомерное проникновение к компьютерной информации возможно различными способами, например, преступниками могут

[1] Доронин А.М. Уголовная ответственность за неправомерный доступ к компьютерной информации: дисс. … канд.юрид.наук. М., 2003. С. 89.

использоваться поддельные разрешения, обманным путем преодолевается защита компьютера, незаконно достигается подход к чужим логинам и паролям, возможно и противодействие интеллектуальному уровню защиты киберинформации (например, может вводиться команда прекращения диалога) и т.д. Способы совершения компьютерного преступления постоянно совершенствуются и преумножаются.

Неправомерный доступ является достаточно сложным понятие, которое включает в себя следующие действия:

– физическое, мышечное вторжение, позволяющее извлекать информацию с компьютерного устройства;

– действия по осуществлению запрещенного оперирования киберинформацией.

Наличие лишь одного из обозначенных последствий позволяет квалифицировать деяние в качестве фактически совершенного. Вместе с тем, применение ст. 272 УК РФ невозможно, даже при наличии одного из указанных последствий, если деяние признано незначительным, что исключает уголовную ответственность в соответствии с ч. 2 ст. 14 УК РФ. В то же время, как верно указывает Р.А. Магомедалиев : «преступник не может быть освобожден от уголовной ответственности, если есть возможность уничтоженную им информацию восстановить при помощи программного обеспечения, получения её от других пользователей или иным способом»[1].

Под уничтожением киберинформации понимается ее стирание (убирание) из памяти компьютерного устройства без технической возможности восстановления. Если преступник переводит информацию на иной носитель и законный владелец информации не имеет к данному носителю беспрепятственный доступ, то такие действия нельзя расценивать как уничтожение компьютерной информации, а, значит, такое деяние нельзя

[1]Магомедалиев Р.А. Объективная сторона преступлений в области компьютерной информации // Проблемы совершенствования законодательства: сборник научных статей. Махачкала: Алеф, 2020. С. 173.

квалифицировать по ст. 272 УК РФ.К уничтожению информации не относятся такие действия, как переименование файла, осуществление замены старой версии файла новыми версиями (например, файл Word 2003 сохранен в версии Word 2010). Под блокированием компьютерной информации понимается искусственное, техническое затруднение доступа законного пользователя к киберинформации, при ее сохранении, т.е. само уничтожением информации не происходит.Отличается от уничтожения и блокирования такой способ совершения преступления, как вывод из нормального режима работы программного обеспечения. В этом случае программа может и иметь место в какой-либо файле, но пользователь не имеет возможности выполнять определенные действия на компьютере при помощи данной программы.

Одной из причин выхода из строя программного обеспечения может быть, как раз и уничтожение или блокирование определенной информации, содержащейся в компьютерном устройстве. В таком случае действия преступника должны также квалифицироваться по ст. 272 УК РФ.

В диспозиции ст. 272 УК РФ также указаны такие последствия преступного деяния, как модификация и копирование информации.В компьютерную информацию могут быть внесены определенные изменения без согласия ее собственника (законного пользователя), что приводит к модификации компьютерной информации, но при этом такое изменение не связано с адаптацией компьютерной программы или базы данных. Адаптацию следует рассматривать как правомерное внесение изменений в компьютерную информацию, программу, выполняемую исключительно с целью обеспечения нормального обеспечения или оптимизации работы компьютерного устройства и его технических характеристик.Под копированием компьютерной информации понимается тиражирование и устойчивое сохранение этой информации на определенном носителе, при этом у пользователя сохраняется возможность и далее беспрепятственно

пользоваться первоначальной информацией. Копирование, как правило, осуществляется на флэш-карты, диски иные записывающие устройства, в том числе обычная техническая распечатка посредством принтера. Запечатление (копирование) информации способом записывания рукой на лист бумаги или фотографирование информации с экрана монитора, а также считывание информации путем перехвата излучения компьютерного устройства и т.п. не позволяет квалифицировать действия преступника по ст. 272 УК РФ, т.к. субъект технически не проникает в файловую систему компьютерного устройства.От копирования компьютерной информации, о котором идет речь в диспозиции ст. 272 УК РФ, необходимо отличать размножение информации, при котором информация сохраняется повторно или множество раз не на отдельном носителе, а повторяется в определенном месте первоначального компьютерного устройства.

Например, файл с информацией первоначально находился на диске С, а в результате размножения он сохранился и на диске Е этого же компьютерного устройства. Такое «размножение» конкретного файла, содержащего информацию, приводит к размножению, а не неправомерному копированию информации, что, соответственно, исключает возможно квалификации по ст. 272 УК РФ.Следует знать, что при наличии определенного программного обеспечения отдельный файла могут копироваться при всяком обращении к ним пользователя и это происходит без каких-либо дополнительных нажатий клавиш. Такое копирование нельзя признать неправомерным и подпадающим под ст. 272 УК РФ, даже если оно произошло в момент, когда преступник проник в базу компьютерного устройства.Копирование компьютерной информации, о котором указано в диспозиции ст. 272 УК РФ, рассматривается в качестве неблагоприятного последствия, предусмотренного указанной статьей УК РФ, только в том случае, если информация охраняется законом именно от несанкционированного, неправомерного копирования.

Рассматривая объективную сторону преступления, предусмотренного ст. 272 УК РФ, следует понимать, что нередко преступления совершается в одной стране (преступник удаленно проникает к компьютерной информации законного пользователя), само последствие наступает в абсолютно другом государстве[1]. Если рассматривать объективную сторону преступления, предусмотренного ст. 273 УК РФ, то прежде всего, следует понимать, что она представляет собой некую реализацию планов, разрабатываемых субъектом преступления в целях достижения определенного намеченного результата, путем своего активного вмешательства в цепь событий и явлений, имеющих месть во внешнем мире, или, субъект отказывается от такого влияния, несмотря на то, что юридически обязан был совершить определенные действия. В объективной стороне преступления отражены последствия преступного деяния, а также непосредственная связь действия (бездействия) и наступившими последствиями. По утверждению справедливому ряда исследователей объективная сторона преступления является тем элементом состава преступления, который характеризует внешние проявления определенного общественно опасного деяния, имеющего место в фактически существующих условиях, в определенном пространстве и времени, причиняющее урон (ущерб) социально значимым ценностями и интересам, охраняемым действующим уголовным законом[2].

Объективные признаки находят отражение как в общей, так и специальной частях Уголовного кодекса РФ. При этом, существо объективной стороны преступления излагается в диспозиции уголовно-правовой нормы, что является одним из факторов, определяющим различия определенных преступлений по объективной стороне. Отдельные свойства

[1]Лядова К.Э. Расследование преступлений в сфере компьютерной информации: типичные следственные ситуации // Евразийское научное объединение. 2018. № 1. С. 161.
[2]Грабельников В.А., Щербань Г.О. Компьютерное преступление, виды, способы совершения // Вестник Донбасской юридической академии. Юридические науки. 2018. № 4. С. 58.

преступлений определяет именно их объективная сторона. К таким свойствам следует относить:

– характер причиненного преступным деяния ущерба, то есть его общественная опасность;

– последствия преступных действий (бездействий);

– характер взаимосвязей между последствиями преступного деяния;

– обстоятельства, при которых совершалось преступление и наносился вред общественным интересам. Обстоятельства характеризуются условиями, местом, временем, способами, орудиями и средствами совершения преступления и т.п.

Среди вышеуказанных свойств профессор Г.С. Курбанов перечисляет: «цель совершения преступления»[1], что, на наш взгляд, является не совсем обоснованным, так как такая характеристика относится к свойствам субъективной стороны преступления.

Все вышеуказанные свойства преступлений выражают суть объективной стороны деяния, предусмотренного ст. 273 УК РФ.

Объективная сторона преступления, предусмотренного ст. 274 УК РФ, заключается в нарушении правил эксплуатации предмета преступления либо доступа к нему (к информационно-телекоммуникационным сетям).

Достаточно специфичной является объективная сторона преступления, ответственность за которое предусмотрена ст. 274.1 УК РФ. Объективная сторона указанного состава преступления выражается в том, что субъект своими активными действиями осуществляет неправомерное воздействие на критическую информацию государства.[2]

[1]Курбанов Г.С. Объективная сторона преступления, связанного с неправомерным доступом к компьютерной информации // Правовая информатика. 2013. № 4. С. 17.

[2]Пыхтин И.Г. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации (ст. 274.1 УК РФ) // Общественные и технологические факторы развития научного знания: сборник трудов конференции. Смоленск, 2019. С. 48.

В результате анализа объективных признаков компьютерных преступлений возможно сформулировать следующие выводы:

– общим объектом компьютерных преступлений являются общественные отношения в области гарантированности информационной безопасности. Непосредственными объектами преступного деяния могут рассматриваться базы и банки определенных компьютерных систем или сетей, в том числе их отдельные файловые составляющие. В качестве непосредственного объекта в компьютерной сфере выступают и компьютерные технологии, и программное обеспечение, включая множество средств защиты компьютерной и киберинформации;

– объективная сторона в большинстве случаев заключается в активных действиях субъекта, направленных на объект посягательства.

Проводя анализ научной юридической литературы в рассматриваемой области можно утверждать, что до настоящего времени отсутствует единой мнение о формах вины в компьютерных преступлениях.

Обратимся к сущности отдельных точек зрения. По одной из них, незаконный доступ к компьютерной информации возможен только при наличии прямого умысла.

