ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(Н И У « Б е л Г У »)

ЮРИДИЧЕСКИЙ ИНСТИТУТ НИУ «БЕЛГУ»

КАФЕДРА УГОЛОВНОГО ПРАВА И ПРОЦЕССА

ТЕМА: «РАССЛЕДОВАНИЕ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО В СЕТИ «ИНТЕРНЕТ»: КРИМИНАЛИСТИЧЕСКИЕ И УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ»

Выпускная квалификационная работа
обучающегося по магистерской программе «Уголовный процесс, криминалистика и судебная экспертиза, теория оперативно-розыскной деятельности», направление подготовки 40.04.01 Юриспруденция, заочной формы обучения, группы 01001665
Епифанова Николая Яковлевича

Научный руководитель:
доцент кафедры уголовного права и процесса, к.п.н., доцент
Савельева И.В.

Рецензент:
старший прокурор отдела по надзору за уголовно-процессуальной и оперативно-розыскной деятельностью
младший советник юстиции, к.ю.н.,
Баранов С.А.

БЕЛГОРОД 2018

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Развитие современных государств и переход от индустриального к информационному обществу послужило причиной повсеместного внедрения высоких технологий практически во все сферы человеческой жизнедеятельности. Стремительная, практически неконтролируемая информатизация общества, при всех ее достоинствах, породила и ряд новых актуальных на сегодняшний день проблем, одной из которых является криминализация телекоммуникационных и компьютерных систем связи. Появление новых угроз и с ростом числа компьютерных преступлений по всему миру обусловило принятие рядом зарубежных государств специального законодательства в сфере информационной безопасности. Российская Федерация не стала исключением и включила в Уголовный Кодекс (далее - УК РФ) главу 28, посвященную преступлениям в сфере компьютерной информации.

Стремительный рост информатизации, захвативший практически все стороны жизни нашего общества, увелечение автоматизированных рабочих мест, используемых в России, вместе с тем недостаточный уровня защищенности компьютерной информации от несанкционированного доступа и противоправных посягательств ведет к тому, что проблема информационной безопасности встанет на ряду с глобальными проблемами современностями такими как экологическим кризисом, организованной преступностью, экстремизом, терроризмом, коррупцией.

В качестве примера хочу привести следующую статистику: количество преступлений, совершаемых в сфере компьютерной информации, с каждым годом растет. По данным ГИЦ МВД России, если в 1998 году было зарегистрировано всего 12 преступлений в сфере компьютерной информации,

то в 2009 году их число возросло до 4050 таких преступлений, в 2014 году составило 10214 случаев, а к 2017 году число преступлений в сфере информационно-телекоммуникационных технологий увеличилось с 65949 до 90587. Их доля от числа всех зарегистрированных в России преступных деяний составляет 4,4% — это почти каждое 20 преступление.

Статистика данного вида преступлений, показывает, что от 30% до 40% киберпреступлений совершаются подростками в возрасте от 14 до 16 лет — к таким выводам пришли авторы исследования «Threat Zone 17/18: новые вызовы цифрового мира», осуществленного Сбербанком совместно с дочерней компанией BI.ZONE. Данные результатов исследования были обнародованы на Международном конгрессе по кибербезопасности в Москве. Также данное исследование показало, что целями примерно половины хакерских атак становятся крупные компании финансового сектора. При этом общественность узнает только о 20% инцидентов, в частности, потому, что компании не желают раскрывать эту информацию в связи с их репутацией. Естественно, указанные деяния отличаются высокой латентностью. Как показывают уголовная, судебная практика и статистика, значительная часть таких преступлений остается за рамками реально выявленных и раскрытых[1].

Безусловно, развитие информационных технологий является в большей степени положительным явлением, улучшающим все условия существования людей, делающим эту жизнь более комфортной. Однако к нашему большому сожалению, технический прогресс имеет и обратную сторону, порождая ряд негативных последствий. Одно из них – развитие новых направлений преступной деятельности, связанной с применением информационных технологий.

Одним из таких преступных деяний, обусловивших внесение изменений в действующее уголовное законодательство, стало мошенничество в сфере

[1] Официальный сайт МВД России. Общие сведения о состоянии преступности. www.mvdinform.ru.

компьютерной информации ст. 159.6 УК РФ[2]. Случаи мошенничества, в основе которых лежит использование разнообразной экономически значимой компьютерной информации, в настоящее время получают все большее распространение. В данной работе разберем уголовно-правовую, процессуальную и криминалистическую характеристику мошенничества в сфере компьютерной информации.

Степень научной разработанности проблемы. Научно-правовую основу исследования составляют работы: К.Э. Шеннона, А.М. Тьюринга, Д.Ф. Неймана, Норберт Винера, Л.И. Шершнева, Н.И. Шумилова, В.В. Крылова, Т.Г. Смирнова, И.А. Клепицкого, А.И. Гурова, Ю.М. Батурина, А.М. Жодзишского, Ю.М. Батурина, В.Б. Вехова, В.В. Крылова, В.Д. Курушина, В.А. Минаева, и др.

Однако в целом данная тематика еще недостаточно разработана, находится на этапе своего формирования и развития. Имеется относительно небольшое число монографических исследований, большинство материалов составляют научные статьи в периодической печати.

Тем не менее, несмотря на обилие трудов, посвященных обозначенным вопросам, в науке и на практике отсутствуют исследования, комплексно рассматривающие проблематику данной темы.

Объектом выпускной квалификационной работы являются общественные отношения, складывающиеся в сфере обмена электронными документами, базами данных и программным обеспечением. Мошенничество в сфере компьютерных технологий, как и мошенничество вообще - это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием в соответствии со ст. 159.6 УК РФ.

Предмет исследования являются особенности расследования мошеннических действий, совершенных с использованием информационно-коммуникационных технологий.

---

[2] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ // СПС КонсультантПлюс.

Цель исследования: выявить теоретические и практические проблемы противодействия преступлениям, совершенным с использованием информационно-коммуникационных технологий, а также проанализировать возможности международного сотрудничества государств при расследовании рассматриваемого вида преступлений. Поставленная цель требует решения взаимосвязанных исследовательских задач.

Задачи исследования:

– проанализировать внесение изменений в Российское уголовное законодательство в сфере компьютерной информации при развитии информационно-коммуникационных технологий;

– провести сравнительный анализ зарубежного опыты противодействия преступлениям совершаемым в сфере компьютерной информации;

– предложить идеи и решения по совершенствованию государственной политики в области противодействия преступлениям, совершаемых с использованием информационно-коммуникационных технологий;

– определить уголовно-правовую характеристику мошенничества, совершенного с использованием информационно-коммуникационных технологий;

– определить криминалистическую характеристику мошенничества, совершенного с использованием информационно-коммуникационных технологий;

– выявить тактические особенности при осуществлении оперативно-розыскных мероприятий и следственных действий, проводимых при расследовании мошенничества, совершаемого с использованием информационно-коммуникационных технологий;

– предложить тезисы, способствующие улучшению методов противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

Теоретическая и практическая значимость результатов исследования. Современный этап характеризуется устойчивой тенденцией роста компьютерных преступлений, как в России, так и во всем мировом информационном пространстве.

Необходимость совершенствования государственной политики по противодействию преступлениям в сфере информационных технологий подтверждается тем, что в последнее время данные преступления стали глобальной международной проблемой, многие из них имеют трансграничный характер.

Указанные обстоятельства обусловили выбор темы настоящего исследования, ее актуальность.

Методологическая и методическая основы исследования. В настоящей научной работе для достижения целей исследования диссертантом были использованы следующие общенаучные и частнонаучные методы правового регулирования: индукции, дедукции, анализа, синтеза, сравнительно-правовой метод, исторический и иные.

Нормативную базу работы составляют: Конституция Российской Федерации, Уголовный кодекс РФ, Уголовно-процессуальный кодекс РФ. Нормативно-правовые акты регламентирующие вопросы информационной безопасности и защиты информации в РФ, иные Федеральные законы, постановления Правительства РФ, отраслевые и ведомственные акты Министерства внутренних дел РФ, ФСБ РФ, ФСТЭК РФ и др.

При проведении диссертационного исследования были использованы законодательные источники зарубежного уголовного права, регламентирующие охранительные правоотношения в области информационных технологий и защиты информации.

Научная новизна выпускной квалификационной работы: состоит в том, что предлагается создание межгосударственного ведомства по борьбе с

киберпреступлениями, включающего в свой штат наиболее подготовленных и компетентных специалистов в рассматриваемой сфере из числа государственных служащих стран - участников данного ведомства, наделенных полномочиями, позволяющими осуществлять правоохранительную деятельность на их территориях, уровень обеспечения которого будет соответствовать уровню технического развития в сфере компьютерных технологий, также разработка и введение единого, для всех государственных служб и подконтрольных подразделений (а также лиц, взаимодействующих с ними в силу своей деятельности), ресурса (с применением блокчейн технологий), представленного в виде «гибрида» централизованной и децентрализованных систем, обеспечивающего электронный документооборот и хранение информации. При этом, на основе указанного ресурса необходимо объединить имеющиеся базы данных и создать новую, единую электронную базу данных.

Основные положения, выносимые на защиту:

1. Результаты теоретико-методологического анализа исследований, а также практики работы правоохранительных органов показали, что в деятельности по раскрытию, расследованию, предупреждению и пресечению мошенничества, совершенного с использованием информационно-коммуникационных технологий, возникают различного рода противоречия, вызванные проблемами как теоритического, так и практического свойства. В частности, до настоящего времени нет единого подхода к определению понятия компьютерных преступлений, четко не выстроена система подобных преступлений.

2. На основе анализа отечественного и зарубежного законодательства в области компьютерной информации предлагается первоначальное авторское определение дефиниции «компьютерные преступления».

«Компьютерное преступление - предусмотренное уголовным законом, противоправное, виновное нарушение чужих прав и интересов, связанное с

использованием, модификацией, уничтожением компьютерной информации, причинившее вред либо создавшее угрозу причинения вреда подлежащим уголовно-правовой охране правам и интересам физических и юридических лиц, общества и государства (личным правам и неприкосновенности частной сферы, имущественным правам и интересам, общественной и государственной безопасности в области высоких технологий и конституционному строю)».

3. Любые компьютерные преступления имеют свои характерные криминалистические особенности, в том числе особенности проведения оперативно-розыскных мероприятий и следственных действий, представляющих наибольшую трудность для субъектов расследования интернет-мошенничества. Такими особенностями являются предмет, способ и обстановка совершения мошенничества в среде «Интернет». В целях единообразного подхода к процедуре выявления и расследования интернет-мошенничеств, предлагается следующее определение обстановки совершения интернет-мошенничества:

«Под обстановкой совершения интернет-мошенничества понимается система взаимообусловленных и взаимосвязанных элементов, в пространственных и временных границах которых происходит взаимодействие между преступниками и их жертвами, а также тех обстоятельств объективной среды, которые имели место на момент расследования и оказывали влияние на формирование следов преступления, его выявление и расследование».

4. В процессе расследования исследуемых преступлений следует учитывать, что подготовка, написание, тестирование специальных компьютерных программ для взлома, внедрение вредоносных «троянских» программ, программ-шпионов, поиск паролей или определение способов беспарольного входа будет оставлять виртуальные следы в памяти компьютера или иного технически сложного устройства, используемого мошенником.

В связи с чем, предлагается создание межгосударственного ведомства по борьбе с киберпреступлениями, включающего в свой штат наиболее

подготовленных и компетентных специалистов в рассматриваемой сфере из числа государственных служащих стран - участников данного ведомства, наделенных полномочиями, позволяющими осуществлять правоохранительную деятельность на их территориях, уровень обеспечения, которого будет соответствовать уровню технического развития в сфере компьютерных технологий, также разработка и введение единого, для всех государственных служб и подконтрольных подразделений (а также лиц, взаимодействующих с ними в силу своей деятельности), ресурса (с применением блокчейн технологий), представленного в виде «гибрида» централизованной и децентрализованных систем, обеспечивающего электронный документооборот и хранение информации. При этом на основе указанного ресурса необходимо объединить имеющиеся базы данных и создать новую, единую электронную базу данных.

5. Правотворческая деятельность по уголовно-правовому противодействию преступлениям в сфере использования информационно-коммуникационных технологий на сегодняшний день имеет ряд существенных недоработок, обусловленных бессистемным и хаотичным изменением законодательства в указанной сфере, что неизбежно порождает трудности и сложности при квалификации деяний по указанным нормам.

Руководствуясь критерием оценки опасности действия в зависимости от вероятности наступления общественно опасных последствий, полагаем, что использование ИКТ должно признаваться квалифицирующим признаком составов преступлений, объективная сторона которых связана с распространением деструктивной информации. В связи чем, предлагаем дополнить соответствующие части статей 230 «Склонение к потреблению наркотических средств, психотропных веществ или их аналогов», ст. 354 «Публичные призывы к развязыванию агрессивной войны, ст. 354.1 «Реабилитация нацизма», ст. 298.1 «Клевета в отношении судьи, присяжного

заседателя, прокурора, следователя, лица, производящего дознание, судебного пристава» пунктом следующего содержания:

«совершенные с использованием информационно-коммуникационных технологий».

