МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»
Институт права
(наименование института полностью)

Кафедра «Уголовное право и процесс»
(наименование)

40.04.01 Юриспруденция
(код и наименование направления подготовки)

Уголовное право и процесс
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему «Правовое регулирование преступлений, связанных с использованием компьютерных технологий»

Студент А.О. Ращупкин
(И.О. Фамилия) (личная подпись)

Научный руководитель канд. юрид. наук., доцент, П.А. Кабанов
(ученая степень, звание, И.О. Фамилия)

Тольятти 2021

Оглавление

Введение

Актуальность темы исследования. Современный цифровой мир полон угроз, как для интересов частных лиц, так и для интересов государств и международного сообщества в целом. Не вызывает сомнения тот факт, что большинство современных информационных технологий обладают ярко выраженным враждебным потенциалом, способным быть направленным против безопасности государств и прав, и свобод личности. Широкий спектр воздействия кибернетических угроз на множество сфер жизни государства, базирующихся на виртуальных данных, позволяет данному типу угроз охватывать как частную собственность, так и функционирование городской инфраструктуры в целом. Современный уровень развития государств позволяет смещать интересы правительств и частных лиц в новую сферу – кибернетическое пространство, существующее по собственным правилам и сложно поддающееся правовому регулированию.

Опасность преступлений в виртуальном пространстве в последние годы начали понимать во всем мире, ее признают даже правоохранительные органы в России. Однако, до сих пор, как в мире, так и в России единой концепции борьбы с киберпреступностью не выработано.

Степень научной разработанности темы. По теме квалификации преступлений в сфере компьютерных технологий выполнен ряд диссертаций (например, С.Д. Бражник, В.В. Воробьев, В.С. Карпов, С.Г. Спирина и др.). Помимо этого, в указанной сфере активно разрабатывали проблематику преступлений с применением компьютерных технологий Вехов В.Б., Волевод А.Г., Номоконов В.А., Мазуров В.А. и другие.

Киберпреступность как явление, охватывающее обширный спектр преступлений, совершаемых в информационных сетях, активно исследовали зарубежные ученые, например, М. Бреннер и С. Гудман, Ф. Вильямс, У. Зибер и многие другие [50].

Объект исследования. Общественные отношения в сфере привлечения к уголовной ответственности за преступные деяния, совершаемые с применением компьютерных технологий, глобальных сетей.

Предмет исследования. Научная литература по тематике, в том числе труды отечественных и иностранных авторов; уголовное законодательство РФ, международное законодательство в области совершения киберпреступлений, а также судебная практика по делам о преступлениях, связанных с использованием компьютерных технологий, статданные, а также Интернет-ресурсы.

Цель исследования. Выявление и анализ теоретических и практических проблем правового регулирования преступлений, связанных с применением компьютерных технологий, а также внесение предложений по совершенствованию уголовного законодательства и практики его применения в указанной сфере.

Для достижения указанной цели необходимо решить следующие задачи исследования:

- рассмотреть определения «преступлений, связанных с использованием компьютерных технологий»;
- изучить общественную опасность незаконных действий, совершаемых с использованием компьютерных технологий;
- проанализировать проблемы привлечения к уголовной ответственности за преступления с использованием компьютерных технологий на международном уровне и в РФ;
- выработать предложения по совершенствованию уголовного законодательства об ответственности за киберпреступления.

Методы исследования. Автор в диссертационном исследовании применил методы анализа и синтеза, аналогии, сравнительный, формально-юридический, статистический, историко-правовой и др.

Теоретическая база исследования. Диссертационное исследование опиралось на научные мысли отечественных авторов по вопросам совершения,

выявления и предупреждения преступлений в сфере использования компьютерных технологий, таких как, например: Ю.М. Батурина, В.Б. Вехова, А.М. Доронина, В.А. Голубева, А.П. Кузнецова, С.С. Медведева, И.М. Рассолова, А.И. Халиуллина, Д.А. Ястребова и др.

Научная новизна исследования обусловлена комплексным подходом автора к существующей проблематике, объединяющей в себе научные труды, результаты правоприменительной деятельности, а также в том, что магистрант внес свои предложения по решению проблем, связанных с выявлением и квалификацией преступлений в сфере компьютерных технологий. Кроме того, новизна также выражается в положениях, выносимых на защиту:

- Дано авторское определение понятия информационной безопасности – сумма отношений, возникающих в обществе, которые способны обеспечить связанную с ними деятельность, хранение, систематического пополнения, использования и передачу сведений, участниками которых являются обладатели данных сведений и владельцы, которые пользуются данной информации в своих целях.
- Доказана необходимость внесения дополнений для классификации признака относительно того, что преступление было совершено посредством использования интернета, при этом совершение преступления с помощью сети «Интернет» должно являться стандартным способом осуществления противоправного действия, наносящего вред обществу. Данное изменение наиболее необходимо в ст. 110, 128.1, 137, 138, 146, 150, 151, 174, 174.1, 205.1, 205.2, 230, 242, 272, 273, 280 Уголовного кодекса РФ.
- Выявлена необходимость законодательного закрепления критериев отнесения программы к вредоносной и наносящей угрозу обществу.
- Обоснована целесообразность внесения дополнений в гл. 29 УК РФ, включив в диспозицию преступных деяний указание на способ

совершения «…посредством использования информационно-коммуникативных сетей».

Теоретическая и научная значимость исследования. Автор предложил свои определения дефиниций в данной области, а также развил положения, направленные на повышение качества выявления и квалификации киберпреступлений в правоприменительной практике. При этом некоторые теоретические выводы могут лечь в основу дальнейших научных исследований по данной проблематике.

Практическая значимость работы заключается том, что предложенные выводы и рекомендации могут найти свое применение как в законодательной, так и в правоприменительной сферах. Предложения и обобщения, подготовленные автором, могут быть использованы для разработки отдельного спецкурса для студентов «Характеристика преступлений в сфере компьютерной информации».

Апробация результатов исследования. Отдельные аспекты исследуемой проблематики освещались автором в ранее опубликованной статье «Правовое регулирование доступа правоохранительных органов к данным пользователей».

Структура магистерской диссертации. Обусловлена задачами исследования и требованиями к структуре данного вида работ – включает введение, три главы, шесть параграфов, заключение, а также список используемой литературы и используемых источников.

Глава 1 Понятие преступлений, совершаемых с использованием компьютерных технологий

1.1 Дефиниции и терминология, используемые для описания преступлений, совершаемых с использованием компьютерных технологий

Преступления с использованием компьютерных технологий включают обширную категорию преступлений. Некоторые из таких преступлений могут быть связаны с компьютерными системами, например, кража или мошенничество, другие могут иметь связь с непосредственным устройством и использовать его лишь как «передатчик» или «приёмник» при передвижении по Интернет-сетям. В понятие преступлений, связанных с компьютерными технологиями, включаются и вредоносные действия, непосредственно связанные с компьютерами, например, взлом устройства или пользовательских данных на конкретном устройстве [43].

Отметим, что преступления с использованием компьютерных технологий в УК РФ закреплены, прежде всего, в гл. 28 «Преступления в сфере компьютерной информации», поэтому разумно определить, что можно под ними подразумевать. Так, Старичков М.В. определил под ними «…запрещенные УК РФ под угрозой наказания виновно совершенные общественно опасные деяния, посягающие на общественные отношения, связанные с правомерным и безопасным использованием охраняемой законом информации ЭВМ» [42, с. 16.]. Дворецкий М.Ю. к подобным деяниям относит только те, которые направлены на нарушение неприкосновенности охраняемой законом компьютерной информации и ее материальных носителей [10, с. 76]. М.А. Зубкова направленность данных преступных деяний определяет как: «…посягающие на нормальный порядок обращения охраняемой законом компьютерной информации…» [14, с. 13].

Лошенкова Е.В. характеризует преступные деяния, совершенные с применением компьютерных технологий, как «...причиняющие вред или создающие опасность причинения вреда безопасности производства, хранения, использования либо распространения информации или информационных ресурсов…» [20, с. 112].

Законы, посвящённые регулированию правонарушений с использованием компьютерных средств, наиболее часто содержат следующий перечень ограничения действий пользователя:

- запрет на неправомерный доступ к компьютеру, системе или Сети;
- изменение повреждение, использование, раскрытие, копирование или получение программ, или данных;
- введение вируса или другого загрязнителя в компьютерную систему;
- использование компьютера в схеме мошенничества;
- вмешательство в систему чужого компьютерного устройства или его использование;
- использование шифрования для совершения преступления;
- фальсификация информации об источнике электронной почты;
- кража услуг сети-провайдера [44].

Особой разновидностью угроз по мнению экспертов является «потеря компьютера или учётной записи в Интернете». Подобное может привести владельца устройства или записи к ситуации «виновности» в чужом правонарушении, установить виновного, в котором часто представляется в случае с преступлениями в виртуальной среде весьма проблематично.

С понятием «преступлений, связанных с использованием компьютерных технологий», связаны два других понятия – «киберпространство» и «киберпреступность». В настоящее время данные термины часто употребляются как синонимы, что обусловливается наличием в большинстве современных преступлений с использованием компьютерных средств, выхода деяния в пространство Интернет-сети, то есть – «киберпространства».

Следует отметить, что помимо термина «киберпреступность» широко используется ряд синонимичных понятий, таких как электронное преступление, цифровое преступление, компьютерное преступление и высокотехнологичное преступление. В Уголовном кодексе Российской Федерации, например, эти преступления квалифицируются как преступления в области компьютерной информации (глава 28) [45]. При этом законодательное определение общеупотребляемого термина «киберпреступление» в последнем отсутствует.

Киберпреступления в своих проявлениях настолько могут различаться между собой (традиционные или совершенные онлайн, например), что единых универсальных критериев в отношении действий, составляющих преступное деяние, до сих пор не выработано ни на международном уровне, ни на уровне отечественного законодательства. Следует согласиться с Л.И. Бутусовой, которая отметила: «…отсутствие общепринятых и нормативно закрепленных дефиниций «Интернет», «киберпреступление», «киберпреступность», «компьютерные преступления», позволяет преступникам избегать юридической ответственности, пользуясь несогласованностью правовых баз различных государств. Преступники могут совершать преступления из страны, где подобная деятельность не является противозаконной» [4, с. 49].

В научной юридической литературе в качестве синонимов или схожим терминов используют формулировки: «преступления в сфере компьютерной информации», «информационные преступления», «преступления в информационном пространстве» и многие другие [18].

Такой «разброс» в терминологии требует выработки единого категорийного аппарата, что позволило бы значительно упростить деятельность правоохранительных органов в выявлении и квалификации подобных преступлений. Следует указать, что несмотря на активное использование в литературе терминов «киберпреступность», «киберпреступление», единого и четкого понятия до сих пор не выработано. Различный смысл этих понятий, который вкладывают при проведении

авторских исследований ученые, значительно затрудняет аналитическую работу по их сопоставлению и анализу. Более того, отдельные авторы зачастую слишком широко определяют диапазон киберпреступлений. Так, например, Т. Тропина включает в киберпреступления не только с использованием компьютеров, но с использованием любых информационных технологий и глобальный сетей [24, с. 45]. Сложно согласиться с подобным утверждением, поскольку преступления, связанные с использованием информационных технологий, могут касаться не только глобальных сетей, но и закрытых локальных систем.

Отечественный социолог Д.Н. Карпова в своей статье максимально полно описал киберпреступление через перечисление видов ущерба (экономического, политического, морального, идеологического и пр.), причиненного организации, индивидууму, государству «…посредством любого технического средства с доступом в интернет» [15, с. 46].

Считаем, что понятие «компьютерная преступность» весьма многогранно, поскольку под ним можно подразумевать, во-первых, только определенные составы преступлений, у которых в качестве объекта посягательства можно выделить «…охраняемые законом общественные отношения в сфере безопасного создания, хранения, обработки и передачи компьютерной информации…» [13, с. 28]. А, во-вторых, под этой дефиницией можно объединить весь спектр преступных деяний, для которых в качестве объекта преступления можно определить «…общественные отношения в сфере компьютерной информации и информационных технологий, безопасного функционирования средств создания, хранения, обработки, передачи, защиты компьютерной информации, но при этом компьютерная информация, информационно-телекоммуникационные сети; средства создания, хранения, обработки, передачи компьютерной информации (компьютеры, смартфоны, айфоны, кассовые аппараты, банкоматы, платежные терминалы и иные компьютерные устройства) являются не только

предметами преступного деяния, но и используются в качестве средства и орудия совершения преступления» [13, 29].

Логично для нашего исследования сгруппировать по видам преступные деяния следующим образом:

- преступления, связанные с движением безналичных средств (мошенничество с банковскими картами, похищение денежных средств в момент совершения банковских операций и т.д.);
- преступления, связанные с получением информации от граждан по банковским счетам (фишинг);
- преступное деяние по скрытому перенаправлению жертвы на ложный IP-адрес (фарминг);
- удаленный взлом компьютеров с целью похищения информации либо внедрения вирусов;
- киберпорнография;
- торговля наркотиками онлайн
- кибертерроризм;
- азартные игры онлайн;
- преследование в Интернет-сетях;
- доведение до самоубийства в глобальных сетях и т.д.

При этом следует отметить, что вышеназванные деяния в отечественном законодательстве до сих пор не нашли полноценного закрепления. Так, ответственность, например, за фишинговые действия и спам не установлена. А максимальный размер ответственности за киберпреступления не превышают штрафа в размере 1 млн. рублей и 10 лет лишения свободы [17].

Следует отметить, что с учетом роста числа и разновидностей киберугроз, наличие в международных договорах и в соглашениях между государствами положений с перечнем киберпреступлений видится несколько устаревшим и не может соответствовать современной ситуации.

Таким образом, можно отметить, что до сих пор в науке отечественного права нет четкого понимания киберпреступлений, и, как следствие, возникают

проблемы с квалификацией преступлений, предусмотренных в данной сфере УК РФ.

1.2 Общественная опасность преступлений, совершаемых с использованием компьютерной техники и компьютерных технологий

Успешность международного сотрудничества зависит от унификации национальных законодательств в области борьбы с преступлениями, использующими компьютерные технологии, и от наличия двусторонних и многосторонних международных соглашений, регулирующих данный вопрос.

Унификация национальных законодательств подразумевает унификацию понятийного аппарата в вопросе регулирования преступности, установление норм доказательного права, унификацию процессуальных процедур и правил осуществления уголовного судопроизводства. Сходство понятийного аппарата позволяет государствам конкретизировать внешние запросы на получение информации и позволяет избежать неточности в передаче информации, в том числе свидетельских показаний. Принятие двусторонних и многосторонних соглашений между странами и их ратификация упрощает транснациональное регулирование предотвращения организованной преступности при условии наличия в данных соглашениях обоюдного признания в законодательстве государств соответствующего деяния противозаконным. Транснациональное регулирование предотвращения преступлений имеет особое значение в случае с преступлениями в киберпространстве, охватывающими преимущественно несколько стран. В случае отсутствия обоюдного признания в государствах деяния противозаконным, злоумышленник получает возможность избежать наказания, как это стало возможным для распространителя вируса «LOVE BUG»: на момент совершения им деяния, в 2000 году, его действия не считались противоправными в стране его проживания (на Филиппинах) [59].

Следует отметить, что с учетом роста числа и разновидностей киберугроз, наличие в международных договорах и в соглашениях между государствами положений с перечнем киберпреступлений видится несколько устаревшим и не может соответствовать современной ситуации. В большей степени отвечает требованиям угроз современности подход, при котором страны договариваются сотрудничать в расследованиях всех преступлений, относимых к преступлениям в киберпространстве по их внутренним национальным законодательствам [1].

Сотрудничество РФ в области противодействия преступлениям, связанным с использованием компьютерных технологий в международных соглашениях включает в себя обозначение следственных полномочий и границ следственных действий, процедуры получения данных от провайдеров услуг, процедуры сбора цифровых доказательств, уточнение юрисдикций государств, осуществление оперативного сотрудничества, в том числе выдачи и оказания правовой помощи, техническое содействие, осуществление судебного преследования и создание особой процессуальной практики.

В международных соглашениях между государствами уточняются формы сотрудничества между государствами (обмен информацией, предоставление правовой помощи, предупреждение, выявление, пресечение и расследование преступлений в сфере компьютерной информации) (ст. 5-7 Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации) [40], способы предоставления международной помощи, уточнение причин для отказа в предоставлении помощи и руководящие указания в отношении исполнения запросов. Создание информационной базы в области киберпреступности позволяет странам упрощать поиск необходимой информации по соответствующим правонарушениям [23].

Основная сложность предоставления межгосударственной помощи в раскрытии преступлений, связанных с использованием компьютерных технологий, связана со специфическим характером данного вида

правонарушений. Имея дело с передачей личной информации, преступления в киберпространстве осложняют процесс международного сотрудничества привлечением к уголовным процедурам законодательств, регулирующих обращения с личными данными граждан различных государств. Особым образом данное обстоятельство подчеркивается в Конвенции Совета Европы о преступлениях с использованием компьютерных технологий от 2001 года [16].