А.И. Абовсчитает: «неправомерный доступ к охраняемой компьютерной информации может быть совершен только с прямым умыслом»[1]. С.В. Григоренко, А.А. Каспаров, Д.Г. Малышев, С.Н. Ткаченко также считают, что компьютерное преступление, предусмотренное ст. 272 УК РФ, совершается только при наличии прямого умысла.Отдельные научные работы содержат анализ возможности неправомерного доступа к компьютерной информации по неосторожности. С.А. Пашин вообще твердо убежден, что рассматриваемое преступление в действительности совершается не только при наличии умысла субъекта, но и по

[1]Абов А.И. Преступления в сфере компьютерной информации: неправомерный доступ к компьютерной информации. М., 2002. С. 16.

неосторожности[1].Лавирующая позиция усматривается в работе С.В. Озерского, Ю.Н. Лазарева, А.Ю. Лаврова, где указано, что компьютерное преступление совершается или по прямому, или по косвенному умыслу, вместе с тем, может иметь место и неосторожная форма вины, когда субъект неверно оценивает правомерность личного доступа к компьютерной информации, а также имеет заблуждение относительно неблагоприятных последствий содеянного, которые выражены в диспозиции уголовно-правовой нормы[2].

Аргументацию такой позиции мы можем увидеть в исследования А.Е. Шаркова, утверждающий, что лицо, осуществляющее именно по неосторожности неправомерный доступ к информации, или имеет осознание опасности своих действий, но деяние совершает легкомысленно, или вообще не предвидит возможности наступления опасных последствий, несмотря на то, что мог и должен был их предвидеть[3].

Среди юристов и практиков имеет место точка зрения, согласно которой форма вины непосредственно зависит от вида наступивших последствий. В качестве примера приводится ситуация, когда копирование информации осуществляется именно с прямым умыслом, а вот, такие последствия, как уничтожения, модификация и блокирование имеют место и при умысле, и при неосторожности[4]. Рассуждения сторонников данной позиции основываются на том, что производство копии информации направлено осуществляется с целью достичь определенный результат – получить эту информацию на свой носитель, в том время, как уничтожение, модификация и блокирование могут быть только сопутствующими

---

[1] Пашин С.А. Преступления в сфере компьютерной информации // Комментарий к УК РФ / Под ред. В.М. Лебедева. М., 2014. С. 640.

[2] Озерский С.В., Лазарев Ю.Н., Лавров А.Ю. Компьютерные преступления: методы противодействия и защиты информации: учебное пособие. Саратов, 2004. С. 24.

[3] Шарков А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дисс. …канд.юрид.наук. Ставрополь, 2004. С. 149.

[4] См.: Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: дисс. … канд. юрид.наук. Красноярск, 2002. С. 134.

последствиями совершенного действия по копированию, то есть к таким последствиям возможна и неосторожная форма вины.Наибольшее количество ученых, чьи труды были проанализированы, придерживаются той точки зрения, в рамках которой доступ к компьютерной информации возможен при наличии обоих видов умысла. В основе аргументации изложенной позиции приводится следующий пример: выполняющий неправомерный, незаконный доступ из-за озорства или хулиганства, субъект в большинстве случаев имеет безразличное отношение к вредным последствиям. Лицо, стремящееся получить доступ к компьютерной информации, скорее всего имеет осознание отсутствия или ограничения свободного доступа к такой информации, и лицо знает, что именно он не имеет права воспользоваться данной информацией. Такое осознание у человека может исходить из того, что лицо видит различные способы зашиты информации, например, компьютер просит ввести определенные коды, пароли, логины и т.п. и только при выполнении запроса системы возможно получить доступ к информации. Параллельно с этим на экран могут выводятся различные предупреждающие сообщения относительно запрета доступа к информации. В то же время, совершенно прав К.Н. Евдокимов, утверждающий, что в отношении последствий вина может быть не только умышленной, но и неосторожной[1].

В.А. Мазуров вообще предлагает скорректировать действующую ст. 272 УК РФ, исходя из того, что неблагоприятные последствия возможны в результате неосторожного к ним отношения со стороны субъекта, исходя из чего, делает вывод В.А. Мазуров, виновный должен привлекаться к ответственности только за покушение на совершение преступления[2].Исходя из ч. 2 ст. 24 УК РФ следует, что если действие (бездействие) совершается по неосторожности, то оно считается преступлением только в случае его

[1] Евдокимов К.Н. Субъективная сторона неправомерного доступа // Вестник Академии генеральной прокуратуры РФ. 2009. № 12. С. 61.

[2] См.: Мазуров В.А. Компьютерные преступления: классификация и способы противодействия: учебно-практическое пособие. М., 2002. С. 115.

фиксации в определенной статье Особенной части УК РФ. Как представляется, для преступления, предусмотренного ст. 272 УК РФ, характерен только умысел, так как лицо осознаёт, что несмотря на защиту осуществляет неправомерный, незаконный подход к информации.

К обязательным признакам субъективной стороны компьютерных преступлений не относятся мотивы и цели. Вместе с тем, их установление является необходимым условием определения причин совершения преступления, индивидуализировать ответственность, что необходимо для назначение справедливого уголовного наказания. Мотивы преступления характеризуют намерения субъекта совершить преступное деяние, а цель свидетельствует о стремлении человека к конкретному результату. Корыстные мотивы, зависть, хулиганские побуждения, стремление испортить чью-либо репутацию, чувство мести – всё это наиболее распространенные побуждающие мотивы совершения компьютерного преступления. В определенных случаях именно правильное, верное установление мотивов и целей действий преступника существенно влияет на квалификацию деяния.

Отсутствие в уголовном законодательстве прямого указания на установление мотивов и целей по компьютерным преступлениям в обязательном порядке свидетельствует о наличии пробела в действующем уголовном законодательстве.

С субъективной стороны преступление, предусмотренное ч. 1 статьи 273 УК РФ, может быть совершено только с прямым умыслом, так как в этой статье определено, что создание вредоносных программ заведомо для создателя программы должно привести к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы компьютерной системы. Использование или распространение вредоносных программ тоже может осуществляться только умышленно. Разработка вредоносных программ доступна только квалифицированным программистам.

Субъект преступлений в сфере компьютерной информации - это физическое вменяемое лицо, достигшее возраста, установленного уголовным законом, виновное в совершении рассматриваемых преступлений[1].

Характерно, что среди общих субъектов, предусмотренных в ч. 1 ст. 272 УК РФ, может быть любое лицо как работающее в автоматизированной информационной системе или сети либо пользующееся их услугами (законный пользователь), но не имеющее права работы с информацией определенной категории, так и постороннее лицо (лицо не являющееся законным пользователем).

В ходе исследования произведенного в рамках выпускной квалификационной работы было проведено анкетирование среди пользователей персональных компьютеров, в котором приняло участие 100 человек. В ходе анкетирования опрашиваемым было предложено ответить на 18 вопросов с вариантами ответом, а так же и без таковых, об использовании компьютера, а так же установления случаев появления вредоносных компьютерных программ и другие (см. Приложение 3). Перейдем непосредственно к вопросам, содержащимся в вышеуказанной анкете и их анализу.

На вопрос анкетирования «сталкивались ли вы когда-нибудь с вредоносными компьютерными программами?» 90 % опрашиваемых ответили положительно, и только 10 % из них ответили, что никогда не встречались с вредоносными компьютерными программами. На основании этого можно сделать вывод о том, что данное преступление является распространенным.

На следующий вопрос «При обнаружении вредоносной компьютерной программы вы»: 30 % опрашиваемых ответили, что они самостоятельно боролись с ней, 45 % ответили, что они просили помощи знакомых, и 25 %

[1] Гончарова Ю.В., Аласханов А.М. Субъект преступления в сфере компьютерной информации // Свобода и право: сборник статей. Кемерово: Плутон, 2019. С. 13.

ответили, что они просили помощи у людей, профессионально занимающихся обслуживанием компьютеров.

На следующий вопрос «Обращались ли Вы после обнаружения вредоносной компьютерной программы в полицию?» все из тех опрашиваемых, кто ответил, что сталкивался с данной программой ответили что не обращались в полицию. Данный опрос показал, что преступление, предусмотренное ст.273 является достаточно распространенным и 90 % опрашиваемых сталкивались с ним, но после этого 100% из них не сообщали в полицию, что говорит о латентности преступления данного вида.

На вопрос анкеты «Сталкивались ли Вы когда-либо с тем, что информация на вашем компьютере была незаконно уничтожена, блокирована или модифицирована, скопирована?» 30 % опрашиваемых ответило «да», и 70% опрашиваемых ответило отрицательно.

На вопрос «Обращались ли Вы после этого в полицию?» все из опрашиваемых ответили отрицательно, что еще раз говорит о большом проценте латентности преступлений данного вида. Опрашиваемые пояснили свой ответ тем, что не обращаются в полицию из-за нехватки времени для участия в следственных действиях, так же они считают, что данные преступления имеют малую долю раскрываемости, поэтому не хотят терять своего времени на подачу заявления в полицию.

Отсюда, подводя итоги анкетирования можно сделать вывод о том, что почти все пользователи (90%) сталкивались с вредоносными компьютерными программами, однако опрашиваемые после случившегося не обращаются в полицию, мотивируя это затратами времени на следственные действия, а также на предполагаемую нераскрываемость данной категории дел. Это еще раз подтверждает, что сами граждане в самых редчайших случаях обращаются в правоохранительные органы за рассматриваемое деяние.

Таким образом, можно заключить, что компьютерные преступления совершаются с прямым умыслом. Субъектами компьютерных преступлений

являются вменяемые лица, достигшие 16-летнего возраста, но в ряде преступлений имеет место и специальный субъект, а именно в ч. 3 ст. 272 УК РФ, ст. 274 и ч. 3, 4 ст. 274.1 УК РФ.