6. С целью улучшения качества работы правоохранительных органов по раскрытию, расследованию, а также противодействию преступлениям совершаемым с использованием информационно-коммуникационных технологий, предлагается осуществление существенных изменений как в структуре, так и в организации учебного процесса в образовательных учреждениях, организующих подготовку специалистов в области информационной безопасности, не только технических профилей, но и будущих (а также действующих) сотрудников правоохранительных органов (сотрудники оперативных подразделений, дознаватели, следователи, прокуроры, судьи).

Структура выпускной квалификационной работы соответствует логике построения научного исследования и состоит из введения, трех глав, выключающих в себя 3 параграфа, 2 параграфа, 2 параграфа, заключения и списка используемой литературы.

Апробация работы. Результаты исследования нашли свое отражение в двух публикация автора, кроме того активно используются в практике работы специального подразделения УМВД России по Белгородской области.

ГЛАВА 1. СИСТЕМА ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СВЯЗАННЫМ С КОМПЬЮТЕРНОЙ ИНФОРМАЦИЕЙ

§ 1. Становление и развитие российского уголовного законодательства в сфере компьютерной информации

Американский ученый К.Э. Шеннон в 1948 году впервые определил само понятие «информация» и дал вероятностно-статистическое определение понятию «количество информации», связывая это явление с кибернетикой[3]. Кибернетика занимается общими законами преобразования информации в сложных управляющих системах. Она рассматривает информацию не как общественный феномен, т.е. информацию, производимую и потребляемую обществом, а в более узком техническом аспекте, как информацию, циркулирующую по электронным каналам связи. Кибернетика доказала, что информация имеет непосредственное отношение к процессам управления и развития, обеспечивающим функционирование любых систем.

В широком смысле «информация» – это отражение реального (материального, предметного) мира, выражаемое в виде сигналов и знаков. Сигналы отражают физические (физически - химические) характеристики различных процессов и объектов. Действия, выполняемые с информацией, называются информационными процессами. Информационные процессы можно разложить на три составляющие: «хранение, передачу и обработку информации».

Качественное измерение информации предполагает понимание смысла, необходимости информации для определенных потребителей. Для человека содержание такой информации важнее, чем ее объем. Значимость информации

[3] Shannon C.E. A Mathematical Theory of Communication. Bell Systems Technical Journal. July and Oct. 1948 //Claude Elwood Shannon. Collected Papers. N. Y., 1993. P. 8-111

определяется через изменение вероятности достижения некоторой цели после получения информации.

Информационные отношения долгое время не признавались самостоятельным объектом правового регулирования, однако в настоящее время роль информации настолько возросла, что информационные отношения признаны специфическим предметом правового регулирования.

Под социальной информацией понимается: сложное многоаспектное явление, что обуславливает сложности в правовом регулировании информационных отношений. С этой целью создается новое «информационное» законодательство и система мер уголовно-правовой защиты данной группы отношений. Наблюдается большое разнообразие мнений российских ученых-юристов в определениях таких понятий как «информационная безопасность» и «компьютерная преступность».

Л.И. Шершнев «информационную безопасность» понимает как: «способность государства, общества, социальной группы, личности обеспечить с определенной вероятностью достаточные и защищенные информационные ресурсы и информационные потоки для поддержания своей жизнедеятельности и жизнеспособности устойчивого функционирования и развития; противостоять информационным опасностям и угрозам, негативным информационным воздействием на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические системы информации; вырабатывать личностные и групповые навыки и умения безопасного поведения; поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно не было навязано»[4].

Н.И. Шумилов предлагает определять «информационную безопасность» как: «состояние защищенности информационной сферы государства, общества, личности, обеспечиваемое комплексом мер по снижению, предотвращению или исключению негативных последствий от воздействия на элементы

[4] Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: Инкомбук, 1997.

информационной сферы»[5]. Думается, что, понятие информационной безопасности, данное Л.И. Шершневым, более емкое, не требующее дальнейшего толкования такого понятия как информационная сфера, чем у Н.И. Шумилова.

Результативность противодействия преступности в целом и отдельным её видами напрямую зависит, как известно, от качества и глубины знаний о ней, от специфики вида преступности, уяснения сущностных характеристик ее причин. В юридических науках при анализе конкретного вида преступности используются уголовно-правовая, криминалистическая, криминологическая и иные характеристики, концентрирующие внимание исследователя на определенных сторонах одного и того же явления. Конкретное содержание криминологической характеристики преступлений заключается в выявлении всех признаков, составляющих в своей совокупности и взаимосвязи её структуру, в которой выделяется три блока: первый блок – криминологически значимые признаки преступления; второй блок – данные, раскрывающие криминологическую ситуацию совершения преступлений таких типов; третий блок – признаки, определяющие специфику деятельности по предупреждению преступности.

По характеру проявлений и своей сущности основными элементами криминологической характеристики компьютерной преступности являются: её общественная опасность, отграничение компьютерной преступности от других смежных явлений, её типичные свойства и на этой основе выделение типологии компьютерных преступлений, сведения о социальных условиях компьютерных преступлений (социально-политических, геополитических, социально-экономических, временных и иных), проблемы латентности, личность компьютерного преступника, мотив и цель преступления, свойства личности потерпевшего, а также комплекс мер противодействия на основе установления причин и условий, воспроизводящих данный вид преступности, иных факторов,

[5] Шумилов Н.И. Информационная безопасность: методическое пособие для сотрудников. правоохранительных органов / Под ред. И.А. Возгрина. СПб: СПб. Академия МВД России, 1997, 26с.

способствующих совершению компьютерных преступлений. В основе криминологической характеристики, безусловно, лежит процесс выделения данного вида преступности в качестве самостоятельного предмета научного исследования, уточнение понятийного аппарата и особенностей компьютерных преступлений в конкретных общественно-социальных условиях, определенных пространственно-временными границами.

Компьютерные преступления и компьютерная преступность стали предметом научного исследования сравнительно недавно. Термин «компьютерная» или «электронная» преступность впервые появился в зарубежной печати в связи с выявлением первых правонарушений, совершенных с использованием возможностей электронно-вычислительных машин, и не имел ни терминологического, ни иного (в том числе и криминологического) обоснования. Он возник применительно к так называемому «компьютерно-телефонному фанатизму», который выражался в недобросовестном использовании компьютеров и телефонов для заказа различных товаров и услуг через информационные сети различных торговых фирм без оплаты. Тем не менее, этот термин стал широко использоваться в правоприменительной практике и распространяться как в национальном, так и в международном масштабе. В настоящее время однозначной трактовки понятия компьютерного преступления и взаимосвязанного с ним понятия компьютерной преступности не выработано.

В.В. Крылов под информационными преступлениями считает: «общественно опасные деяния, совершенные в области информационных правоотношений и запрещенные уголовным законом под угрозой наказания[6]».

Общеюридическая терминология в сфере информационных отношений вообще, и в отношении компьютерной информации в частности, до сих пор не установлена. В настоящее время в Уголовном кодексе Российской Федерации криминализированы далеко не все правонарушения в информационной сфере,

[6] Крылов В.В. Расследование преступлений в сфере информации. М., 2005. – 180 с.

или как их называют, в области высоких технологий, а лишь часть компьютерные правонарушения.

Понятие «компьютерные преступления» до сих пор в литературе трактуется по-разному. Существует мнение, что «с точки зрения уголовно-правовой охраны под компьютерными преступлениями следует понимать предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства». В данном случае «в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть».

Т.Г. Смирнова под преступлениями в сфере компьютерной информации подразумевает «запрещенные уголовным законом общественно-опасные виновные деяния, которые, будучи направлены на нарушение неприкосновенности охраняемой законом компьютерной информации и ее материальных носителей (в частности, компьютерной техники (ЭВМ), систем ЭВМ или их сетей), причиняют либо создают угрозу причинения вреда жизни и здоровью личности, правам и свободам человека и гражданина, государственной и общественной безопасности»[7]. Также, Т.Г. Смирнова полагает, что нарушение правил эксплуатации ЭВМ и распространение зловредных программ деструктивного характера следует рассматривать как разновидность диверсий, наносящих значительный ущерб компьютерной информации посредством разрушительных воздействий в отношении материальных носителей и зафиксированных на них данных.

В настоящее время в России накоплен определенный опыт выявления составов компьютерных преступлений, привлечения к уголовной ответственности, их квалификации и расследования. Поэтому все больше встает необходимость в представлении компьютерных преступлений как

[7] Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации. Дис… канд. юрид. наук. М., 1999. – 230 с. Степанов-Егинянц В. Ответственность за компьютерные преступления // Законность. – 2005. – №12. – С. 49.

подкласса преступлений, совершаемых посредством возможностей высоких технологий. По мнению А.И. Гурова, к преступлениям в области высоких технологий относятся[8]:

– нарушение тайны переписки, телефонных переговоров, телеграфных и иных сообщений с использованием специальных технических средств, предназначенных для негласного получения информации, и также незаконный сбыт или приобретение в целях сбыта таких средств;

– незаконный экспорт технологий научно-технической информации и услуг, используемых при создании вооруженной техники, оружия массового уничтожения;

– неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ);

– создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);

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

В связи с вышеизложенным можно определить термин «компьютерные преступления» следующим образом – это предусмотренное уголовным законом, противоправное, виновное нарушение чужих прав и интересов, связанное с использованием, модификацией, уничтожением компьютерной информации, причинившее вред либо создавшее угрозу причинения вреда подлежащим уголовно-правовой охране правам и интересам физических и юридических лиц, общества и государства (личным правам и неприкосновенности частной сферы, имущественным правам и интересам, общественной и государственной безопасности в области высоких технологий и конституционному строю).

[8] Гуров А.И. Криминогенная ситуация в России на рубеже XXI века. М., 2000. – 96 с

В России впервые закон о правовой охране программ для электронно-вычислительных машин и баз данных был принят в 1992 году. В ст. 128 Гражданского кодекса РФ, принятого 25 октября 1994 года, информация определялась как особый объект гражданских прав, наряду с вещами, иным имуществом и интеллектуальной собственностью.

20.02.1995 был принят закон «Об информации, информатизации и защите информации». Этот нормативный акт регулировал правовые отношения в сфере обмена и обработки информации с использованием технических средств. Под информацией в нем подразумевались «сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления». Продолжением развития отечественного законодательства стала разработка в проекте Уголовного кодекса РФ в 1996 года группы статей, предусматривающих уголовную ответственность за преступления в сфере компьютерной информации. Первые попытки составления статей, предусматривающих уголовную ответственность за компьютерные преступления в отечественной научной литературе, были ориентированы на выработку необходимых рекомендаций по совершенствованию ранее действующего уголовного законодательства в этой области.

На смену закону «Об информации, информатизации и защите информации» от 08.07.2006 пришел Федеральный закон «Об информации, информационных технологиях и о защите информации»[9] – базовый нормативный документ, юридически описывающий понятия и определения области информационной технологии и задающий принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации, а также регулирует отношения при осуществлении права на поиск, получение, передачу, производство и распространение информации, при применении информационных технологий.

[9] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // СПС КонсультантПлюс.

Ю.М. Батурин и А.М. Жодзишский в своем исследовании, посвященном компьютерным посягательствам, выделили среди преступлений в сфере компьютерной информации два основных вида – связанные с вмешательством в работу компьютера и предполагающие его использование в качестве необходимого технического средства.[10]

К первому можно отнести:

1) несанкционированный доступ к информации, хранящейся в компьютере;

2) ввод в программное обеспечение «логической бомбы», активирующейся при определенных условиях и частично или целиком выводящей из строя компьютерную систему;

3) разработку и распространение компьютерных программ разрушительного характера – вирусов;

4) некачественную разработку, изготовление и использование программно-вычислительного комплекса, проводящую к тяжким последствия;

5) подмену компьютерной информации;

6) хищение информации, содержащейся на компьютерных носителях.

В связи с тем, что, по мнению Ю.М. Батурина и А.М. Жодзишского, статьями Уголовного кодекса РСФСР 1960 г. охватывалась только часть этих преступлений (умышленное и неосторожное уничтожение или модификация компьютерной информации, небрежность в обращении с компьютерной системой), то предлагалось установить специальные основания уголовной ответственности за несанкционированное проникновение в вычислительные системы; похищение компьютерной информации; заражение компьютерными программами деструктивного характера.

Таким образом, возможно выделить в некоторых «обычных» преступлениях (хищении и т.д.) новый квалифицирующий признак: «совершение деяния с использованием средств компьютерной техники»

[10] Батурин Ю.М., Жодзишский А.М., Б28 Компьютерная преступность и компьютерная безопасность. – М.: Юрид, лит. 1991.- 160 с.

(второй вид компьютерных вмешательств), учитывая значительную общественную опасность данной категории преступлений.

Создатели проекта Уголовного кодекса, основываясь на схожих представлениях об объекте уголовно-правовой охраны, предложили включить компьютерные посягательства в одну из глав раздела «Преступления против общественной безопасности», где нашли место почти все виды преступлений, относимых данными авторами к вмешательству в работу компьютерных систем и компьютера. Уголовный кодекс РФ не учел данных формулировок, что, по мнению автора, взывает определенные сложности в правоприменительной практике.