В ст. 29 настоящей Конвенции позволяет отклонять запрос на предоставление информации по совершенному правонарушению в ряде случаев. Сторона, действующая в рамках взаимной помощи запрашиваемой Стороне, может отказать в предоставлении данных в случаях: наличия основания полагать, что в момент раскрытия условие о квалификации правонарушения как уголовно наказуемого обеими Сторонами не будет выполнено (ст. 29, п. 4), возможной квалификации правонарушения как имеющего характер политического правонарушения (ст. 29, п. 5а), при возможной угрозе выполнением данной просьбы «нанести ущерб суверенитету, безопасности, общественному порядку или другим важным интересам» отвечающей на запрос Стороны (ст. 29, п. 5в), а также при наличии риска, что запрашиваемая сторона «не обеспечит в будущем сохранность этих данных, или поставит под угрозу их конфиденциальность» (ст. 29, п. 6) [16].

Обязательное сохранение конфиденциальности данных является требованием установления международного сотрудничества и соблюдением международных обязательств, принятых государствами в области прав человека. Возможное нарушение государством обязательств по поддержанию прав человека становится основанием для отклонения просьбы об оказании международной помощи [36].

В ряде международных соглашений о сотрудничестве содержатся положения об унификации процедур раскрытия правонарушений в киберпространстве и призывы к созданию внутренних служб оперативного реагирования на угрозы. Так, Конвенция Африканского союза о кибербезопасности и защите персональных данных утверждает создание

групп реагирования на компьютерные правонарушения (CERT) и правонарушения в области компьютерной безопасности (CSIRT) [51].

Особое значение на международном уровне имеют такие международные и региональные соглашения по данному вопросу, как Соглашение СНГ в области обеспечения информационной безопасности, Конвенция Африканского союза о кибербезопасности и защите персональных данных, Конвенция Совета Европы – Будапештская конвенция о преступности в сфере компьютерной информации, Конвенция Лиги Арабских государств и Соглашение ШОС [39].

Рассмотрим основные положения каждого из обозначенных актов и влияние каждого из них на сокращение угроз в киберпространстве, а также проанализируем соответствие содержащихся в них положений угрозам современной действительности.

Первым международным документом, созданным по вопросам регулирования киберпреступности, является Будапештская конвенция. Конвенция была принята 23 ноября 2001 года и своей задачей ставит выработку методики прекращения преступлений в Интернете. Основными направления регулирования являются преступления, совершаемые через Интернет-сеть, в число которых входят нарушения авторских прав, мошенничество с использованием компьютеров, распространение детской порнографии и общие нарушения безопасности сети. В своем выступлении от 20.11.2019 года Генеральный Секретарь Совета Европы Мария Пейчинович-Бурич вновь подтвердила мнение о том, «что Будапештская конвенция остается наиболее актуальным международным стандартом в области предотвращения киберпреступности. Компьютерные преступления влияют не только на бизнес, но и оказывают влияние на выборы и демократию, ведут к распространению порнографических изображений детей и миллиардным кражам персональных данных» [37]. Происходящие в мире правовые, политические и технологические события диктуют свой уровень необходимого развития и принятой конвенции: в декабре 2012 года

Комитетом по конвенции о киберпреступности (T-CY) на 8-м пленарном заседании было принято решение об издании Руководящих указаний к действующей конвенции в целях ее более эффективной реализации [56]. В преамбуле к Указаниям указывается на намеренное использование «нейтральных» формулировок, позволяющих широко толковать содержащиеся в Указаниях нормы. В результате широты используемых формулировок «новые формы вредоносных программ или преступлений всегда будут охватываться Конвенцией». В настоящее время Конвенцию о киберпреступности дополняют изданный Советом Европы Протокол о ксенофобии и расизме, проекты Комитета по конвенции о киберпреступности (T-CY) и программы технического сотрудничества в области борьбы с киберпреступностью [54].

Одним из направлений регулирования указаний предлагается считать контроль за появлением и последующей деятельностью ботнетов. «Ботнеты могут быть использоваться для совершения или оказания помощи, или содействия совершению нескольких типов преступлений», перечень которых представлен в Конвенции о киберпреступности. Создатели Указаний отмечают, что одна сторона может предусмотреть в своем внутреннем законодательстве санкции, которые в итоге оказываются недостаточными для бесповоротного прекращения преступлений, связанных с ботнетами. В таком случае может не допускаться рассмотрение отягчающих обстоятельств, наличия прямого намерения, пособничества или подстрекательства. Последнее может повлечь за собой необходимость корректирования внутреннего законодательства стран, ведь отсутствие правового видения отягчающих обстоятельств может в свою очередь нарушать действующее международное законодательство в области защиты общих прав и свобод человека и гражданина, включая право на невиновность. Сторонам-участникам следует уделить внимание широкому влиянию ботнетов и виртуальных атак, влекущих за собой наступление санкций за различные уголовные преступления [53]. Необходимо сделать акцент на необходимости

обеспечения трансграничного доступа к данным (ст. 32 Будапештской конвенции). Кстати, данная конвенция не была ратифицирована на территории Российской Федерации. Россия оставила за собой право принимать решение о своем участии в Конвенции с учетом возможного пересмотра положений пункта «б» статьи 32, что «может нанести ущерб суверенитету и безопасности государств-участников конвенции, и правам их граждане». В этом пункте говорится, что «Сторона может без согласия другой стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получить их, если эта сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой стороне через такую компьютерную систему» [16].

Африканский союз сотрудничает с Управлением программы Совета Европы по борьбе с киберпреступностью (C-PROC) в рамках проекта «Расширенные глобальные действия по борьбе с киберпреступностью» (GLACY+). Рост киберпреступности в Африке побудил правительства разработать «надежные основы для обеспечения кибербезопасности в Африке». Основными направлениями будущего правового регулирования виделись в 2011 году организация электронных операций, защита персональных данных, усиление кибербезопасности электронного управления и общая линия борьбы с киберпреступностью [58].

Советом Европы с целью содействию укреплению потенциала в области предупреждения киберпреступности было создано особое Управление по программе в области киберпреступности [55]. Результатом работы данного Управления в том числе стала согласованная Африканским союзом в июне 2014 года Конвенция Африканского союза о кибербезопасности и защите персональных данных. Данная Конвенция сосредоточена главным образом на проблемах электронных операций, защиты данных и поддержанию безопасности в киберпространстве. В правовом отношении в ней явно выделяются три основные области правового регулирования:

– электронные транзакции,

– защита персональных данных,

– предотвращение киберпреступности.

Соглашение СНГ – Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности – было принято Решением Совета глав государств СНГ от 10 октября 2008 года с целью усиления сотрудничества в сфере обеспечения информационной безопасности. Российская Федерация входит в состав государств-участников данного соглашения и приняла соответствующие нормативные правовые акты [47, 34]. Решение явилось ответом на принятие необходимости усиления правового регулирования растущих угроз, связанных с использованием новых информационно-коммуникационных технологий. «Принимая во внимание важное значение информационной безопасности для реализации основных прав и свобод человека и гражданина», участники СНГ в сфере обеспечения информационной безопасности стремятся «создать правовые и организационные основы сотрудничества государств СНГ» [40].

Конвенция Лиги Арабских государств о борьбе с преступлениями в области информационных технологий дополняет принятые арабские и международные договоры, хартии о правах человека, обеспечивает гарантированные уважение и защиту. Конвенция принимает во внимание «высокие религиозные и моральные принципы, особенно предписания исламского права (шариата), а также культурное наследие арабской нации, отвергающее все формы преступления и поддерживающее общественный порядок в каждом штате» [57]. Конвенция становится необходимой частью общей уголовной политики, направленной на защиту арабского общества от преступлений, связанных с информационными технологиями» [52].

Эффективность неофициального международного сотрудничества имеет особое значение в раскрытии преступлений, связанных с использованием компьютерных технологий. Значительные временные

задержки, возникающие по причине соблюдения всех необходимых правовых формальностей при использовании официальных механизмов, могут негативно сказываться на эффективности раскрытия киберпреступлений с «неустойчивыми цифровыми доказательствами».

Можно отметить, что, учитывая повышенную общественную опасность для общества преступных деяний в сфере компьютерной безопасности, можно говорить о том, что международное сообщество сейчас находится в стадии формирования глобального информационного сообщества, что позволит облегчить взаимодействие правоохранительных органов различных стран в процедуре выявления преступлений и привлечения к юридической ответственности. Коме того, очень важно отдельным странам создать единое правовое поле для регулирования общественных отношений в сфере компьютерной безопасности, поскольку преступные деяния в данной сфере характеризуются космополитизмом и игнорированием территориальных границ.

Необходимо создание развернутой и единой инфраструктуры по всему миру, необходимой для полноценного и профессионального проведения расследования преступных деяний в данной сфере.

Поскольку преступления, совершаемые с применением компьютерных технологий, давно вышли за пределы отдельного государства, то для борьбы с ними необходимо объединить усилия Российской Федерации с международным сообществом путем ратификации международных договоров и включения унифицированных норм международного права в данной области в национальное законодательство, в том числе и уголовное.

1.3 Анализ уголовного законодательства РФ

В Российской Федерации вопросами обеспечения информационной безопасности занимается Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

Тенденции развития внутреннего регулирования преступлений, связанных с использованием компьютерных технологий, в Российской Федерации отражены в Программе МВД России «Создание единой многоинформационной телекоммуникационной системы органов внутренних дел» [33], особое внимание в которой уделяется регулированию преступлений с использованием телекоммуникационных, информационных и биометрических данных.

Наибольшую трудность, по мнению сотрудников МВД, представляет раскрытие преступлений, совершаемых против собственности. Это объясняется спецификой механизма совершения данного вида преступлений: сравнительная лёгкость совершения деяния, высокая скорость распространения по Интернет-сети, широкий охват и частая сложность обнаружения подлинного виновника деяния. Особо выделяются сотрудниками МВД преступления, совершаемые через банковские счета. Раскрываемость подобных преступлений напрямую зависит от своевременного оповещения уполномоченных органов о произошедшем правонарушении.

Сохраняют свою актуальность мошенничество через SMS / MMS-оповещения, а также иные формы телефонного мошенничества [21].

Сравнительно новым типом угроз становятся возрастающие правонарушения с использованием мобильных приложений. Рост рынка мобильных приложений сопровождается появлением новых типов правовых угроз, в числе которых нарушение авторских прав пользователей, загружающих в приложения авторский контент, подмена приложений на его вредоносную копию, нарушение прав пользователей через условия пользовательского соглашения, утечка персональной информации в Интернет [6].

Особым образом регулируется деятельность сотрудников органов внутренних дел, по долгу службы осуществляющих приём персональных и государственных данных. Деятельность сотрудников ОВД регулируется на

основании нормативных правовых актов Российской Федерации, ведомственных и межведомственных приказов, распоряжений и инструкций.

Для наглядности необходимо провести анализ главы 28 Уголовного Кодекса Российской Федерации.

Статья 272 Уголовного кодекса Российской Федерации предусматривает незаконный доступ к компьютерной информации, охраняемой законом, если эта деятельность была связана с уничтожением, блокировкой, изменением или копированием компьютерной информации. Из положения статьи можно сделать вывод, что состав данного правонарушения наносит значительный ущерб. Говоря о санкциях, следует отметить, что до недавнего времени компьютерные информационные преступления относились к преступлениям средней тяжести, за исключением ч. 2 ст. 273 УК РФ является тяжким преступлением.

В статье 273 УК РФ необходимо детально рассмотреть части 1 и 2, которые имеют формальный состав, и их содержание вызывает ряд вопросов.

В соответствии с ч. 1 ст. 273 УК РФ создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

В соответствии с ч. 2 ст. 273 Уголовного кодекса Российской Федерации деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности.

Следует отметить, что в частях 1 и 2 ст. статье 273 Уголовного кодекса Российской Федерации, законодательный орган не определяет характер субъекта вмешательства, как в статьях 272 и 274 Уголовного кодекса Российской Федерации. Это, на наш взгляд, значительно затрудняет применение данной статьи, поскольку без указания информации как

компьютерной информации, охраняемой законом, существует конкуренция между применением статьи 273 Уголовного кодекса Российской Федерации или статьи 146 Уголовного кодекса Российской Федерации.

Принимая во внимание положения ч. 1 и ч. 2 в статье 273 Уголовного кодекса Российской Федерации, можно предположить, что лицо, использовавшее программу для копирования информации, преследовало цель, например, получение прибыли, использовало ее в свою пользу, но при этом заблуждалось в оценке последствий использования этой программы. При этом сама программа, как и в принципе компьютер, имели прикладное значение, а мотивы и цели были совершенно разными. Хотя в ст. 273 Уголовного кодекса Российской Федерации мотивы и цели не имеют квалифицирующего значения, слова «использование компьютерных программ, заведомо предназначенных для …» вызывают аналогичное толкование и понимание данной статьи.

Вместе с тем, нельзя не согласиться с тем, что лицо осознает потенциальную опасность при создании и распространении программ, и поэтому определение состава как формального оправданно, но на наш взгляд было бы логичнее выделить в самостоятельный состав использование этих программ, определив состав как материальный.

Таким образом, на наш взгляд, современное российское уголовное законодательство не содержит нормы, которые принципиально решали бы вопрос уголовной ответственности за «киберпреступления». Наличие трех статей в главе 28 УК РФ не только является недостаточной в решении существующих задач, но создает проблему для правоприменителей.

Глава 2 Классификация посягательств, совершаемых с использованием компьютерных технологий

2.1 Теоретические основания классификации преступлений, совершаемых с использованием компьютерных технологий

В качестве первой классификационной группы рассмотрим преступления против жизни, совершаемые в сети-Интернет.

Преступления такого рода звучат очень странно, поскольку еще недавно не было такого понятия как преступление против жизни человека, совершаемые в интернете. Однако, на сегодняшний день такие преступления наносят ущерб здоровью людей и их финансовому состоянию, а также жизни.

Самым известным случаям совершения убийства человека с помощью интернета была ситуация, когда важного свидетеля убили посредством подключения к его кардиостимулятору и изменения его настроек, что привело к смерти человека. Этот случай произошел в США в 1998 году, а убитый являлся свидетелем, которого скрывали в стенах госпиталя на военной базе [19, с. 61].

Информационные технологии получили очень широкое развитие в наши дни, практически каждый человек имеет свое устройство, с помощью которого он выходит во всемирную паутину или просто поддерживает связь. Благодаря этому преступники получают всё больше способов для совершения преступлений. Если смотреть в будущее, то можно сделать прогноз, что виды таких преступлений будут только увеличиваться: так, могут быть захвачены управляемые с помощью компьютеров и искусственного интеллекта самолёты, машины и поезда, а нанесение вреда жизни и здоровью может быть совершено при получении доступа хакеров к новым и разрабатываемым устройствам поддержания жизни.

Преступники также могут использовать интернет для получения личной информации о жертве, на основе которой будет подготавливаться само

преступление. Так, преступники могут собрать информацию о месте проживания жертвы, её социальное состояние, наиболее часто посещаемые места и расположение работы и т. д. С помощью интернета преступники могут осуществлять поиск необходимого орудия преступления, организации нападения и сбора группы, шантажа, пособничества – всё это можно осуществлять через Darknet без особого труда, стоит только воспользоваться защищенными каналами связи.

Однако, в Российской Федерации угрозы убийства или нанесения вреда здоровью, которые получили свое распространение посредством социальных сетей, различных электронных почтовых ящиков, обмена сообщений в разных мессенджер приложениях и т.д. относятся в Уголовном кодексе Российской Федерации к ст. 119. А именно: наступление ответственности за угрозу жизни и причинение тяжкого вреда здоровью [8].

Сегодня наблюдается тенденция зависимости людей, особенно молодёжи от социальных сетей. В частности, на психику морально неокрепших личностей влияют лайки, буллинг в социальных сетях, активные призывы к совершению каких-либо действий и присоединение к какой-либо девиантной субкультуре. Таким образом, возникла так называемая мода на самоубийства. Уголовный кодекс Российской Федерации имеет статью - доведение до самоубийства ст. 110. Несмотря на то, что, что статья является очень серьезной, доказать причастность к призыву и доведения до самоубийства очень сложно, особенно, если в этом участвовал преступник, который является специалистом в ИТ сфере. Существование групп и клубов для самоубийц в социальных сетях приводят к печальным последствиям, а инструкции и указания для совершения самоубийств реализуются в реальности. Это делает нормой в сознании людей такое явление как самоубийство.

Однако, на практике количество дел, открытых по данной статье, имеет небольшое число. Хотя ещё в 2013 году уже был прецедент вынесения

приговора за доведение до самоубийства посредством использования сети интернет.