1.3 Международное законодательство и зарубежный опыт уголовно-правового регулирования отношений в сфере компьютерной информации

В настоящее время основным документом, который определяет принципы и механизмы общего международного сотрудничества, а также границы криминализации, совместные стандарты для совершенствования национальных норм, а также международных инструментов противодействия киберпреступности, рассматривается Конвенция о преступности в сфере компьютерной информации (ETS № 185) (далее по тексту - Конвенция), которая была заключена 23 ноября 2001 г. в г. Будапеште[1].

Воспрепятствование интернет-преступности, которая обладает такими характеристиками, как глобальность и трансграничность, необходимо осуществлять непосредственно путём международного взаимодействия, в рамках которого возможно унификация национального уголовного законодательства конкретных стран в борьбе с преступлениями, которые совершаются посредством использования глобальной сети Интернет.

Общее международное взаимодействие в рамках борьбы с интернет-преступностью достаточно осложнено как объективными трудностями процесса расследования рассматриваемого вида преступлений (эти трудности заключаются, например, в необходимости достаточно быстрого анализа, а также возможности итогового сохранения электронной информации в качестве доказательств), так и соблюдением общеизвестного принципа «nullumcrimen, nullapoenasinelege», который переводится как: «Без закона нет

[1]Конвенция Совета Европы по киберпреступности (ETS № 185) (23 ноября 2001 г., г.Будапешт) // Действующее международное право. Документы в 2-х томах. Т. 2 / Сост.: Колосов Ю.М., Кривчикова Э.С. М.: Юрайт, Международные отношения, 2007. С. 570–572.

ни преступления, нет ни наказания» в случаях возникновения ситуаций, когда преступный акт совершен в определенной стране, а привлечение к уголовной ответственности будет происходить в другой стране. В этом случае имеет место принцип двойной криминализации преступного деяния: криминализация происходит как в государстве, против законных интересов которого совершено преступное деяние, так и в государстве, в котором преступник будет привлекаться к уголовной ответственности.

Проблематика заключается также и в том, что киберпреступления совершаются нередко на территории нескольких государств. В этом случае нет полной ясности, территорию какого государства необходимо признавать фактическим местом совершения преступного акта: место расположения самого оборудования (сервера), или место нахождения преступников, либо место проявления последствий преступления.

Считается возможным исходить из конкретного адреса интернет-сайта (то есть за основу берётся доменное имя, на котором размещен сайт), так как именно такая принадлежность доменного имени к конкретной стране и даёт возможность определить применяемое уголовное законодательство.

По данному вопросу имеются некоторые возражения, заключающиеся в следующем: адрес конкретного сайта не всегда выступает единственным признаком, по которому возможно определить его территориальную принадлежность; наоборот, регистрация в определенной доменной зоне никак не может означать, что какой-либо интернет-сайт осуществляет деятельность в соответствующем государстве, не говоря уже о такой категории, как домены первого уровня, среди которых можно выделить: com, net, biz и другие[1].

Имеет место точка зрения, в рамках которой местом совершения преступного деяния следует считать непосредственное место нахождения

[1]Гайберкова А.О. Преступления в сфере компьютерной информации // Приоритетные направления развития российской науки: сборник трудов конференции. Саратов: Академия Бизнеса, 2020. С. 58.

компьютерного оборудования, являющегося средством совершения преступного акта. Вместе с тем, данный подход не позволяет учитывать случаи размещения серверов в различных государствах.

Исходя из изложенного можно констатировать, что интернет-преступления весьма часто являются транснациональными преступлениями, а порядок привлечения и степень уголовного наказания за совершение указанных деяний необходимо урегулировать международно-правовыми актами.

В настоящее время нет международных договоров, в которых бы были определены меры борьбы государств с глобальными компьютерными преступлениями отсутствуют совместные правила об уголовной ответственности за совершение таких деяний.

Следует отметить, что анализ отдельных действующих в настоящее время многосторонних договоров позволяет говорить о том, что использование компьютерной техники и Интернет-ресурсов приводит к факту совершения не только некоторые преступных деяний международного характера, но и к совершению международных преступлений.

Так, например, в Уголовном кодексе Франции нормы, предусматривающие ответственность за компьютерные преступления, содержатся в двух книгах. информации, Уголовный кодекс Франции не содержит[1]

В 1986 году в США принят закон «О мошенничестве и злоупотреблениях, связанных с компьютерами». Этот закон

– одна из немногих составляющих федерального законодательства, посвященных хищениям с применением компьютерных систем. Параграф

[1]Чернякова А.В. Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации // Юридическая наука и правоохранительная практика. 2018. №4 (46). URL: https://cyberleninka.ru/article/n/mezhdunarodnyy-i-zarubezhnyy-opyt-ugolovno-pravovogo-protivodeystviya-hischeniyam-sovershaemym-s-ispolzovaniem-kompyuternoy (дата обращения: 08.12.2020).

1030 главы 47 раздела 18 Свода законов США, устанавливающий ответственность за совершение мошенничества путем доступа к компьютеру, стал частью этого закона.

Согласно данной норме уголовная ответственность наступает за доступ к компьютеру, осуществляемый с мошенническими намерениями, и его использование с целью получения чего бы то ни было ценного посредством мошенничества, включая незаконное использование компьютерного времени стоимостью более 5 тысяч долларов в течение года, то есть без оплаты использования компьютерных сетей и сервисов. Таким образом, законодательством США компьютерное мошенничество отграничено от традиционного.

Можно предположить, что с развитием компьютерных технологий страны будут согласовывать все новые нормы, определяющие меры по борьбе с преступными деяниями, связанными с использованием компьютерных систем и технологий, а сфера преступлений международного характера значительно расширится.

В связи с этим считаем актуальным необходимость пересмотра международных договоров, которые содержат комплекс мер борьбы с преступными деяниями против безопасности воздухоплавания, а также морского судоходства, для того чтобы была фактическая возможность пресечения в вышеуказанной области незаконного использования компьютерных систем и технологий.

Проблематика уголовного преследования за совершение преступлений в сфере компьютерной безопасности является актуальной как для Российской Федерации, так и для зарубежных стран. В качестве общего, совпадающего для всех стран является установление уголовной ответственности за преступления в сфере компьютерной информации, исходя из понимания той

угрозы, которая от них исходит и как оценивается эта угроза в конкретном государстве[1].

Данное обстоятельство является одной из причин того, что в уголовном законодательстве разных стран перечень компьютерных преступлений достаточно отличается между собой. Вместе с тем, исследователи отмечают тенденцию к унификации, к выработке единой позиции по перечню компьютерных преступлений.

Может и согласования по данному вопросу и не происходят, но реальная практика, реально совершаемые деяния приводят к тому, что в разных государствах постепенно вырабатывается такой перечень компьютерных преступлений, который характерен и для иных государств. Кроме того, многие компьютерные преступления имеют трансграничный характер, что приводит к необходимости установления ответственности за совершение такого деяния в сопряженных странах.

Рассматривая зарубежный опыт регулирования ответственности за компьютерные преступления, следует обратить внимание на приоритеты тех или иных государств.

Для отдельных государств (США, многие страны Евросоюза) характерно установление повышенного уровня уголовного наказания в отношении деяний, посягающих на работоспособность государственных компьютерных устройств, на информацию, содержащуюся в таких устройствах, а, значит, в отношении деяния, посягающих на национальную безопасность[2].Если обратиться к анализу уголовного законодательства стран ближнего зарубежья, то следует отметить, что в данных странах также

[1] Шульга А.В., Ширинян А.В. Преступления в сфере компьютерной информации в зарубежных странах // Верховенство права и правовое государство: сборник трудов конференции. Уфа: Аэтерна, 2020. С. 47.

[2]Лукьянов Н.Е. Законодательное регулирование ответственности за информационные преступления. Зарубежный опыт // Устойчивое развитие науки и образования. 2019. № 2. С. 136.

активно осуществляется борьба с компьютерной преступностью уголовно-правовыми методами.

В УК Республики Беларусь[1] преступления против информационной безопасности сконцентрированы в главе 31. В УК Республики Азербайджан[2] имеет отдельная глава 30, именуемая «Киберпреступления». Опыт Азербайджана и Беларуси представляется прогрессивным, в той части, что объединение компьютерных преступлений в одной главе уголовного кодекса, т.е. их систематизация, позволяет в дальнейшем, без ущерба для общей системы особенной части УК, включать новые статьи в области киберпреступности, что неизбежно в будущем ввиду активного развития и динамики киберпреступности как в мире, так и в отдельно взятой стране.

Таким образом, борьба с современной компьютерной преступностью непосредственно связана как с возможностью использования традиционных средств, используемых международными странами.

Отсюда, следует сделать вывод по главе. Развитие института ответственности за компьютерные преступления имеет относительно не продолжительный период. Первые нормы, определяющие уголовную ответственность за преступления в рассматриваемой сфере, были включены в отечественное уголовное законодательство в конце XX века.

Несмотря на вносимые в УК РФ дополнения, кардинального изменения уголовного законодательства не происходит, по-прежнему законодательство «отстаёт» от развития технологии информационных систем и от развития отношений в кибепространстве. Преступления, совершаемые в области компьютерной информации и в киберпространстве, представляют собой достаточно распространенное противозаконное явление, при этом, число данных деяний в ближайшем будущем будет увеличиваться.

