РЕЦЕНЗИЯ

на курсовую работу по Уголовному праву
на тему „Преступления в сфере компьютерной информации"

выполненную студентом 1 *курса* заочной *формы обучения* 11 3 *группы*

Косяченко Наталья Федоровна
(Ф.И.О.)

1. Все требования предъявляемые к написанию курсовой работы выполнены (план, введение, содержание, заключение, список использованной литературы) (да, нет)
2. Тема курсовой работы раскрыта (полностью, частично, нет)
3. Использование научной литературы при выполнении курсовой работы (2, 3, 4, 5)
4. Использование эмпирического материала при написании курсовой работы (2, 3, 4, 5)
5. Наличие собственных выводов, предложений, точек зрения и их аргументация (2, 3, 4, 5)
6. Стиль и уровень грамотности выполнения курсовой работы (2, 3, 4, 5)
7. Качество оформления курсовой работы (2, 3, 4, 5)
8. Основные вопросы, выносимые на защиту курсовой работы, или замечания, требующие дополнительной письменной переработки (да, нет)

Курсовая работа допущена к защите «____» _____

Преподаватель _____ _____
подпись Ф.И.О.

Курсовая работа защищена на оценку отл

«____» _____

Преподаватель _____ _____
подпись Ф.И.О.

НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКАЯ АКАДЕМИЯ АДВОКАТУРЫ И НОТАРИАТА»

КУРСОВАЯ РАБОТА
на тему:

«ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

Выполнила:
Студентка 1 курса
Костюченко Наталья Федоровна

Москва, 2019

Введение

В XXI веке с появлением первых компьютеров и новых технологий появились новые методы преступлений, а также новые сферы незаконной деятельности. Если до середины XX века преступники плелись в хвосте технических, организационных и финансовых технологий, то сегодня они находятся в авангарде, превосходя и в плане осведомленности, логистики и финансирования государственные структуры в разных странах мира. Сегодня масштабы киберпреступности нарастают, как снежный ком. Есть основания полагать, что с каждым годом не только объёмы, но и динамика выручки компьютерных преступников увеличивается.

«Невидимость» компьютерного преступника и одновременно доступ к любым охраняемым секретам (военным, финансовым, иным) делают его весьма привлекательным для представителей преступного мира. Компьютерные махинации, как правило, остаются незамеченными на фоне уличной преступности. Даже по неполным оценкам экспертов, эти преступления обходятся минимум в 200 млрд. долларов ежегодно. Банковский грабитель рискует жизнью за 10 тыс. долларов, электронный — манипулируя компьютером и ничем не рискуя — может получить миллионы.

Особенностью современной преступностью является то, что мошенничество в компьютерной сфере требует более высокого технического уровня преступников, одновременно являясь высокодоходной и мало рискованной криминальной деятельностью. Современные преступники быстро адаптируются к техническим новациям и сами создают и продвигают технологии.

Жертвами преступников становятся учреждения, предприятия и организации, использующие автоматизированные компьютерные системы для обработки бухгалтерских документов, проведения платежей и других операций. Чаще всего мишенями преступников становятся банки. Особая актуальность вопросов защищенности технических средств приема, передачи и накопления

информации от несанкционированного доступа была отмечена и отечественным законодателем.

С развитием общественно-экономических отношений объемы перерабатываемой информации постоянно увеличиваются. Информация обрела реальную цену и с развитием информационных технологий становится все более ценным товаром. Достижения науки и техники, создание всемирной сети Интернет позволили преступности выйти на новый уровень — теперь ему не нужен прямой контакт с жертвой, и всего несколько человек могут стать угрозой для каждого пользователя «глобальной паутины», крупных корпораций и целых государств.

Сегодня складывается ситуация, что чем быстрее развивается научный и технологический прогресс, тем острее становятся коллизии между законом и действительностью, тем больше «серых» зон и «черных» дыр, где нет законодательных рамок и где преступники получают шансы и возможности, которых у них никогда не было.

Компьютерная преступность в Российской Федерации

Информатизация современного общества привела к формированию новых видов преступлений, при совершении которых используются вычислительные системы, новейшие средства телекоммуникации и связи, средства негласного получения информации и т.п. За последние 10-15 лет резко увеличилось количество преступлений с использованием вычислительной техники или иной электронной аппаратуры, хищения наличных и безналичных денежных средств. Для совершения преступлений все чаще используются устройства, в основе которых лежат высокоточные технологии их изготовления и функционирования, иными словами, это преступления, в которых используются высокие технологии.

Так, исходя из статистических данных ГИАЦ МВД России за 2015 год, среди преступных деяний, образующих компьютерную преступность в

Российской Федерации, преобладают: мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и мошенничество, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 159 УК РФ), — 30,2 %; неправомерный доступ к компьютерной информации (ст. 272 УК РФ) — 21,2 %; нарушение авторских и смежных прав, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 146 УК РФ), — 11,1 %; создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) — 9,8 %; кража, совершенная с использованием компьютерных и телекоммуникационных технологий (ст. 158 УК РФ), — 9,78 %.

Таким образом, наибольший удельный вес среди совершенных компьютерных преступлений приходится на преступления в сфере компьютерной информации (ст.ст. 272, 273 УК РФ) и мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), которые в данное время и составляют основу компьютерной преступности в России.