§ 2. Зарубежный опыт противодействия преступлениям в сфере компьютерной информации

Законодательство об уголовной ответственности за компьютерные преступления в различных странах мира существенно отличается. Историческое развитие зарубежного законодательства показывает, что первый шаг в направлении защиты компьютерной информации был сделан зарубежным законодательством Швеции 04.04.1973, когда был принят «Закон о данных», который ввёл новое понятие в традиционное законодательство – «злоупотребление при помощи компьютера»[11].

Одной из первых стран мира, принявшей меры по установлению уголовной ответственности за совершение преступлений рассматриваемого вида, явились Соединенные Штаты Америки, где компьютерная преступность появилась несколько раньше, чем в других государствах. В 1977 г. в США был разработан законопроект о защите федеральных компьютерных систем. Он предусматривал уголовную ответственность за:

–введение заведомо ложных данных в компьютерную систему;

[11] https://ria.ru/20130809/955198703.html.

–незаконное использование компьютерных устройств;

–внесение изменений в процессы обработки информации или нарушение этих процессов;

–хищение денежных средств, ценных бумаг, имущества, услуг, ценной информации, совершенные с использованием возможностей компьютерных технологий или с использованием компьютерной информации.

На основе данного законопроекта в октябре 1984 году был принят Закон о мошенничестве и злоупотреблении с использованием компьютеров – основной нормативно-правовой акт, устанавливающий уголовную ответственность за преступления в сфере компьютерной информации. В последующем он неоднократно (в 1986, 1988, 1989, 1990, 1994 и 1996 гг.) дополнялся в связи с развитием информационных технологий и появлением новых угроз[12].

Сейчас же он включен в виде § 1030 Титула 18 Свода законов США. Данный закон установил ответственность за деяния, предметом посягательств которых является «защищенный компьютер» (находящаяся в нем компьютерная информация). Под ним понимается:

1) компьютер, находящийся в исключительном пользовании правительства или финансовой организации, либо компьютер, функционирование которого было нарушено при работе в интересах правительства или финансовой организации;

2) компьютер, являющийся частью системы или сети, элементы которой расположены более чем в одном штате США.

Одновременно уголовный закон устанавливает, что уголовная ответственность наступает в случаях:

1) несанкционированного доступа – когда посторонний, по отношению к компьютеру или компьютерной системе, человек вторгается в них извне и пользуется ими;

[12] https://megalektsii.ru/s21781t1.html.

2) превышение санкционированного доступа – когда законный пользователь компьютера или системы осуществляет доступ к компьютерным данным, на которые его полномочия не распространяются.

Данный закон устанавливает ответственность за семь основных составов преступлений, которыми признаются:

–компьютерный шпионаж, состоящий в несанкционированном доступе или превышении санкционированного доступа к информации, а также получение информации, имеющее отношение к государственной безопасности, международным отношениям и вопросам атомной энергетики (§ 1030 (a) (1));

–несанкционированный доступ или превышение санкционированного доступа к информации из правительственного ведомства США, из какого бы то ни было защищенного компьютера, имеющего отношение к межштатной или международной торговле, а также получение информации из финансовых записей финансового учреждения, эмитента карт или информации о потребителях, содержащейся в файле управления учета потребителей (§ 1030 (a) (2));

–воздействие на компьютер, находящийся в исключительном пользовании правительственного ведомства США, или нарушении функционирования компьютера, используемого полностью или частично Правительством США (§ 1030 (a) (3));

–мошенничество с использованием компьютера – доступ, осуществляемый с мошенническими намерениями, и использование компьютера с целью получения чего бы то ни было ценного посредством мошенничества, включая незаконное использование машинного времени стоимостью более 5 тысяч долларов в течении года, т.е. без оплаты использования компьютерных сетей и серверов (§ 1030 (a) (4));

–умышленное или по неосторожности повреждение защищенных компьютеров (§ 1030 (a) (5));

–мошенничество путем торговли компьютерными паролями или аналогичной информацией, позволяющей получить несанкционированный доступ к информации, если такая торговля влияет на торговые отношения между штатами и с другими государствами, или на компьютер, используемый правительством США (§ 1030 (a) (6));

–угрозы, вымогательство, шантаж и другие противоправные деяния, совершаемые с использованием компьютерных технологий (§ 1030 (a) (7)).

Также можно выделить § 1029 Титула 18 Свода законов США, которым предусмотрена ответственность за торговлю похищенными или поддельными устройствами доступа, которые могут быть использованы для получения денег, товаров или услуг.

Несмотря на столь детальную регламентацию вопросов уголовной ответственности за компьютерные преступления, правоохранительные органы США испытывают значительные затруднения в случаях, когда речь ведется о привлечении к ответственности лиц, которые совершают компьютерные преступления, осуществляя доступ к компьютерам США из-за рубежа. По мнению экспертов этого можно было бы избежать при условии включения в статьи уголовного закона квалифицирующих признаков – совершения преступлений с использованием возможностей глобальных компьютерных сетей и осуществления несанкционированного доступа с компьютеров, находящихся за пределами США, или через них.

Была вынуждена отреагировать на компьютерные преступления и Великобритания, известная консерватизмом правовой системы. Длительное время Великобритания пыталась справляться с данным явлением, используя свой многовековый опыт судопроизводства, но под «напором» компьютерной преступности «сдалась». С августа 1990 г. вступил в силу Закон о злоупотреблениях компьютерами. В соответствии с ним к уголовно наказуемым отнесены:

–умышленный противозаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам (ст. 1);

–умышленный противозаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам для их последующего использования в противозаконных целях (ст. 2);

–неправомерный доступ к компьютерной информации на машинном носителе, в компьютере, компьютерной системе или сети, с целью, или если это повлекло уничтожение, блокирование, модификацию, либо копирование информации, нарушения работы компьютера, компьютерной системы или сети (ст. 3).

Среди европейских государств, которые повели решительную борьбу с компьютерными преступлениями с момента их появления в жизни общества одно из ведущих мест занимают Нидерланды (Голландия). В Нидерландах был создан Консультативный комитет по компьютерным преступлениям, который предложил конкретные рекомендации по внесению изменений в Уголовный кодекс и Уголовно-процессуальный кодекс Нидерландов. Консультативный комитет не дал определения компьютерных преступлений, но разработал их классификацию.

В то же время полицейское разведывательное управление, занимающееся регистрацией всех случаев компьютерных преступлений, использует следующее определение компьютерного преступления: это поведение, которое (потенциально) вредно и имеет отношение к устройствам, связанным с компьютерами с точки зрения хранения, передачи и обработки данных. Полицейское разведывательное управление делает различие между компьютерными преступлениями, в которых компьютер является объектом преступления, и теми, в которых он – орудие преступления. Начиная с 1987 г. полицейское разведывательное управление использует для анализа пять видов компьютерных преступлений:

–совершаемые обычным способом, но с использованием технической поддержки в компьютерной среде;

–компьютерное мошенничество;

–компьютерный террор (совершение преступлений с целью повреждения компьютерных систем):

1) использование несанкционированного доступа;

2) использование вредоносных программ, типа компьютерных вирусов;

3) совершение других действий, включая физическое повреждение компьютера;

–кража компьютерного обеспечения (пиратство);

–остаточная категория, включающая все другие типы преступлений, которые не подпадают под вышеперечисленные категории. Данный перечень видов преступлений в целом соответствует приведенной выше Рекомендации №R (89) 9 Совета Европы, но отличается более простым их описанием. Причина отсутствия общепризнанного определения компьютерного преступления заключается в том, что, по мнению нидерландских ученых, существует множество трудностей при формулировании определения, которое, с одной стороны, было бы достаточно емким, а с другой – достаточно специальным. Применяется два понятия компьютерного преступления – в узком и широком смысле. В узком смысле – это совершение преступления, которое невозможно выполнить без использования компьютера или другого автоматического устройства как объекта или инструмента преступления. В 1993 г. в Нидерландах был принят Закон о компьютерных преступлениях, дополняющий УК Голландии новыми составами:

–несанкционированный доступ в компьютерные сети (ст. 138a (1));

–несанкционированное копирование данных (ст. 138a (2));

–компьютерный саботаж (ст. 350a (1), 350b (1));

–распространение вирусов (ст. 350a (3), 50b);

–компьютерный шпионаж (ст. 273 (2)).

В ряд статей УК Голландии, предусматривающих ответственность за совершение традиционных преступлений (вымогательство (ст. 317, 318), запись (прослушивание, копирование) информационных коммуникаций, кража путем обмана служб (ст. 362c), были внесены дополнения, в редакции других статей (саботаж (ст. 161, 351), подлог банковских карточек (ст. 232) – даны специальные разъяснения. Были значительно изменены такие составы, как шпионаж (ст. ст. 98, 98a), вмешательство в коммуникации (ст. 139a, 139b), порнография (ст. 240b), что позволяет в настоящее время использовать данные составы преступлений, в соответствующих случаях, и для борьбы с компьютерными преступлениями.

Таким образом, уголовное законодательство Нидерландов предоставляет достаточно широкие возможности для борьбы с различными видами компьютерных преступлений, устанавливая помимо специальных норм дополнительные квалифицирующие обстоятельства в уже существующие уголовно-правовые нормы.

Исходя из вышеизложенного, можно сделать вывод, что зарубежное законодательство пошло по пути разграничения компьютерных преступлений в зависимости от той сферы общественных отношений, на которую посягает преступник. Данные сферы соответствуют криминологическим группам компьютерных преступлений. Можно выделить следующие три группы:

1) экономические компьютерные преступления (наиболее распространенные и опасные преступления), например, компьютерное мошенничество § 263a УК ФРГ;

2) компьютерные преступления против прав и свобод индивидуальных субъектов и организаций, нарушающие неприкосновенность частной сферы, например, незаконные злоупотребления информацией, находящейся на компьютерных носителях, разглашение сведений, имеющих частную,

коммерческую тайну (сведения помимо конфиденциального характера, должны находиться на компьютерных носителях);

3) компьютерные преступления против государства и общества в целом, например, дезорганизация работы различных систем (оборонных, энергетических, газоснабжения), изменения данных при подсчете на выборах и др.

§ 3. Государственная политика в области противодействия преступлениям, совершаемых с использованием информационно-коммуникационных технологий

Известно, что вопросы информационной безопасности, защиты компьютерной информации, обеспечения защищенности сведений, образующих охраняемую законом тайну, и иные подобные проблемы вызывают серьезную озабоченность как в России, так и во всем мире. Данные вопросы самым непосредственным образом связаны с обеспечением национальной безопасности государств, защитой конституционных прав и свобод человека и гражданина.

Необходимость совершенствования государственной политики по противодействию преступлениям в сфере информационных технологий подтверждается тем, что в последнее время данные преступления стали глобальной международной проблемой, многие из них имеют трансграничный характер.

Среди недавних, наиболее известных сообщений о подобных преступлениях можно выделить:

Май 2017 г. — компьютерные системы в более чем 150 странах мира поразил вирус—шифровальщик под названием WannaCry. На экране зараженных компьютеров появлялось сообщение о том, что все файлы зашифрованы, а за расшифровку пользователю предлагалось выплатить

эквивалент $300 в биткоинах. По некоторым оценкам кибератака с использованием вируса WannaCry привела к ущербу свыше миллиарда долларов[13].

Июнь 2017 г. компьютерные системы по всему миру были атакованы вирусом Petya. Сильнее всего пострадала Украина — там кибератака парализовала работу сайтов правительства, банков, энергетических и транспортных компаний. В России вирус атаковал компьютерные системы «Роснефти» и «Башнефти». В конце июня вирус-шифровальщик Petya, распространился на компьютерные системы в Европе, США, странах Азии. Частично была парализована работа системы управления крупнейшего контейнерного порта имени Джава-харлала Неру в Индии, оператором которого выступает A.P. Moller—Maersk[14].

По большинству из данных инцидентов возбуждены уголовные дела, однако использование преступниками средств анонимизации существенно усложняет расследование этих преступлений.

По первоначальным подсчетам государство потратило более 300 млн руб. на эвакуацию людей из различных объектов из—за массовых анонимных звонков о «минировании» по всей стране.

Представленные примеры наглядно демонстрируют нарастающую активность преступников в сфере информационных технологий, свидетельствуют об изощренности и масштабе их противоправной деятельности.

Ущерб от подобных преступлений всегда значительный, однако в Российской Федерации некоторые негативные последствия (например, от программы—шифровальщика WannaCry) были нейтрализованы благодаря внедряемой государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

---

[13] https://www.kaspersky.ru/blog/wannacry-ransomware/16147.
[14] https://ru.wikipedia.org/wiki/Petya.

Указанная система является одним из элементов создаваемого современного механизма противодействия информационным инцидентам и является результатом реализации соответствующей государственной политики, направленной на достижение определенной цели — обеспечение полноценного противодействия преступлениям в сфере информационных технологий[15].