Суть дела была в том, что молодая девушка Анна Семененко довела до самоубийства своего бойфренда, который ее бросил. Мотив преступления состоял в желании отомстить своему бойфренду за расставание с ней. Девушка завела несколько анкет в социальных сетях и начала спам-рассылку о том, что её молодой человек имеет нетрадиционную ориентацию, это повлияло на психику парня и привело к самоубийству. Дело рассматривалось очень долго, доказательства также собирались долго, в результате рассмотрения дела девушка была приговорена к 31 году проживания в колонии-поселении [7].

Появление нового способа самоубийства повлияло на и без того высокую статистику смертности в результате самоубийств. Законодательство Российской Федерации должно реагировать на такие события и вносить необходимые коррективы. Для этого необходимо внести в ст. 110 дополнение в виде того, что он доведение до самоубийства является опасным явлением, которое наносят огромный вред обществу. Стоит также отметить создание «Единого реестра доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» [32]. Данный документ помогает в борьбе с совершениями населением самоубийств.

С помощью интернета преступник может осуществлять свои преступные действия по всему миру, что может нанести вред жизни большому количеству людей. Особенность использования сети интернет для совершения преступлений заключается в том, что злоумышленник чувствует себя безнаказанным, интернет является для него своеобразным способом защиты от наказания, его уверенность в своих силах повышается. Хотя, нельзя однозначно сказать о том, что наблюдается рост убийств при помощи использования интернета.

Ко второй группе отнесем преступления против свободы, чести и достоинства личности.

На сегодняшний день интернет является универсальным средством распространения массовой информации и обладает такими характерными чертами как анонимность, стремительное распространение сведений и данных, а также наличие большой аудитории. Однако, интернет обладает чрезмерной свободой слова, что может нанести вред обществу. Это происходит в результате отсутствия контроля государственных органов. Пользователи всемирной сети часто могут высказываться по каким-либо поводам и в отношении кого-либо лица, не неся при этом никакой ответственности. Такие высказывания могут иметь негативную окраску и быть потенциальной клеветой, носить оскорбительный характер.

Данный пункт можно отнести к ст. 128.1 то, то есть распространение заведомо ложной информация, которая порочит честь и достоинство другого человека, наносит вред репутации. Сюда можно отнести любой вид информации – голосовое сообщение, фото и рисунки, а также в письменной форме. Таким образом преступник может распространить заведомо ложную информацию в отношении конкретного человека на широкую аудиторию. Распространение информации при помощи интернета и социальных сетей получают очень широкую огласку. А возможность работать анонимно в социальных сетях делает поиск преступников, которые распространяют клеветнические данные, очень сложно. Часто появляются такие виды преступления в интернете, как сфабрикованным фото и видео с участием того или иного лица.

Таким образом, в статью 128.1 необходимы дополнения, связанные с распространением клеветы и оскорбительных выражений в сети интернет, в том числе с помощью использования социальной сетей. Это поможет пресечь распространение в интернете клеветы, наказать преступников за их совершенное противоправное деяние.

Третью группу составляют преступления против конституционных прав и свобод человека и гражданина.

На сегодняшний день жертвы преступлений зачастую сами провоцируют совершение преступления против них мошенниками, так как они оставляют свои личный конфиденциальные данные в социальных сетях, блогах, форумах. Сведения, находящиеся на компьютере пользователя, а также информация, которая проходит через передачу электронных сообщений является доступной для преступников, которую они могут получить с использованием преступных методов. Таким образом, преступники совершают преступления, обозначенные в ст.137 и ст.138 как «Нарушение неприкосновенности частной жизни» и «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений». При этом данные виды преступления претерпели модернизацию, получили более доступный и быстрый способ совершения преступлений.

Согласно ст.137 преступление характеризуется двумя действиями:

- преступник может ознакомиться с личными конфиденциальными данными жертвы непосредственно в его месте проживания, месте работы, либо у его родственников. При этом преступник не совершает кражи документов потенциальной жертвы, только анализирует информацию о ней. Таким образом, интернет является универсальным инструментом для ознакомления с потенциальными данными о жертве;
- распространение сведений о личной жизни жертвы может совершаться различными путями: в устной форме, в письменной форме, а также при помощи использования средств массовой информации. Интернет при этом не выделяется как место распространения конфиденциальных данных, однако не исключается. К распространению данных о личной жизни жертвы относятся действия, направленные на сообщение заинтересованным лицам таких сведений.

На сегодняшний день получила широкое распространение развитие информационных технологий в том числе использование мобильных телефонов практически каждому человеку. При помощи использования различных методов перехвата информации, преступник может получить практически любые конфиденциальные сведения о потенциальной жертве.

Россия занимает одно из ведущих мест, где совершаются преступления в отношении нарушения прав авторских и смежных.

Ответственность за преступления, совершенные с целью кражи личных конфиденциальных сведений наступает согласно ст. 146 Уголовного кодекса Российской Федерации. Однако, стоит отметить, что пользователи интернета также виноваты в том, что преступники совершают такую деятельность. Низкий уровень образования в сфере ИТ-технологий, знание основных правил защиты персональных данных и свободное распространение персональных данных в интернете, а также скачивания нелегальных копий различного контента приводят к тому, что хакеры могут получить доступ к персональным компьютерам пользователей, а также информации, которая передается по локальной сети.

В ст. 146 УК РФ нормативно закреплено определение «Интеллектуальная собственность»: это результат творческой деятельности человека, которая не зависит от сферы осуществления деятельности. Это можно назвать объектом авторского права, которое существует в виде опубликованных и неопубликованных работ и выражено в какой-либо форме: устной, в письменной форме или фото и видео контент и т.д. Любой результат деятельности – товар, произведение, статья оцифровывается и выставляется в интернет в электронном виде. Среди пользователей распространено скачивание такого контента, как видео, аудио, книги, пиратские версии компьютерных программ и т. д. Количество скачиваемых файлов во всемирной паутине такое огромное, что его просто невозможно регулировать, соответственно государство не имеет таких инструментов для осуществления контроля. Автор произведения, которое скачивается пользователем

бесплатным пиратским способом получает ущерб, таким образом наступает ответственность по ст. 146 Уголовного кодекса Российской Федерации.

Довольно давно уже существует такая программа, как торрент-трекер, когда пользователи обмениваются программами и файлами, в том числе и теми, которыми они делиться не имеют права. В некоторых европейских странах торрент-трекеры были приравнены к пиратским в силу того, что они нарушают авторские права, в России пока такого не произошло. В Российской Федерации предусмотрено наказание за распространение нелицензионных товаров, при этом наказание за опубликование различных видов файлов не предусмотрено.

Авторы программ и различных произведений получают серьёзный экономический ущерб, поэтому данный вид преступлений представляет собой серьезную опасность. Если, например, в создании кинофильма участвовало государство, то оно недополучит прибыль. В данную статью необходимо внести дополнение: «…как преступление, которое было совершено при использовании интернета и информационно-коммуникационной сети».

К четвертой группе относятся преступления против семьи и несовершеннолетних.

Так как дети имеют доступ к интернету сегодня, они также могут быть вовлечены в противоправную деятельность и совершение преступлений посредством использования сети интернет. Привлечение детей к совершению преступлений и наступление ответственности за это предусматривается статьей150 УК РФ. Действие преступника при этом заключается в том, чтобы привлечь к преступной деятельности ребёнка путем угроз, обмана, ложных обещаний или любым другим способом воздействия на сознание ребёнка, кроме насилия. Данные действия могут быть совершены не только непосредственно, но также удалённым способом. Интернет — это универсальный инструмент для преступника для привлечения к преступной деятельности детей, поскольку общение в интернете с ребенком полностью анонимно, преступник имеет большой выбор жертв, так как очень много детей

сегодня имеют доступ к интернету. Преступник ищет психологически неустойчивую личность, которая не знает о возможности вовлечения её в противоправную деятельность, или наоборот хочет вступить в деятельность для совершения какого-либо преступления.

Привлечь ребенка к совершению преступления для опытного преступника в сфере ИТ пространства является нетрудной задачей, достаточно лишь показать все возможности и преимущества взломов программ и сайтов в пространстве интернет.

Часто подросток может быть вовлечен в совершение антиобщественных деяний, статья по которым предусмотрено ст. 151 УК РФ, в интернете можно найти призывы к употреблению различных психотропных веществ, алкоголя и т.д. Социальные сети располагают широкой возможностью для привлечения внимания подростков и призыва к совершению антиобщественных деяний.

Чем более популярен сайт или социальная сеть, которая осуществляет такие действия, тем больше возможности реализации целей, для которых это осуществляется. Однако, правоохранительные органы не могут справиться с задачей предотвращения вовлечения подростков к антиобщественной деятельности, большую роль здесь должны сыграть родители. Родители должны разговаривать с подростками и объяснять те или иные события.

Пятую группу, и пожалую, самую обширную, составляют преступления против собственности преступления в сфере экономической деятельности.

Интернет обладает множеством возможностей, которые позволяют преступнику совершать различные схемы мошеннических действий и обманывать пользователей. Объяснение этому очень простое – мошенник пользуется анонимностью в интернете, может поменять свой социальный статус, изменить возраст и профессию, то есть выдать себя за абсолютно другую личность. Таким образом, киберпреступники имеют множество преимуществ, которые его отличают от обычных преступников. Для совершения преступления в интернете существует множество схем действий, которые позволяют обманным путем получить денежные средства от

потенциальных жертв. Данные действия при этом не являются сложной задачей для преступников, поскольку зачастую сами жертвы выходят на преступника, отвечая на рассылки преступников в интернете или иные действия. Можно сделать вывод, что интернет позволяет сделать многие из преступлений и их стадий совершения против собственности людей, кроме применения насилия [38].

В 2012 году в Уголовный кодекс РФ была введена ст. 159.6 предусматривающая ответственность за совершение мошенничества в сфере компьютерной информации, то есть хищения чужого имущества или приобретения 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.

Интернет облегчает совершение противоправных действий для преступников, так как он обеспечивает злоумышленнику полную анонимность и сохранение конфиденциальности при пользовании сетью интернет. Интернет обладает не только анонимностью, которая позволяет преступнику совершает различные противоправные деяния, он обладает также мгновенностью: преступник может мгновенно отправлять сообщения жертве, жертва может мгновенно совершать финансовые операции и распоряжаться денежными средствами посредством использования электронных платежей.

Социальные сети являются идеальной платформой для совершения преступлений преступниками, поскольку они имеют очень большую аудиторию, а сам контент, который размещается в сетях, редко контролируется администрацией социальных сетей на предмет наличия мошеннических действий с целью совершения противоправных деяний. Всё это в совокупности приводит к росту схем для совершения преступлений в различных социальных сетях, что в свою очередь приводит к росту подобного рода преступлений.

В интернете есть множество возможностей для создания и разработки собственных сайтов, что позволяет пользователям интернета открывать интернет-магазины, платформы для оказания услуг и т.д. Таким образом мошенники имеют много возможностей для осуществления предпринимательской деятельности посредством использования интернет-магазинов, они зачастую обманывают покупателей. Деятельность, которую они осуществляют, не имеет соответствующих разрешений и лицензий, таким образом это относится к категории осуществление незаконной деятельности согласно ст. 171 Уголовного Кодекса Российской федерации. Помимо осуществления незаконной предпринимательской деятельности мошенники осуществляют также и ведение деятельности в банковской сфере, что относится к статье 172 171 Уголовного кодекса РФ.

Преступления в сфере банковской деятельности характеризуются осуществлением различных банковских операций без разрешений и лицензий, которые необходимы для этого. Банковские операции здесь совершаются с помощью таких платежных систем как PayPal, WebMoney и другие системы перечисления денег в электронном формате. Также отмечается рост организаций, которые является посредником в сфере осуществления финансовой деятельности и при этом не имеет никаких соответствующих для этого лицензии. Широкое распространение получили обменные пункты, с помощью которых можно вывести денежные средства заграницу или обменять деньги без какого-либо документального оформления [2]. Таким образом происходит легализация доходов, которые были получены при совершении преступных действий статья уголовный кодекс Российской Федерации (ст.ст. 174, 174.1 Уголовного кодекса РФ), организация и проведение азартных игр в Интернете (ст. 192.1 Уголовного кодекса РФ), не говоря уже об уклонении от уплаты налогов (ст. 198, 199 Уголовного кодекса РФ).

Совершение финансовых операций в интернете зачастую не оставляет за собой цифровых следов, что очень выгодно для преступников. Использование преступниками защищенных соединений, например VPN,

делает сложным операцию их идентификации и определения того персонального компьютера, с которого были совершены противоправные действия, связанные с денежными средствами.

В интернете частым явлением является совершение нескольких преступных действий одновременно, так, преступники могут оплачивать порнографические материалы посредством использования системы электронных платежей PayPal, провести идентификацию таких преступников очень и очень сложно. Киберпреступники в сфере интернета таким образом совершают преступление, которое относится к главе 22 Уголовного кодекса Российской Федерации и нарушает границы государства.

Распространение виновным лицом ложных сведений в сфере рынка ценных бумаг и акций с помощью использования средств массовой информации, интернета и других средств связи является противоправным действием, если таким образом оказывается влияние на конъюнктуру рынка - спрос, цена, предложение, объем торгов и финансовой валюты. Если результаты таких торгов существенно отличаются от тех, которые могли бы быть при нормальных условиях осуществления данного вида деятельности, то это противоправное действие можно отнести к статье 185.3 Уголовного кодекса Российской Федерации.

В седьмую группу выделяем преступления против общественной безопасности.

Кибернетический терроризм (кибертерроризм) является одной из самых распространенных угроз деятельности в пространстве интернет, так как интернет проникает практически во все сферы жизнедеятельности человека.

Кибертерроризм на сегодняшний день в интернете прогрессирует, так как интернет обладает всеми необходимыми качествами своего развития, а именно большая аудитория, анонимность преступника, доступность к большому массиву информации и многое другое. А отсутствие цензуры на распространяемый контент способствует развитию разной негативной

информации, угроз, сообщений, которые могут оказать отрицательное воздействие на подсознание и в целом на психику человека.

Сейчас можно отметить тревожное состояние населения в связи наличием множества пабликов, форумов и групп на просторах интернета, которые дискредитируют государство и его направления деятельности. А наличие сайтов, которые имеют целью распространения террористической информации, а также наносящих вред определенным системами путём поделки данных и вывода их из строя с помощью специализированных программ, наносит огромный ущерб и является своеобразным дополнением к основному виду терроризма. Такие преступления, совершенные в киберпространстве, можно отнести к ст. 205, 205.1, 205.2 Уголовного кодекса РФ.

В Российской Федерации специальными службами отслеживается информация и появление новых сайтов, которые распространяет негативный и противозаконный контент, призывает к совершению преступных действий, наносят непоправимый вред государству. Этим занимаются специальные подразделения МВД Российской Федерации, они проверяют информационные ресурсы, которые носят экстремистский и террористический характер. Стоит отметить, что за последнее время было обнаружено более 70 сайтов, которые носят подобный характер. МВД России принимает решение о закрытии таких сайтов и привлечение к уголовной ответственности лиц, которые занимаются распространением подобного рода информации [5]. Однако, это не мешает владельцам закрытых сайтов открывать их заново как на отечественных платформах, так и на зарубежных, используя различных поставщиков услуг связи и телекоммуникаций. Будет полезным налаживание контактов в международной сфере между странами для ликвидации сайтов, содержащих такой контент и их собственников, так как при закрытии сайта в одной стране, как правило, они открывают сайты подобной направленности на хостингах других стран. Установление международных отношений со странами СНГ

помогает преодолеть повышающийся уровень международной преступности в сети интернет.

Интернет может стать источником для вербования людей, для совершения террористических актов, информации о совершении тех или иных террористических актов, и, соответственно, дает возможность террористам обмениваться информацией непосредственно. Интернет очень удобен для террористов в этом плане, потому что он обладает, как уже было выше сказано, анонимностью, для него не существует границ, он по своей сути глобален и распространён во всем мире, имеет огромную аудиторию, которая потенциально может быть вовлечена в террористическую деятельность.

Всемирная сеть используется террористами для организации таких явлений как массовые беспорядки, совершение таких незаконных операций как организация массовых беспорядков (ст. 212 Уголовного кодекса РФ), покупка оружия, взрывчатого устройства, запасных частей и патронов для незаконного оружия (ст. 222 Уголовного кодекса РФ) и т.д. При помощи использования защищенных каналов связи и интернета террористы могут обмениваться непосредственно информацией, которая касается противоправного изготовления оружия и боеприпасов (ст. 223 Уголовного кодекса РФ). Распространению с помощью интернета информации о террористических актах и призыв к ним наносит большую угрозу для общественности, широкое распространение такой информации может нанести огромный вред и привести к тяжелым результатам [41].

Восьмую классификационную группу составляют преступления против здоровья населения и общественной нравственности.

Глава 25 Уголовного кодекса Российской Федерации распространение информации с помощью интернета, которые наносят вред здоровью населения и нравственности в обществе.

Сегодня практически везде в интернете можно найти информацию о наркотических веществах, способов их изготовления, способов их

употребления. Если использовать Darknet и защищенные каналы связи, то преступник может найти поставщиков наркотических веществ напрямую.