В 2015 году в Российской Федерации по фактам совершения компьютерных преступлений были возбуждены уголовные дела: за неправомерный доступ к компьютерной информации (ст. 272 УК РФ) — 1 396; создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) — 974; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) — 12; мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) — 1 352.[1]

Анализируя динамику компьютерной преступности, можно прийти к выводу о том, что количество преступлений, предусмотренных ст. 272 УК РФ (неправомерный доступ к компьютерной информации), ст. 273 УК РФ (создание, использование и распространение вредоносных компьютерных программ),

---

[1] Преступления в сфере компьютерной информации. сводный и сборник по России за январь – декабрь 2015 г. Ф-615 кн. 1. URL: http://mvd.ru

ст.159.6 УК РФ (мошенничество в сфере компьютерной информации), в ближайшей перспективе будет возрастать в силу множества объективных причин (дальнейшее развитие IT-технологий и информатизация российского общества, несовершенство уголовного законодательства, недостатки и ошибки в судебно-следственной практике по уголовным делам о преступлениях в сфере компьютерной информации, отсутствие в правоохранительных органах необходимого количества высококвалифицированных специалистов для раскрытия компьютерных преступлений и т.д.).

Так, уже в 2018 году Генпрокуратура России отметила семикратный рост мошенничеств с использованием электронных средств платежей. Распространение получили мошеннические действия, совершенные с использованием электронных средств платежа (статья 159.3 УК РФ). Наибольшее число таких преступлений пришлось на Ставропольский край (66), Мурманскую область (52), Татарстан (37), Москву (34) и Саратовскую область (31).

Согласно статистическим данным, в 2017 г. число преступлений в сфере информационно-телекоммуникационных технологий увеличилось с 65 949 (в 2016 г.) до 90 587. Киберпреступления составляют почти каждое двадцатое среди всех преступлений, зарегистрированных в России (4,4% среди всех преступлений).

Самыми распространенными среди них являются неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ). Если в 2017 г. зарегистрировано 1 883 таких преступлений (рост на 7,7%), то за первое полугодие 2018 г. — 1 233 (рост на 3,4%)" (данные Генпрокуратуры).

Наибольшее их количество выявлялось в 2017 г. в Удмуртии (194), Республике Коми (132), в Омской (75), Владимирской (66), Кировской (64), Волгоградской областях (60), в Москве (60) и в Краснодарском крае (51).

При этом на 19,6% уменьшилось количество расследованных преступлений по этим статьям (с 903 до 726), выросло на 30,5% (с 790 до 1031) число нераскрытых преступлений. Раскрываемость данных преступлений составила 41,3%.

Генпрокуратура отметила, что были и факты вынесения незаконных постановлений об отказе в возбуждении уголовных дел. После их отмены возбуждено 204 уголовных дела (в 2016 г. - 161). Наибольшее число таких фактов отмечено в Коми, Марий Эл, Удмуртии, в Красноярском крае, в Волгоградской, Кемеровской, Московской и Челябинской областях.

Возникновение и быстрое развитие электронно-вычислительной техники вызвали к жизни новые виды общественно опасных посягательств. Эффективная борьба с ними возможна при наличии соответствующих уголовно-правовых средств.

Понятие и общая характеристика преступлений в сфере компьютерной информации

Современный Уголовный кодекс Российской Федерации (УК РФ) содержит целый ряд взаимосвязанных норм о мошенничестве. Это, во-первых, общая норма о мошенничестве (ст. 159 УК РФ), а также специальные нормы о мошенничестве в различных сферах (ст. 159.1-159.6 УК РФ). Данное нововведение должно было отразить разнообразие видов мошеннических уловок, которые появляются и всегда приспосабливаются к изменяющейся экономической ситуации в стране[2]. Кроме того, общая норма ст. 159 УК РФ не в полной мере учитывала особенности тех или иных экономических отношений, а потому не позволяла должным

[2] Безверхов, А. Г. Мошенничество и его виды: вопросы законодательной регламентации и квалификации / А. Г. Безверхов // Уголовное право. – 2015. – № 5.

образом обеспечить защиту интересов граждан, пострадавших от мошеннических действий[3].

Все вышеуказанные проблемы обусловили принятие Федерального закона от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»[4], которым была проведена дифференциация различных видов мошенничества: из общего состава мошенничества были выделены 6 специальных составов: мошенничество в сфере кредитования, при получении выплат, с использованием платежных карт, в сфере предпринимательской деятельности (впоследствии утратила силу), в сфере страхования, а также рассматриваемое мошенничество в сфере компьютерной информации.

Легальное понятие мошенничества в сфере компьютерной информации содержится в ч. 1 ст. **159.6**. Согласно данной норме, оно представляет собой хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Однако вопрос об отнесении указанного деяния к мошенничеству представляется спорным.

Криминализация хищения в сфере компьютерной информации в качестве мошенничества предполагает, что деяние, ответственность за которое установлено ст. 159.6 УК РФ, может быть не сопряжено с обманом конкретного человека, например, когда деньги перечисляются с одного счета на другой в результате неправомерного доступа к компьютерной информации в

---

[3] Мусаелян, М. Ф. О некоторых проблемах, связанных с введением в УК РФ специальных составов мошенничества / М. Ф. Мусаелян // Российский следователь. – 2016. – № 10.