Отдельные стратегические направления данной политики периодически освещаются на самом высоком уровне. Так Президент Российской Федерации В.В. Путин неоднократно акцентировал внимание на необходимости внедрения цифровых технологий в различные сферы жизни и важности усиления информационной безопасности. Среди последних наиболее значимых, по мнению автора, заявлений на данную тему можно выделить:

01.12.2016 в послании Федеральному Собранию Российской Федерации Президент определил следующее: «Необходимо укреплять защиту от киберугроз, должна быть значительно повышена устойчивость всех элементов инфраструктуры, финансовой системы, государственного управления. Предлагаю запустить масштабную системную программу развития экономики нового технологического поколения, так называемой цифровой экономики. В ее реализации будем опираться именно на российские компании, научные, исследовательские и инжиниринговые центры страны. Это вопрос национальной безопасности и технологической независимости России, в полном смысле этого слова — нашего будущего (выделено авт.)».

26.04.2017 В.В. Путин поручил председателю правительства Д.А. Медведеву до 01.12.2017 обеспечить внесение изменений в федеральные законы для усиления безопасности государственных информационных систем.

07.07.2017 вопросам кибербезопасности было уделено значительное внимание на встрече Президентов РФ и США, которые отметили что данная

[15] Указ Президента РФ от 15 января 2013 г. N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

тема становится все более рискованной, порождающей разные угрозы, включая террористическую, и угрозы нормальному функционированию общества.

08.07.2017 на Пресс-конференции по итогам саммита «Группы двадцати» В.В. Путин отметил, что существует договоренность с Президентом Соединенных Штатов о создании рабочей группы и совместной работе по контролю за безопасностью в области киберпространства, совместном обеспечении безусловного соблюдения международных правовых норм в этой сфере. Кроме того, была отмечена необходимость выработать общие правила в сфере цифровой экономики, обозначить, что такое кибербезопасность, разработать систему правил поведения в этой сфере.

3-5 сентября 2017 года В.В. Путин посетил Китай для участия в саммите БРИКС. В преддверии данного саммита Президент в своей статье, опубликованной в ведущих СМИ стран БРИКС отметил, что Россия выступает за расширение взаимодействия стран БРИКС в сфере глобальной информационной безопасности. Президент предложил сообща сформировать соответствующую международно-правовую базу сотрудничества, а в перспективе - разработать и принять универсальные правила ответственного поведения государств в этой области. Отметил, что важным шагом могло бы стать заключение межправительственного соглашения БРИКС по международной информационной безопасности[16].

Приведенные заявления «на высшем уровне» имеют конкретное воплощение в нормативно-правовых актах, активно принимаемых в последнее время. Данные акты изменяют устаревшую и формируют ту самую, так необходимую сейчас правовую основу для реализации государственной политики по противодействию современным угрозам в области информационной безопасности.

Из наиболее значимых правовых актов последнего времени, регламентирующих вопросы информационной безопасности следует выделить:

[16] http://www.kremlin.ru/events/president/news/55495.

Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». В данной Доктрине указано: «Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую не имеют комплексной основы».

Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы». Одним из основных принципов данной Стратегии является обеспечение государственной защиты интересов российских граждан в информационной сфере. Так же закреплены 17 новых информационных понятий, среди которых: индустриальный интернет, интернет вещей, информационное общество, облачные вычисления, туманные вычисления, цифровая экономика, экосистема цифровой экономики. В стратегии также обращено внимание на то, что с использованием сети «Интернет» все чаще совершаются компьютерные атаки на государственные и частные информационные ресурсы и на объекты критической информационной инфраструктуры.

Федеральный закон от 01.07.2017 № 156-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации». Данным Федеральным законом регламентирован новый порядок ограничения доступа к сайту в информационно-

телекоммуникационных сетях (в том числе в сети «Интернет») сходному до степени смешения с сайтом в сети «Интернет», доступ к которому ограничен по решению суда в связи с неоднократным и неправомерным размещением информации, содержащей объекты авторских и (или) смежных прав (копия заблокированного сайта). Нормы закона, в частности, предусматривают принятие Минкомсвязью России по поступающей информации, мотивированного решения о признании сайта в сети «Интернет» копией заблокированного сайта и направление данного решения владельцу такого сайта и в Роскомнадзор для принятия мер по внесудебному ограничению доступа к копии заблокированного сайта.

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Законом устанавливаются основные принципы обеспечения безопасности критической информационной инфраструктуры (далее - КИИ), полномочия государственных органов в области обеспечения безопасности КИИ. Так же, определяются права, обязанности и ответственность лиц, владеющих на праве собственности или ином законном основании объектами КИИ, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов[17].

Структурой, контролирующей безопасность КИИ, становится Национальный координационный центр по компьютерным инцидентам. Кроме того, устанавливаются «основные принципы обеспечения безопасности КИИ, полномочия государственных органов РФ в области обеспечения данной безопасности, а также права, обязанности и ответственность лиц, владеющих на праве собственности или ином законном основании объектами КИИ, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов». Собственниками или лицами, пользовавшимися объектами

[17] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ.

КИИ на праве аренды или иного законного основания, должны быть «российские юридические лица или индивидуальные предприниматели». Указано, что иностранные компании, если они представляют свои интересы на территории России через российские юридические лица, смогут продолжить свою работу без ограничений.

Законом вводится реестр значимых объектов КИИ, а также устанавливаются требования по обеспечению безопасности значимых объектов КИИ с учетом их категорий. Создаются системы безопасности значимых объектов КИИ РФ и обеспечение их функционирования. Безопасность КИИ будет обеспечиваться в том числе за счет «взаимодействия этих систем с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, созданной в соответствии с указом Президента РФ от 15.01.2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Постановление Правительства Российской Федерации от 19.07.2017 г. № 983 «О представлении Президенту Российской Федерации предложения о подписании Соглашения о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» и Распоряжение Президента Российской Федерации от 26.07.2017 № 297-рп «О подписании Соглашения о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий». В данных нормативных актах предлагается проект Соглашения «О сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» и закрепляется целесообразность его скорейшего подписания на высшем уровне.

Вывод:

Следует отметить, что рассмотренные нормативно-правовые акты являются достаточно прогрессивными, направленными на противодействие современным угрозам в области информационной безопасности. Кроме того, можно сделать вывод, что в настоящее время происходит активное переформатирование существовавшей и создание новой правовой основы использования информационных технологий в различных сферах жизни общества и функционирования государства, а также формируются институты, обеспечивающие реализацию основных направлений государственной политики по противодействию преступлениям в сфере информационных технологий.

Представляется очевидным, что данный процесс будет продолжен. Однако для успешного противодействия преступлениям в сфере информационных технологий, наличие качественной и современной правовой базы является необходимым, но не достаточным условием.

Преступления, представляющие наибольшую общественную опасность, среди совершаемых в сфере компьютерных технологий, обусловлены следующими обстоятельствами: трансграничным характером используемых при их совершении сетевых ресурсов; а также изменчивостью (волатильностью) и скоростью уничтожения цифровой информации.

Для успешного расследования подобных преступлений, по мнению автора требуется своевременное, оперативное установление следов совершенного преступления и их надлежащее закрепление, что зачастую связанно с необходимостью анализа значительных массивов информации. Однако действующий порядок международного сотрудничества между государствами не обеспечивает оперативность взаимодействия правоохранительных органов в данной сфере, не способствует своевременному выявлению и фиксации следов, а в некоторых случаях и вовсе не позволяет производить дальнейшее расследование данных преступлений, в части

установления обстоятельств их совершения за пределами территории Российской Федерации.

Наиболее эффективным решением в данном вопросе представляется создание межгосударственного ведомства по борьбе с киберпреступлениями, включающего в свой штат наиболее подготовленных и компетентных специалистов в рассматриваемой сфере из числа государственных служащих стран - участников данного ведомства, наделенных полномочиями, позволяющими осуществлять правоохранительную деятельность на их территориях, уровень обеспечения которого будет соответствовать уровню технического развития в сфере компьютерных технологий.

Я убеждён, что основой успешного выполнения принимаемых норм и залогом реализации государственной политики в области информационной безопасности является обучение и воспитание соответствующих кадров, которые бы обеспечили «прорывные» результаты в данной области.

Успешная реализация столь «амбициозной» цели предусматривает необходимость существенных изменений как в структуре, так и в организации учебного процесса в образовательных учреждениях (особенно в ВУЗах), организующих подготовку специалистов в области информационной безопасности. К данной категории специалистов, наряду со специалистами технических профилей безусловно относятся сотрудники правоохранительных органов (сотрудники оперативных подразделений, дознаватели, следователи, прокуроры, судьи).

Бюджетные должности в государственных учреждениях Российской Федерации, на сегодняшний день не во всех случаях могут предоставить IT специалистам с высоким уровнем подготовки надлежащий уровень материального и социального обеспечения, соответствующий приобретенным ими познаниям, в связи с этим в экспертных подразделениях органов внутренних дел имеется «кадровый голод» на IT-специалистов. Считаю, что эффективным способом решения данной проблемы может стать активная

реализация на федеральном и региональном уровнях Российской Федерации положений о государственно-частном партнерстве (закрепленном в Федеральном законе от 13.07.2015 № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации»)[18].

[18] Федеральный закон «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации" от 13.07.2015 N 224-ФЗ».

ГЛАВА 2. СОВРЕМЕННАЯ УГОЛОВНО-ПРАВОВАЯ И КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Уголовно-правовая характеристика мошенничества, совершенного с использованием информационно-коммуникационных технологий

Понятие мошенничества раскрыто в ст. 159 Уголовного Кодекса Российской Федерации, а именно, это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Федеральным законом от 29.11.2012 № 207 в действующий УК РФ внесены изменения. Глава 21 была дополнена. в связи с реалиями нашего времени, шестью новыми составами, среди которых ст. 159.6 «Мошенничество в сфере компьютерной информации». Данная статья призвана защитить отношения собственности, имущественные интересы, отношения, обеспечивающие охрану компьютерной информации и безопасность информационно-телекоммуникационных сетей. Уголовная ответственность предусмотрена за хищение чужого имущества или приобретение права на чужое имущество посредством ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации, или информационно-телекоммуникационных сетей[19]. Совершение преступного деяния, указанного в ст. 159.6 УК РФ возможно исключительно посредством использования современных компьютерных технологий. Компьютерная информация - это информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме доступной

[19] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: федеральный закон от 29.11.2012 г. № 207-ФЗ // Российская газета. 2012. 3 дек.

восприятию электронно-вычислительными машинами. У компьютерной информации есть свои особенности, которые заключаются в следующем:

– она относительно просто пересылается, преобразовывается, размножается;

– при изъятии информации, в отличие от изъятия вещи, она легко сохраняется в первоисточнике;

– доступ к одному и тому же файлу, содержащему информацию, могут иметь одновременно несколько пользователей.

Согласно ст. 6 Федерального закона от 27.07.2006 № 149 «Об информации, информатизации и о защите информации» информационные ресурсы находятся в собственности юридических и физических лиц, включаются в состав их имущества, на них распространяется действие гражданского законодательства. Преступления в сфере информационных технологий включают взлом паролей, кражу номеров кредитных карточек и других банковских реквизитов (фишинг). Наиболее опасными и распространенными преступлениями, совершаемыми с использованием сети Интернет, является мошенничество. В частности, инвестирование денежных средств на иностранных фондовых рынках с использованием сети Интернет сопряжено с риском быть вовлеченными в различного рода мошеннические схемы. Другой пример мошенничества – «интернет-аукционы», в которых сами продавцы делают ставки, чтобы поднять цену выставленного на аукцион товара.

Мошенничество в сфере компьютерной информации является закономерным шагом интеграции российского законодательства о борьбе с компьютерными преступлениями в международное законодательство. До настоящего времени основная деятельность в указанной сфере осуществлялась в рамках требований ст. 272-274 УК РФ. Прослеживается схожесть объективной стороны деяний ст. 159.6 УК РФ и ч. 2 ст. 272 УК РФ, предусматривающей неправомерный доступ к компьютерной информации,

совершенный из корыстной заинтересованности. Однако если при мошенничестве ввод, удаление, блокирование, модификация либо иное вмешательство являются способами преступления, то, по смыслу диспозиции ст. 272 УК РФ, уничтожение, блокирование, модификация либо копирование информации выступают скорее обязательными последствиями[20].

По моему мнению, предметом преступного посягательства по ст. 159.6 УК РФ являются: 1) компьютерная информация, под которой в уголовно-правовом аспекте понимаются сведения (или сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения,обработки и передачи, согласно положениям Примечания к ст. 272 УК РФ; 2) имущество, т. е. совокупность вещей, которые находятся в собственности лица, в т. ч. включая деньги и ценные бумаги, а также имущественных прав на получение вещей или имущественного удовлетворения от других лиц. Как мне представляется, в случае если лицо оперировало сведениями, не относящимися к компьютерной информации (в понимании уголовного закона), либо его действия не были связаны с завладением имуществом, а преследовали иные цели, (например, создание препятствий в реализации прав собственника), уголовная ответственность по ст. 159.6 УК РФ исключается.

По мнению автора, уголовно-наказуемыми по ст. 159 УК РФ являются только лишь следующие общественно опасные способы завладения чужим имуществом:

1) ввод компьютерной информации, т. е. размещение сведений в устройствах ЭВМ для их последующей обработки и (или) хранения;

2) удаление компьютерной информации, т. е. совершение действий, в результате которых становится невозможным восстановить содержание компьютерной информации, и (или) в результате которых уничтожаются

[20] Маленкин А.С. Вопросы разграничения мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) и неправомерного доступа к компьютерной информации, совершенного из корыстной заинтересованности (ч. 2 ст. 272 УК РФ) // Противодействие преступности: от теории к практике день за днем: научно-практическая интернет-конференция Омской юридической академии. Омск, 2013.