В случае, если установлено, что преступник склонял свою жертву к употреблению наркотических веществ, а также психотропных и их аналогов, то преступник может быть привлечен к статье 230 Уголовного кодекса Российской Федерации. Здесь необходимо включить дополнение, которое касается совершения противоправного действия, направленного на склонение к употреблению наркотических веществ с помощью сети интернет.

Помимо распространения наркотиков посредством сети интернет, огромной проблемой является распространение порнографической продукции через сеть интернет и её изготовление с использованием видео и изображений несовершеннолетних (ст. 242.1 Уголовного кодекса Российской Федерации), а также вовлечение и использование труда несовершеннолетних в изготовлении порнографических материалов и предметов (ст. 242.2 Уголовного кодекса Российской Федерации).

Поскольку данный вид бизнеса приносит большую прибыль преступникам, он имеет широкое распространение и является серьезной проблемой. Существует широкая сеть группировок, которая занимается вербовкой несовершеннолетних в данный вид бизнеса, размещается реклама, они занимаются распространением порнографической продукции, а также осуществляют денежные операции, связанные с этим бизнесом, посредством использования электронных платежей [49].

Сеть точно также используется и при незаконном изготовлении и обороте порнографических материалов или предметов (ст. 242 Уголовного кодекса РФ).

Как уже упоминалось ранее, в октябре 2012 года был принят «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в

Российской Федерации запрещено» или как его окрестили в народе – «Черный список сайтов».

Данный документ создан для поиска, обнаружения и остановки деятельности веб-страниц, которые, согласно указанному документу, имеют запрещенные сведения:

- сведения, которое распространяются в сети интернет и имеют следующую направленность: привлечение несовершеннолетних подростков для участия в создании порнографического материала либо участие в соответствующих мероприятиях, а также работа над фотографиями порнографического характера, продажи порнографических материалов;
- сведения, которое содержат в себе советы и способы создания наркотических веществ, также психотропных веществ и их аналогов, сведения о местах продажи этих веществ, сведения о местах выращивания наркотических растений и культур, способах совершения самоубийства и призывов к самоубийству, которые размещается в сети «Интернет».

Девятую группу собственно относятся преступления в сфере компьютерной информации.

Согласно Главе 28 Уголовного Кодекса Российской Федерации обеспечивается сохранность отношений в обществе в сфере компьютерной информации. Противоправный доступ к информации, которая размещена на компьютере (ст. 272 Уголовного кодекса Российской Федерации) может происходить и без возможности использования интернета, но широкое распространение сети «Интернет» влечет за собой увеличение числа преступлений, связанных с компьютерной информацией. Объектом преступления может стать абсолютно любой компьютер, независимо от его статуса - компьютер обычного пользователя или компьютер государственного служащего, имеющего конфиденциальные сведения.

Несмотря на то, что создание и распространение программ, с помощью которых хакеры могут взламывать компьютерную информацию (ст. 273 Уголовного Кодекса Российской Федерации) возможно только при наличии компьютера, но наибольшей угроза обществу происходит при распространении таких хакерских программ с использованием сети «Интернет». Вирусной программой или вредоносной называется такая программа, которая может совершать кражу информации с компьютера, повредить её, а злоумышленник может шантажировать пользователя с целью вымогания денежных средств за компьютерную информацию и т.д. Однако, в законодательстве отсутствуют критерии, согласно которым ту или иную программу можно отнести к вредоносной и наносящей угрозу жизни общества. Для отнесения программы к вредоносной необходимо провести соответствующую экспертизу с соблюдением всех необходимых тонкостей. Создание, использование и распространение вредоносных программ (ст. 273 Уголовного кодекса РФ) стало возможным только с появлением компьютеров, но, как и преступление предусмотренной ст. 272 Уголовного кодекса РФ, наибольший вред оно наносит именно при доступе к сети «Интернет».

Наибольшие угрозы могут нанести такие вирусы, которые могут самостоятельно распространятся и самовоспроизводиться. Такого рода вредоносные программы могут быть использованы при совершении различного рода преступных деяний, предусмотренных ст.ст. 105, 128.1, 137, 138, 205, 281 Уголовного кодекса РФ.

Хакерские программы могут нанести непоправимый вред как обществу, так и государству, поэтому в ст. 272 и ст. 273 Уголовного кодекса Российской Федерации необходимо внести дополнение о совершении преступления с помощью использования сети «Интернет».

Согласно ст. 274 Уголовного кодекса Российской Федерации пользователь компьютера может быть привлечен к ответственности при неправильном использовании компьютера и несоблюдения средств защиты информации. Сюда можно отнести нарушение правил пользования и

хранения, обработки и отправки очень важной конфиденциальной информации, а также нарушение правил доступа к сетям.

Наконец десятую группу преступлений, совершаемых с использованием сети-Интернет представляют преступления против конституционного строя и безопасности государства.

С помощью сети «Интернет» злоумышленник может совершить преступление и получить нелегитимным путем сведения пользователей и различных фирм, но и также получить доступ к сведениям, составляющим государственную тайну. С появлением Интернета значительно возросла общественная опасность преступлений, предусмотренных Главой 29 Уголовного кодекса РФ. Непосредственно с помощью Интернета могут совершаться: государственная измена (ст. 275 Уголовного кодекса РФ), шпионаж (ст. 276 Уголовного кодекса РФ), публичные призывы к осуществлению экстремистской деятельности (ст. 280 Уголовного кодекса РФ), диверсия (ст. 281 Уголовного кодекса РФ), возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 Уголовного кодекса РФ), разглашение государственной тайны (ст. 283 Уголовного кодекса РФ), утрата документов содержащих государственную тайну (ст. 284 Уголовного кодекса РФ). Целесообразно дополнить эти статьи, указав, что данные преступные действия могут быть совершены посредством использования информационно-коммуникационных сетей.

На основании вышеизложенных фактов охарактеризуем преступления, совершаемые с помощью компьютерных технологий и сети «Интернет»:

- понятием «интернет-преступление» можно охватить практически всю Особенную часть УК РФ;
- доступность и бесконтрольность глобальных сетей, в том числе для несовершеннолетних и прочих незащищенных слоев населения, позволяет говорить о повышенной общественной опасности преступлений в сфере компьютерной информации;

– интернет-технологии в преступных деяниях могут использоваться как на стадии подготовки, так и на стадии непосредственного совершения деяния, а также для сокрытия следов преступного деяния;
– доступность и, в то же время, определенная анонимность при совершении интернет-преступления вызывает у субъекта чувство безнаказанности, поэтому можно говорить здесь и о повышенной общественности опасности самого преступника;
– и, как следствие вышесказанного – несовершенство технических средств и возможности анонимности глобальных сетей зачастую позволяют преступнику остаться безнаказанным.

Естественно, что необходимы дополнения для классификации признака относительно того, что преступление было совершено посредством использования интернета. Однако, в данном случае совершение преступления с помощью сети «Интернет» должно являться стандартным способом осуществления противоправного действия, наносящего вред обществу. Данное изменение наиболее необходимо в ст.ст. 110, 128.1, 137, 138, 146, 150, 151, 174, 174.1, 205.1, 205.2, 230, 242, 272, 273, 280 Уголовного кодекса РФ.

Исходя из вышесказанного, нужно сделать вывод о необходимости контроля со стороны государства сети «Интернет» с целью снижения интернет – преступности. Этого можно достичь при усовершенствовании нормативно-правовую базу в вопросах регулирования отношений, возникающих в сети Интернет.

2.2 Мотивация «компьютерных» преступлений

Преступления в интернет-пространстве связаны прежде всего с развитием информационных технологий и их внедрением. Однако, при сравнении преступлений в интернет-пространстве с другими видами

преступлений, первые превосходят своим числом вторые. Это может быть объяснено следующим:

- рост аудитории всемирной сети и пользователей программно-вычислительной техники;
- совершенствование навыков и знаний преступников в сфере ИТ, освоение новых программ с целью совершения противоправных действий;
- постоянное развитие и усовершенствование в сфере информационных технологий.

Таким образом, широкое распространение и усовершенствование информационных технологий приводит к росту киберпреступности в сети.

Однако, не только усовершенствование ИТ дает возможности для роста преступлений в сети, также рост киберпреступности обусловлен и иными причинами. Здесь можно выделить, например:

- в условиях существующей анонимности в глобальных сетях и технические возможности сокрытия существенно снижают риск привлечения к ответственности за преступное деяние;
- пропаганда в фильмах, книгах привела к появлению «новых героев-хакеров», которые за свободу информации и открытый доступ к ней, что привело к росту позитивного отношения к подобным преступникам со стороны общества;
- обилие информации, в том числе и по поводу способов совершения преступлений при помощи компьютерных технологий.

Киберпреступники при совершении преступления чувствуют себя безнаказанными, потому что очень тяжело правоохранительным органам идентифицировать их при совершении преступлений. Особенно это тяжело при совершении международных преступлений, так как в таком случае международное расследование и кооперация требуют значительных финансовых и иных ресурсов. Небольшой риск наказуемости и глобальность

являются главными факторами, которые влияют на повышение доступности в киберпространстве [22].

Совершение преступлений киберпреступниками становятся в современных реалиях в глазах общества благородным делом и пользуется лояльностью. Это связано прежде всего с тем, что киберпреступники передают бесплатно проприетарное программное обеспечение, которое было ими взломано, выражение свобода слова в интернете и прочие блага всемирной паутины. Таким образом, собственники бизнеса часто начинают вести теневой бизнес через интернет. а на защиту бизнеса становятся теневые киберструктуры, государственные органы в таком случае становятся для бизнеса угрозой [22].

В современном мире в сети «Интернет» можно найти множество советов и рекомендаций, способов совершения киберпреступлений, разбора алгоритмов совершения киберпреступлений и прочего материала, связанного с этим. Поэтому неудивителен рост преступлений в киберпространстве.

Преступники или группа преступников, которые имеют соответствующие знания, навыки и компетенции в области совершаемого ими ИТ преступления наносят обществу наибольшую угрозу и обладают следующими характеристиками: такие преступления являются международными и пересекают границы одного государства; преступники в сфере информационных технологий обладают навыками в автоматизированном режиме объединять несколько устройств в одно, что облегчает совершение преступления; преступник в сфере информационных технологий обладает всеми необходимыми навыками и умениями, повышает знания своевременно и достигает довольно высокого уровня в ИТ технологиях; преступления в сфере информационных технологий являются анонимными; совершение преступления осознается жертвой по прошествии какого-то времени, а не сразу поскольку преступление совершается в интернет-пространстве, у преступника нет необходимости контактировать с жертвой.

Исходя из вышесказанного, можно отметить, что рост преступлений в сфере информационных технологий растёт в связи с тем, что киберпреступники обладают высокими знаниями и умениями в этой сфере, тогда как общество является по сути своей низко образованным в этой сфере. Также рост киберпреступности объясняется анонимностью и глобальностью совершения киберпреступлений.

Преступления в сфере информационных технологий сегодня развиваются быстрыми темпами и имеют множество способов и методов осуществления преступных действий. Злоумышленники в интернет-пространстве становятся высококвалифицированными специалистами, которых обычным пользователям тяжело заподозрить в наличии мошеннических мотивов. Хакеры могут нанести угрозу как отдельным пользователям и бизнесам, так и государству в целом.

Кроме того, использование компьютера и Интернета позволяет преступникам совершать преступление более легким способом ввиду того, что эти преступления отличаются высокой степенью анонимности, быстротой и не требует большого количества денежных средств для осуществления действий. Также важно упоминать, что совершение противоправного деяния с помощью компьютера и интернета возможно из любой точки мира и может пересекать границы нескольких стран.

2.3 Классификация по объекту посягательств, совершаемых с использованием компьютерных технологий

При совершении преступления с применением информационных технологий для определения мотивов и целей преступления необходимо рассматривать его объективную сторону, так как субъективные влияют через внешнее поведение на общественную угрозу. При этом можно разделить объективную сторону противоправного деяния в сфере ИТ на само деяние и последствие совершенного деяния.

В уголовном праве можно выделить два подхода для разъяснения объективной стороны:

- элемент преступления, объективная сторона – это реальное явление, объективная сторона;
- элемент состава преступления – это элемент научной абстракции, которая необходима для более глубокого познания преступления [38].

Преступной деятельностью при этом можно признать поведение человека, сопровождающееся действием в активной фазе и бездействием в пассивной фазе. Исходя их этого, для привлечения к уголовной ответственности необходимо такое поведение человека, при котором оно носит преступный характер.

Действия при этом должны иметь умышленный характер и быть «волевым» поступком, как это указано в уголовном праве. Значение такого определения объясняется совершением действия, которое носит волевой характер, то есть человек должен совершить действие по собственной воле и желанию в зависимости от имеющихся условий и обстоятельств.

В случае, если человек совершил противоправное деяние по принуждению, под угрозой нанесения вреда здоровью и жизни или другими условиями непреодолимой силы, то такое преступление не может быть признано и человек не может быть привлечен к уголовной ответственности. Также в случае совершения преступления в соответствии с рефлексом, такое преступление не может быть отнесено к уголовной ответственности, так как невозможно это проконтролировать со стороны подсознания [12].

Согласно уголовному праву преступления можно разделить на действие и бездействие, в соответствии с этим подразделяются конкретные виды преступлений, на основании которых действует уголовное законодательство. То есть, в соответствии с нормами Уголовного права человек должен либо действовать определённым образом на какую-либо ситуацию, либо не должен совершать его под страхом привлечения к уголовной ответственности за

совершенное деяние. Таким образом, к человеку могут быть применены санкции и запреты уголовного права, в зависимости от совершения либо не совершения действия. Уголовно-правовое действие — это такое действие индивида, которое было совершено по собственной воле и желанию, которое наносит вред и угрозу обществу в соответствии с уголовным законом.

Уголовно-правовое бездействие - напротив выражает собой то действие, которое не было осуществлено, таким образом человек не выполнил своих юридических обязанностей.

Преступное деяние характеризуется тем, что наносит вред и угрозу жизни общества. В случае, если действия не наносят ущерб общественной безопасности, такое преступление не может быть объективной стороной состава преступления. А преступление должно быть общественно опасным, так как оно несет за собой предумышленное нанесение какого-либо вреда общественным отношениям. Таким образом, общественная опасность - это объективное свойство уголовно-правового деяния.

С помощью использования различных программно-вычислительных систем и компьютеров общественным отношениям может быть нанесен вред. Однако стоит отметить, что характер совершаемого преступления зависит от свойства объекта, такого как наличие компьютера при взломе компьютерной системы и кражи определённых конфиденциальных сведений.

Противоправное действие, которое совершено преступниками должно содержать в себе признаки, определенные уголовным законодательством, с одной стороны, и одновременно с этим противоправное действие является юридической характеристикой нанесения вреда общественным отношениям. Также уголовное законодательство дает трактовку действий, которые могут и должны считаться противоправными и общественно опасными.

Если состав преступления нельзя идентифицировать и определить форму действия, то принимается во внимание тяжесть совершенного противоправного деяния - нанесённый ущерб и его размер.

Преступление характеризуется способом действия – это совокупность методов и приёмов, которые совершаются в определенном порядке в процессе совершения преступления. При этом сам способ не зависит от формы преступления, поскольку является объективной характеристикой совершаемого действия. Преступления совершаются с использованием материальных предметов, которые являются средствами совершения преступления и орудия.

Зачастую в качестве характеристики объективной стороны преступления может выступать время и территория противоправного деяния, так как это может оказать воздействие на степень ущерба, наносимого общественным отношениям. В таких случаях они указываются в диспозиции уголовного закона и приобретают значение обязательных признаков состава преступления.

Преступное деяние характеризуется способом совершения, это конкретизирует совершенное противоправное деяние, дает характеристику, которая отличает его от других преступлений. Способ совершения преступления является важным как при имеющимся его определении в законе, так и тогда, когда этот способ в законе не указан.

Способ совершения преступления имеет влияние на субъективную сторону преступления по типу обратной связи: субъективная сторона в некоторой степени определяется способом совершения преступления.

Таким образом, разрабатывается сценарий о совершении преступления преступником, он предварительно выбирает способ для осуществления противоправного деяния. Таким образом, способ и объект преступления взаимосвязаны, так как выбор способа определяется исходя из объекта будущего преступления.

Глава 3 Современные проблемы правового регулирования преступлений, связанных с использованием компьютерных технологий

В случае, если злоумышленник получит доступ к компьютерной системе, взломает её или попытается изменить, то будет нанесен вред общественным отношениям, а также возможно нанесение угрозы определенным сферам государства, например транспортной сфере, оборонной сфере и энергетической. Получение доступа к таким сферам киберпреступниками может привести даже к человеческим смертям.

Согласно главе 28 Уголовного кодекса Российской Федерации, преступления в сфере компьютерных технологий можно подразделить на преступления, имеющие следующие составы (действующая редакция):

- статья 272. Неправомерный доступ к компьютерной информации;
- статья 273. Создание, использование и распространение вредоносных компьютерных программ;
- статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
- статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

Программно-вычислительное устройство пользователя является средством, с помощью которого совершается киберпреступления. В то же время запреты оказывают влияние на действия, которые наносят вред общественным отношениям посредством нарушения безопасного использования компьютерных технологий и информации, также её обработки.