[4] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : федер. закон от 29 ноября 2012 г. № 207-ФЗ // Собрание законодательства РФ. – 2012. – № 49. – Ст. 6752.

компьютерной системе банка. До введения в действие ст. 159.6 УК РФ к подобным деяниям также применялась общая норма о мошенничестве — ст. 159 УК РФ, но, по существу, по аналогии.

Совершение этого преступного деяния возможно исключительно посредством использования современных компьютерных технологий. Компьютерная информация — это информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ. Особенность компьютерной информации является то, что она просто пересылается, преобразовывается, размножается; при изъятии информации, в отличие от изъятия вещи, она легко сохраняется в первоисточнике; доступ к одному и тому же файлу, содержащему информацию, могут одновременно иметь несколько пользователей.

Согласно ст. 6 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информатизации и о защите информации» (в ред. от 28.07.2012) информационные ресурсы находятся в собственности юридических и физических лиц, включаются в состав их имущества, на них распространяется действие гражданского законодательства.

Преступления в сфере информационных технологий включают взлом паролей, кражу номеров кредитных карточек и других банковских реквизитов (фишинг). Наиболее опасными и распространенными преступлениями, совершаемыми с использованием сети Интернет, является мошенничество. В частности, инвестирование денежных средств на иностранных фондовых рынках с использованием сети Интернет сопряжено с риском быть вовлеченными в различного рода мошеннические схемы. Другой пример мошенничества — «интернет-аукционы», в которых сами продавцы делают ставки, чтобы поднять цену выставленного на аукцион товара.

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они

могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьезное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные с имущественным ущербом.

Объектом мошенничества в сфере компьютерной информации являются общественные отношения, сложившиеся в сфере электронного документооборота.

Предметом преступного посягательства по статье 159.6 УК РФ кроме имущества являются:

компьютерная информация — это информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме электрических сигналов, независимо от средств их хранения, обработки и передачи,

имущество, т.е. совокупность вещей, которые находятся в собственности лица (включая деньги и ценные бумаги), а также имущественных прав на получение вещей или имущественного удовлетворения от других лиц.

Объективная сторона мошенничества, предусмотренного ст. 159.6 УК РФ, состоит из действий, связанных с завладением чужим имуществом или приобретением права на него путем обмана или злоупотребления доверием, совершенным путем:

ввода компьютерной информации, т.е. размещения сведений в устройствах ЭВМ, системе ЭВМ или их сети для их последующей обработки и (или) хранения,

удаления компьютерной информации, т.е. совершения действий, в результате которых становится невозможным восстановить содержание

компьютерной информации, и (или) в результате которых уничтожаются носители компьютерной информации,

блокирования компьютерной информации, т.е. совершения действий, приводящих к ограничению или закрытию доступа к компьютерной информации (в ЭВМ, системе ЭВМ или их сети), но не связанных с ее удалением,

модификации компьютерной информации, т.е. совершения любых изменений сведений (сообщений, данных), представленных в форме электрических сигналов, независимо от средств их хранения, обработки и передачи,

вмешательства в функционирование средств хранения, средств обработки, средств передачи компьютерной информации, информационно-телекоммуникационные сети, т.е. путем осуществления неправомерных действий, нарушающих процесс обработки, хранения, использования, передачи и иного обращения с компьютерной информацией, установленный ФЗ «Об информации, информационных технологиях и о защите информации» и другими нормативными правовыми актами.

Преступление образует состав преступления при условии, что в результате его действий виновный завладевает чужим имуществом (деньгами) или приобретает право на него. С этого момента данный вид мошенничества образует состав оконченного преступления.

Сам по себе факт манипуляций с компьютером может содержать признаки приготовления к мошенничеству в сфере компьютерной информации или покушения на совершение такого преступления.

Квалифицированными видами мошенничества в сфере компьютерной информации (ч.2 ст. 159.6 УК РФ) являются те же деяния, совершенные группой лиц, а равно с причинением значительного ущерба гражданину (см. прим.2 к ст.158 УК РФ).

Особо квалифицированные виды мошенничества в сфере компьютерной информации (ч.3 ст.159 УК РФ) образуют мошенничество, совершенное лицом с использованием своего служебного положения, а равно в крупном размере, (с банковского счета, а равно в отношении электронных денежных средств).

В ч.4 ст. 159 УК РФ установлена ответственность за деяния, предусмотренные ч. 1, 2 и 3 настоящей статьи, совершенные организованной группой либо в особо крупном размере. Крупным размером в комментируемой статье признается стоимость похищенного имущества — 1 млн. 500 тыс. руб., особо крупным размером — 6 млн. руб.

Неправомерный доступ к компьютерной информации (ст. 272 УК). В рассматриваемой статье предусмотрена ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Непосредственным объектом данного преступления является безопасность (состояние защищенности) компьютерной информации. *Дополнительным объектом* преступления могут быть имущественные и иные общественные отношения, которым неправомерным доступом к компьютерной информации причинен вред.

Потерпевшим может быть физическое или юридическое лицо, которому причинен вред в результате совершения данного преступления.

Объективная сторона рассматриваемого преступления имеет следующие признаки:

1) общественно опасное деяние в виде неправомерного доступа к охраняемой законом компьютерной информации;

2) общественно опасные последствия в виде уничтожения, блокирования, модификации либо копирования компьютерной информации;

3) причинная связь между совершенным деянием и наступившими последствиями.