носители компьютерной информации;

3) блокирование компьютерной информации, т. е. совершение действий, приводящих к ограничению или закрытию доступа компьютерной информации, но не связанных с ее удалением;

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

5) вмешательство в функционирование:

– средств хранения;

– средств обработки;

– средств передачи компьютерной информации;

– информационно-телекоммуникационные сети.

Под «вмешательством в функционирование» следует понимать осуществление неправомерных действий, нарушающих установленный процесс обработки, хранения,использования, передачи и иного реального обращения с компьютерной информацией. В современной следственно-судебной практике в Российской Федерации конструкция ст.159.6 УК РФ не всегда будет охватывать собой «традиционные» общественно опасные схемы хищения чужого имущества с использованием компьютерной техники и информации и должна применяться к виновному лицу в совокупности с иными статьями УК РФ. Так, например, исходя из современной следственно судебной практики наиболее распространенным является деяние в виде хищения «электронных денег», состоящее из следующих «преступно логичных», последовательных «технических этапов»:

1) неправомерное завладение компьютерной информацией (например, путем незаконного получения ключа доступа, логина,пароля и т. п.);

2) использование похищенной компьютерной информации в целях дальнейшего присвоения чужого имущества.

Как мне кажется, «первый этап» заключается в неправомерном копировании компьютерной информации (ст. 272 УК РФ), либо в неправомерном использовании вредоносного программного обеспечения (ст. 273 УК РФ). В свою очередь, «второй этап» состоит уже в использовании полученной неправомерным путем компьютерной информации в целях хищения имущества потерпевшего. И как следствие, повышенно общественно опасный способ хищения «электронных денег» повлечет за собой квалификацию данного способа мошенничества и ответственность для виновного сразу по нескольким статьям уголовного закона, в число которых входит и ст. 159.6 УК РФ. Необходимо констатировать, что аналогичная правоприменительная практика также имела широкое распространение и до введения в российское отраслевое законодательство ст. 159.6 УК РФ. Так, действия виновных лиц квалифицировались по совокупности статей, согласно положениям ст. 272 (или 273) и ст. 159 (или 158) УК РФ.

По моему мнению, ст. 159.6 УК РФ имеет уголовно-правовое разграничение с «классическим» мошенничеством только лишь в способе совершения хищения чужого имущества. Так, если ст. 159 УК РФ предусматривает возможность уголовного преследования виновного за хищение имущества путем обмана или злоупотребления доверием, то ст. 159.6 УК РФ применяется к злоумышленнику, если подобное хищение было совершено с использованием компьютерной информации общественно опасными способами.

При анализе ст. 159 и 159.6 УК РФ видно, что российский законодатель расценивает мошенничество в сфере компьютерной информации как менее опасное преступление, т.к. устанавливает за него менее строгие виды наказания. Положениями п. 166 Резолюции X Конгресса ООН по предупреждению преступности и обращению с правонарушителями, состоявшегося 10–17 апреля 2000 г. в Вене, определено: «если компьютерные данные поддаются идентификации и контролю по конкретному носителю

данных, то с юридической точки зрения они могут рассматриваться как единый и ощутимый материальный предмет»[21]. Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьезное нарушение работы электронно-вычислительных машин и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные с имущественным ущербом.

Преступление, предусмотренное комментируемой статьей, следует отграничивать от неправомерного доступа к компьютерной информации (ст. 272 УК РФ), а также создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ) и нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

Диспозиция комментируемой нормы имеет бланкетный характер, следовательно, ее применению должен предшествовать факт установления конкретной нормативной базы, регламентирующей отношения виновного и потерпевшего в области компьютерных технологий. Поскольку таковые образуют область специальных познаний, то предъявлению обвинения по комментируемой статье должно предшествовать проведение соответствующих технических экспертиз.

Объект анализируемого преступления полностью совпадает с родовым

---

[21] Доклад 10 Конгресса ООН по предупреждению преступности и обращению с правонарушителями // 10 Конгресс ООН по предупреждению преступности и обращению с правонарушителями: сборник документов / сост. А.Г. Волеводев. М., 2001.

объектом хищения - это общественные отношения, сложившиеся в сфере электронного документооборота. Квалифицированное мошенничество в сфере компьютерных технологий, как и мошенничество в общем, это всегда хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием (см. п. п. 2 и 3 комментария к ст. 159)[22].

При этом форма объективной стороны содеянного строго ограничена законодателем: хищение чужого имущества, равно приобретения права на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации, или информационно-телекоммуникационных сетей.

Преступное деяние считается законченным с момента получения виновным суммы денег (чужого имущества), а равно приобретения им юридического права на распоряжение такими деньгами (имуществом).

Сам по себе факт ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации, или информационно-телекоммуникационных сетей в зависимости от обстоятельств дела может содержать признаки приготовления к мошенничеству в сфере компьютерной информации или покушения на совершение такого преступления.

Преступление, предусмотренное ч. 1 ст. 159.6 УК РФ, является преступлением небольшой степени тяжести, преступления, предусмотренные ч. 2 и 3 ст. 159.6 УК РФ, преступлениями средней тяжести, а преступления, предусмотренные ч. 4 указанной статьи, – отнесены к тяжким.

Анализ указанной статьи позволяет сделать следующие выводы. Включение мошенничества в сфере компьютерной информации в состав гл. 21 УК РФ предусматривает в качестве видового объекта отношения

[22] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А.И. Чучаева. М., 2013.

собственности, а непосредственным объектом выступает чужое имущество или права на него.

Объективную сторону мошенничества в сфере компьютерной информации составляет хищение чужого имущества или приобретение права на чужое имущество.

Способом совершения преступления выступает:

1) ввод, удаление, блокирование, модификация компьютерной информации;

2) иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации, или информационно-телекоммуникационных сетей[23].

Субъект – общий, по ч. 3 ст. 159.6 УК РФ – специальный, квалифицирующим признаком выступает совершение преступления группой лиц по предварительному сговору либо организованной группой. Субъект - любое дееспособное лицо, достигшее 16-летнего возраста.

Субъективная сторона предполагает прямой умысел. Виновный осознает, что завладевает чужим имуществом или правами на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации, или информационно-телекоммуникационных сетей. Субъективная сторона - прямой конкретизированный умысел.

Перечисленные обстоятельства сами по себе не обязательно свидетельствуют о наличии мошенничества в сфере компьютерных информаций, в каждом конкретном случае должно быть достоверно установлено, что лицо, совершившее определенные в диспозиции комментируемой статьи действия, заведомо намеревалось использовать полученную информацию в корыстных целях.

---

[23] Елин В.М. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. 2013. № 2 (24). С. 70-76.

Законом предусмотрены как квалифицированный состав преступления - мошенничество в сфере компьютерной информации, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба потерпевшему (ч. 2), так и особо квалифицированные составы: во-первых, деяния, совершенные с использованием виновными своего служебного положения, а равно в крупном размере (ч. 3); во-вторых, деяния, совершенные организованной группой либо в особо крупном размере (ч. 4).

Применительно к квалифицирующим признакам - группа лиц по предварительному сговору, причинение значительного ущерба гражданину, использование виновными своего служебного положения, организованной группой лиц.

Согласно примечанию к ст. 159.1 УК РФ крупным размером в комментируемой статье признается стоимость похищенного имущества - 1 млн. 500 тыс. руб., особо крупным размером - 6 млн. руб.

Состав, описанный в ст. 159.6 УК РФ, является специальным по отношению к составу ст. 159 УК РФ, к тому же основной состав (ч. 1 ст. 159.6 УК РФ) конкурирует с основными составами, предусмотренными ч. 1 ст. 272, ч. 1 ст. 273 УК РФ. Нельзя не отметить отсутствие системности законодательства, что проявляется в различных подходах к установлению наказания за преступное хищение, сопряженное с незаконным использованием компьютерной информации, и фактически за то же деяние в сфере компьютерной информации, но без признаков хищения: мошенничество, причинившее ущерб до 2,5 тыс. руб. (ч. 1 ст. 159.6 УК РФ), карается мягче, чем преступление, предусмотренное ч. 1 ст. 272 и ч. 1 ст. 273 УК РФ. Вместе с тем, мошенничество, причинившее ущерб от 2,5 тыс. до 1 млн руб. (ч. 2 ст. 159.6 УК РФ), карается жестче, чем преступление, предусмотренное ч. 1 ст. 272, и соразмерно преступлению, описанному в ч. 2 ст. 273 УК РФ. Это противоречие тем более остро, что в случае, если деяние не завершено, умысел на хищение трудно установить. Кроме того, есть проблема с конкуренцией в применении

норм, предусматривающих квалифицирующие и особо квалифицирующие признаки: при совершении преступления, предусмотренного ч. 3 ст. 272 УК РФ, группой лиц по предварительному сговору с причинением значительного ущерба (до 2,5 тыс. руб.), совершенного из корыстной заинтересованности, и квалифицированного мошенничества в сфере компьютерной информации (ч. 2 ст. 159.6 УК РФ)[24].

Что касается общественно-опасных последствий, данное преступление, предусмотренное ст. 159.6 УК РФ, является преступлением с материальным составом, обязательным условием его совершения выступает хищение чужого имущества или приобретение права на чужое имущество. При этом возникает вопрос о том, что конкретно похищено в результате совершения преступления: деньги, информация, права или что-то еще. Таким образом, особую актуальность приобретает проблема информации как вещи, имущества. Между тем информация исключена из перечня объектов гражданских правоотношений с 1 января 2008 г.

Подводя итог, можно констатировать, что формальное отнесение преступлений данной категории к преступлениям против собственности неминуемо порождает правовые коллизии в связи с невозможностью правоохранительных органов ответить на вопросы:

– о собственнике информации;

– о размере ущерба;

– об имущественных характеристиках компьютерной информации;

– о взаимосвязи правомерных действий (ввода, удаления, блокирования, модификации компьютерной информации) и общественно-опасных последствий (хищение чужого имущества или приобретение права на чужое имущество);

– о разграничениях между ст. 159.6 УК РФ и смежными составами

[24] Александрова И.А. Новое уголовное законодательство о мошенничестве // Юридическая наука и практика. Вестник Нижегородской академии МВД России. 2013. № 21. С. 54-62.

преступления и др.[25]

§ 2. Криминалистическая характеристика мошенничества, совершенного с использованием информационно-коммуникационных технологий

Проанализируем отдельные элементы механизма мошенничества в сфере компьютерной информации с целью определения их взаимодействия между собой и влияния каждого из них на формирование криминалистических знаний о противоправном деянии.

Прежде всего, необходимы знания о компьютерных средствах. Как следообразующие объекты компьютерные средства выступают в двух аспектах:

– как носители информации об объективной стороне преступного деяния;

– как носители информации о самом субъекте преступления[26].

Особенность заключается в том, что компьютерные средства сами не являются следами преступной деятельности, так как не обладают характерными специфическими особенностями, но при этом несут на себе следовую картину преступного деяния. Об этом свидетельствует анализ следственной практики, когда, например, при производстве следственных действий из компьютера изымается только его «жесткий диск» — запоминающее устройство для хранения информации. Между тем, технические характеристики компьютерно-технических средств и их наличие или отсутствие в общем должны свидетельствовать о возможности реализации преступного умысла (например, подключение или не подключение компьютера к телекоммуникационной сети).

Большинство ученых сходятся во мнении, что основной характерной особенностью компьютерно-технических средств (с проекцией на потребности расследования) является их свойство сохранять информацию. С этим следует

---

[25] Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 201 № 1. С. 9 - 22.

[26] Евдокимов К.Н. Проблемы квалификации и предупреждения компьютерных преступлений. Иркутск: Иркутский юридический институт (филиал) Академии Генеральной прокуратуры РФ, 2009.

согласиться, потому что это и есть определяющий момент формирования криминалистического знания о компьютерных преступлениях и, в частности, такого вида, как мошенничество в сфере компьютерной информации. К источникам компьютерной информации относятся системы, компоненты которых обеспечивают размещение, доступность, а также целостность сведений, составляющих информацию:

– постоянное запоминающее устройство компьютера — его внутренняя память, включающая несколько микросхем, постоянно хранящих определенную информацию;

– оперативное запоминающее устройство — оперативная память, содержащая информацию, необходимую для работы компьютера;

– сверхоперативная память (кэш) — сверхбыстродействующие микросхемы памяти, кэш-память для повышения производительности компьютера.

Существуют также внешние источники — внешняя (долговременная) память, предназначенная для долговременного хранения программ и данных, не используемых в данный момент, которая требует наличие устройства, обеспечивающего запись/считывание информации (накопителя или дисковода), а также устройства хранения информации (носителя). К ним относятся накопители на оптических компакт-дисках (CD-R/RW, DVD R/RW); флэш-накопители (MMC Plus (Multimedia Card), SD Mini (Secure Digital), SD Micro (Secure Digital), MS Pro (Memory Stick Pro), MS Pro Duo (Memory Stick Pro Duo), CF (Compact Flash), SD (Secure Digital) и др.). Таким образом, средства накопления криминалистически значимой информации представляют собой довольно сложные объекты — компьютеры (устройства), состоящие из множества элементов, а также средства накопления, обработки и хранения информации. Следует заметить, что привести полный перечень таких устройств в настоящее время достаточно затруднительно в связи с быстрым темпом научно-технического прогресса в области компьютерных технологий и

появлением новых форм накопителей. Однако поскольку указанные объекты имеют специфические свойства, то и характер функционирования их следует учитывать при разработке практических рекомендаций по расследованию мошенничества в сфере компьютерной информации. Интерес для формирования криминалистического знания об исследуемом виде мошенничества представляют также компьютерные сети.