Родовой объект преступления, связанный прежде всего с развивающимися ИТ, располагается в главе 28 Уголовного кодекса Российской Федерации «Преступления против общественного порядка и общественной безопасности». К такому объекту относится, прежде всего,

безопасность общества. Под общественными отношениями принято понимать такие отношения общества, которые способны защитить безопасность участников общественных отношений и общества в соответствии с имеющимися нормативными правовыми актами, традиционными нормами и обычаями. Также преступления в сфере компьютерных технологий могут нарушать закон о праве людей на тайну, которая должна охраняться законом. К таким правам также относятся обеспечение: врачебной тайны, семейной, государственной тайны и т.д.

В качестве видового объекта преступления, которое связано с применением компьютерных технологий, выступают отношения в процессе жизни общества, которые складываются в сфере обеспечения безопасного использования компьютерных устройств и их соответствующей информации.

Понятие такого обеспечения безопасности включает в себя обеспечение сохранения данных на компьютерном устройстве. Такая безопасность должна обеспечивать сохранность данных на компьютерах и также является аспектом информационной безопасности. Но данный термин не обладают точностью и определенностью, поскольку невозможно классифицировать типы возможной информации на компьютере, методы и объекты переноса информации, носитель информации и так далее.

Во время накопительных процессов сведений и данных, соответствующей их обработке и хранению происходит формирование отношений информационной безопасности. В них входят сами данные; осуществляемая с ними деятельность; автоматизированные действия, которые проводятся с ними; применение ИТ инструментов; инструменты информационного обмена и многое другое.

Исходя из вышесказанного, можно дать понятие информационной безопасности и следующее определение: эта сумма отношений, возникающих в обществе, которые способны обеспечить связанную с ними деятельность, хранение, систематического пополнения, использования и передачу сведений,

участниками которых являются обладатели данных сведений и владельцы, которые пользуются данной информации в своих целях.

Согласно Федеральному закону «Об участии в международном информационном обмене» № 85-ФЗ от 4 июля 1996г. [48] под информационной безопасностью понимается такое состояние, при котором информационная сфера общественных отношений является защищенной, при которой использование сведений и данных происходит исключительно в соответствии с интересами населения и государства, а также организаций. Безопасность информации обеспечивается необходимыми мерами, которые направлены на ликвидацию и нивелирование отрицательных результатов от попыток влияния и оказания ущерба объектам информационной среды.

После того, как данный закон был упразднен, термин информационной безопасности был закреплен законодателем в соответствующем документе - Доктрине информационной безопасности Российской Федерации, утвержденной Президентом России 9 сентября 2000г. [11]. Определения этого термина здесь дается следующее: такое состояние в Российской Федерации, когда ее интересы защищаются, позволяя реализовывать интересы личности, всего общества и государства в целом.

Согласно главе 28 Уголовного кодекса Российской Федерации объектом различных составов преступлений являются те объекты, которые можно взять исходя из наименования в конкретной статье Уголовного кодекса Российской Федерации и её внутреннего содержания.

Как известно, при преступлениях, совершаемых в области компьютерной информации, помимо безопасности защищенности сведений на пользовательском устройстве также ущерб должен быть нанесен безопасности сохранности сведений о личной жизни, прав человека, интересов собственника, безопасность в сфере общества, также государственная. Такие объекты являются дополнительными объектами для посягательств в сфере преступления в среде ИТ. Однако, если нанесенный ущерб здесь был

небольшой или невозможно его доказать, то в таком случае уголовная ответственность не наступит согласно ч. 2 ст. 14 УК РФ.

Согласно главе 28 Уголовного кодекса Российской Федерации предметом противоправного деяния являются данные, которые размещены в компьютерном устройстве. Под термином компьютерной информации исходя Рих примечания 1 к ст. 272 УК РФ понимается данные, представляющие, по сути, из себя электрические сигналы. Эти сигналы не находятся в зависимости от метода хранения, обработки или их передачи.

Преступления в компьютерной сфере могут характеризоваться наличием действия или бездействия с точки зрения объективной стороны. Так, к бездействию можно отнести нарушение правил пользования средствами хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ). Однако, действие людей или бездействие должны наносить ущерб безопасности сведений и данных человека, общественных отношений, государства в целом. Преступления в компьютерной сфере должны характеризоваться материальным составом, помимо использования хакерских программ (часть 1 статьи 273 УК РФ, имеющее формальный состав). При совершении преступления в компьютерной сфере между противоправными действиями и его результатами должно быть установлена причинно-следственная связь, а также оно должно быть доказано.

Для установления времени совершения противоправного деяния в сфере компьютерной безопасности необходимо установить время нажатия на клавишу, которое будет являться спусковой командой для запуска вредоносной программы или любой другой, которая нанесет вред общественным отношениям. И нет абсолютно никакой разницы, через какое время наступят последствия.

То есть, по факту, промежуток времени, который разделяет завершенное преступление и его результат может быть коротким либо длительным. Мгновенным может быть результат в случае, если была дана какая-то команда,

а компьютер провел необходимые анализ и сразу осуществил действие. Однако, бывают ситуации, когда посредством хакерских программ осуществляются изменения в необходимую для совершения преступления программу и хакеры начинают взламывать компьютерную информацию гораздо позже.

Для правоохранительных органов является тяжелой для расследования ситуация, когда киберпреступление совершено неизвестно в каком месте и на территории какого государства, так как это совершается во всемирной сети и часто IP адреса хакера зашифровываются. Так, например, киберпреступление может пересекать границы одного или нескольких государств.

В Уголовном кодексе Российской Федерации не закреплено определение места совершенного преступления в компьютерной сфере, здесь можно принимать во внимание место, где было осуществлено само преступление, то место, где наступили последствия, либо там, где преступление было закончено или какими-то методами пересечено.

Важной задачей является определение места совершения преступления в компьютерной среде в том случае, если преступление пересекло границы одного или нескольких государств. Например, известное преступление Левина, который используя компьютер в Санкт-Петербурге совершил мошеннические действия в «Ситибанк», который находится в США. Результатом его противоправных действий стала кража денег клиентов банка на общую сумму больше 10 млн долларов. Великобритании и США отказывались выдать преступника Российской Федерации по причине того, что преступление совершено на территории Российской Федерации, а результат совершенного преступления наступил в США и такие ситуации не регламентированы Уголовным Кодексом этих стран. Злоумышленник в итоге был задержан и осужден в Лондоне [3].

Объектом преступления, совершаемого в компьютерной среде, является лицо, возраст которого достиг совершеннолетия, в Российской Федерации

именно с этого возраста наступает уголовная ответственность – в 16 лет. Субъект преступления в компьютерной среде является общим.

Преступление в компьютерной среде может быть совершено со злым умыслом, но оно также может быть совершенно по неосторожности. Чаще всего среди криминальных хакеров существуют два мотива для совершения преступления в компьютерной среде: это извлечение прибыли в виде финансов и желание доказать всем свой высокий класс профессионализма, бросив вызов интеллектуалам в его хакерском сообществе.

Согласно гл. 28 Уголовного кодекса Российской Федерации изменения касаемо преступлений в компьютерной среде внеслись недавно, до этого применялись санкции в виде штрафов, при этом размеры штрафов составляли фиксированные суммы, затем проводилось ужесточение санкций, но при этом сумма штрафов опустилась до минимальной для конкретных видов наказаний.

После этого в гл. 28 были внесены изменения с учетом того, что накопились определённые знания и данные в этой сфере, то есть практический опыт. Таким образом, гл. 28 Уголовного кодекса Российской Федерации была видоизменен с принятием Федерального закона «О внесении изменений в уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»168 № 420-ФЗ от 7 декабря 2011г. [46]. Изменения произошли как в структуре запретов, так и в их содержании. Однако, законодательство в сфере преступлений в компьютерной среде и на сегодняшний день имеет некоторые несоответствия с реальной ситуацией, так как не были решены наиболее часто возникающие проблемы. Прежде всего проблема состоит в том, что для определения объективной стороны совершенного преступления необходимо использование специальных технических знаний в сфере ИТ и программно-вычислительных систем как для законодателя, так и для представителя закона.

Большое количество изменений произошло в статье 272 Уголовного кодекса Российской Федерации «Неправомерный доступ к компьютерной информации».

До обновления редакции статьи ее состав был из двух частей, в первой из которых санкции применялись при преступлении средней тяжести, вторая часть статьи характеризовалась отличительными чертами субъекта, что относилось к средней тяжести.

Согласно старому формату ч. 1 ст. 272 Уголовного кодекса Российской Федерации нелегитимный доступ к компьютерной информации, которая охраняется законом, наказывается. Законодательными органами обеспечивается защита данных компьютера: данные на машине ЭВМ, в её системе или сети.

Наказание наступает в случае уничтожения сведений, блокирования, неправомерного распространения либо копирования. В качестве квалификационного состава выступала лицо, которое могло использовать своё особое служебное положение, либо группировка лиц, которые совершали преступление по предварительному оговоренному сговору либо организованная группа.

Однако, после изменения, обозначение статьи осталось прежним как до редакции. Произошло изменение внутреннего содержимого части один при сохранении прежнего смысла «Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации».

В данной статье появились новые санкции: ограничение свободы преступника за совершенное противоправное деяние, лишение его свободы, назначение в качестве санкций принудительных работ. Совершенные противоправные деяния по этой части являются преступлениями небольшой части.

В обновленной ст.272 Уголовного кодекса Российской Федерации слово «Электронно-вычислительная машина» заменяется законодателем на наиболее современное слово «Компьютер», что обозначает стремление законодателя привести содержание ст. 272 УК РФ в единообразный вид.

Согласно Российскому законодательству, электронно-вычислительная машина и компьютер являются тождественными понятиями. Однако, в значение электронно-вычислительной машины закладывается прежде всего устройство, предназначенное для осуществления определенных вычислений. Компьютер осуществляет решения целого комплекса задач, вычисление является лишь одной из множества решаемых им задач.

Хотя при обновлении ст. 272 Уголовного кодекса Российской Федерации существуют противоречия в определениях основного функционала компьютерных устройств, объектом преступлений является отношения в обществе, которые непосредственно связаны с неприкосновенностью компьютерных сведений.

Однако, произошло изменение в понятии предмета уголовно-правовой охраны. Раньше информация компьютера сравнивались с некоторыми видами носителей, например, электронно-вычислительная машина или её система, и отсутствовало определение понятия информации. На сегодняшний день толкование понятия компьютерная информация дано в примечании 1 ст. 272 Уголовного кодекса Российской Федерации, и главная роль принадлежит форме, в которой имеет место быть информация, при этом отсутствует зависимость от особенности её хранения либо обработки, что расширяет предмет преступления.

Однако новое определение уже сейчас вызывает нарекания. Так, Верховный Суд в официальном отзыве на проект федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации» указал, что «в примечании к статье 272 УК РФ даётся понятие «компьютерная информация» – сведения (сообщения, данные), представленные в форме электрических сигналов независимо от средств их хранения, обработки и передачи [35]. Предложенный в примечании термин «электрические сигналы», на наш взгляд, не вносит достаточной ясности в определение понятия и требует дополнительного пояснения».

Критиками было сделано замечание о том, что информация не может быть существующей сама по себе, так как она всегда привязана к носителю информации.

Согласно законам компьютерной информации являются сведения, которые представлены посредством электрических сигналов. Но на сегодняшний день помимо электрических сигналов также для передачи данных используется оптоволокно, которое отличается передачей данных посредством использования света. Таким образом, с технической точки зрения это определение не соответствует текущей реальности. делом. Согласно ст. 272 Уголовного кодекса Российской Федерации если преступное действие было совершено при передаче данных через оптоволокно, такая информация не может быть преступной, просто потому что в законе отсутствует понятие оптоволокна.

Согласно ч. 1 ст. 272 Уголовного кодекса Российской Федерации в качестве объекта для преступления выступают отношения общества, в которых осуществляется реализация прав собственника компьютерной информации или законного владельца, связанная с этой информация и предоставление безопасности и защиты её он противоправных действий злоумышленников.

В качестве объективной стороны совершения преступления здесь является получение доступа к информации, которое является противоправным действием, то есть, на это не было дано согласие собственника информации. Присутствует формально-материальный состав преступного деяния.

Для привлечения к ответственности за совершенное преступление необходимо наличие определенных последствий: удаление информации, осуществление блокирования или её изменения, копирование и разглашение данных. Для наступления ответственности за преступления необходимо доказать мотив преступника, который бы соответствовал указанным целям совершения преступления согласно ст. 272 Уголовного кодекса Российской Федерации., в противном случае состав преступления отсутствует.

Преступник, получая противоправный доступ к компьютерной информации, вполне осознает, что это осуществляется в соответствии с его злым замыслом, вопреки воле собственника информации, а также осознаёт возможное наступление ответственности за совершение противоправного деяния и наступления в результате этого ущерба собственнику информации. В этом выражается субъективная сторона совершенного преступления.

Субъектом преступления неправомерного доступа к компьютерной информации является лицо, которое достигло 16 лет. Данное лицо должно быть вменяемым.

Обновленные ч.ч. 2-4 ст. 272 Уголовного кодекса Российской Федерации имеют определенные признаки для классификации преступлений в зависимости от степени нанесения опасности общественным отношениям. Данный перечень является более расширенным по сравнению со старой версией ст. 272 УК РФ.

Так, согласно ч. 2 ст. 272 УК РФ ответственность наступает за преступление, мотив которого состоит в заинтересованности и корысти, также нанесения крупного ущерба.

В старой редакции статьи наказание за такое противоправное деяние составляло 2 года при установленных квалифицирующих признаках, в новой же редакции статьи 272 УК РФ санкция за это находится в пределах шести месяцев, за что новая редакция получила много критических оценок. Исходя из этой редакции получается, что нет справедливой соразмерности между совершенным противоправным деянием и его тяжестью и степенью наступления ответственности.

Таким образом, здесь отсутствовала соразмерность между тяжестью совершенного преступления и понесенного наказания. Чтобы устранить данный недостаток санкции, законодатель Федеральным законом от 28 июня 2014 года внес в конструкцию статьи изменения, в соответствии с которыми из санкции ч. 2 ст. 272 УК РФ исключены слова «либо арестом на срок до шести месяцев».

Это уникальный случай, когда принимается Федеральный закон в Уголовном кодексе Российской Федерации, в котором исключается возможность такого наказания как арест в будущем, что было бы очень актуально для преступления в компьютерной среде. В связи с этим предлагается другая норма санкции, которая бы сохранила арест как санкцию за совершенное преступление в компьютерной среде, предусмотренной частью второй статьи 272 УК РФ и изложить ее в следующей редакции: «наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, или исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо арестом на срок до шести месяцев, либо лишением свободы на срок до четырех лет».

В ч. 2 ст. 272 Уголовного кодекса Российской Федерации дается следующее определение нанесению крупного ущерба - таким ущербом является ущерб на общую сумму свыше 1 млн. руб., это определение применительно ко всей гл. 28 Уголовного кодекса Российской Федерации. Объективная сторона преступления заключается в наличии у преступника мотивов корыстной заинтересованности. Таким образом, совершение действия, которое связано с получением нелегитимного доступа к компьютерной информации можно назвать преступлением с корыстной заинтересованность и может быть квалифицировано согласно ст. 272 УК РФ.

Обновлённая ч. 3 ст. 272 УК РФ является по сути своей копией второй части старой версии, но имеет некоторые отличия в части обновлений. Новизна состоит в том, что статьей предусмотрено наказание за использование лицом своего служебного положения для получения доступа к компьютерной информации либо организация совершения преступления по предварительному сговору группой лиц, или организованная группировка. В старой версии присутствовали слова касаемо электронно-вычислительной

машины, в новой же они удалены. Первые два критерия раскрыты в положениях ст. 35 УК РФ.

Преступление, которое совершено по предварительному сговору группой нескольких лиц является преступлением, когда предварительно несколько человек заранее договорились о совершении действий преступления, обсудили все его подробности, подготовились к совершению преступления.

В случае если противоправное деяние было совершено организованной группой лиц – два или больше человек при простой форме соучастия лиц или при сложной, что подразумевает под собой заранее распределенные роли преступников. Классификация действий преступников осуществляется без ссылок на статью 33 УК РФ.

В случае, когда лицо воспользовалось служебным положением и занимаемой должностью для получения доступа к важным данным на компьютере, то такое преступление требует определения, в ч. 3 ст. 272 УК РФ нет характеристики данного квалификационного признака. Однако такой признак был разъяснен Пленумом Верховного Суда Российской Федерации и согласно постановлению «О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней)» № 12 от 10 июня 2010г. [30], согласно которой к лицам, совершившим деяние, предусмотренное ч. 2 ст. 210 УК РФ, к лицам, которые используют свою должность и соответствующее положение на рабочем месте необходимо отнести должностных лиц, а также лиц, которые работают на государственной службе либо служащих органов местного самоуправления, которые в свою очередь не являются должностными лицами.