Поскольку информация – это сведения (сообщения, данные) независимо от формы их представления, доступ к компьютерной информации представляет собой обращение к ней и получение возможности, как минимум, ознакомления с такой информацией, а в целом возможности воздействия на ее свойства (целостность, доступность, конфиденциальность).

Однако не всякий доступ является признаком объективной стороны рассматриваемого преступления. Доступ должен быть неправомерным, что означает отсутствие у субъекта для наличия доступа к компьютерной информации законных оснований, устанавливаемых законодательством РФ, в том числе Федеральным законом «Об информации, информационных технологиях и о защите информации». В соответствии с положениями этого Закона обладатель информации, во-первых, вправе разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа, а во-вторых, при осуществлении своих прав обязан принимать меры по защите информации (ст.ст. 6, 16). Таким образом, если обладатель компьютерной информации ограничил любым способом к ней доступ, принял правовые, организационные или технические меры по защите информации от неправомерного доступа (например, установил различные пароли и коды), то получение доступа к такой информации в нарушение законодательства и без согласия обладателя информации будет являться неправомерным доступом. Помимо деяния обязательным признаком объективной стороны неправомерного доступа к компьютерной информации являются наступившие в результате совершения данного деяния общественно опасные последствия: уничтожение, блокирование, модификация либо копирование информации.

Уничтожение компьютерной информации – это прекращение ее существования, т. е. удаление ее с определенного машинного носителя без возможности восстановления.

Блокирование информации – это создание препятствий доступа к ней, в результате чего информацию невозможно использовать при ее сохранности. Модификация – это видоизменение, преобразование информации. Копирование – это точное повторение или перенос информации с одного носителя на другой.

В связи с тем, что в диспозиции ч. 1 ст. 272 УК предусмотрены указанные последствия в качестве обязательного признака объективной стороны, данный состав преступления является материальным.

В качестве примера совершения рассматриваемого преступления можно привести встречающиеся в судебной практике уголовные дела о неправомерном доступе к охраняемой законом компьютерной информации, когда виновные лица используют чужие регистрационные имена (логины) и пароли для доступа в Интернет. Также встречаются случаи неправомерного доступа к компьютерной информации в виде несанкционированной модификации программ, осуществляющих функционирование тех или иных сайтов в Интернете и размещения на их страницах различной информации, в том числе, рекламного, оскорбительного или порнографического характера.

Субъективная сторона преступления характеризуется умышленной формой вины. Умысел может быть прямым либо косвенным, так как виновный сознает, что своими действиями совершает именно неправомерный доступ к компьютерной информации, в результате чего наступают указанные в законе последствия, наступление которых он желает или допускает либо к которым относится безразлично.

Субъект преступления – лицо, достигшее 16-летнего возраста.

Квалифицирующими признаками, предусмотренными ч. 2 ст. 272 УК, являются причинение крупного ущерба или совершение деяния из корыстной

заинтересованности. Согласно п. 2 примечаний к ст. 272 УК причинением деянием крупного ущерба признается наступление таких его последствий в виде уничтожения, блокирования, модификации либо копирования компьютерной информации, которые нанесли ущерб, превышающий один миллион рублей.

В *ч. 3 ст. 272 УК* установлена более строгая ответственность за совершение рассматриваемого преступления группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения. В последнем случае субъект преступления является специальным. Использование служебного положения означает, что виновный при осуществлении неправомерного доступа к охраняемой законом компьютерной информации использует свои полномочия, вытекающие из его служебной деятельности. Таким лицом может быть должностное лицо, обладающее признаками, предусмотренными п. 1 примечаний к ст. 285 УК, государственный или муниципальный служащий, не являющийся должностным лицом, а также иное лицо, отвечающее требованиям, предусмотренным п. 1 примечаний к ст. 201 УК.

По *ч. 4 ст. 272 УК* квалифицируется совершение деяний, предусмотренных частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления. Таковыми могут быть, например: крупный имущественный ущерб, выход из строя важных технических средств, техногенная авария, дезорганизация производства, смерть человека или тяжкий вред его здоровью.

Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК).

Непосредственным объектом рассматриваемого преступного деяния являются общественные отношения, обеспечивающие безопасное использование компьютерной информации.

Объективная сторона рассматриваемого состава преступления характеризуется только одним обязательным признаком – деянием в виде: 1) создания компьютерных программ либо иной компьютерной информации; 2) распространения таких программ и такой информации; 3) использования указанных программ и информации.

В соответствии со ст. 1261 ГК РФ программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения. Вредоносная компьютерная программа, как следует из диспозиции ч. 1 ст. 273 УК, – это программа, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации либо копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Для того, чтобы считать программу вредоносной, недостаточно, чтобы ее работа приводила к перечисленным последствиям, например, к уничтожению информации. Вредоносная программа должна быть предназначена для осуществления заведомо несанкционированных действий. Вредоносность программы определяется не самими действиями с информацией, для осуществления которых она разработана, а тем, предполагает ли осуществление ею определенных действий (уничтожение, блокирование, модификация, копирование) уведомление владельца информации или добросовестного пользователя об этих действиях и получение его согласия на их выполнение. Так, существуют и широко применяются программы форматирования машинных носителей, полностью уничтожающие информацию на данных носителях. Эти программы не являются вредоносными, поскольку не предназначены для заведомо несанкционированных действий с информацией.