---

[1] Уголовный кодекс Республики Беларусь (принят Палатой представителей 2 июня 1999 г., с изм. от 17 июля 2018 г. – Режим доступа: http://www.pravo.by/document/?guid=3871&p0=Hk9900275 (дата обращения: 09.12.2020).

[2] Уголовный кодекс Азербайджанской республики. СПб.: Юридический центр Пресс, 2001. С.325.

Такая тенденция обусловлена активным развитием компьютерных технологий и программного обеспечения, что предопределяет необходимость разработки рекомендаций по правильной квалификации деяний, совершаемых в сфере компьютерной информации.

2. ВЫЯВЛЕНИЕ И ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

2.1 Особенности выявления преступлений в сфере компьютерной информации

В последние десятилетия информация стала неотъемлемой частью таких важных сфер деятельности государства, как связь, транспорт, энергетика, добыча и хранение стратегически важных ресурсов, банковская система, системы жизнеобеспечения населения, оборона, структуры обеспечения устойчивой работы государственного аппарата, что закономерно привело к проникновению преступности в сферу компьютерной информации.

Под преступлениями в сфере компьютерной информации мы понимаем виновно совершенное общественно опасное деяние, совершенное в сфере информационных технологий путем воздействия на сведения (сообщения, данные), представленные в электронно-цифровой форме, независимо от средств их хранения, обработки и передачи.

Традиционно, к числупреступлений рассматриваемой категории относят, прежде всего, составы 28 главы Уголовного кодекса.

Однако они часто являются лишь способомсовершения других преступлений. Так, по статистике МВД о состоянииипреступности за 2020 год, 8,4% всех зарегистрированных преступлений за отчётный период совершены с использованием компьютерных и телекоммуникационных технологий.

Общее количество зарегистрированных преступлений в сфере высоких технологий с каждым годом возрастает, при этом раскрываемость преступлений остается на крайне низком уровне. По данным МВД на 2019 год зарегистрировано 90587 таких преступлений, из них раскрыто 20424. За

2020 год зарегистрировано уже 156307 преступлений, из них раскрыто только 38773[1].

Основными причинами, на наш взгляд, является недостаточность специальных знаний следователей, отсутствие видимых материальных следов преступлений, а так же обезличенный характер информации, не позволяющий указать на преступника[2].

В сложившейся ситуации, особое внимание правоохранительных органов должно быть сосредоточено на уточнении и повышении эффективности применения частной методики расследования преступлений в сфере компьютерной информации.

Несомненно, можно сказать, что в случае выявления этих преступлений, можно сказать, что большую роль играет объект и субъект этого вмешательства. В эпоху цифровых технологий проблема уголовного преследования преступлений, совершенных в информационном секторе, является наиболее острой.

При выявлении, раскрытии и расследовании преступлений в сфере компьютерной информации применяется комплекс оперативно-розыскных и следственных мероприятий. Особую сложность представляет процедура обнаружения, фиксации и изъятия компьютерной информации.

Что касается обнаружения следов данных в одном ряду с традиционными поисковыми мерами и специальными для этой категории преступлений, то « это комплекс действий по перехвату и расследованию трафика, установлению протоколов веб – и почтовых серверов, системных протоколов, доменов, принадлежностей адресов электронной почты, исследований кейлоггеров.»

---

[1]Официальный сайт Министерства внутренних дел российской федерации – статистика https://мвд.рф/ (дата обращения:25.04.2021)

[2]Лядова, К.Э. Расследование преступлений в сфере компьютерной информации: типичные следственные ситуации / К.Э. Лядова // Евразийское научное объединение. - 2018. - № 1. - С. 160-162

Значительное место в деятельности по выявлению, раскрытию и расследованию данной категории преступлений занимает производство судебно-медицинских экспертиз, а именно судебно-вычислительно-технических, где проводится анализ «цифровых следов».

С точки зрения компьютерных преступлений наиболее сложными являются проблемы определения места преступления, раскрытия преступления и его расследования. Эти преступления имеют высокую степень задержки, методы которой вызывают значительные трудности в раскрытии, поскольку преступники, использующие компьютер и коды доступа, по существу остаются анонимными.

Кроме того, раскрытие подобных преступлений возможно только за счет привлечения высококвалифицированных специалистов в области вычислительной техники, обладающих не меньшими знаниями, чем хакеры. Раскрытие преступлений осложняется тем, что преступник, как правило, может находиться в одном государстве, а результаты преступной деятельности проявляются на территориях других государств.

На основании этого необходимо сделать вывод о том, что на современном этапе уголовное законодательство и практика в области преступлений в сфере компьютерной информации имеют существенные пробелы.

В целом оценка состояния борьбы с преступлениями в данной области является удовлетворительной.

Дальнейшее осуществление мер по совершенствованию данного института будет способствовать правильному и единообразному применению закона, что будет способствовать раскрытию и предупреждению преступлений в данной области уголовного права.

2.2 Предупреждение преступлений, совершаемых с использованием информационно-телекоммуникационных технологий и в сфере компьютерной информации

Одной из социальных проблем в современном российском обществе является возникновение и активное развитие компьютерной преступности, причиняющей колоссальный вред экономической, политической, культурной, научной, образовательной и информационной сферам Российской Федерации.

Все более актуальным становится вопрос о защите граждан, муниципальных и государственных учреждений, предприятий, органов власти от несанкционированного доступа к компьютерной информации, вредоносных компьютерных программ и иных компьютерных угроз.

В настоящее время профилактика компьютерных преступлений является одним из главных направлений деятельности правоохранительных органов по обеспечению информационной безопасности российского общества.

Общепревентивные меры предупреждения компьютерных преступлений носят всеобщий характер и направлены на профилактику как компьютерной преступности в частности, так и преступности в целом. Достаточно ясно и лаконично, на наш взгляд, они сформулированы в указе Президента РФ от 12.05.2009 N 537«О Стратегии национальной безопасности Российской Федерации до 2020 года» № 537[1].

Например, кобщеполитическим мерам предупреждения преступлений в сфере компьютерной информации в России можно отнести: развитие демократии и гражданского общества, обеспечение незыблемости конституционного строя, территориальной целостности и суверенитета Российской Федерации; превращение Российской Федерации в мировую

[1]Указ Президента Российской Федерации «О Стратегии национальной безопасности Российской Федерации» от 12 мая 2009 № 537 // СЗ РФ. 2016. № 1. Ст. 212

державу, деятельность которой направлена на поддержание стратегической стабильности и взаимовыгодных партнерских отношений в условиях многополярного мира.

Общеэкономические превентивные меры включают: повышение конкурентоспособности национальной экономики; экономический рост, который достигается прежде всего путем развития национальной инновационной системы и увеличения инвестиций в человеческий капитал; повышение производительности труда и др.

Общие социальные меры предполагают: снижение уровня социального и имущественного неравенства населения, стабилизацию его численности в среднесрочной перспективе, а в долгосрочной перспективе — коренное улучшение демографической ситуации; обеспечение личной безопасности, а также доступности комфортного жилья, высококачественных и безопасных товаров и услуг, достойной оплаты активной трудовой деятельности и т.д.

К научно-техническим общепревентивным мерам относятся: формирование системы целевых фундаментальных и прикладных исследований и ее государственной поддержки в интересах организационно-научного обеспечения достижения стратегических национальных приоритетов; создание сети федеральных университетов, национальных исследовательских университетов, обеспечивающих в рамках кооперационных связей подготовку специалистов для работы в сфере науки и образования, разработки конкурентоспособных технологий и образцов наукоемкой продукции, организации наукоемкого производства и др.

Духовно-культурные меры общей превенции включают: признание первостепенной роли культуры для возрождения и сохранения культурно-нравственных ценностей, укрепления духовного единства многонационального народа Российской Федерации и международного имиджа России в качестве страны с богатейшей традиционной и динамично

развивающейся современной культурой, создание системы духовного и патриотического воспитания граждан России.

Однако представляется необходимым остановиться именно на специальных мерах предупреждения компьютерной преступности.

К специальным правовым мерам предупреждения компьютерных преступлений можно отнести следующие:

1. Совершенствование действующего уголовного законодательства, то есть решить проблемы квалификации преступлений в сфере компьютерной информации, которые обозначены в подразделе 1 данной главы. Кроме того, совершенствование судебной практики требует разъяснений Пленума Верховного Суда РФ по вопросам квалификации деяний, предусмотренных ст. 272-274.1 УК РФ.

2. Совершенствование судебной практики по уголовным делам о компьютерных преступлениях в Российской Федерации. До сих пор отсутствуют разъяснения Пленума Верховного Суда РФ о практике рассмотрения судами уголовных дел по преступлениям в сфере компьютерной информации, что негативно сказывается на следственно-судебной практике и единообразии применения уголовно-правовых норм правоохранительными органами.

3. Активизация и совершенствование международно-правового сотрудничества в сфере предупреждения компьютерных преступлений и борьбы с ними. Учитывая транснациональный и трансграничный характер рассматриваемых преступлений, большое значение приобретает вопрос взаимодействия правоохранительных органов России и зарубежных стран в сфере противодействия компьютерной преступности.

Так, 11 ноября 2013 г. Тушинским районным судом г. Москвы за совершение преступлений, предусмотренных ч. 3 ст. 30, п. «б» ч. 4 ст. 158, ч. 3 ст. 272 УК РФ, граждане Республики Молдова Б. и А. были осуждены к наказанию в виде двух лет шести месяцев лишения свободы без штрафа и без

ограничения свободы с отбыванием наказания в исправительной колонии общего режима каждый. Преступная группа, состоявшая из граждан Республики Молдова, длительное время занималась скиммингом в Москве, осуществляя хищение денежных средств с банковских карт физических лиц с помощью специального оборудования, устанавливаемого на картоприемник банкомата.