По мнению В. П. Косарева и Л. В. Еремина, компьютерная сеть — это совокупность компьютеров, между которыми возможен информационный обмен без промежуточных носителей информации[27]. Подобное суждение выглядит не бесспорным, поскольку в данном определении не в полной мере отражена техническая особенность передачи данных в сети. Авторы акцентируют внимание лишь на наличии промежуточных звеньев в сети при передаче информации. Вместе с тем, к промежуточным звеньям при передаче информации можно отнести различные носители информации (например, переносные жесткие диски, USB и флеш-карты, лазерные CD, DVD диски и т. д.). При этом их наличие или отсутствие предопределяет тип компьютерной системы, которая, в свою очередь, может включать как автономные вычислительные системы, так и их сети. Таким образом, нельзя назвать компьютерной сетью систему, которая не включает в себя помимо рабочих станций (технически сложных устройств, например, компьютера, смартфона, компактного персонального компьютера или планшетного персонального компьютера, посредством которого пользователь (абонент) получает доступ к ресурсам компьютерной сети) каких-либо промежуточных накопителей информации. Следовательно, особенностью компьютерных сетей является то, что их существует несколько видов, и в зависимости от территориальной распространенности они делятся на сети:

– локальные компьютерные (ЛВС, LAN — Local Area Network) — создаются и используются юридическими лицами, как правило, в пределах

[27] Экономическая информатика / под ред. В. П. Косарева, Л. В. Еремина. — М.: Финансы и статистика, 2001. — 592 с.

своего размещения, либо физическими лицами в обособленной административно-территориальной единице;

– региональные компьютерные (РВС, MAN — Metropolitan Area Network), связывающие абонентов района, города, области;

– глобальные компьютерные (ГВС, WAN — Wide Area Network), соединяющие абонентов, удаленных друг от друга на любом расстоянии. Наиболее распространенной, безусловно, является всемирная глобальная сеть Интернет. При этом анализ изученных материалов уголовных дел о преступлениях, совершаемых в сфере компьютерной информации, свидетельствует, что для совершения таких деяний в 95 % случаев использовались глобальные компьютерные сети, в 4 % — региональные и лишь в 1 % — локальные компьютерные.

Таким образом, любые компьютерные сети также имеют свои характерные криминалистические особенности и, по сути, могут эффективно использоваться субъектами преступной деятельности в целях совершения мошенничества. При этом характерной особенностью компьютерных сетей, как орудия и средства совершения исследуемого мошенничества, является то, что они также содержат следы осуществления операций, направленных на реализацию преступного замысла. Например, независимо от отправляющего и принимающего устройства, в электронной почте хранятся электронные письма, отправленные и принятые на определенный адрес. Зная свойства и принцип работы телекоммуникационной сети, следователь или лицо, производящее дознание, способны обнаружить в ней значительный объем информации о преступном деянии. Компьютерная сеть также является средством передачи информации между абонентами сети. Нельзя не подчеркнуть, что практически все формы незаконной деятельности, имеющие место в сфере компьютерной информации, в том числе мошенничество, осуществляются с использованием различных программ, разработка и внедрение в компьютерную систему которых является средством обеспечения совершения преступлений.

В процессе расследования исследуемых преступлений следует учитывать, что подготовка, написание, тестирование специальных компьютерных программ для взлома, внедрение вредоносных «троянских» программ, программ-шпионов, поиск паролей или определение способов беспарольного входа будет оставлять виртуальные следы в памяти компьютера или иного технически сложного устройства, используемого мошенником. При этом примененные способы воздействия на компьютер «жертвы» будут аналогичным образом оставлять следы в памяти ее компьютера. Как справедливо отмечает А. Смушкин, для указанных преступных действий могут использоваться программы различного уровня сложности: «стандартные» — составлены максимально просто и их легко найти в сети Интернет или в специальной области закрытого участка Интернет; «приспособленные» — переделанные самим злоумышленником под свои нужды; самостоятельно написанные[28]. Рассматривая вопросы формирования криминалистических знаний о мошенничестве в сфере компьютерной информации, отдельными учеными предлагаются новые варианты определения понятия и механизма следообразования. Однако по мнению автора, к этому надо подходить достаточно осторожно. Так, П. В. Мочагин, предлагает к двум традиционным формам отражения следообразования (материально-фиксированной и идеальной), добавить еще одну — виртуально-информационную и технико-компьютерную сферу[29]. Данная позиция представляется достаточно спорной, поскольку специфика образования, обработки и хранения компьютерной информации предусматривает использование для этих целей вполне материальных средств (компьютерно-технических). Именно это обстоятельство предусматривает возможность материально-фиксированного отображения компьютерной информации на носителях указанных средств. Следовательно, в

[28] Смушкин А. Виртуальные следы в криминалистике / А. Смушкин // Законность. — 2012. — № 8. — С. 43–45.

[29] Мочагин П. В. Новые формы следообразований в криминалистике и судебной экспертизе / П. В. Мочагин // Судебная экспертиза в парадигме российской науки (к 85-летию Ю. Г. Корухова) : сб. материалов 54-х кримин. чтений : в 2 ч. — М. : Академия управления МВД России, 2013. — Ч. 2. — С. 97–101.

качестве следов мошенничества в сфере компьютерной информации вполне можно рассматривать электронные сигналы (команды), отправленные с компьютера субъекта преступной деятельности, которые предаются по телекоммуникационным сетям с целью 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. У этих сигналов есть точки начала и окончания их движения (имеются в виду компьютеры, между которыми они предаются), и они, в конечном итоге, имеют материально-фиксированное выражение — персональный компьютер или иное технически сложное устройство, его IP-адрес. В криминалистической литературе такие следы предлагается именовать информационными или виртуальными, и в том виде, в котором их представляют ученые, они являются, ничем иным, как материальными следами-отображениями. Обусловлено это тем, что они имеют вполне материально-фиксированное отражение на материальных носителях, именно это позволяет их идентифицировать с помощью разработанных наукой средств и методов. Иначе такой подход, предложенный учеными, по мнению автора, позволял бы говорить о таких видах следов, как военные следы (по делам о военных преступлениях), террористические следы (по делам о терроризме), технические следы и т. д. Подобный подход способствовал бы лишь загромождению разработанных криминалистикой знаний о рассматриваемых проблемах.

Вывод:

Подводя итог вышеизложенному, хотелось бы сказать, что включение статьи о мошенничестве в сфере компьютерной информации в российское уголовное законодательство, с одной стороны, упростило процедуру выявления и расследования преступлений данной категории как на национальном, так и на международном уровне, исключило возможность уголовного преследования

граждан Российской Федерации за совершение киберпреступлений на территории других стран и их ответственность по зарубежному уголовному законодательству.

Мошенничество в сфере компьютерной информации является закономерным шагом интеграции российского законодательства о борьбе с компьютерными преступлениями в международное законодательство. До настоящего времени основная деятельность в указанной сфере осуществлялась в рамках требований ст.ст. 272-274 УК РФ, формально подпадающих под положения Раздела «Offences against the confidentiality, integrity and availability of computer data and systems» (C.2, S.1, T1 Европейской Конвенции о киберпреступности), фактически оставляя без внимания вопросы ответственности за совершение преступлений, связанных с использованием компьютерных средств («Computer-related offences»).

Необходимость криминализации компьютерного мошенничества назрела давно, обоснованность принятия данной статьи раскрывается рядом научных статей, отражается в существующей практике. Фактически с включением ст. 159.6 УК РФ в национальное законодательство разрешен вопрос об участии Российской Федерации в мировых интеграционных процессах в сфере борьбы с киберпреступностью, вектор которых определяется положениями Конвенции. Складывается ситуация, когда наша страна, формально не участвуя в Конвенции, тем не менее, развивает собственное национальное законодательство в соотнесении с существующей практикой борьбы с киберпреступностью.

Включение указанной статьи в уголовное законодательство способствовало конкретизации компьютерных преступлений, наряду с преступлениями в сфере компьютерной информации выделяя преступления, осуществляемые с использованием компьютерных средств.

ГЛАВА 3. УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО В СЕТИ «ИНТЕРНЕТ»:

§ 1. Особенности выявления и расследования уголовных дел, по преступлениям, совершенным с использованием информационно-коммуникационных технологий

Выявление и пресечение данных преступлений, как правило, осуществляется сотрудниками органов внутренних дел. В тоже время обнаружение и процессуальная фиксация преступлений по статье 159.6 УК РФ может осуществляться и иными правоохранительными органами, реализующими полномочия, предусмотренные Федеральным законом № 144-ФЗ от 12.08.1995 года «Об оперативно-розыскной деятельности».

Порядок возбуждения дел

В соответствии с уголовно-процессуальным законодательством уголовное дело по статье 159.6 УК РФ может быть возбуждено в публичном порядке, то есть без заявления потерпевшей стороны. Исключение делается лишь для индивидуальных предпринимателей и членов органа управления коммерческой организации, если они совершили преступление в связи с осуществлением ими предпринимательской или иной экономической деятельности. В данном случае для возбуждения уголовного дела потребуется соответствующее заявление потерпевшей стороны.

Ведомственная подследственность

Расследование уголовных дел по части 1 статьи 159.6 УК РФ осуществляется органами дознания Министерства внутренних дел РФ. Предварительное следствие по частям второй — четвертой осуществляется уже следователями МВД РФ. Кроме того, закон допускает, что предварительное

следствие по комментируемой статье может производиться следователями органа, выявившего преступление: ФСБ РФ, СК РФ.

Подсудность дел

Рассмотрение преступлений, предусмотренных статьей 159.6 УК РФ, отнесено к подсудности районных судов.

Территориальная подследственность и подсудность

В соответствии с общими принципами уголовно-процессуального законодательства расследование и рассмотрение уголовных дел судами по статье 159.6 УК РФ осуществляется по месту совершения преступления.

Для примера рассмотрим статью в которой авторский коллектив рассматривает актуальные вопросы и даёт практические рекомендации по определению территориальной подследственности преступлений, связанных с хищением денежных средств путем использования информационно-коммуникационных систем, в ситуации, когда не представляется возможным определить место их окончания.

Современные достижения на рынке коммуникаций, их опережающее развитие по отношению к созданию систем безопасности привело к появлению новых рисков и угроз. Количество киберпреступлений в России из года в год увеличивается.

О масштабах распространения киберпреступлений было озвучено Генеральным прокурором РФ 23 сентября 2016 года на Координационном совещании руководителей правоохранительных органов по вопросам выявления и расследования преступлений в области информационно-коммуникационных технологий. Ю.Я. Чайка отметил, что основной причиной этого стал резкий рост мошенничества (с 2,2 тыс. до 13,4 тыс.), а также краж (с 2,3 тыс. до 8,5 тыс.), увеличилось количество преступлений, связанных с хищением, удалением, блокировкой компьютерной информации (ст. 159.6 Уголовного кодекса Российской Федерации (далее - УК РФ).

В 2015 году их зарегистрировано около 44 тысяч, что в 4 раза превышает показатели 2014 года[30].

На территории Белгородской области показатель количества преступлений, связанных с хищением денежных средств путем использования информационно-коммуникационных систем, за 2016 год является достаточно тревожным и измеряется сотнями противоправных деяний (792). Общая сумма причиненного жителям региона ущерба, по данным прокуратуры Белгородской области, составила более 25 млн. рублей.

Одной из острых проблем по противодействию преступлениям данной категории является определение места их совершения, чему также способствует отсутствие единообразной практики применения уголовно-процессуального законодательства, ведомственных нормативных правовых актов и иных организационно-распорядительных документов в данной сфере, а также пробелы в законе.

Об этом свидетельствуют допускаемые органами предварительного расследования в работе грубые нарушения действующего законодательства, регулирующего принципы территориальной подследственности при рассмотрении сообщений о преступлениях обозначенной категории, что затрудняет эффективность противодействия указанным преступным проявлениям.

Данные принципы определены в статье 152 Уголовно-процессуального кодекса Российской Федерации (далее - УПК РФ) «Место производства предварительного расследования», согласно которой предварительное расследование может производиться по месту совершения деяния (часть 1), по месту окончания преступления (часть 2), по месту совершения большинства преступлений или наиболее тяжкого из них (часть 3), по месту нахождения обвиняемого или большинства свидетелей (часть 4), а если преступление совершено вне пределов РФ - по месту жительства или месту пребывания

[30] http//genproc.gov.ru/smi/news/archive/news-112274 [Официальный сайт ГП РФ].

потерпевшего в РФ, либо по месту нахождения большинства свидетелей, либо по месту жительства или месту пребывания обвиняемого в РФ, если потерпевший проживает или пребывает вне пределов РФ.