В настоящее время количество и функциональное разнообразие вредоносных программ очень велико. К ним относятся компьютерные вирусы и черви, у которых основные цели – распространиться как можно шире или при запуске на конкретном компьютере повредить информацию, либо нарушить нормальную работу компьютера. Троянские кони (так называемые, «трояны»), проникая на компьютер под видом полезных программ и информации, осуществляют несанкционированное копирования информации и ее передачу, что часто используется для хищения данных доступа в «Интернет».

Спам несанкционированно распространяет рекламную информацию, что зачастую приводит к нарушению нормальной работы компьютерных средств (например, в результате появления рекламных картинок или роликов увеличивается время на выполнение требуемых операций).

Существуют также мошеннические вредоносные программы, которые регистрируют последовательность нажимаемых на клавиатуре клавиш, делают снимки экрана при посещении пользователем сайтов, предлагающих банковские услуги, загружают на компьютер дополнительный вредоносный код, предоставляют хакеру удаленный доступ к компьютеру и т. д. Одной из разновидностей мошеннических программ являются вредоносные программы для осуществления «фишинга» (англ. fishing – рыбалка), который заключается в том, что создается подложный сайт, который выглядит в точности так же, как сайт банка или сайт, производящий финансовые расчеты через сеть Интернет. При посещении потенциального потерпевшего данного фальшивого сайта преступники обманным путем добиваются того, чтобы он ввел на нем свои конфиденциальные данные, например, регистрационное имя, пароль или PIN-код своей банковский карты. Все эти мошеннические программы, а иногда и «трояны», объединяет то, что они позволяют собирать конфиденциальную информацию и использовать ее для хищения денег у пользователей.

Применительно к системам сотовой связи к вредоносным программам можно отнести программы для несанкционированного законным владельцем (компанией производителем или определенным ею лицом) изменения IMEI кода (международного идентификатора мобильного оборудования) сотового телефона.

Вредоносные программы создаются и для контрольно-кассовых машин с целью изменения данных для исчисления налоговых данных путем воздействия на установленные производителем программы таких аппаратов.

В соответствии с ч. 1 ст. 273 УК никаких последствия для признания преступления оконченным не требуется, поэтому состав, как уже было отмечено, является формальным.

Субъективная сторона преступления характеризуется прямым умыслом: субъект осознает общественную опасность совершаемых им действий и желает их совершить. Кроме того, на прямой умысел указывает и признак заведомости, который означает, что субъект осознает вредоносные свойства программы. При отсутствии такого осознания уголовная ответственность исключается.

Субъект преступления – лицо, достигшее 16-летнего возраста.

Квалифицированный состав преступления, предусмотренного ч. 2 ст. 273 УК, содержит следующие признаки: совершение деяния группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а также причинение деянием крупного ущерба либо его совершение из корыстной заинтересованности.

Часть 3 ст. 273 УК предусматривает ответственность за совершение деяний, предусмотренных частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления.

По своему содержанию названные квалифицирующие и особо квалифицирующие признаки преступления не отличаются от соответствующих признаков, предусмотренных ч.ч. 2-4 ст. 272 УК.

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК).

Непосредственным объектом преступления являются общественные отношения, обеспечивающие безопасное использование компьютерной информации, а также безопасное и нормальное функционирование средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Предметом преступления является охраняемая законом компьютерная информация, подробная характеристика которой была дана выше.

Объективная сторона преступления содержит следующие обязательные признаки: 1) деяние (действие или бездействие) в виде нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой законом компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям; 2) последствия в виде уничтожения, блокирования, модификации либо копирования компьютерной информации, причинившие крупный ущерб; 3) причинную связь между совершенным деянием и наступившими последствиями.

Диспозиция ч. 1 ст. 274 УК является бланкетной, т. е. для установления признаков совершенного деяния в виде нарушения правил эксплуатации необходимо обратиться к соответствующим нормативным правовым актам, регламентирующим данные правила. Для понимания технических терминов диспозиции следует, в первую очередь, руководствоваться федеральными законами «Об информации, информационных технологиях и о защите информации» и «О связи».

Следует заметить, что единых правил эксплуатации указанных в данной статье УК технических систем, принятых на федеральном уровне на сегодня нет,

поэтому чаще всего такие правила закрепляются в ведомственных или локальных правовых актах. Эти правила могут касаться, например, обязанностей субъекта использовать компьютеры (ЭВМ) только в соответствии с техническими требованиями эксплуатации, установленными изготовителями аппаратного или программного обеспечения, использовать ЭВМ только в рамках своих должностных обязанностей, принимать меры по предотвращению использования ЭВМ другими лицами от его имени, пользоваться средствами антивирусной защиты, выполнять требования по защите информации. Также правила эксплуатации ЭВМ могут предусматривать запрет на осуществление определенных действий, например, записывать и хранить информацию на неучтенных носителях информации, оставлять включенной без присмотра свою рабочую станцию, не активизировав средства защиты от несанкционированного доступа, использовать ЭВМ для хранения и обработки информации, не имеющей отношения к выполнению должностных обязанностей, использовать свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению функционирования ЭВМ, производить массовую рассылку электронных сообщений, не согласованных предварительно с получателем, пересылать файлы, содержащие вирусы, самовольно вносить какие-либо изменения в конфигурацию программно-аппаратных средств и т. п.