Несколько участников преступной группы скрылись от следствия и суда за пределами Российской Федерации[1].

Общепризнанным является вывод о том, что, для того чтобы быть эффективной, профилактика любого, в том числе и компьютерного, преступления должна носить комплексный системный характер. А применяемые на практике методы и мероприятия по обеспечению информационной безопасности объектов должны быть тесно связаны друг с другом.

К специальным организационно-управленческим и техническим мерам предупреждения компьютерных преступлений можно отнести следующее:

1. Подготовка специалистов по специальностям «Информационная безопасность», «Защита информации и информационно-телекоммуникационных сетей» в высших учебных заведениях МВД, ФСБ, и др. с целью дальнейшего комплектования правоохранительных органов профессиональными и компетентными сотрудниками.

При этом следует также осуществлять повышение квалификации и профессорско-преподавательского состава вышеуказанных вузов, включая проведение стажировок, обмена опытом, мастер-классов, семинаров в соответствующих образовательных учреждениях за рубежом, а также в российских и иностранных компаниях, занимающихся информационной безопасностью, защитой информации, разработкой антивирусного программного обеспечения и т.п.

[1] Уголовное дело № 1-520/2013 // Архив Тушинского районного суда г. Москвы. 2014 (дата обращения:20.05.2021)

2. Создание в технических вузах, а также в НИИ МВД, ФСБ и др. научно-исследовательских лабораторий по разработке и модификации программных систем компьютерной защиты с правом реализации (продажи) своей продукции заинтересованным физическим и юридическим лицам. Работа в лабораториях должна проводиться как в научных, так и в коммерческих целях на договорной основе, в том числе для государственных и муниципальных нужд.

3. При технических образовательных учреждениях, специализирующихся на подготовке специалистов по информационной безопасности, следует создать курсы обучения и повышения квалификации для сотрудников служб безопасности банков, предприятий, учреждений либо заинтересованных компьютерных пользователей.

4. Требуется тесное взаимодействие органов прокуратуры, органов внутренних дел (отделов «К»), органов Федеральной службы безопасности со средствами массовой информации при предупреждении и раскрытии преступлений в сфере компьютерной информации.

Анализ правоприменительной практики показывает эффективность такого взаимодействия, тем более что основные формы сотрудничества правоохранительных органов и средств массовой информации давно уже апробированы и активно используются.

5. Создание в Российской Федерации национальной операционной системы для компьютерных устройств, а также общенациональной компьютерной системы фиксации, анализа и учета преступлений в сфере компьютерной информации и компьютерных преступников (разработку таких систем можно поручить российским компаниям: «Лаборатория Касперского», Dr. Web, Group-IB).

К криминалистическим мерам предупреждения преступлений в сфере компьютерной ин формации можно отнести:

1. Создание новых и существующих методик выявления компьютерных преступлений с привлечением специалистов в области информационной безопасности (например, вышеуказанных специалистов компаний «Лаборатория Касперского», Dr. Web, Group-IB).

2. Обобщение и анализ юридической практики Прокуратурой РФ, СК РФ, МВД РФ, ФСБ РФ для дальнейшей выработки методических рекомендаций по вопросам раскрытия и расследования компьютерных преступлений[1].

3. Создание во всех экспертно-криминалистических центрах МВД, ГУВД, ОВД отделов компьютерных экспертиз и технологий для производства необходимых судебно-компьютерных экспертиз, выдачи заключений и справок заинтересованным лицам.

4. Совершенствование подготовки экспертов-криминалистов, осуществляющих судебно-компьютерные экспертизы, на базе единого учебного центра.

В заключении данного параграфа, следует сделать вывод, что перечень мер по предупреждению компьютерной преступности может быть продолжен.

Однако, вне всякого сомнения, только интегративный и комплексный подходы в применении правоохранительными органами профилактических мер могут повысить уровень информационной безопасности России и сделать предупреждение компьютерных преступлений более эффективным.

При этом не стоит забывать, что предложенные превентивные меры дадут ощутимый результат только в случае совместных действий государства с институтами гражданского общества (органами местного самоуправления, образовательными и научными учреждениями, средствами массовой информации, общественными объединениями и т.д.).

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации: утв. генер. прокурором РФ. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_161817 (дата обращения: 25.04.2021)

2.3 Актуальные проблемы обеспечения национальной безопасности в сфере противодействия компьютерной преступности

Одной из проблем противодействия компьютерной преступности является правильная уголовно-правовая квалификация преступлений в сфере компьютерной информации на стадии предварительного следствия.

Сложности в квалификации преступлений в сфере компьютерной информации могут исходить из неверного установления всех признаков состава преступления, в том числе из неправильного определения предмета преступного посягательства.

Предметом посягательства при совершении преступления в сфере компьютерной информация является сама же компьютерная информация, определяемая как сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Обратим внимание на то, что несмотря на многообразие предметов посягательства при совершении преступлений в компьютерной сфере, у большинства сотрудников правоохранительных органов при расследовании практически не существует проблем в определении компьютерной информации как предмета преступления[1].

Предметом посягательства является и киберинформация, которая в отличие от компьютерной информации, находящейся на жестком диске компьютера или на ином носителе (например, флэш-карте), поступает в компьютерное устройство через присоединенную или удаленную сеть.

В связи с этим, считаем целесообразным дополнить ст. 271 УК РФ указанием на киберинформацию. В частности, название ст. 271 УК РФ сформулировать следующим образом: «Неправомерный доступ к компьютерной и киберинформации».

[1]Лядова К.Э. Расследование преступлений в сфере компьютерной информации: типичные следственные ситуации // Евразийское научное объединение. 2018. № 1. С. 161.

По одному из уголовных дел к средствам хранения компьютерной информации была отнесена АИПС – автоматизированная информационно-поисковая система, предназначенная для автоматизации документооборота, для учёта и используется с целью ускорения поиска информации[1].

Таким образом, средства компьютерной информации достаточно разнообразны, действующее законодательство не содержит их перечень, а, значит, судебные органы, по каждому конкретному случаю определяют относится ли то или иное средство к предмету преступного посягательства по делам в сфере компьютерной информации.

Проблемы квалификации имеют место и при установлении субъективной стороны рассматриваемых деяний.

Так, при разбирательствах уголовных дел, в рамках которых лицо обвиняется по ст. 272 УК РФ, суды устанавливают факт того, что обвиняемый имел умысел не только на неправомерный доступ к охраняемой компьютерной информации, но и умысел по отношению к последствиям. К таковым относятся: модификация, уничтожение, копирование, блокирование информации[2], именно такие понятия используются и в судебной практике при рассмотрении конкретных дел[3].

---

[1] Кассационное определение Судебной коллегии по уголовным делам Верховного Суда РФ от 13 августа 2018 г. № 89-О18-49. – Режим доступа: http://www.consultant.ru/ (дата обращения: 17.12.2020).

[2] Приговор по уголовному делу Каменского городского суда Алтайского края от 5 мая 2011 г.; Приговор по уголовному делу № 1-313/2015 Пятигорского городского суда Ставропольского края от 26 июня 2015 г.. Режим доступа: http://судебныерешения.рф/bsr/case/6993929; Постановление судьи Советского района г. Махачкалы Республики Дагестан от 14 марта 2012 г. по апелляционной жалобе на приговор мирового судьи судебного участка № 14 Советского района г. Махачкалы. Режим доступа: http://судебныерешения.рф/bsr/case/6993929 (дата обращения: 17.12.2020) и др.

[3] Приговор Железнодорожного суда г. Самары от 2 февраля 2011 г. по делу № 6/198/11; Приговор мирового суда судебного участка № 45 Егорьевского судебного района Московской области от 13 февраля 2013 г. по делу № 1-12/2013; Постановление о прекращении уголовного дела за примирением сторон Первомайского районного суда г. Ижевска Удмуртской Республики от 14 марта 2012 г. по делу № 1-155/12. – Режим доступа: http://www.consultant.ru/ (дата обращения: 17.12.2020).

Относительно квалификации деяния по ст. 274 УК РФ, сложным моментом оценки действий, причинивших крупный ущерб, повлекших или создавших реальную угрозу наступления тяжких последствий, выступает определение вида соответствующих им субъективных признаков состава преступления, предусмотренного в ст. 274 УК РФ.

В самой ст. 274 УК РФ, в отличие от ранее присутствовавшего в ней указания на неосторожную вину по отношению к наступившим тяжким последствиям, форма вины не определена. В теории взгляд, исключающий возможность вменения названных последствий при умышленной форме вины, сохранился.

В заключении следует отметить, в результате развития всё новых компьютерных технологий достаточно быстрыми темпами развиваются и формы преступной деятельности.

В связи с чем, можно с уверенностью утверждать о необходимости принятия соответствующего Постановления Верховного Суда РФ, учитывающего современные реалии, и которое будет способствовать правильной квалификации судами преступных деяний, совершаемых в области компьютерной информации.

Оптимизация уголовно-правовых норм, предусматривающих ответственность за компьютерные преступления, представляется необходимым начать с совершенствованием терминологического аппарата.

Особую озабоченность вызывает активность юридических лиц в направлении нарушения закона посредством использования компьютерных технологий.

Относительно субъекта компьютерных преступлений, прежде всего, следует отметить, что по сравнению с отечественным уголовным законодательством и научной доктриной, в международном праве дефиниция субъекта компьютерных преступлений представлен в некоторой степени шире.