Аналогичное разъяснение Пленум Верховного Суда РФ дал и в постановлении «О судебной практике по делам о мошенничестве, присвоении и растрате» № 51 от 27 декабря 2007 г. [31]. Согласно данному разъяснению лицами, которые используют своё служебное положение для совершения мошеннических действий, присвоения денежных средств или их траты (ч. 3

ст. 159, ч. 3 ст. 160 УК РФ) нужно признавать не только лица, которые являются должностными, а также лица, состоящие на государственной и муниципальной службе, а также лица, которые соответствуют требованиям примечания 1 к ст. 201 Уголовного Кодекса Российской федерации.

Пленум Верховного Суда РФ также и в постановлении «О судебной практике по делам о незаконном предпринимательстве и легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем» № 23 от 18 ноября 2004г. под лицами, использующими свое служебное положение (п. «б» ч. 3 ст. 174 и п. «б» ч. 2 ст. 174-1 УК РФ), к числу специальных субъектов отнес как должностных лиц, так и служащих, а также лиц, осуществляющих управленческие функции в коммерческих и иных организациях [29]. Именно так, на наш взгляд, следует трактовать признаки специального субъекта в ч. 3 ст. 272 УК РФ.

Если лицо совершило противоправное действие, связанное с компьютерной информацией, но при этом не использовало свои должностные обязанности, то за такое преступление наступает ответственность на общих основаниях.

Часть 4 ст. 272 Уголовного кодекса Российской Федерации закрепляет положение, в котором преступление повлекло за собой тяжёлые последствия или была создана угроза для наступления этих последствий. В данной части закрепляется ответственность за преступлениями с компьютерной информацией, которые указаны и перечислены выше. И такие преступления относятся к категории тяжких.

Так, например, термин тяжести совершенного преступления имеет различные оценочные категории, которые отличаются каждой конкретной ситуацией преступления: могут быть таким образом сбои в работе жизнеобеспечивающих систем общества, а также важных для государства организаций.

Процесс определения тяжести последствий должен отличаться объективностью, это значит, что к каждой ситуации получения

неправомерного доступа к сети нужно применять определенные оценочные категории; для одного человека стоимость данных на компьютере может быть равна нолю, для другого информация стоит заоблачных денег.

Факт наличия махинаций с компьютерными данными может повлиять на их цену – она может вырасти или упасть в цене. При отсутствии рекомендации и практики Верховного Суда Российской Федерации возможно осуществление сравнительного анализа противоправных действий в киберпространстве с данными и преступлениями, связанными с нарушениями авторских и смежных прав и по степени нанесенного ущерба.

Так, согласно ч. 1 ст. 1259 Гражданского кодекса Российской Федерации [9] программы для электронно-вычислительных машин являются объектом авторского права и должны охраняться также как литературные произведения. Однако, компьютерная информация — это более широкое понятие, чем просто программа для электронно-вычислительных машин, она включает в себя множество аспектов, поэтому такое предложение о сравнении преступлений является неактуальным. Но, учитывая отсутствие практики, также имеет место быть.

Статья 272 Уголовного кодекса Российской Федерации теперь имеет примечания, так, первое примечание имеет определение компьютерной информации, во втором примечании даётся конкретизация крупного ущерба. Подытоживая вышесказанное, статья 272 Уголовного кодекса Российской Федерации на сегодняшний день имеет четыре части и два примечания.

По сравнению со старой редакцией ст. 272 УК РФ увеличилось количество санкций, которые применяются по отношению к совершенному преступлению, появились и новые их виды.

К ч. 1 ст. 272 УК РФ прибавлены новые виды наступления ответственности за совершение преступлений - осуждение к принудительным работам и ограничение свободы, но при этом удалено из статьи обязательные работы. Появилось больше вариантов лишить человека возможности заниматься определенной деятельностью или работать на определенной

должности, наказание в виде ограничения свобод и принудительных работ указано в новой редакции в ч. 3 ст. 272 УК РФ, тогда как в старой это было в ч. 2 ст. 272 УК РФ. Наказание в ч. 3 ст. 272 Уголовного кодекса Российской Федерации в виде штрафа увеличено, в старой редакции оно составляло до 300000 руб., в новой редакции максимальная сумма штрафа увеличена до 500000 рублей.

Изменения, которые были внесены в ст. 272 Уголовного кодекса Российской Федерации показали, что законодательные органы Российской Федерации осознали необходимость того, что в связи с возникновением новых видов преступлений в компьютерной среде, потребовались переработки и обновления в существующей редакции статьи, которая содержит санкции за совершение данных преступлений. Причины, по которым возникла необходимость в изменениях, заключаются в неконтролируемом росте и распространении новых информационных технологий, способов и методов совершения преступлений в компьютерной среде. Однако, работа законодателем по обновлению законодательства касаемо преступлений в компьютерной среде не должна ограничиваться редакцией только данной статьи, так как это не отвечает всем потребностям в сфере противодействия преступлениям в компьютерной среде.

Проблемой сегодня является тот факт, что Верховный суд Российской Федерации не разъяснил того, что можно отнести к признакам неправомерного доступа к компьютерной информации. На сегодняшний день отсутствует такая классификация признаков, которая позволила бы правоохранительным органам отнести факт совершения противоправного доступа к компьютерной информации к тому или иному признаку для его классификации и определения состава преступления.

Часто правоохранительным органам сложно определить сущность уголовно-правовой охраны и обеспечения безопасности информации в случае, если при определении признаков квалификации неправомерного доступа к

компьютерной информации они пересекаются с преступлениями, которые связаны с нарушением авторских прав.

Согласно опубликованным данным, в Рязанской области проходил суд над злоумышленником, который незаконным путем получил доступ к учетным сведениям пользователей в ООО «ЦентрТелеком» и использовав одну из учетных записей клиента, получил доступ к сети «Интернет». Таким образом, злоумышленник смог оставить в сети «Интернет» 111 случаев совершения нелегитимных действий, в то время как собственник учётной записи просто не мог зайти в личный кабинет и осуществить необходимые ему операции. Захаровским районным судом Рязанской области в данном случае был вынесен приговор с учетом нанесения ущерба и похищения средств, так как в результате мошеннических действий он получил на свой счёт 16124 руб.

Судом противоправные действия злоумышленника были определены по ч. 1 ст. 272 УК РФ и ч. 1 ст. 165 УК РФ, в связи с тем, что преступник получил нелегитимный доступ к интернету и оттуда черпал данные. Таким образом, благодаря «стараниям» хакера компьютерные данные, размещенные на серверной устройстве ОАО «ЦентрТелеком» получили изменение, последствием чего стало получением сервером неправильных и недостоверных сведений о времени и стоимости отработанного времени, объеме полученной и отправленной информации.

При оценке совершенного преступления мошенником суд проводил квалификацию каждому из его 111 противоправных деяний отдельно согласно ч. 1 ст. 272 УК РФ, в процессе которых был получен незаконный доступ к сведениям компьютера. Согласно ч. 1 ст. 165 УК РФ квалифицирующий признак совершенного преступления был определен как нанесение ущерба владельцу данных, но сама кража не была осуществлена.

На наш взгляд, квалификация данного преступления была совершена неправильно, помимо нанесения ущерба в результате неправомерного получения доступа к сведениям на компьютере, нужно было квалифицировать каждое преступление и каждый неправомерный доступ к данным компьютера.

После осуществления редакции части 2 статьи 272 УК РФ также было осуществлено внесение информации касаемо квалификационного признака, а именно получении незаконного доступа к сведениям на компьютере, что привело в результате злого умысла злоумышленников к ущербу.

Размером большого нанесенного ущерба согласно примечанию 2 к ст. 272 УК РФ считается сумма, которая выше 1 млн. руб. Однако, на настоящий момент времени судебные приговоры о наступлении ответственности лиц, за противоправные действия по ст. 272 и ст. 165 УК РФ отсутствуют с момента внесения изменений и по настоящий момент времени.

Статья 273 УК РФ получила название «Создание, использование и распространение вредоносных компьютерных программ». До внесения изменений данная статья называлась иначе: «Создание, использование и распространение вредоносных программ для ЭВМ». После редактирования и внесения необходимых изменений такое понятие как электронно-вычислительная машина стало устаревшим и было заменено на более современное на сегодняшний день «Компьютер», которое также является более емким понятием.

Как и до редакции видовым объектом преступления данной статьи является отношение общества. Преступления, которые связаны с общественными отношениями и безопасным использованием компьютера, его сведений и средств защиты являются объектом согласно ст. 273 Уголовного кодекса Российской Федерации. Действие может быть отнесено к объективной стороне в случае создания и разработки, распространения и осуществления деятельности с компьютерными программами или её сведениями. На данный момент времени можно сказать, что состав такого преступления является формальным, так как преступление оканчивается с момента соответствующего создания и разработки, распространения или внедрения компьютерной программы.

Для того, чтобы привлечь к ст. 273 УК РФ не требуется доказательство о том, повлекла ли данная компьютерная программа за собой последствия, так

как достаточно доказать, что действие было совершено. Взаимозаменяемые в новой редакции статьи фраза «За внесение изменений в компьютерной информации» заменена на создание «Иной компьютерной информации».

При этом под компьютерной программой понимается такая программа, последовательность выполнения действий которой необходимо осуществлять для того, чтобы компьютерные устройства выполнили свою работу. Понятие компьютерной информации было дано нами ещё в ч. 1 ст. 272 УК РФ при внесении злоумышленником каких-либо изменений в программу, которая функционирует на компьютере, преступник тем самым вносит изменения в компьютерную программу. Как вывод, «иная компьютерная информация» подразумевает под собой осуществление изменение программы.

Согласно старой редакции статьи, злоумышленник, который осуществил непосредственную разработку программного кода, но при этом не применил его на деле не привлекается к ответственности и не несет за это никаких санкций. Однако, по новой редакции ответственность за такое противоправное деяние возникает. Таким образом, законодательством Российской Федерации была справедливо расширена объективная сторона преступления.

Понятие создания и разработки компьютерной программы подразумевает под собой написание хакером соответствующего программного кода и встройка его в компьютерную программу, посредством которой в дальнейшем будут происходить противоправные действия. То есть, любые действия, которые направленны на результат - получения вредоносной программы или вредоносного программного кода, подходит под фразу «создание иной компьютерной информации».

Под устранением компьютерной программы можно понимать такое действие, которое направлено на введение в оборот людям данные программы либо предоставление возможности использовать данную программу в любой форме. Например, продажа компьютерной программы в интернете или ее размещение для свободного скачивания на сервере и т. д. В качестве

использования программы подразумевается то, что купивший или скачавший ее с сервера пользователь будет применять данную программу в действии.

Согласно диспозиции статьи, данное действие должно быть уничтожено, заблокировано, изменено или скопировано, при этом средства защиты информации будут заблокированы.

В качестве уничтожения компьютерных сведений можно рассматривать деяние, последствием которого является невозможность просмотра информации, которая была размещена на компьютере или любом носителе информации. Так, информация может быть удалена с компьютера или с физического носителя. Для того, чтобы классифицировать такое преступление, необходимо понимать, в чём состоял мотив преступника и с какой целью он уничтожал данную информацию. Если преступник хотел лишь уничтожить информацию или повредить носитель, то согласно ст. 273 УК РФ состав преступления отсутствует.

В случае, если пользователь не может получить доступ к своей размещенной на компьютере информации, но при этом она не удалена с компьютера, то такое действие можно назвать блокированием компьютерных данных.

В случае, если в компьютерную информацию были внесены изменения без согласия пользователя владельца, то данное действие называется модификацией компьютерной информации.

В случае, если компьютерная информация была скопирована незаконным путем, то такое действие называется копированием компьютерной информации.

Средствами защиты компьютерной информации выступают следующие виды средств: технические, криптографические, программные и т. д. Цели применения средств защиты компьютерной информации состоят в обеспечении защиты размещенных на компьютере сведений, средств их реализации и контроль работоспособности защиты информации.

Если средства защиты компьютерной информации не выполняют свои функции и является по сути своей бездействующими, то в такой ситуации можно говорить о нейтрализации работы средств защиты компьютерной информации.

Согласно ч. 1 ст. 273 УК РФ для совершения преступления необходимо средство и способ совершения преступления, к которым можно отнести непосредственно деяние, которое должно быть противоправным и последствия, в качестве средства совершения преступления выступает компьютерная программа или иная компьютерная информация.

К субъективной стороне преступления относятся вина, которая наступила в результате причинение вреда с прямым или косвенным умыслом. Прямой умысел преступника означает то, что злоумышленник создает свою компьютерную программу с определенной целью уничтожения, блокирования копирования или иных противоправных действий, при этом он осознает, что использование данной программы может нанести вред компьютерной информации пользователя. Косвенный умысел означает то, что человек при создании компьютерной программы не хотел нанести вред какому-либо определенному пользователю, но не предусмотрел возможные неблагоприятные последствия использования программы. Однако, при распространении и использовании компьютерной программы умысел может быть только прямым. Для квалификации данного преступления и определения признаков состава преступления мотив и цель не являются обязательными.

Согласно статье 273 УК РФ действие имеет состав преступления в том случае, если преступник имел главной целью уничтожить компьютерную информации, заблокировать её, копировать или нейтрализовать защиту средств защиты компьютерной информации, в таком случае состав преступления можно определить. При этом, если преступник, используя компьютерную программу, заранее знает о том, что она несет какой-то вред и повлечет за собой ущерб для пользователей и для компьютерной информации, окажет негативное, то преступление считается преступлением, совершенным

со злым умыслом. Даже если преступник знает не обо всех видах вреда, который способны принести вредоносные программы, он всё равно будет отвечать в соответствии с санкциями согласно статье 273 УК РФ.

Субъектом преступления по статье 273 УК РФ выступает лицо, которое достигло своего совершеннолетия 16 лет и являются дееспособным.

Не всегда действия, которые сопряжены с применением компьютерной информации, могут считаться противоправными и образовывать состав преступления. Так, например, если по просьбе владельца компьютера специалист пытается взломать программу и восстановить забытые владельцем логин и пароль, то такое действие не будет образовывать состав преступления. То есть, не всегда за использование вредоносной программы будет наступать ответственность, это зависит от конкретного случая. Поэтому здесь может быть использована часть вторая ст. 14 УК РФ.

Ч. 2 ст. 273 включает в себя квалифицирующие признаки следующих преступлений: преступления, совершенные группой лиц по предварительному сговору, организованной группой или лицом, которое использует служебное положение для совершения преступления, которое повлекло за собой нанесение ущерба и было совершено из личной корысти. Квалифицирующие признаки в данной части статьи аналогичны, по сути, с квалифицирующими признаками ч. 2 и 3 статьи 272 УК РФ.

В случаи совершения преступления преступником, который использует своё служебное положение, субъектом преступления будет являться то лицо, которое имеет возможности получения свободного доступа к закрытой компьютерной информации, её распространения и копирования в силу наличия у него для это полномочий и обязанностей.

Если противоправные действия, связанные с компьютерной информацией, повлекли за собой тяжкие последствия или было созданы условия для возникновения угрозы нанесения ущерба, то за такие деяния наступает ответственность согласно ч. 3 ст. 273. При этом тяжесть совершенного преступления определяется в каждой конкретной ситуации,

поскольку является категорией оценки. Так, тяжесть совершенного деяния может проявляться в нанесении материального ущерба, причинении вреда репутации фирмы, простоев работы организации в результате нанесения вреда компьютерным программам, самоубийства человека и т. д.

На основании этого можно сделать вывод, что состав преступления согласно ч. 3 ст. 273 УК РФ является формально-материальным. Деяние может быть признано преступным в результате наступления последствий совершенного преступления, а также при наличии угрозы их наступления.

В последней редакции ст. 273 УК РФ в части, касаемо санкции и ответственности, изменилась мера ответственности за совершенное преступление: если в старой редакции было предусмотрено лишение свободы сроком до 3 лет и штрафом с высшей границей в 200000 руб. или размере зарплаты преступника за период до восемнадцати месяцев, то в новой редакции лишение свободы предусмотрено сроком до четырех лет, лишение свободы может быть заменено на принудительные работы сроком на четыре года. Что касается размера штрафа, то он так же остался на уровне до 200000 руб. либо в размере заработной платы или иного дохода преступника за период до восемнадцати месяцев.

Таким образом, в качестве санкции за совершенное преступление преступник может быть лишён свободы на четыре года, при этом лишение свободы может быть заменено на принудительные работы. Если посмотреть в целом по ч. 1 ст. 272 УК РФ, то главное отличие в санкциях это увеличение отбывания срока наказания до четырех лет вместо трёх.