Помимо совершенного деяния объективная сторона состава преступления включает последствия в виде уничтожения, блокирования, модификации или копирования охраняемой законом компьютерной информации, причинившие крупный ущерб. Крупным ущербом признается ущерб, сумма которого превышает один миллион рублей.

Субъективная сторона преступления характеризуется как умышленной, так и неосторожной формой вины, так как субъект может нарушить соответствующие правила как умышленно (сознавая, что не выполняет те или иные правила), так и по неосторожности (не сознавая, что нарушает какие-либо

правила ввиду, например, забывчивости). Однако ответственность за нарушение правил эксплуатации может наступать только при условии, что нарушенные виновным лицом правила были в установленном порядке приняты и доведены до его сведения.

Субъект преступления специальный, так как данное лицо должно иметь правомерный доступ к эксплуатации соответствующих технических средств и сетей и обязано соблюдать установленные для них правила эксплуатации. Наличие у виновного лица такого доступа обусловлено установленным собственником или иным законным владельцем технических средств и сетей порядком осуществления доступа к ним, и, как правило, этот доступ связан с характером выполняемых субъектом служебных обязанностей, касающихся эксплуатации или технического обслуживании технических средств.

В соответствии с *ч. 2 ст. 274 УК* более строгая ответственность наступает, если нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей повлекло тяжкие последствия или создало угрозу их наступления. Содержание этого признака было раскрыто при анализе составов преступлений, указанных в ст.ст. 272 и 274 УК.

Пример из судебной практики

Таганский районный суд столицы в июне 2016 г. приговорил работавшего в 2012 году системным администратором Алексея С. к одному году лишения свободы условно по обвинению в использовании вредоносного программного обеспечения.

Приговор, оглашенный судьей, пока не вступил в законную силу, точку в деле поставит Московский городской суд после рассмотрения апелляционных жалоб. Защита убеждена: в случае, если существующий приговор будет подтвержден вышестоящей инстанцией, это затронет интересы производителей программ, в числе которых — американский IT-гигант «Apple». К примеру,

огромное количество людей, пользующихся компьютерами фирмы «Apple» с позиции Таганского районного суда, преступают закон. В такой ситуации у компаний-производителей появится возможность обратиться с иском против России в суд, требуя восстановления деловой репутации и возмещения ущерба. Вступление в законную силу данного судебного решения окажет негативное воздействие на развитие процессов импортозамещения, набирающих силу в нашей стране — сообщил адвокат.

Представители компании «Apple» из европейского офиса в ирландском Корке для выяснения подробностей уже звонили Алексею С. По его словам, они просили держать их в курсе дела. Осведомлены о приговоре и российские производители: ООО «НПрофи» и ООО «Безопасность», констатирует осужденный.

Алексей, впервые в жизни, столкнувшийся с правосудием, называет дело абсурдным и подчеркивает, что не выходил за рамки своих полномочий, не использовал таких программ. При этом программы, признанные судом вредоносными, — сообщил он — являются лицензионными, безопасны и общедоступны, получены непосредственно от производителей. Производители программ не создавали их вредоносными, заведомо не предназначали для нанесения вреда компьютерам, сетям, информации, не закладывали преднамеренно в них вредоносные функции. Данными программами много лет пользуются миллионы человек в России, десятки тысяч компаний. И за это время не было прецедента назвать их вредоносными, тем более приговором суда. Если бы поводы для этого малейшие были, вряд ли это не заметили бы за столько лет. В стране бурно развиваются компьютерные информационные технологии, повышается их роль в управлении, в экономических процессах, на производстве, транспорте, в повседневной жизни. С высоких трибун заявлен курс на цифровизацию экономики, на импортозамещение компьютерного оборудования

и программного обеспечения на отечественные разработки. Тем более непонятна позиция суда, который не разобрался в существе вопроса.

По словам осужденного, он, будучи системным администратором, согласно договору с работодателем ЗАО «ГК «Т.», имел законный свободный доступ к компьютерам, сетям и оборудованию, поэтому «на уровне правовой аксиомы» не мог осуществить ни неправомерный доступ к информации, ни несанкционированно на нее воздействовать, в том числе несанкционированно копировать с помощью вышеперечисленных программ.

Приговором судьи Таганского суда Москвы вредоносными и заведомо предназначенными для незаконного копирования данных была признана лицензионная программа, предназначенная для резервного копирования и изначально установлена производителем на всех компьютерах марки «Apple», а также российские программы «LAS» и «Security», которые предназначены производителями для защиты информации и предупреждения ее утечки за пределы локальных сетей.

Исчерпывающую информацию о программах можно найти на официальных сайтах производителей. Там указано, что эти российские программы распространяются дилерами в большинстве регионов страны, а их производителям удалось выйти на зарубежные рынки. В свою очередь программа марки «Apple» законно находится на таможенной территории России и продается в составе штатной комплектации компьютеров «Apple» через официальных реселлеров. Резервное копирование — для чего программа предназначена — объясняет Алексей, — это обязательный элемент защиты, сохранения и восстановления информации на случай аварий и технических сбоев, о чем написано во всех учебниках.

Алексей Стариков указывает на то, что «Lan Agent Standard» — одна из признанных судом вредоносными программ — внесена Минкомсвязи России в Единый реестр российского программного обеспечения для ЭВМ и баз данных.