По общему правилу субъектом преступления, предусмотренного статьей 272 УК РФ, может быть лицо, достигшее 16-летнего возраста,[1] что и отражается в судебной практике[2].

Специальный субъект характерен для ч. 3 ст. 272 УК РФ. Например, Судебная коллегия по уголовным делам Верховного Суда РФ в своём надзорном определении от 12 декабря 2009 г. № 48-Д09-62 указала, что инженер по ремонту компьютерной техники С. имел доступ к компьютеру в силу своих служебных обязанностей, но вносить какие-либо изменения в информацию, находящуюся в памяти компьютера, не имеет права, данное обстоятельство, в связи с этим приговор в отношении осужденного С. за покушение на хищение денежных средств путем использования компьютерных устройств сотрудников организации оставлен без изменений, поскольку наказание судом назначено с учетом обстоятельств дела и данных о личности осужденного[3].

В результате анализа возможно считаем целесообразным дополнить ст. 272 УК РФ указанием на киберинформацию.

В частности, название ст. 272 УК РФ сформулировать следующим образом: «Неправомерный доступ к компьютерной и киберинформации». Такое изменение обосновывается различием в предмете преступного посягательства.

Относительно возраста ответственности за компьютерные преступления также есть определенные предпосылки в направлении совершенствования действующих уголовно-правовых норм.

---

[1] Токарь И.Д. Особенности определения и классификации преступника в компьютерных преступлениях // Синергия Наук. 2018. № 24. С. 899.

[2] Определение Судебной коллегии по уголовным делам Верховного Суда РФ от 16 ноября 2010 г. № 46-Д10-54 // Бюллетень Верховного Суда РФ. 2011. № 4.

[3] Надзорное определение Судебной коллегии по уголовным делам Верховного Суда РФ от 12 декабря 2009 г. № 48-Д09-62– Режим доступа: http://www.consultant.ru/ (дата обращения: 18.12.2020).

В научной литературе достаточно часто встречается мнение, которое на наш взгляд не безосновательно, снижения возраста уголовной ответственности за компьютерные преступления с 16 лет до 14 лет[1].

Такие предложения основаны на осознании того факта, что в XXI веке, в веке информационных технологий и широких киберотношений, молодые люди во многих случаях больше владеют компьютерными технологии, чем люди старшего поколения.

«Омоложение» преступности в сфере компьютерных технологий должно повлечь за собой и изменение действующего законодательства. Уголовно-правовые нормы должны идти «в ногу со временем», а не отставать от развития общественных отношений.

Однако, несмотря на научную разработанность данной проблемы, на практике, при квалификации преступлений в сфере компьютерной информации правоприменитель часто сталкивается с затруднениями технико-юридического характера.

Так, например, у следователя или судьи возникает проблема при уяснении некоторых понятий, содержащихся в диспозициях ст. 272-274 УК РФ, а именно: «компьютерная программа», «несанкционированное уничтожение, блокирование, модификация, копирование компьютерной информации», «нейтрализация средств защиты компьютерной информации», «средства хранения, обработки или передачи охраняемой компьютерной информации».

Кроме того, при квалификации деяний, предусмотренных ст. ст. 272-274 УК РФ возникает ряд вопросов, требующих толкования для правоприменителя. Например, будет ли являться уничтожением компьютерной информации, деяние при котором информация была изначально уничтожена, но спустя определенное время частично или

[1]См.: Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: Дис. ... канд. юрид. наук. М., 2002. С. 20; Шарков А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: Дис. ... канд. юрид. наук. Ставрополь, 2004. С. 149

полностью восстановленная специалистами? Будет ли являться копированием компьютерной информации действия преступника при получении копии путем распечатывания информации на принтере, фотографирования или видеосъемки изображения с монитора компьютера? Наконец, как квалифицировать несанкционированное ознакомление с компьютерной информацией, когда преступник, визуально запомнив конфиденциальные сведения (например, персональные данные лица; информацию о содержании коммерческой сделки и сторонах договора; сведения об усыновлении (удочерении), врачебную тайну и т.д.), впоследствии переносит их на другой материальный носитель информации, создав ее копию (написав на листе бумаги, введя информацию в память своего компьютера или иного компьютерного устройства).

Поэтому полагаем целесообразным дополнить главу №28 УК РФ статьей 272.1: «Статья 272.1 Незаконное завладение носителем компьютерной информации с целью осуществления неправомерного доступа к компьютерной информации».

Данная позиция обусловлена тем, что преступник тайно, открыто или обманным путем завладев, например, флэш-картой или DVD-диском с компьютерной информацией для последующего ее использования, избегает уголовной ответственности.

Наконец, как квалифицировать несанкционированное ознакомление с компьютерной информацией, когда преступник, визуально запомнив конфиденциальные сведения (например, персональные данные лица; информацию о содержании коммерческой сделки и сторонах договора; сведения об усыновлении (удочерении), врачебную тайну и т.д.), впоследствии переносит их на другой материальный носитель информации, создав ее копию (написав на листе бумаги, введя информацию в память своего компьютера или иного компьютерного устройства: айфона, смартфона, планшетного компьютера, коммуникатора и т.п.).

По мнению автора, описанные деяния и последствия носят противоправный характер и должны учитываться при квалификации преступлений в сфере компьютерной информации.

В результате изложенного считаем возможным констатировать, что действующее уголовное законодательство требует своего совершенствования, как в направлении корректировки категорийно-понятийного аппарата, так и в направлении понижения возраста уголовной ответственности лиц, совершающих преступления в сфере компьютерной информации.

Перспективным видится и введение уголовной ответственности юридических лиц за компьютерные преступления, но данный вопрос является дискуссионным и требующим соответствующей научной разработки в связи с тем, что отечественное уголовное законодательство признаёт субъектом преступных деяний только физических лиц.

ЗАКЛЮЧЕНИЕ

В результате проведённой работы на тему «Преступления в сфере компьютерной информации: вопросы квалификации» возможно сформулировать следующие выводы и предложения:

1. Развитие отечественного уголовного законодательства в сфере защиты компьютерной информации имеет относительно не продолжительный период. Первые нормы, определяющие уголовную ответственность за преступления в рассматриваемой сфере, были включены в отечественное уголовное законодательство в конце XX века.

В настоящее время преступные деяния в сфере компьютерной и цифровой информации, позволяет их классифицировать на:

1) преступления, квалифицируемые по статьям, входящим в главу 28 УК РФ;

2) иные преступные деяния, которые совершаются с использованием механизмов и возможностей информационно-телекоммуникационных сетей, в том числе Интернета.

Предметам исследования данной работы являются преступные деяния, предусмотренные в нормах главы 28 УК РФ.

2. Под преступлениями в сфере компьютерной информации следует понимать совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

Действующее законодательство предусматривает уголовную ответственность за совершение компьютерных преступлений.

Компьютерные преступления наносят вред законным интересам непосредственно собственникам или владельцам информации, могут причинять вред жизни и здоровью личности, наносят вред правам и

законным интересам человека и гражданина, а также государственной или общественной безопасности.

3. Для конкретизации рассмотренных в данной работе общественно опасных деяний и обеспечения стабильности понятийно-терминологического аппарата считаем целесообразным вместо термина «преступления в сфере компьютерной информации» использовать термин «преступления в сфере информационных технологий»,

Наряду с этим необходимо изменить название всей главы 28 УК РФ, сформулировав ее как «Преступления в сфере информационных технологий», так как данная корректировка даст возможность законодателю своевременно реагировать на криминализацию новых общественно-опасных деяний, а также позволит точно и своевременно включать новые нормы в УК РФ в связи с появлением новейших видов преступлений в области компьютерной информации, даст возможность своевременно дополнять главу 28 УК РФ новыми составами.

4. Общим объектом компьютерных преступлений являются общественные отношения в области гарантированности информационной безопасности.

Непосредственными объектами преступного деяния могут рассматриваться базы и банки определенных компьютерных систем или сетей, в том числе их отдельные файловые составляющие, а также критическая информационная инфраструктура государства.

В качестве непосредственного объекта в компьютерной сфере выступают и компьютерные технологии, и программное обеспечение, включая множество средств защиты компьютерной и киберинформации.

5. Считаем целесообразным дополнить ст. 272 УК РФ указанием на киберинформацию. В частности, название ст. 272 УК РФ сформулировать следующим образом: «Неправомерный доступ к компьютерной и

киберинформации». Такое изменение обосновывается различием в предмете преступного посягательства.

Киберинформация, в отличие от компьютерной информации, находящейся на жестком диске компьютера или на ином носителе (например, флэш-карте), поступает в компьютерное устройство через присоединенную или удаленную сеть.

6. Субъектами компьютерных преступлений являются вменяемые лица, достигшие 16-летнего возраста, в отдельных случаях - субъект специальный (например, ч. 3 ст. 272, ст. 274, ч. 3, 4 ст. 274.1 УК РФ).

7. Компьютерные преступления совершаются только умышленно: с прямым или косвенным умыслом.

Считаем необходимым повысить степень наказания за неправомерный доступ к компьютерной информации, совершенный с целью скрыть другое преступление или облегчить его совершение.

Также, ввиду большей общественной опасности преступлений, приводящих к разжиганию какой-либо ненависти и вражды, необходимо ч. 2 ст. 273 УК РФ дополнить следующим положением: «то же деяние, если оно повлекло модификацию компьютерной информации и было совершено по мотивам политической, идеологической, расовой, национальной или религиозной ненависти, или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы».