Часть два статьи 273 УК РФ включает в себя следующие виды санкций: лишение свободы сроком до 4 лет, либо осуждение на принудительную работу сроком до пяти лет с лишением право лица, которое совершило противоправное деяние, занимать определенную должность или выполнять определенные обязанности с оговоренным сроком до трех лет или без него, а также возможность осуждения лишения свободы до пяти лет с вынесением штрафа размером от 100000 руб. до 2001000 руб. либо заработной платы

преступника за 2 или 3 года или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

По сравнению с 1 ч. ст. 273 УК РФ можно отметить, что появилась возможность лишения лица, которое совершило преступление, занимаемой им должности, а также заниматься определенным видом деятельности. При этом наименьшее количество предусмотренного штрафа составляет 100000 руб., однако, в соответствии с ч. 2 ст. 273 УК РФ фраза «или без такового» подразумевает под собой, что наложение штрафа на преступника является мерой ответственности, которую законодатель вправе накладывать, а в части первой это является обязанностью законодателя. Таким образом, не выполняется принцип соразмерности совершенного преступления и понесенного за это наказания. Поэтому есть предложение внести изменения в ч. 1 ст. 273 УК РФ, а именно убрать формулировку «или без такового» в фразе «со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев». Таким образом, необходимо внести изменения в ч. 1 ст. 273 УК РФ и сделать назначение штрафа как наступление ответственности за совершенное противоправное деяние альтернативным наказанием, а не обязательным как есть в существующей редакции.

Лишение свободы и отбывания наказания на срок до семи лет является санкцией из ч. 3 ст. 273 УК РФ. Однако, в старой редакции это было в части два. При наступлении ответственности в ч. 2 ст. 273 УК РФ старая редакция была сопряжена с закрепление материального состава и наступлении ответственности за совершенное неосторожное преступление.

Согласно части 3 ст. 273 УК РФ в настоящей редакции состав рассматривается формально-материальный, то есть здесь рассматривается ситуация совершения преступником преступления с умыслом или неосторожно. Таким образом, произошло обновление редакции и соответствующих санкций в сторону либерализации ответственности за

разработку вредоносных компьютерных программ, их распространения и повсеместного использования.

Подытоживая вышесказанное, хочется отметить, что изменения, которые произошли в ст. 273 Уголовного кодекса Российской Федерации, на наш взгляд, являются удачными, и, возможно, в дальнейшем понадобится редактирование ст. 273 УК РФ только в технической части. Для успешного применения на практике необходимо перевести терминологию статьи в соответствующую диспозицию статьи, что облегчит применение нормы на практике.

Однако, некоторые решения необходимо корректировать в ближайшем будущем, в связи с тем, что имеются нелогичные решения касаемо санкции уголовно-правовых норм.

Существует сложность правильности уголовно-правовой квалификации преступлений, которая связана с разработкой хакерских компьютерных программ, их распространением и использованием в связи с тем, что отсутствует широкая судебная практика по этим вопросам, а также сотрудники судебной системы не имеют достаточного уровня практической подготовленности по вопросам обеспечения компьютерной безопасности и вредоносных компьютерных программ.

Так, например, изменение ст. 273 УК РФ при совершении такого преступления, как использование программ для генерирования лицензионных ключей (кейгены) является сложным для квалификации вопросом. Для иллюстрации сказанного обратимся к судебной практике. Рассмотрим ситуацию вынесения приговора судьей Самарского судебного участка № 48 в отношении преступника от 6 июня 2011 года [27]. Квалификация совершенного преступления состояла в следующем: преступник разместил в сети на файлообменнике ссылку на лицензионные экземпляры программного обеспечения «Microsoft Windows XP», «Microsoft Office Word», «Microsoft Office Excel», «Microsoft Office Outlook», «Microsoft Office Visio», «Microsoft Office Access», «Microsoft Office Power Point», «Microsoft Office 2003». При

загрузке на файлообменник данной ссылки было видно, что отсутствует защита от нелицензионного копирования и экземпляры программного обеспечения являются контрафактом. При установке программного обеспечения на компьютер, они не требовали введения необходимого для оригинальных программ лицензионного ключа.

Согласно статье 273 Уголовного кодекса Российской Федерации преступник совершил следующее преступление: он осуществил распространение компьютерная программа с внесенными в неё изменениями, которое заведомо модифицировало компьютерную информацию. Однако, в данном деле судья руководствовался в вынесении приговора исключительно ч. 2 ст. 146 УК РФ, не беря во внимание при этом ст. 273 УК РФ. На наш взгляд, это ошибка.

Рассмотрим подобную ситуацию совершения преступления в Томске от 10 марта 2011 года. Злоумышленник Регнер И.В. решил подзаработать и установить клиенту ПО «Microsoft Windows XP», «Microsoft Office 2007», «AutoCAD», «1С: Предприятие» на его компьютерное устройство. Чтобы получить лицензионный ключ к этому ПО и не платить за него деньги злоумышленник осуществил на программе «MSOE2007KG» генерацию ключа для «Microsoft Office 2007». Согласно решению суда, противоправное деяние было отнесено к ч. 2. ст. 146 УК РФ как незаконное использование объектов авторского права, которое было совершено в крупном размере [28].

В данном деле интересен следующий факт: согласно экспертизе программы для генерации ключей «MSOE2007KG» и «AutoCAD-2008-keygen» имели своей целью непосредственное осуществление генерации лицензионных ключей, но при этом они не модифицировали никоим образом компьютерную информацию. И в соответствии с этой экспертизой данное преступление нельзя отнести к ст. 273 или к ст. 272 УК РФ. В соответствии с этой экспертизой суд не смог предоставить доказательства совершения преступления согласна ч. 1 ст. 272 УК РФ модификация компьютерной информации.

Суд также оправдал подсудимого по ч. 1 ст. 273 УК РФ в связи с тем, что не произошло изменения программы, которое бы заведомо приводило к уничтожению, блокированию, модификации или копированию информации, нарушению работы электронно-вычислительной машины, системы ЭВМ и их сети. Однако, в соответствии с экспертизой программы генерации лицензионных ключей не вносили изменения в само программное обеспечение и при отсутствии необходимых доказательств суд оправдал в этой части подсудимого.

Исходя из вышесказанного можно сделать вывод, что суд не посчитал совершением преступления согласно ст. 273 УК РФ использования «кейгена» для генерации ключей.

Рассмотрим еще один вариант преступления, которое было совершено при схожих обстоятельствах и рассмотрено Октябрьским районным судом города Кирова 24 декабря 2013 года. Подсудимый Сиков Д.В. осуществил копирование программ «Autodesk 3ds Max 2012», «Autodesk 3ds Max 9», «CorelDRAW» из сети «Интернет» и установил данную программу на пользовательский компьютер, который был предоставлен сотрудником отдела К. Данное преступление было отнесено к ч. 2 ст. 146 УК РФ незаконное использование объектов авторских прав. Вместе с тем суд установил наличие квалифицирующего признака ч. 1 ст. 272 УК РФ. Обоснование наступления ответственности по ч. 1 ст. 272 УК РФ объяснил следующим: подсудимый при активации незаконного скопированных авторских программ использовал также программу «xf-adesk2012x32.exe» - программу перехвата генерации активации ключа для «Autodesk 3ds Max 2012». Таким образом, произошла модификация памяти электронно-вычислительной машины, которая содержала исполняемый код «Autodesk 3ds Max 2012», что в свою очередь привело к блокировке функции необходимой проверки правильности кодов активации этого ПО и нелегитимному способу выдачи кода для активации программы. Также преступником была совершена нейтрализация средств защиты программы путем введения полученного нелегитимным путём, когда

активации программы «Autodesk 3ds Max 2012», что произошло умышленно и по воле подсудимого [26].

В деле подсудимого города Кирова, которое было рассмотрено октябрьским районным судом 11 ноября 2013 года [26], содержится следующая ситуация: злоумышленник решил осуществлять платные услуги по установки ПО за деньги клиентам. Для этого он скачал из интернета незаконные версии ПО «Microsoft Windows 7» и программы «КОМПАС-3D», «КОМПАС-Электрик» и «КОМПАС-Электрик V14». В данной ситуации в отношении злоумышленника, который совершил данное противоправное деяние было прекращено рассмотрение дело, так как состоялось примирение с потерпевшим. Однако, дело относится к ст. 272 и ст. 273 УК РФ.

Так как в судебной практике нет большого опыта в подобных разбирательствах, то суд часто может совершать ошибки при квалификационных действиях противоправного деяния.

В г. Егорьевске Московской области было рассмотрено следующее дело 26 октября 2011 года: Миленин А.С. осуществил покупку IP адресов удаленных клиентов интернета. Данное действие он совершил для того, чтобы в дальнейшем с помощью интернета получить доступ к сведениям компьютеров пользователей. Злоумышленник располагал хакерской программой подбора логинов и паролей. Данное противоправное действие было отнесено судом к ч. 1 ст. 273 УК РФ – применение программы для незаконного копирования личных данных жертв – логина и пароля [25].

Налицо присутствие квалифицирующего признака: противоправное использование логина и пароля, которые являются охраняемой законом компьютерной информацией и противоправное использование данной информации должно относиться к ст. 272 и ст. 273 УК РФ. Суд не осуществил квалификацию данного признака, что на наш взгляд является ошибкой.

После получения незаконным путём логина и пароля подсудимый воспользовался ими для того, чтобы получить доступ к компьютерной информации потерпевшего с помощью сети «Интернет», получив

неправомерный доступ к компьютерной информации таким образом. После этого подсудимый обнаружил на компьютере жертвы установленную программу платёжной системы и попытался подобрать к ней также логины и пароли, но в дальнейшем прекратил свои попытки, так как они не увенчались успехом. Данное преступление относится к ч. 1 ст. 272 УК РФ.

Данные противоправные деяния можно рассматривать не только как нарушение по статье «доступ к охраняемой законом компьютерной информации», но также и как использование вредоносных компьютерных программ по ст. 273 УК РФ, так как было осуществлено использование программы подбора пароля для платежной системы и попытка совершить кражу денежных средств с помощью подбора к платежной системе логина и пароля (ст. 159 УК РФ).

Злоумышленник, используя личное компьютерное устройство, подключился к устройству жертвы и попытался получить доступ к системе совершения платежей жертвы с помощью программы генерации логинов и паролей. Поскольку у злоумышленника не получилось это сделать, он установил хакерскую программу на компьютерное устройство потерпевшего. Таким образом было совершено преступление по ч. 1 ст. 272 УК РФ.

Сам факт использования хакерской программы в любом месте наряду с установкой данной программы третьим лицам является противоправным деянием и может быть квалифицировано по ст. 273 УК РФ. Однако, суд решил по-другому и, на наш взгляд, это является ошибочным мнением суда.

По итогу подсудимым был совершён подбор логина и пароля к платежной системе потерпевшего. В результате данной успешной операции, проведенной злоумышленником, он смогу получить доступ к электронной системе платежей жертвы и украсть с ее счета более чем 400000 руб. Таким образом, на эту сумму потерпевшему был нанесен материальный ущерб.

Данное преступление получило квалификацию согласно пункту «В» ч. 3 ст. 158 УК РФ как кража.

Наряду с фактом совершения кражи преступник осуществил противозаконный доступ к информации на компьютере жертвы, в частности получил с помощью хакерской программы к системе платежей жертвы, что и повлекло за собой ущерб. Таким образом, данное преступление также можно квалифицировать по ст. 272 УК РФ, чего суд не сделал и это является ошибкой.

Исходя из вышеперечисленного можно сделать вывод, что при судебном разбирательстве подобных преступлений отсутствуют единые критерии рассмотрения данных преступлений и определения признаков классификации состава преступления, что ведёт к совершению ошибок в принятии судом решений. Также можно сделать вывод, что Пленуму Верховного суда необходимо в ближайшее время принять специальное постановление, которое ложно дать разъяснения 106 важных и критичных вопросов, касающихся преступлений, которые нарушают безопасность компьютерных систем, также нужно рассматривать соотношение с другими преступлениями.

Рассмотрим последние статьи главы 28 Уголовного кодекса Российской Федерации статьей – ст. 274 УК РФ, которые устанавливают ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Данная статья была также редактирована в содержательной части, а также в терминологии. Старая редакция названия статьи звучала следующим образом: нарушение правил эксплуатации электронно-вычислительных машин, системы ЭВМ и их сети. Однако, после редактирования данных название поменялось - «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей». Как видно из названий статей, произошло изменение термина электронно-вычислительная машина, то есть, оно было заменено словом компьютер.

Общественные отношения, которые связаны непосредственно с соблюдением внутренний безопасности средств хранения, в соответствующей обработке и передачи информации компьютера, сохранении компьютерной

безопасности является объектом преступления. То есть, объектом преступления являются общественные отношения, которые функционируют в рамках правильного использования компьютерной сети и компьютерной системы.

Объективной стороной преступления является несоблюдение правил использования компьютерной системы и компьютерной информации, которые установлены законодателем или разработаны собственником организации. Так, несоблюдение правил внутреннего распорядка и правил использования работы с компьютерными устройствами, которые предусмотрены соответствующими инструкциями, может повлечь за собой наступление ответственности в связи с нарушением 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.

Стоит отметить, что ст. 274 УК РФ не содержит требований технического характера, которые бы внесли конкретику в процессе квалификации преступления. Для того, что определить признаки преступления, необходимо изучить соответствующие инструкции и правила работы с системами и оборудованием, разработанные производителем или собственником организации, которые были доведены до сотрудников под подпись. В качестве примера можно использовать ситуацию – неправильное использование компьютера или режима его эксплуатации, несоблюдение средств защиты информации.

Опасные последствия для общества, которые наступили в результате неправильной эксплуатации компьютерной системы или информации и привели к уничтожению, блокированию, изменению, либо копированию компьютерной информации являются важными для квалификации преступления. Исходя из этого, можно сделать вывод, что состав преступления материальный.

Данное противоправное деяние согласно примечанию 2 ст. 272 УК РФ должно повлечь наличие крупного ущерба. Отметим, что существовавшая в старой редакции категория оценки «Существенный вред» была заменена в новой редакции на «Крупный ущерб». При этом суду необходимо доказать наличие причинно-следственной связи между наступившими последствиями в виде ущерба и совершенного противоправного деяния в результате неправильного выполнения правил эксплуатации. Данное преступление может быть совершено со злым умыслом, но также преступление может быть совершено и по неосторожности, по небрежности, по невнимательности. Согласно ст. 274 УК РФ нарушение правил эксплуатации является способом совершения преступления, а само преступление квалифицируется в зависимости от наступивших в результате противоправного деяния последствий.

Так, ситуация, когда сотрудник медицинского центра скачал нелицензированную программу, не проверил её на наличие вирусов, и установил на компьютер медицинского центра. В результате данного действия приостановилась работа медицинского центра и наступила смерть больного, который был подключен к системе жизнеобеспечения. Данное преступление, совершенное без наличия злого умысла, можно квалифицировать ч. 2 ст. 274 УК РФ и причинением смерти по неосторожности (ст. 109 УК РФ). Но если судом будет доказано, что подсудимый совершил данное противоправное деяние умышленно и при наличии цели убить пациента, то квалификация будет согласно ст. 105 УК РФ – убийство. Личность, которая достигла совершеннолетия, в данном случае 16 лет и является полностью дееспособной является субъектом противоправного деяния. В новой редакции статьи законодательные органы отказались от субъекта преступления: лицо, которое имеет к доступ электронно-вычислительной машине, системе ЭВМ и их сети. Таким образом, лицо, которое в силу своих должностных обязанностей обязано знать правила эксплуатации и средств хранения, обработки и передачи компьютерной информации, отвечает по санкциям равно также как и лицо,

которое по своим должностным обязанностям не обязано знать все соответствующие правила. На наш взгляд, это неправильно и необходимо дифференцировать ответственность лиц в зависимости от их должностных обязанностей и знаний, также как это имеет место быть в ст. 272 и ст. 273 УК РФ.

В ч. 2 ст. 274 УК РФ указан квалифицирующий признак. Так, к нему относится наступление тяжких последствий или угрозы их наступления. Категория тяжести преступления устанавливается судом после изучения соответствующих материалов и является оценочной категорией. Таким образом, категория «Тяжкое преступление» по сути тождественно категории «Крупный ущерб» и не может иметь смысл менее этого. В старой редакции ст. 274 УК РФ было указано на совершение преступления только по неосторожности, в новой же редакции совершение преступления возможно как умышленно, так и по неосторожности.

Наступление ответственности в новой редакции ст. 274 УК РФ получило значительное усиление. В старой редакции присутствовал такой вид наступления ответственности, как лишение права заниматься определенным видом деятельности или занимать определенные должности сроком до 5 лет, совершение обязательных работ сроком от 180 до 240 часов, а также лишение свободы сроком до двух лет. Новая редакция ст. 274 УК РФ предусматривает следующие виды наказания: вынесение штрафа на сумму до 500 000 руб. или в размере заработной платы или иного дохода за период до восемнадцати месяцев, совершение исправительных работ от полугода до года, лишение свободы или ограничение до двух лет, либо замена лишения свободы на принудительные работы сроком до двух лет. Анализируя вышесказанное видно, что суд отказался от такой меры ответственности как лишение права заниматься определенным видом деятельности или занимать определённую должность в течение 5 лет, но при этом ввёл штраф до 500 000 руб., а также суровое наказание в виде лишения свободы сроком до 2 лет. Наступление ответственности по ч. 2 ст. 274 УК РФ также получило более серьезные

санкции: наступление ответственности возможно в виде принудительных работ или лишение свободы, при этом срок увеличен до пяти лет.