Включение программ в данный перечень, продолжает он, служит рекомендацией к использованию в госучреждениях и свидетельствует о соответствии всем стандартам информационной безопасности. А «Security», после ребрендинга «StaffCop», официально зарегистрированная в Роспатенте в 2008 году, тоже известная программа, которой успешно пользуются тысячи коммерческих компаний в России.

При этом вина не доказана по существу: ведь Алексей не использовал вредоносных программ, не нарушал прав доступа к информации.

В основе обвинения лежит личное мнение эксперта, не отвечающее официальным критериям оценки вредоносности компьютерных программ, признакам состава преступления, изложенных в статье уголовного кодекса. При этом дело было возбуждено против неизвестных лиц за неправомерный доступ к компьютерной информации по части 1 статьи 272 Уголовного кодекса РФ, а обвинение предъявлено совсем по другой статье почти через два года после увольнения из компании конкретно Алексею — по части 1 статьи 273 — за использование вредоносных компьютерных программ, заведомо предназначенных для несанкционированного копирования.

После оглашения приговора судья обратилась к нему: «Я не являюсь специалистом в этой области и никогда им являться не буду, в использовании этих компьютерных программ, вам, наверное, это более понятно — с учетом навыков, знаний и так далее. Вы обжалуйте».

По мнению адвоката осужденного, приговор Таганского суда незаконен, поскольку все три эти программы правомочно находились и находятся в гражданском обороте на территории России и в свободной продаже, они никак не могут именоваться вредоносными. Суд необоснованно скопировал обвинение в приговор. Стороной защиты были представлены суду официальные ответы на адвокатские запросы всех компаний-производителей: «Apple», «Профи», «Безопасность» — о предназначении программ, о том, что они не вредоносные и

заведомо не предназначены для несанкционированного копирования. И это важные документы, поскольку вредоносность компьютерных программ по смыслу ч. 1 ст. 273 Уголовного Кодекса связывается с процессом их создания: с техническими свойствами программ, их техническими функциями для нанесения вреда компьютерам, сетям, информации заведомо, то есть преднамеренно, заложенными в них производителями в процессе их создания.

Отстаивая свою позицию в ходе судебного разбирательства, защита получила заключение специалистов испытательной лаборатории, аккредитованной Федеральной службой по техническому и экспортному контролю, которая, в соответствии с Указом президента, является государственным органом исполнительной власти, уполномоченным регулировать отношения в сфере безопасности компьютерных программ, в том числе разрабатывать критерии оценки их вредоносности, руководящие документы и национальные государственные стандарты. Специалисты в своем заключении определили: программы «Apple», «LAS» и «Security» — не вредоносны, заведомо не предназначены для несанкционированного копирования, фактов несанкционированного копирования ими не обнаружено. Обработка на антивирусном оборудовании в ходе судебной экспертизы подтвердила, что вредоносных программ не обнаружено. Не было вредоносных программ, а значит, не было и события использования вредоносных программ, соответственно и события несанкционированного копирования.

Кроме того, защитники Алексея предоставили суду заключение эксперта постоянной комиссии Совета по развитию гражданского общества и правам человека при Президенте РФ (СПЧ), разъясняющее уголовно-процессуальный закон, в части допущенных на предварительном следствии нарушений — сообщил адвокат.

«Вроде бы все понятно и разобраться в этом деле можно достаточно быстро». Однако предварительное расследование данного дела следственным

управлением УВД по ЦАО г. Москвы продолжалось 14 месяцев, 12 раз продлевались его срок. За это время следователем создано 6 томов дела. В этом случае дело длится скоро как три года, не имея ни одного доказательства.

Нарушения продолжились и в Таганском суде. За все время процесса протяженностью в год Алексею и его адвокатам ни разу не дали ознакомиться с протоколом судебных заседаний. Было назначено 17 судебных заседаний, из которых 10, при явке всех участников, были отложены по инициативе суда. Более того, протокол они не могли получить более четырех месяцев уже после оглашения приговора, несмотря на жалобы и обращения. Трижды обращались за помощью к председателю Мосгорсуда. Налицо волокита, затягивание разумных сроков судопроизводства, т.е. передачи дела в Московский городской суд для рассмотрения апелляционных жалоб осужденного и защитников. Этим грубо нарушались Конституционные права осужденного, лишая его доступа к правосудию.

По мнению Алексея и его защитников на следствии были допущены следующие грубые нарушения закона: назначение судебной экспертизы коммерческой организации, не являющейся судебно-экспертным учреждением у которой нет лицензии, аккредитации, а сам эксперт оказался даже без высшего образования; оплата судебных экспертиз произведена не из бюджетных средств как положено по закону, а за счет средств Совета ветеранов Главного управления угрозыска МВД по просьбе руководства следственного органа; в нарушение федерального закона о порядке рассмотрения обращений граждан произведен допрос Алексея С. в следственном управлении по его жалобе прокурору г.Москвы на незаконные действия следователя; выемка компьютерной техники для производства судебной экспертизы проведена без обязательного по требованию закона судебного разрешения; дело не было прекращено, как это было предписано актом амнистии в связи с 70-летием Победы в Великой Отечественной войне. И это только малая толика.