8. Интернет используется для совершения множества преступлений, в том числе в целях разжигания межнациональной и религиозной ненависти, однако, это обстоятельство остается без надлежащей оценки со стороны правоприменителей, поскольку диспозициями соответствующих статей УК РФ не предусмотрено квалифицирующего признака «с использованием информационно-телекоммуникационных сетей».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

РАЗДЕЛ 1 НОРМАТИВНО-ПРАВОВЫЕ АКТЫ И ИНЫЕ ОФИЦИАЛЬНЫЕ АКТЫ

1. Конвенция о борьбе с незаконными актами, направленными против безопасности гражданской авиации, 1971 // Борьба с терроризмом касается каждого. Библиотечка «Российской газеты». Вып. 13. М., 2003. С. 145.
2. Конвенция Совета Европы по киберпреступности (ETS № 185) (23 ноября 2001 г., г.Будапешт) // Действующее международное право. Документы в 2-х томах. Т. 2 / Сост.: Колосов Ю.М., Кривчикова Э.С. М.: Юрайт, Международные отношения, 2007. С. 570.
3. Конституция Российской Федерации, принята всенародным голосованием 12 декабря 1993 г. // Российская газета. 1993. № 237.
4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63–ФЗ // СЗ РФ.1996. № 25. Ст. 2954.
5. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 № 174–ФЗ // СЗ РФ. 2001. № 52 (часть I). Ст. 4921
6. Федеральный закон «О прокуратуре Российской Федерации» от 17 января 1992г. № 2202–1 // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации.1992. № 8. Ст. 366.
7. Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»от 29 ноября 2012 г. № 207–ФЗ // СЗ РФ. 2012. № 49. Ст. 6752.
8. Уголовный кодекс РСФСР от 27 октября 1960 г. // Ведомости Верховного Совета РСФСР. 1960. № 40. Ст. 591.

9. Федеральный закон «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24–ФЗ // Российская газета. 1995. № 39.
10. Федеральный закон «О правовой охране программ для электронных вычислительных машин и баз данных» от 23 сентября 1992 г. № 3523–1 // Российская газета. 1992.20 октября. № 229.

РАЗДЕЛ II ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

11. Абов, А.И. Преступления в сфере компьютерной информации: неправомерный доступ к компьютерной информации / А.И. Абов. М.: Прима-Пресс, 2002. С.125.
12. Ансель, М. Методологические проблемы сравнительного права (фрагменты) / М. Ансель // Вестник Университета имени О.Е. Кутафина. 2015. № 5. С. 187–188.
13. Гайберкова, А.О. Преступления в сфере компьютерной информации / А.О. Гайберкова // Приоритетные направления развития российской науки: сборник трудов конференции. Саратов: Академия Бизнеса, 2020. С. 58–59.
14. Грабельников, В.А., Щербань, Г.О. Компьютерное преступление, виды, способы совершения / В.А. Грабельников, Г.О. Щербань // Вестник Донбасской юридической академии. Юридические науки. 2018. № 4. С. 57
15. Гриб, В.Г. Вопросы совершенствования международного правового регулирования борьбы с киберпреступностью (компьютерными преступлениями) / В.Г. Гриб // Вестник Московского государственного лингвистического университета.2018. № 802. С. 212–220.
16. Добровольский, Д.В. Актуальные проблемы борьбы с компьютерной преступностью: Уголовно-правовые и криминологические проблемы:

автореф. дис. ... канд. юрид. наук: 12.00.08 / Дмитрий Владимирович Добровольский. М., 2006. 23с.

17. Доронин, А.М. Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. … канд. юрид. наук: 12.00.08 / А.М. Доронин. М., 2003. 154с.
18. Дорофеева, М.М. Международные аспекты противодействия преступлениям в сфере компьютерной информации / М.М. Дорофеева // Международный академический вестник. 2018. № 27. С. 89–93.
19. Евдокимов, К.Н. Субъективная сторона неправомерного доступа / К.Н. Евдокимов // Вестник Академии генеральной прокуратуры РФ. 2009. № 12. С. 61–64.
20. Золотухин, С.Н. Уголовно-правовые и криминологические аспекты преступлений в сфере компьютерной информации: учебное пособие / С.Н. Золотухин, А.З. Хун. Краснодар, 2008. 180с.
21. Карпов, В.С. Уголовная ответственность за преступления в сфере компьютерной информации: дис. … канд. юрид.наук: 12.00.08 / Виктор Сергеевич Карпов. Красноярск, 2002. 202с.
22. Комментарий к Уголовному кодексу Российской Федерации / Под ред. В.М. Лебедева. М.: Юрайт, 2014. С.1077 .
23. Курбанов, Г.С. Объективная сторона преступления, связанного с неправомерным доступом к компьютерной информации / Г.С. Курбанов // Правовая информатика. 2013. № 4. С. 16–18.
24. Лукьянов, Н.Е. Законодательное регулирование ответственности за информационные преступления. Зарубежный опыт / Н.Е. Лукьянов // Устойчивое развитие науки и образования. 2019. № 2. С. 134–139.
25. Лядова, К.Э. Расследование преступлений в сфере компьютерной информации: типичные следственные ситуации / К.Э. Лядова // Евразийское научное объединение. 2018. № 1. С. 160–162.

26. Магомедалиев, Р.А. Объективная сторона преступлений в области компьютерной информации / Р.А. Магомедалиев // Проблемы совершенствования законодательства: сборник научных статей. Махачкала: Алеф, 2020. С. 171–177.
27. Мазуров, В.А. Компьютерные преступления: классификация и способы противодействия: учебно-практ. пособие/В.А. Мазуров. М.: Логос, 2002. 148с.
28. Малышенко, Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. ... канд. юрид. наук: 12.00.08 / Д.Г. Малышенко. М., 2002. 166с.
29. Монгуш, Д.Р. Возраст уголовной ответственности в преступлениях в сфере компьютерной информации / Д.Р. Монгуш // Евразийские исследования: сборник трудов конференции. Сочи, 2018. С. 5–10.
30. Настоящий, А.В. История появления и развития преступлений в сфере компьютерной информации / А.В. Настоящий // Студенческий вестник. 2020. № 7–1. С. 62–63.
31. Новичков, В.Е. Понятие видового и непосредственного объекта неправомерного воздействия на критическую информационную структуру Российской Федерации выражающегося в заведомом создании, распространении и использовании вредоносных компьютерных программ либо иной компьютерной информации (ч. 1 ст. 274.1 УК РФ) / В.Е. Новичков // Европейская наука будущего: сборник трудов конференции. Смоленск, 2019. С. 140–143.
32. Озерский, С.В. и др. Компьютерные преступления: методы противодействия и защиты информации: учебное пособие / С.В. Озерский. Саратов, 2004. 156с.
33. Пыхтин, И.Г. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации (ст. 274.1 УК РФ) / И.Г. Пыхтин //

Общественные и технологические факторы развития научного знания: сборник трудов конференции. Смоленск, 2019. С. 48–51.

34. Рахманин, Е.М. Проблемные вопросы терминологии УК РФ, используемой при регулировании вопросов в сфере информационной безопасности / Е.М. Рахманин // Современные научные исследования и инновации. 2019. № 2. С. 15–17.

35. Рускевич, Е.А. Проблемы систематизации современного уголовного законодательства об ответственности за преступления, совершаемые с использованием инфрмационно-коммуникационных технологий / Е.А. Рускевич // Уголовная политика и правоприменительная практика: сборник трудов конференции. СПб., 2019. С. 351–358.

36. Самигуллина, З.Ф. К вопросу о рассмотрении понятия «информация» как объект уголовно-правовой защиты / З.Ф. Самигуллина // Аллея науки. 2019. № 2. С. 630–633.

37. Сафонов, О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. … канд. юрид. наук: 12.00.08 / О.М. Сафонов. М., 2015. 222с.

38. Смирнов, И.Д. Уголовно-правовое противодействие преступлениям, затрагивающим сферу компьютерной информации, совершенным с использованием сети Интернет / И.Д. Смирнов // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений: сборник трудов конференции. Воронеж: Изд-во Воронежского института МВД РФ, 2017. С. 142–144.

39. Строчкина, А.И. Информация как предмет преступления в сфере компьютерной информации / А.И. Строчкина // Актуальные проблемы правоприменения и управления на современном этапе развития общества: сборник трудов конференции. Ставрополь: Фабула, 2020. С. 238–243.

40. Токарь, И.Д. Особенности определения и классификации преступника в компьютерных преступлениях / И.Д. Токарь // Синергия Наук. 2018. № 24. С. 899–905.
41. Трунцевский, Ю.В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов / Ю.В. Трунцевский // Журнал российского права. 2019. № 5. С. 99 – 106.
42. Шарков, А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дис. ... канд. юрид. наук: 12.00.08 / А.Е. Шарков. Ставрополь, 2004. С.174.
43. Шмалева, К.А. Преступления в сфере компьютерной информации / К.А. Шмалева // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации: сборник статей. Пенза: Наука и Просвещение, 2020. С. 109–111.
44. Шульга, А.В. Преступления в сфере компьютерной информации в зарубежных странах / А.В. Шульга, А.В. Ширинян // Верховенство права и правовое государство: сборник трудов конференции. Уфа: Аэтерна, 2020. С. 46–48

РАЗДЕЛ III ПОСТАНОВЛЕНИЯ ВЫСШИХ СУДЕБНЫХ ИНСТАНЦИЙ И МАТЕРИАЛЫ СУДЕБНОЙ ПРАКТИКИ

45. Надзорное определение Судебной коллегии по уголовным делам Верховного Суда РФ от 12 декабря 2016 г. № 48-Д16-62– Режим доступа: http://www.consultant.ru/ (дата обращения: 12.09.2020).
46. Надзорное определение Судебной коллегии по уголовным делам Верховного Суда РФ от 12 декабря 2009 г. № 48-Д09-62– Режим доступа: http://www.consultant.ru/ (дата обращения: 12.09.2020).