При этом следует отметить, что определение места окончания преступления, связанного с хищением денежных средств путем использования информационно-коммуникационных систем, у органов предварительного расследования вызывает объективные трудности, так как данный вид преступлений носит межрегиональный характер и связан с системами безналичного расчета. Используемые при совершении хищений счета и платежные карты финансовых и кредитных организаций, а также сим-карты операторов сотовой связи оформляются в разных регионах Российской Федерации.

Несмотря на разъяснения Пленума Верховного Суда РФ от 27.12.2007 № 51[31], сформировать единую следственную практику по определению места окончания преступления в полной мере не удается и по сей день.

В частности, одни считают местом окончания преступления местонахождение потерпевшего в момент перечисления денежных средств (платежный терминал, банкомат и т.д.), другие – место выполнения виновным лицом объективной стороны преступления, то есть совершение действий, направленных на хищение денежных средств.

Такая ситуация приводит к тому, что поступившие заявления без принятия должных мер по проверке и закреплению доказательств неоднократно пересылаются из одного органа внутренних дел в другой.

Подобные факты являются причиной необоснованного затягивания сроков проведения проверок. При этом утрачиваются следы преступления, что в дальнейшем затрудняет раскрытие противоправного деяния. Как следствие, нарушаются требования статьи 6.1 УПК РФ о соблюдении разумных сроков

[31] Постановление Пленума ВС РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате».

уголовного судопроизводства и конституционное право граждан на доступ к правосудию, однако же само преступление остается нераскрытым.

К сожалению, в уголовно-процессуальном законодательстве и разъяснениях Пленума Верховного Суда РФ отсутствуют положения, регламентирующие ситуацию, при которой невозможно определить место совершения преступления.

В то же время в совместном приказе Генеральной прокуратуры РФ и иных федеральных органов исполнительной власти РФ от 29.12.2005 № 39/1070/1021/253/780/353/399[32] отражено, что если не представляется возможным определить место совершения преступления, оно подлежит учету по месту его выявления.

На регистрацию преступления по месту его выявления также ориентировал своих подчиненных временно исполнявший обязанности Министра внутренних дел Российской Федерации Горовой А.В., который в своем письме от 13.07.2015 № 1/5562 «Об организации работы по противодействию отдельным видам мошенничества» требовал от них, при поступлении заявления (сообщения) о совершении мошеннических действий с использованием мобильных средств связи, осуществлять проверку и при наличии в деянии признаков преступления принимать решение о возбуждении уголовного дела территориальным органом, принявшим заявление либо иное сообщение. При этом в случае установления в ходе расследования точного места совершения преступления за пределами обслуживаемой территории после производства неотложных следственных действий направлять уголовное дело по подследственности в порядке, установленном статьей 152 УПК РФ[33].

По этому поводу существует также позиция Генеральной прокуратуры РФ, отраженная в информационном письме от 03.11.2015 № 36-11- 2015 «Об

---

[32] Приказ Генпрокуратуры России № 39, МВД России № 1070, МЧС России № 1021, Минюста России № 253, ФСБ России № 780, Минэкономразвития России № 353, ФСКН России № 399 от 29.12.2005 (ред. от 20.02.2014) «О едином учете преступлений».

[33] Письмо МВД РФ от 13.07.2015 № 1/5562 «Об организации работы по противодействию отдельным видам мошенничества».

определении места производства предварительного расследования мошенничеств, совершаемых с использованием телефонной (сотовой) связи», в котором содержится следующее: «Поскольку преступления рассматриваемого вида нередко имеют трансграничный и высокотехнологичный характер, не позволяющий своевременно установить место их совершения и обеспечить объективное расследование в установленные законом процессуальные сроки, правомерным является признание территориальной подследственности в субъекте Российской Федерации, где непосредственно выполнялись действия, входящие в объективную сторону преступления, вне зависимости от того, что последствия наступили на другой территории, а также по месту наступления общественно-опасных последствий или обращения потерпевшего в правоохранительные органы»[34].

Между тем, как показывает практика, органами предварительного расследования не всегда соблюдаются требования федерального законодательства и ведомственных нормативных правовых актов в данной сфере, о чем свидетельствуют допускаемые ими нарушения.

Так, в текущем году в прокуратуру Белгородской области из прокуратуры Тюменской области в связи с возникшим спором о территориальной подследственности поступил материал проверки по заявлению К. о совершении в отношении него телефонного мошенничества.

Из материала проверки следует, что в августе прошлого года неустановленное лицо посредством использования средств телефонной связи, путем обмана К., проживающего в п. Северный, временно находившегося в Валуйском районе, завладело его денежными средствами на сумму 10657 рублей, причинив тем самым ему ущерб на указанную сумму.

По данному факту К. в этот же день с заявлением обратился в ОМВД России по г. Валуйки и Валуйскому району.

---

[34] Информационное письмо Генеральной прокуратуры РФ от 03.11.2015 № 36-11-2015 «Об определении места производства предварительного расследования мошенничеств, совершаемых с использованием телефонной (сотовой) связи».

В период нахождения данного материала на исполнении у оперуполномоченных отдела уголовного розыска ОМВД России по г. Валуйки и Валуйскому району ими в ходе проверки достоверно не было установлено место совершения преступления.

Более того, реальная работа по материалу проверки данными сотрудниками полиции не проводилась, она была сведена лишь к получению детализации телефонных переговоров и составлению формального рапорта о результатах проверки.

Несмотря на длительность проведения проверки, в ее материалах не содержалось каких-либо данных о движении денежных средств, похищенных у К., о владельцах, используемых злоумышленником абонентских номеров, о месте нахождения данных абонентских номеров в момент соединений с К., очевидцах произошедшего и др.

В дальнейшем начальником ОМВД России по г. Валуйки и Валуйскому району материал неполной проверки по заявлению К. необоснованно, в нарушение требований ст. ст. 145 и 152 УПК РФ, был направлен по территориальности (по якобы месту окончания совершения преступления) в ОМВД России по Уватскому району Тюменской области.

Таким образом, сотрудниками ОМВД России по г. Валуйки и Валуйскому району без наличия на то достаточных оснований и выполнения необходимых мероприятий было принято незаконное и необоснованное решение о передаче материала проверки по территориальности в ОМВД России по Уватскому району Тюменской области.

Более того, в материале проверки по заявлению К. содержались признаки преступления, предусмотренного ч. 2 ст. 159 УК РФ. При этом необоснованное направление указанного материала проверки по территориальности в другой субъект РФ повлекло укрытие на протяжении полугода от учета и регистрации данного преступления, а также, что более важно, недопустимую волокиту по материалу проверки.

В связи с допущенными нарушениями уголовно-процессуального законодательства и ведомственных нормативных правовых актов первым заместителем прокурора области в адрес начальника УМВД России по области внесено представление, по результатам рассмотрения, которого 4 должностных лица привлечены к дисциплинарной ответственности.[35]

Аналогичные нарушения прокуратурой области выявлялись и раньше, в 2015 и 2014 годах, в различных районах области, в связи с которыми 8 должностных лиц привлечены к дисциплинарной ответственности.

Таким образом, для решения вопроса об определении места совершения преступления, связанного с хищением денежных средств путем использования информационно-коммуникационных систем, в ситуации, когда не представляется возможным определить место его окончания, с учетом указанных положений уголовно-процессуального законодательства, совместного приказа Генеральной прокуратуры РФ и иных федеральных органов исполнительной власти, разъяснений Пленума Верховного Суда Российской Федерации, информационных писем Генеральной прокуратуры РФ и МВД РФ, предлагаю ст. 152 УПК РФ[36] дополнить положениями следующего содержания: «В случае если не представляется возможным определить место совершения преступления, уголовное дело расследуется по месту выявления преступления».

В ходе расследования уголовных дел, по преступлениям, совершенным с использованием информационно-коммуникационных технологий необходимо помнить об особенностях квалификации данных преступлений.

К примеру, в ниже приведенной статье на основе проведенного исследования сформулированы предложения по квалификации преступных деяний в сфере использования информационно-коммуникационных технологий.

---

[35] Материалы, предоставленные прокуратурой Белгородской области.
[36] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 12.11.2018).

Отдельно рассмотрены проблемные вопросы квалификации фишинга и скимминга**.**

Проблема противодействия преступлениям, совершаемым в сфере использования информационно-коммуникационных технологий, продолжает оставаться одной из наиболее злободневных. Обращает на себя внимание непоследовательный подход законодателя к криминализации деяний, совершаемых с использованием информационно-коммуникационных технологий. Не стал исключением и Федеральный закон от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», которым введена ответственность за квалифицированные виды мошенничества, среди которых и преступления, совершаемые с использованием информационно-коммуникационных технологий: ст. 159.3 «Мошенничество с использованием платежных карт» и ст. 159.6 «Мошенничество в сфере компьютерной информации».

Инициатором изменений выступил Верховный Суд РФ[37]. Позиция судебного органа объясняется тем, что «конкретизация в УК РФ составов мошенничества, в зависимости от сферы правоотношений, в которой они совершаются, должна была уменьшить число ошибок и злоупотреблений при возбуждении уголовных дел о мошенничестве, способствовать повышению качества работы по выявлению и расследованию таких преступлений»[38].

В научном мире разразилась бурная полемика по поводу целесообразности отнесения деяния, предусмотренного ст. 159.6 УК РФ, к компьютерному мошенничеству. Так, В.В. Хилюта отмечает сомнительность наличия такого неотъемлемого признака мошенничества, как «обман»: «Компьютер, как и замок у сейфа, нельзя обмануть, поскольку технические

---

[37] Паспорт проекта Федерального закона № 53700-6 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации». Доступ из справочно-правовой системы «Консультант Плюс».

38 О проекте Федерального закона № 53700-6 «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации»: письмо Верховного Суда РФ от 25 мая 2012 г. № 2-ВС-2733/12. Доступ из справочно-правовой системы «Консультант Плюс».

устройства лишены психики»[39]. Возможен обман только физического лица, которое вследствие введения его в заблуждение передает добровольно свое имущество преступнику. Н.Ш. Козаев также отмечает экстраполяцию общих признаков мошенничества на рассматриваемый состав[40].

Противники указанной позиции отмечают, что обман, напротив, имеет место быть, т.к. при несанкционированном видоизменении компьютерной информации возникает искажение действительности в сознании человека, эксплуатирующего модифицированную систему, что можно отнести к обману, как к искажению истины[41].

В свою очередь, автор солидарен с мнением П.С. Яни, относящим мошенничество в сфере компьютерной информации к новому виду хищений, «когда завладение имуществом или приобретение права на имущество сопряжено с проникновением в информационную среду, в которой осуществляются различного рода информационные операции, юридическое значение и последствия которых состоят в приобретении участниками оборота имущества в виде наличных денег, безналичных денежных средств, иных имущественных прав»[42]. П.С. Яни также отмечает тот факт, что название статьи «Компьютерное мошенничество» никак не препятствует ее применению. Учитывая характер использования информационно-коммуникационных технологий в целом и электронных средств платежа в частности при совершении хищений, указанная позиция представляется приемлемой, ввиду чего считаю целесообразным квалифицировать по ст. 159.6 УК РФ все хищения в сети Интернет, совершаемые со всеми видами вмешательств в функционирование средств хранения, обработки и передачи компьютерной информации, в том числе и случаи неправомерного доступа и использования

[39] Хилюта В.В. Уголовная ответственность за хищения с использованием компьютерной техники // Журн. рос. права. 2014. № 3. С. 111–118.
[40] Козаев Н.Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): / под. ред. А.В. Наумова. М., 2015.
[41] Воронцова С.В. К вопросу о квалификации преступлений в сфере электронных платежей // Банковское право. 2009. № 1. С. 35–37.
[42] Яни П.С. Специальные виды мошенничества // Законность. 2015. № 8. С. 35–40.

систем дистанционного банковского обслуживания, электронных кошельков и реквизитов платежных карт. Такое понимание мошенничества в сфере компьютерной информации, по мнению автора, позволит сделать данную норму универсальной и применимой ко всем видам корыстных посягательств в IT-сфере.

Отсутствие системности в действиях законодателя привело к тому, что ряд составов, предусматривающих ответственность за незаконные манипуляции с использованием информационно-коммуникационных технологий, находятся в отношениях полной или частичной конкуренции.

Указанное обстоятельство вызвано тем, что перечень альтернативных действий по совершению мошенничества в сфере компьютерной информации гораздо шире перечня последствий, возможных при неправомерном доступе. Особенно остро это противоречие наблюдается при неоконченном преступлении, когда установить умысел на хищение чужого имущества достаточно сложно. Конкурируют между собой и квалифицирующие признаки указанных статей: неправомерный доступ к охраняемой законом компьютерной информации, повлекший указанные в законе последствия, причинивший крупный ущерб или совершенный из корыстной заинтересованности, идентичен по содержанию мошенничеству в сфере компьютерной информации, совершенному в крупном размере. Так, если лицо из корыстных побуждений осуществило неправомерный доступ к системе «Банк-клиент», повлекший модификацию информации о средствах на счету законного пользователя системы в пользу злоумышленника, то его действия содержат признаки хищения, т.к. имущественные права на активы, переведенные со счета законного владельца, были нарушены. Вместе с тем, был осуществлен неправомерный доступ из корыстной заинтересованности, повлекший модификацию информации и, как следствие, причинение крупного ущерба. В анализируемой ситуации имеет место коллизия уголовно-правовых норм,

поскольку фактически они устанавливают ответственность за одно и то же деяние.