Подведем итоги параграфа и сделаем выводы.

Редакция ст. 274 УК РФ на наш взгляд являются самой успешной из редакций статей главы 28 Уголовного кодекса Российской Федерации. Замена терминологии «Существенный вред» на «Крупный ущерб» позволяет судебную практику привезти в единство, а разнообразное количество наказаний за совершенное противоправное деяние позволяют дифференцировать ответственность по степени наносимого вреда общественным отношениям, индивидуальных характеристик подсудимого и другого, чем отличается каждой преступление от подобных ему.

Преступления в кибепространстве не получили достаточной изученности в правовом поле, нет четкого определения всех возможных квалифицирующих признаков и составов преступлений. Четко прослеживается необходимость во внесении доработок, направленных на доведения до совершенства статей УК РФ в этой области, а также более детальная разработка санкций, применяемых к противоправным деяниям в области киберпространства, которые будут отличаться соразмерностью за совершенные деяния. При этом возможно включение в нормы как новых составов, так и введение дополнительных квалифицирующих признаков, касающихся уточнения объективной стороны деяния как преступления, совершаемого с применением компьютерных технологий.

Поскольку преступления, совершаемые с применением компьютерных технологий, давно вышли за пределы отдельного государства, то для борьбы с ними необходимо объединить усилия Российской Федерации с международным сообществом путем ратификации международных договоров и включения унифицированных норм международного права в данной области в национальное законодательство, в том числе и уголовное.

Заключение

В ходе написания данной работы были сделаны определённые выводы, характеризующие современное состояние уголовного законодательства РФ в сфере регулирования преступлений, совершаемых с применением компьютерных технологий.

В законодательстве РФ отсутствуют критерии, согласно которым ту или иную программу можно отнести к вредоносной и наносящей угрозу жизни общества (Ст. 273 УК РФ). Для отнесения программы к вредоносной необходимо провести соответствующую экспертизу с соблюдением всех необходимых тонкостей.

Согласно ст. 274 Уголовного кодекса Российской Федерации пользователь компьютера может быть привлечен к ответственности при неправильном использовании компьютера и несоблюдения средств защиты информации. Сюда можно отнести нарушение правил пользования и хранения, обработки и отправки очень важной конфиденциальной информации, а также нарушение правил доступа к сетям.

С помощью сети «Интернет» злоумышленник может совершить преступление и получить нелегитимным путем сведения пользователей и различных фирм, но и также получить доступ к сведениям, составляющим государственную тайну. С появлением Интернета значительно возросла общественная опасность преступлений, предусмотренных Главой 29 Уголовного кодекса РФ. Непосредственно с помощью Интернета могут совершаться: государственная измена (ст. 275 Уголовного кодекса РФ), шпионаж (ст. 276 Уголовного кодекса РФ), публичные призывы к осуществлению экстремистской деятельности (ст. 280 Уголовного кодекса РФ), диверсия (ст. 281 Уголовного кодекса РФ), возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 Уголовного кодекса РФ), разглашение государственной тайны (ст. 283 Уголовного кодекса РФ), утрата документов содержащих государственную тайну (ст. 284

Уголовного кодекса РФ). Целесообразно дополнить эти статьи, указав, что данные преступные действия могут быть совершены посредством использования информационно-коммуникационных сетей.

Необходимы дополнения для классификации признака относительно того, что преступление было совершено посредством использования интернета. Однако, в данном случае совершение преступления с помощью сети «Интернет» должно являться стандартным способом осуществления противоправного действия, наносящего вред обществу. Данное изменение наиболее необходимо в ст. 110, 128.1, 137, 138, 146, 150, 151, 174, 174.1, 205.1, 205.2, 230, 242, 272, 273, 280 Уголовного кодекса РФ.

Информационную безопасность можно определить как сумму отношений, возникающих в обществе, которые способны обеспечить связанную с ними деятельность, хранение, систематического пополнения, использования и передачу сведений, участниками которых являются обладатели данных сведений и владельцы, которые пользуются данной информации в своих целях.

Редакция ст. 274 УК РФ на наш взгляд являются самой успешной из редакций статей главы 28 Уголовного кодекса Российской Федерации. Замена терминологии «Существенный вред» на «Крупный ущерб» позволяет судебную практику привезти в единство, а разнообразное количество наказаний за совершенное противоправное деяние позволяют дифференцировать ответственность по степени наносимого вреда общественным отношениям, индивидуальных характеристик подсудимого и другого, чем отличается каждой преступление от подобных ему.

Преступления в кибепространстве не получили достаточной изученности в правовом поле, нет четкого определения всех возможных квалифицирующих признаков и составов преступлений. Четко прослеживается необходимость во внесении доработок, направленных на доведения до совершенства статей УК РФ в этой области, а также более детальная разработка санкций, применяемых к противоправным деяниям в

области киберпространства, которые будут отличаться соразмерностью за совершенные деяния.

При реализации данной работы необходимо указать на то, что использование компьютера и Интернета позволяет преступникам совершать преступление более легким способом ввиду того, что эти преступления отличаются высокой степенью анонимности, быстротой и не требует большого количества денежных средств для осуществления действий. Также важно упоминать, что совершение противоправного деяния с помощью компьютера и интернета возможно из любой точки мира и может пересекать границы нескольких стран.

Уголовный Кодекс РФ закрепляет далеко не полный перечень преступлений с использованием компьютерных технологий, поэтому он требует дальнейшего расширения и систематизации. При этом возможно включение в нормы как новых составов, так и введение дополнительных квалифицирующих признаков, касающихся уточнения объективной стороны деяния как преступления, совершаемого с применением компьютерных технологий.

Поскольку преступления, совершаемые с применением компьютерных технологий, давно вышли за пределы отдельного государства, то для борьбы с ними необходимо объединить усилия Российской Федерации с международным сообществом путем ратификации международных договоров и включения унифицированных норм международного права в данной области в национальное законодательство, в том числе и уголовное.

Список используемой литературы и используемых источников

1. Алавердов О. С. Международное сотрудничество в области борьбы с интернет-преступностью // Общество и право. 2010. № 3 (30). С. 165-168.
2. Батурин Ю. М. Проблемы компьютерного права / Батурин Ю.М. М. : Юрид. лит., 1991. 272 с.
3. Беспалова Е.В., Широков В.А. Киберпреступность: история уголовно-правового противодействия // Информационное право. М. : Юрист, 2006, № 4 (7). С. 3-5.
4. Бутусова Л.И. К вопросу о киберпреступности в международном праве // Вестник экономической безопасности. 2016. № 2. С. 48-52.
5. Быков В.М., Черкасов В.Н. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ // Российский судья. М.: Юрист, 2012, № 5. С. 14-19.
6. Вехов В.Б. Компьютерные преступления. Способы совершения. Методики расследования / Вехов В.Б. М. : Право и Закон, 1996. 182 с.
7. Волеводз А.Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. М. : Юрист, 2007, № 2. С. 17-25.
8. Голубев В.А. Компьютерная преступность: состояние, угрозы и прогнозы // Компьютерная преступность и кибертерроризм. Сборник научных работ: вып. № 2. Запорожье : Центр исследования компьютерной преступности, 2004. С. 20-25.
9. Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4) // Консультант плюс: справочно-правовая система.
10. Дворецкий М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания: Монография / М.Ю. Дворецкий. Тамбов : Изд-во ТГУ, 2003. 197 с.

11. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // Консультант плюс: справочно-правовая система.

12. Доронин А. М. Уголовная ответственность за неправомерный доступ к компьютерной информации. Дис. … канд. юрид. наук: 12.00.08 / Доронин А.М. М., 2003. 154 с.

13. Зверянская Л.П., Протасевич А.А. Борьба с киберпреступностью как актуальная задача современной науки // Криминологический журнал Байкальского государственного университета экономики и права. Иркутск : Изд-во БГУЭП, 2011, № 3. С. 28-33.

14. Зубкова М.А. Компьютерная информация как объект уголовно-правовой охраны. Автореф. дис. ... канд. юрид. наук / Зубова М.А. Казань, 2008. 27 с.

15. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. Т. 22. № 8. С. 46-50.

16. Конвенция о преступности в сфере компьютерной информации (EST № 185) от 23 ноября 2001 // Консультант плюс: справочно-правовая система.

17. Кондратьев Ю.А., Сафонов О.М. Особенности толкования термина «компьютерные технологии» для целей уголовно-правового регулирования // Конвенционные начала в уголовном праве: материалы Международной научно-практической конференции (Москва, 22 ноября 2017 года). М. : РПА Минюста России. С. 165-168.

18. Кочкина Э.Л. Определение понятия «киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3. С. 162-169.

19. Кузнецов А.П. Ответственность за преступления в сфере компьютерной информации по зарубежному законодательству // Международное публичное и частное право. М. : Юрист, 2007, № 3. С. 60-62.

20. Лошенкова Е.В. Понятия и термины в уголовном праве России. Общая и особенная части: учеб. пособие / Отв. ред. проф. А.И. Чучаев; Е.В. Лошенкова. М. : Контракт, 2014. 320 С. [Электронный ресурс]. URL: https://rucont.ru/efd/409949 (дата обращения: 21.01.21).

21. Медведев С.С. Общественная опасность мошенничества в сфере высоких технологий как основание его криминализации // Общество и право. Научно-практический журнал. Краснодар: Изд-во Краснодар. ун-та МВД России, 2008, № 3 (21). С. 164-166.

22. Морар И.О. Как выглядит социально-правовой портрет участника преступного формирования, совершающего компьютерные преступления? // Российский следователь. М. : Юрист, 2012, № 13. С. 34-38.

23. Неофициальные механизмы международного сотрудничества [Электронный ресурс]. URL: https://www.unodc.org/e4j/ru/cybercrime/module-7/key-issues/informalinternational-cooperation-mechanisms.html (дата обращения: 05.11.20).

24. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология. Вчера. Сегодня. Завтра. 2012. № 1 (24). С. 45-55.

25. Официальный сайт Егорьевского городского суда Московской области [Электронный ресурс]. URL: http://egorievsk.mo.sudrf.ru (дата обращения: 11.12.20).

26. Официальный сайт Октябрьского районного суда города Кирова [Электронный ресурс]. URL: http://oktyabrsky.kir.sudrf.ru (дата обращения: 11.12.20).

27. Официальный сайт судебного участка № 48 Промышленного судебного района г. Самары Самарской области [Электронный ресурс]. URL: http://48.sam.msudrf.ru/modules.php?name=sud_delo&op=rd (дата обращения: 11.12.20).

28. Официальный сайт Томского областного суда [Электронный ресурс]. URL: http://oblsud.tms.sudrf.ru (дата обращения: 14.12.20).

29. Постановление Пленума Верховного Суда РФ от 07.07.2015 № 32 (ред. от 26.02.2019) «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» // Консультант плюс: справочно-правовая система.

30. Постановление Пленума Верховного Суда РФ от 10 июня 2010 г. № 12 «О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней)» [Электронный ресурс]. URL: https://base.garant.ru/1795384/ (дата обращения: 11.02.21).

31. Постановление Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/1685377/ (дата обращения: 11.02.21).

32. Постановление Правительства РФ от 26 октября 2012 г. № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» (с изменениями и дополнениями) [Электронный ресурс]. URL: https://base.garant.ru/70248270/ (дата обращения: 11.02.21).

33. Программа Министерства внутренних дел Российской Федерации «Создание единой информационно-телекоммуникационной системы органов внутренних дел» (Извлечение) (утв. приказом МВД РФ от 08.06.2006 № 420) // Консультант плюс: справочно-правовая система.

34. Распоряжение Правительства РФ от 28.05.2012 № 856-р «О подписании Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в области обеспечения информационной безопасности» // Консультант плюс: справочно-правовая система.

35. Рассолов И.М. Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. Общероссийский научно-практический правовой журнал. М. : Юрист, 2008, № 2 (134). С. 44-46.

36. Рекомендация Совета Европы № 89 (9). О преступлениях, связанных с компьютерами от 13 сентября 1989 [Электронный ресурс] // Council of Europe: [сайт]. URL: https://wcd.coe.int/ViewDoc.jsp?Ref=Rec%2889%299&Language=lanEnglish&Ver=original&Site=C%20M&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC 75 (дата обращения: 05.01.2021).

37. Российский дипломат назвал Будапештскую конвенцию по киберпреступлениям устаревшей [Электронный ресурс]. URL: https://tass.ru/politika/4782506 (дата обращения: 05.11.20).

38. Российское уголовное право. Особенная часть: Учебник / Под ред. проф. А.И. Чучаева. М. : НИЦ Инфра-М: Контракт. 2012. 448 с.

39. Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Вместе с «Перечнями основных понятий и видов угроз, их источников и признаков») (Заключено в г. Екатеринбурге 16.06.2009) // Консультант плюс: справочно-правовая система.

40. Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 01 июня 2001 [Электронный ресурс] // Исполнительный комитет СНГ: [сайт]. URL: http://www.cis.minsk.by/page.php?id=866 (дата обращения: 06.03.2021).

41. Соловьев И.Н. Правовое обеспечение борьбы с преступлениями в сфере информационных технологий // Административное и муниципальное право. М. : Nota Bene, 2009, № 3 (15). С. 63-65.

42. Старичков М.В. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института МВД России. Иркутск. 2014. № 1 (68). С. 16-20.

43. Сухаренко А.Н. Российская корпоративная преступность (в зарубежных оценках) // Юридический мир. М. : Юрист, 2012, № 5 (185). С. 12-15.

44. Талимончик В. П. Конвенции о киберпреступности и унификация законодательства // Информационное право. 2008. № 2. С. 27-30.

45. Уголовный кодекс Российской Федерации: федеральный закон РФ от 13.06.1996 № 63-ФЗ (посл. ред.) // Консультант плюс: справочно-правовая система.

46. Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 07.12.2011 № 420-ФЗ (последняя редакция) // Консультант плюс: справочно-правовая система.

47. Федеральный закон «О ратификации Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» от 01.10.2008 № 164-ФЗ (последняя редакция) // Консультант плюс: справочно-правовая система.

48. Федеральный закон «Об участии в международном информационном обмене» от 04.07.1996 N 85-ФЗ (утратил силу) // Консультант плюс: справочно-правовая система.

49. Халиуллин А.И. Подходы к определению компьютерной преступности // Проблемный анализ и государственно-управленческое проектирование. 2011. Т. 4. № 6. С. 16-23.

50. Ястребов Д.А. Неправомерный доступ к компьютерной информации: уголовно-правовые и криминологические аспекты. Дис. … канд. юрид. наук: 12.00.08 / Ястребов Д.А. М., 2005. 243 с.

51. African Union Convention on Cyber Security and Personal Data Protection [Электронный ресурс]. URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (дата обращения: 11.11.20).

52. Arab Convention on Combating Information Technology Offences [Электронный ресурс]. URL: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf (дата обращения: 05.11.20).

53. Criminal Justice (Theft and Fraud Offences) Act, 2001 [Электронный ресурс] // Irish Statute Book: [сайт]. URL: http://www.irishsta tute book.ie/pdf/2001/en.act.2001.0050.pdf (дата обращения: 12.01.2021).

54. Final report of the European Committee on Crime problems [Электронный ресурс] // Council of Europe: [сайт]. URL: http://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fwww.oas.org%2Fjuridico%2Fenglish%2F89-9%26final%2520Report.pdf&ei=geHUUtL1B_HV4QSM2YGIDA&usg=AFQjCNG1j8lttGcwIGrnzpNvbwaXh4OVpA&sig2=aRVF0r3Ah_BxCya ZQ-f5og&bvm=bv.59378465,d.bGE&cad=rja (дата обращения: 14.01.2021).

55. Global Cyber and Intellectual Property Crimes [Электронный ресурс]. URL: https://www.justice.gov/criminal-opdat/global-cyber-and-intellectualproperty-crimes (дата обращения: 05.11.20).

56. Internet Governance Forum: Council of Europe addresses challenges to human rights resulting from Artificial Intelligence [Электронный ресурс]. URL: https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=090000168098dd63 (дата обращения: 11.11.20).

57. League of Arab States, 2010. Arab Convention on Combating Information Technology Offences (League of Arab States Convention) [Электронный ресурс]. URL: https://itlaw.wikia.org/wiki/Arab_Convention_on_Combating_Information_Technology_Offences (дата обращения: 11.11.20).

58. Ligh M., Adair S., Hartstein B., Richard M. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Indianapolis: Wiley Publishing, Inc., 2010. 716 p.

59. Rogers M. A New Hacker Taxonomy. Winniper, 2011. 85 p.