Алексей честно работал, поддерживал в рабочем состоянии сети и оборудование и, спустя более чем через год после увольнения, вдруг попал в такой водоворот событий. Непонятны причины и мотивы такого положения дел, а также чьи интересы за этим стоят, почему разумные сроки затягиваются? Компания, в ноябре 2013 года подавшая на имя начальника московской полиции Анатолия Якунина заявление, подписанное председателем совета директоров, против неизвестных лиц, осуществивших неправомерный доступ к информации и организовавших ее хранение — это ГК «Т». В последствии, из материалов дела, публикаций в прессе, стало известно, что эта компания имеет не однозначную репутацию. В 2012 году против руководителей ее дочерней компании в Казахстане было возбуждено уголовное дело за нецелевое использование заемных средств. И казахстанский банк ведет тяжбу о взыскании с «Т.» значительных сумм. Сейчас эта компания, преодолевая протесты населения, связанные с экологическими проблемами, пытается организовать строительство завода.

Незаконное уголовное преследование уже идет более двух с половиной лет, Алексей С. потратил все сбережения, влез в долги. У него диагностировали серьезное системное заболевание, за это время на фоне несправедливого обвинения, дважды был госпитализирован с ухудшением состояния здоровья.

В итоге Алексея С. Признали виновным в совершении преступления, предусмотренного ст. 272 УК РФ и назначили ему наказание в виде лишения свободы сроком на 1 год. Данное наказание Алексею С. считать условным с испытательным сроком в течение 1 года, а в последствии на основании п. 9 Постановления Государственной Думы Федерального Собрания Российской Федерации «Об объявлении амнистии» Алексей С. был освобожден от отбывания назначенного ему наказания.

Заключение

Преступления в сфере компьютерной информации практически являются безупречной возможностью для преступников совершать свои деяния без наказания. Практическая возможность доказательства таких преступлений сводится к минимуму. Как известно — наиболее опасные преступления — это те, которые носят экономический характер. Например, это неправомерное обогащение путем злоупотребления с автоматизированными информационными системами, экономический шпионаж, кража программ и так называемого «компьютерного времени», традиционные экономические преступления, совершаемые с помощью компьютера. Также можно отметить, что при расследовании компьютерных преступлений зачастую трудно бывает установить как объективную, так и субъективную сторону преступления. Сложность для следствия заключается здесь и в том, что очень часто преступник не может в полной мере представить себе последствия своей деятельности. Такая неопределенность часто возникает, например, при попытках несанкционированного доступа в компьютерные сети. Преступник не всегда правильно представляет себе ценность копируемой, уничтожаемой или искажаемой информации, а тем более дальнейшие последствия, к которым могут привести его действия.

Так же проблема заключалась в том что, изначально, как показывает история, правоохранительные органы боролись с компьютерными преступлениями при помощи традиционных правовых норм о преступлениях против собственности: краже, присвоении, мошенничестве, злоупотреблении доверием и тому подобное. Практика показывает, что такой подход не отвечает всем требованиям сложившейся ситуации, поскольку многие преступления в сфере компьютерной деятельности не охватываются традиционными составами преступлений. Во многих преступлениях отсутствовал материальный признак,

так как предмет отсутствует как материальная вещь, существующая в реальном физическом мире.

Необходимо также отметить, что для эффективного раскрытия компьютерных преступлений и поиске преступников необходимо наладить тесное международное сотрудничество, так как данный вид преступления в основном совершаются на международном уровне. В 90 процентах из 100 компьютерные преступлении совершают лица являющиеся гражданами другого государства, так как для компьютерных преступлений не существует территориальных границ.

Согласно статистическим данным численность компьютерных преступлений с каждым годом заметно растет. Поэтому необходимо принимать радикальные меры, для совершенствования законодательства и его практической реализации. Как показывает практика, наличие всего лишь трех статей в Уголовном кодексе недостаточно для регулирования для регулирования отношений в сфере компьютерных преступлений.

Литература

1. Уголовный кодекс Российской Федерации от 24.05.96г. - СПб.: Альфа, 1996.
2. Федеральный закон от 22 февраля 1995г. № 24-ФЗ «Об информации, информатизации и защите информации». // Российская газета. -- 1995. -- 22 февраля.
3. Комментарий к Уголовному кодексу Российской Федерации (постатейный) // Г.Н. Борзенков, А.В. Бриллиантов, А.В. Галахова и др.; отв. ред. В.М. Лебедев. 13-е изд., перераб. и доп. М.: Юрайт, 2013.
4. Александрова И.А. Новое уголовное законодательство о мошенничестве // Юридическая наука и практика. Вестник Нижегородской академии МВД России. 2013. № 21. С. 62.
5. Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. М.: Юрлитинформ, 2001.
6. Вехов Б.В. Компьютерные преступления: способы совершения, методика расследования. - М.: Право и закон, 1996.
7. Гаврилин Ю.В., Шипилов В.В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. 2013, №23, с. 2-6.
8. Гладких В.И. Компьютерное мошенничество: а были ли основания его криминализации? // Российский следователь. 2014, №2., с.25-31.
9. Егорышев А.С. Безопасность компьютерной информации в XXI веке. / Общество, государство и право России на пороге XXI века: теория, история. Межвузовский сборник научных трудов. / Под редакцией проф. К.Б. Толкачева, проф. А.Г. Хабибулина. - Уфа: УЮИ МВД России, 2000.
10. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия - Телком, 2002.