47. Кассационное определение Судебной коллегии по уголовным делам Верховного Суда РФ от 13 августа 2018 г. № 89-О18-49– Режим доступа: http://www.consultant.ru/ (дата обращения: 12.09.2020).
48. Определение Судебной коллегии по уголовным делам Верховного Суда РФ от 16 ноября 2010 г. № 46-Д10-54 // Бюллетень Верховного Суда Рос. Федерации. 2011. № 4.
49. Апелляционное постановление Приморского краевого суда № 22К-600/2020 от 30 января 2020 г. - Режим доступа: https://sudact.ru/regular/doc/RrroHXtZdFZg/ (дата обращения: 12.09.2020).
50. Приговор Чебаркульского городского суда Челябинской области от 26 декабря 2019 г. по делу № 1-349/2019 - Режим доступа: https://sudact.ru/regular/doc/i8uMeLpvrKQh/ (дата обращения: 12.09.2020).
51. Приговор по уголовному делу № 1-587/2017 Хорошевского районного суда г. Москвы от 1 декабря 2017 г. Режим доступа: http://судебныерешения.рф/bsr/case/6993929 (дата обращения: 12.09.2020).
52. Приговор по уголовному делу № 1-313/2015 Пятигорского городского суда Ставропольского края от 26 июня 2015 г. Режим доступа: http://судебныерешения.рф/bsr/case/6993929 (дата обращения: 12.09.2020).
53. Приговор по уголовного делу № 1-15/2014 Илимпийского районного суда Красноярского края. Режим доступа: http://судебныерешения.рф/bsr/case/6993929 (дата обращения: 12.09.2020).
54. Приговор по уголовному делу № 1-141/2014 Элистинского городского суда Республики Калмыкия от 2 июня 2014 г. Режим доступа: http://судебныерешения.рф/bsr/case/6993929 (дата обращения: 12.09.2020).
55. Приговор Железнодорожного суда г. Самары от 2 февраля 2011 г. по делу № 6/198/11– Режим доступа: http://www.consultant.ru/ (дата обращения: 12.09.2020).

56. Приговор по уголовному делу Каменского городского суда Алтайского края от 5 мая 2011 г.– Режим доступа: http://www.consultant.ru/ (дата обращения: 12.09.2020).
57. Приговор мирового суда судебного участка № 45 Егорьевского судебного района Московской области от 13 февраля 2013 г. по делу № 1-12/2013– Режим доступа: http://www.consultant.ru/ (дата обращения: 12.09.2020).
58. Постановление о прекращении уголовного дела за примирением сторон Первомайского районного суда г. Ижевска Удмуртской Республики от 14 марта 2012 г. по делу № 1-155/12– Режим доступа: http://www.consultant.ru/ (дата обращения: 12.09.2020).
59. Постановление судьи Советского района г. Махачкалы Республики Дагестан от 14 марта 2012 г. по апелляционной жалобе на приговор мирового судьи судебного участка № 14 Советского района г. Махачкалы. Режим доступа: http://судебныерешения.рф/bsr/case/6993929 (дата обращения: 12.09.2020).

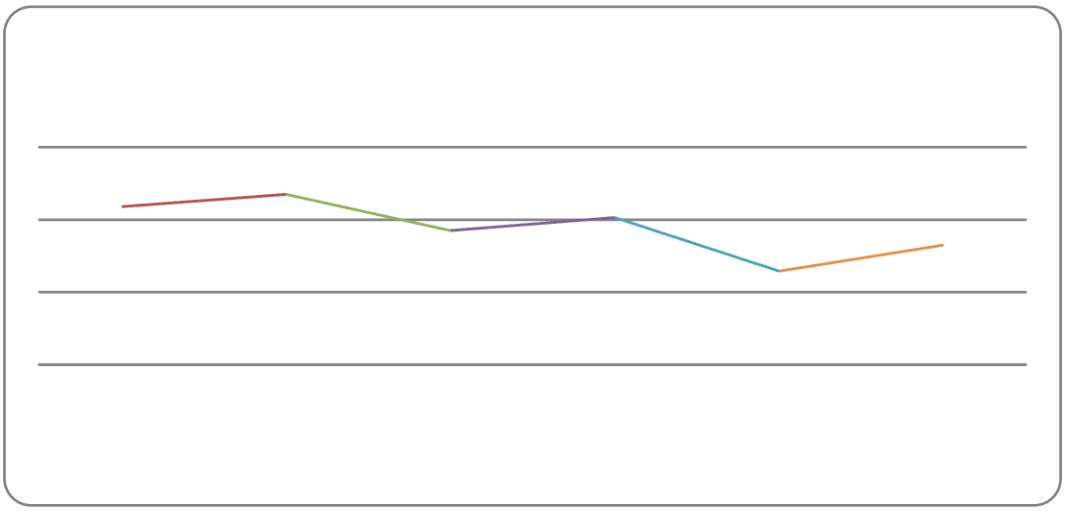
ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1

Статистические данные о количестве лиц, осужденных за преступления в сфере компьютерной информации (глава 28 УК РФ)[1]

	2014 г.	2015 г.	2016 г.	2017 г.	2018 г.	2019 г.
ст. 272 УК РФ	64	71	62	75	50	85
ст. 273 УК РФ	154	164	123	128	79	76
ст. 274 УК РФ	-	-	-	-	-	-
ст. 274.1 УК РФ	-	-	-	-	-	4
Всего:	**218**	**235**	**185**	**203**	**129**	**165**

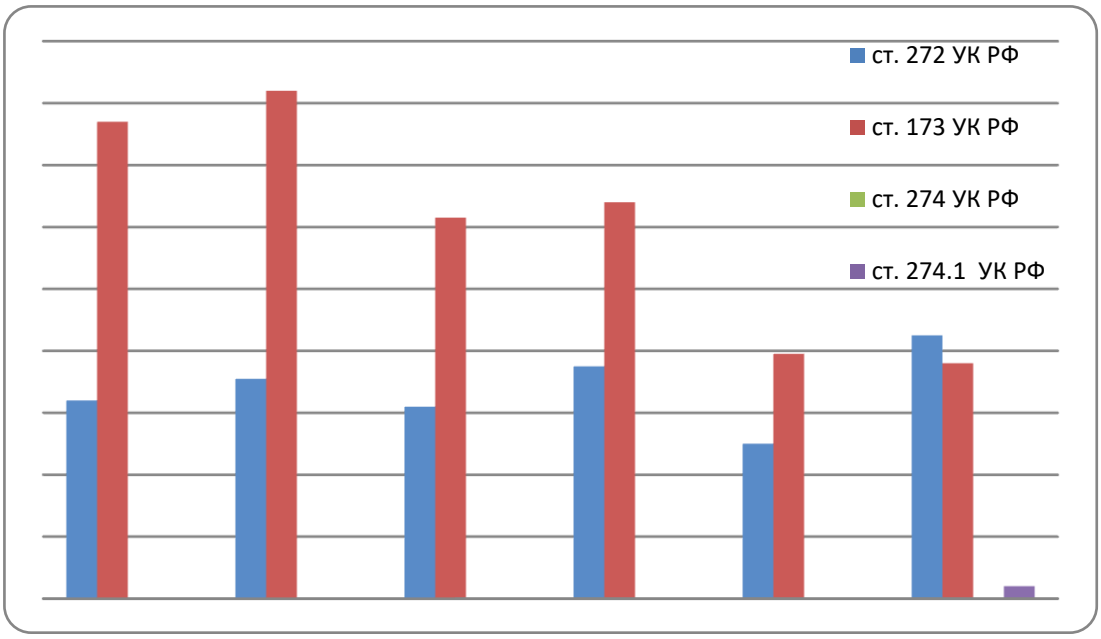
Динамика компьютерной преступности за шесть лет (2014-2019 гг.)



[1] Судебный департамент при Верховном Суде Российской Федерации [Электронный ресурс]. Режим доступа: http://www.cdep.ru (дата обращения: 12.12.2020).

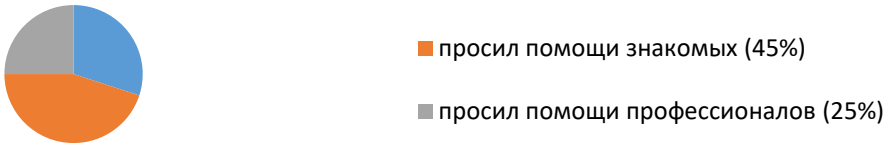
ПРИЛОЖЕНИЕ 2

Соотношение количества осужденных лиц по отдельным видам компьютерных преступлений

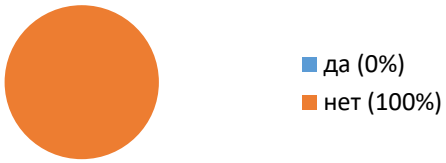


Сталкивались ли вы когда-нибудь с вредоносными компьютерными программами?

При обнаружении вредоносной компьютерной программы вы:



Обращались ли Вы после обнаружения вредоносной компьютерной программы в полицию?



Сталкивались ли Вы когда-либо с тем, что информация на вашем компьютере была незаконно уничтожена, блокирована или модифицирована, скопирована?

Обращались ли Вы после этого в полицию?