По моему мнению, ст. 159.6 УК РФ является специальной по отношению к ст. 272, 273 УК РФ, поскольку неправомерный доступ к компьютерной информации из корыстной заинтересованности представляет собой действия, направленные на хищение, т.е. компьютерная информация выступает средством доступа к чужому имуществу, что охватывается объективной стороной ст. 159.6 УК РФ, ввиду чего в силу ч. 3 ст. 17 УК РФ дополнительной квалификации по ст. 272, 273 УК РФ преступных посягательств в IT-сфере не требуется.

Относительно ситуации, связанной с использованием подложной карты для оплаты товаров в торговых и иных организациях, хотелось бы отметить, что законодателем указанные неправомерные действия криминализованы в рамках ст. 159.3 УК РФ, однако следует подчеркнуть, что под объективную сторону рассматриваемой статьи подпадает мошенничество конкретно указанным способом – путем обмана сотрудника кредитной, торговой или иной организации в подлинности карты и ее принадлежности. То есть под уголовно-правовой запрет подпадают действия, характеризующиеся сознательным сообщением заведомо ложных, не соответствующих действительности сведений работнику банка, например оператору, либо сотруднику магазина или кассиру.

Иные виды незаконных действий по использованию платежной карты под действие данной нормы не подпадают и, по мнению автора, должны быть квалифицированы либо пост. 158 УК РФ как тайное хищение – при использовании банкомата (в соответствии с разъяснениями, данными в постановлении Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате»), либо по ст. 159.6 УК РФ – при иных видах хищений и использовании различных видов информационно-коммуникационных технологий.

Правоохранительные органы также нередко сталкиваются со случаями совершения преступлений путем использования нескольких разновидностей информационно-коммуникационных технологий: возможностей сети Интернет с созданием и распространением вредоносных программ, влекущих неправомерный доступ к компьютерной информации, которая впоследствии необходима для создания поддельной (подложной) карты, используемой через систему АТМ-банкинга либо для осуществления платежей с использованием онлайн-банкинга**.** Очевидно, что деяния должны быть квалифицированы по совокупности различных составов УК РФ. Если с квалификацией действий злоумышленников по использованию вредоносных программ и неправомерному доступу ситуация более или менее ясная, то вопрос, как быть с изготовлением подложной карты и использованием ее реквизитов, требует изучения.

Долгое время однозначного ответа на данный вопрос не было, кроме того, эксперты и аналитики были едины во мнении, что конструкция ст. 187 УК РФ неэффективна. И законодатель длительное время не предпринимал никаких мер в данном направлении. Однако 08.06.2015 был принят Федеральный закон № 153-ФЗ «О внесении изменений в ст. 187 Уголовного кодекса РФ», вступивший в силу 19 июня 2015 г. Данным законом полностью изменены название ст. 187 УК РФ и диспозиция, в то время как санкция осталась прежней. Так, в статью включен ряд противоправных и альтернативных действий со средствами платежа, таких как приобретение, хранение, транспортировка в целях использования или сбыта, а статья получила название «Неправомерный оборот средств платежей». Вместе с тем, данная новелла уголовного закона порождает ряд вопросов правоприменительного плана, среди которых и разграничение этого общественно опасного деяния с другими преступными посягательствами.

Указание в диспозиции рассматриваемой нормы на создание компьютерных программ, предназначенных для неправомерного

осуществления приема, выдачи, перевода денежных средств, по мнению автора, создает конкуренцию со ст. 273 УК РФ, предметом которой, как известно, является «компьютерная программа либо иная компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации».

Неправомерный оборот средств платежей выражен рядом альтернативных действий: изготовление, приобретение, хранение, транспортировка в целях использования или сбыта, а равно сбыт средств платежей, таких как поддельные платежные карты, распоряжения о переводе денежных средств, документов или средств оплаты, электронные средства, электронные носители информации, технические устройства, компьютерные программы, пред назначенные для неправомерного осуществления приема, выдачи и перевода средств.

Так, создание, распространение вредоносной компьютерной программы в целях фишинга – действий, направленных на получение конфиденциальной информации о владельце средств платежа посредством установки на компьютер клиента вредоносного программного обеспечения либо путем перенаправления на подложный сайт, охватывается ст. 187 УК РФ, т.к. действия по созданию указанной вредоносной программы, заведомо предназначенной для копирования и модификации компьютерной информации, посягают в первую очередь на общественные отношения в сфере установленного законом порядка эмиссии, выпуска и оборота информационно-коммуникационных технологий в банковской сфере, а затем уже на отношения, складывающиеся в сфере безопасного использования электронных средств платежа, обеспечения информационной безопасности в сфере компьютерной информации. Ввиду чего представляется, что ст. 187 УК РФ выступает в качестве специальной по отношению к ст. 273 УК РФ в случаях создания, распространения или использования электронных средств, электронных носителей информации, технических устройств или компьютерных программ

для неправомерного осуществления приема, выдачи, передачи денежных средств.

Обратимся к наглядному примеру. В ноябре 2016 г. в ходе совместной операции управления «К» МВД России и центра информационной безопасности ФСБ России был задержан предполагаемый главарь преступной группы, грабившей клиентов крупного российского банка с помощью Android-троянца. Было установлено, что злоумышленники действовали на территории России около полутора лет и использовали «банкер» для хищения данных, необходимых для проведения мошеннических транзакций. В целом преступникам удалось заразить более 16 тыс. мобильных устройств на базе операционной системы «Андроид». Украденная у их владельцев информация передавалась на четыре командных сервера, размещенных на территории Украины. Материалами предварительной проверки установлено, что реализацией мошеннической схемы руководил задержанный житель Ярославля. Все C&C-серверы банковского троянца уже обезврежены[43]. Представляется уместным квалифицировать действия указанного лица по ч. 4 ст. 159.6 УК РФ. Вместе с тем, подозреваемый также должен быть привлечен к ответственности за действия по изготовлению, в данном случае созданию либо приобретению компьютерной программы для фишинга. Указанные действия должны быть квалифицированы по ч. 2 ст. 187 УК РФ.

Необходимо отметить, что ряд депутатов Государственной Думы предлагают внести изменения в Уголовный кодекс и предусмотреть в рамках гл. 28 отдельную норму за «фишинг»[44], что, по мнению автора, необоснованно и лишено достаточной аргументации, поскольку указанные действия охватываются объемом диспозиции ст. 187 УК РФ.

Следует также подчеркнуть, что «скимминг» – противоправные действия по установке накладок на банкоматы для считывания пин-кода карты либо для

[43] URL: www.threatpost.ru

[44] Согласно новому законопроекту киберпреступникам грозит до 4 лет заключения за создание фишинговых ресурсов. URL: http://www.itsec.ru/newstext.php?news_id=106860

ее удержания – также охватывается диспозицией ст. 187 УК РФ, т.к. указанные устройства представляют собой технические устройства, предназначенные для неправомерного осуществления приема, выдачи и перевода денежных средств.

В целом, приходится констатировать, что правотворческая деятельность по уголовно-правовому противодействию преступлениям в сфере использования информационно-коммуникационных технологий на сегодняшний день имеет ряд существенных недоработок, обусловленных бессистемным и хаотичным изменением законодательства в указанной сфере, что неизбежно порождает трудности и сложности при квалификации деяний по указанным нормам.

Выход из сложившейся ситуации возможен только при комплексном подходе к разрешению проблем противодействия преступлениям в IT-сфере, к которому будут привлечены как специалисты по информационной безопасности, представители банковского сообщества, так и сотрудники правоохранительных органов. Вместе с тем, учитывая специфику рассматриваемых правоотношений, считаю необходимым разъяснение в постановлении Пленума Верховного Суда РФ правил квалификации по указанным нормам и содержания использованных при конструкции уголовно-правовых норм понятий.

§ 2. Противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий

Увеличение числа пользователей современными электронными средствами связи («виртуализация» жизнедеятельности[45]) открыло новые возможности не только для политики, экономики и культуры, но и для преступной деятельности.

[45] См.: Гилинский Я. И. Криминологические основы уголовного права в эпоху постмодерна // Криминологические основы уголовного права // Материалы X Российского конгресса уголовного права, состоявшегося 26-27 мая 2016 г. / отв. ред., докт. юрид. наук, проф. В.С. Комиссаров. М., 2016. С. 296.

Построение информационно-коммуникационной инфраструктуры закономерно вызвало появление не только новых форм общественно опасного поведения личности (компьютерной преступности), но и изменение облика преступности в целом, которая в связи с использованием ИКТ приобрела несвойственные ей ранее признаки.

По мнению автора, указанные явления представляют собой результат информатизации преступности – процесса проникновения кибернетических методов, а также инструментария информационно-коммуникационных технологий в механизм преступления.

В связи с этим современное общество столкнулось с необходимостью решения двух взаимосвязанных уголовно-политических задач:

1) построение эффективной системы защиты информации и информационно-коммуникационной инфраструктуры;

2) приведение в соответствие сложившихся положений уголовного права с последствиями глобальной информатизации преступности.

Очевидно, что решение первой задачи требует определения круга деяний, посягающих на информационную безопасность, противодействие которым необходимо и эффективно осуществлять посредством уголовно-правовых предписаний.

Значительно более сложной видится вторая задача. Информатизация преступности рождает ряд непростых вопросов модификации уголовного закона:

1) пригодны ли классические положения института соучастия к случаям виртуального преступного взаимодействия, являющегося дистанционным и, как правило, анонимным?

2) каким должно быть оптимальное количество составов преступлений, посягающих на информацию и элементы информационно-коммуникационной инфраструктуры?

3) есть ли необходимость и насколько обширно следует изменить диспозиции традиционных составов преступлений путем детализации их совершения специфическим способом – с использованием ИКТ?

4) будет ли модернизация традиционных составов преступлений достаточной для противодействия современным криминальным угрозам и не потребуется ли определение ряда специальных норм?

5) какую роль использование ИКТ должно занять в сложившейся системе дифференциации уголовной ответственности?

Хотя накопившиеся проблемы сделали перемены не только насущно необходимыми, но и уже серьезно запоздалыми, до настоящего времени, пожалуй, нет четкого понимания относительно того, насколько современное уголовное право должно измениться, адаптируясь к условиям информационного общества. Во многом это объясняется таким обстоятельством как нехватка или недостоверность криминологического знания[46]. Следует признать, что на уровне профессиональных субъектов уголовной политики нет не только стратегически выверенного плана модернизации уголовного законодательства, но и относительно внятного представления о специфике и масштабах проблемы. Опыт криминализации мошенничества в сфере компьютерной информации (ст. 159^6 УК РФ) является, пожалуй, наглядным тому подтверждением[47].

В связи с этим на первоначальном этапе необходимо добиться смысловой определенности проблемы, ясного понимания ее сущности. Достижение этой цели, прежде всего, требует тщательно проработать вопрос о типологизации преступлений, совершаемых с использованием ИКТ, что позволит выявить и

---

[46] Бабаев М. М., Пудовочкин Ю. Е. Проблемы российской уголовной политики. М., 2014. С. 93.

[47] Благое намерение Верховного Суда Российской Федерации облегчить жизнь правоприменителя и упорядочить судебно-следственную практику, пожалуй, так и осталось нереализованным. Появление специальной нормы о мошенничестве в сфере компьютерной информации имело по существу обратный эффект, поскольку вызвало еще больше проблемных вопросов. См., на пример: Кауфман М. А. Пробельность, неопределенность, избыточность уголовного законодательства как криминогенные факторы // Материалы X Российского конгресса уголовного права, состоявшегося 26-27 мая 2016 г. / отв. ред., докт. юрид. наук, проф. В.С. Комиссаров. М., 2016; Третьяк М.И. Проблемы понимания способа компьютерного мошенничества в судебной практике // Уголовное право. 2015. №5; Чупрова А.Ю. Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. 2015. №5 и др.

лучше уяснить содержание данного явления. Не вызывает сомнений, что самостоятельным видом преступлений, совершаемых с использованием ИКТ, являются компьютерные преступления, то есть деяния, посягающие на охраняемую законом информацию и безопасность информационно-коммуникационной инфраструктуры. Природа данных преступлений специфична в том смысле, что само их происхождение, существование и, следовательно, совершение немыслимы без информационной среды.

В этом аспекте отечественное уголовное законодательство, а именно Глава 28 УК РФ, требует серьезной доработки. Научному сообществу и законодателю еще потребуется оценить необходимость криминализации DDos атаки, а именно, хакерской атаки на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён, спаминга, фишинга, действий по сбыту ботнета, а именно, компьютерной сети, состоящей из некоторого количества хостов с запущенными ботами — автономным программным обеспечением. Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании. и др. Следует отметить, что этому должна сопутствовать реалистичная оценка текущих и перспективных возможностей государства, включая материальные, организационные и технические.

Близкую по природе, но качественно иную группу деяний образуют новые формы общественно опасных посягательств на традиционно охраняемые уголовным законом общественные отношения, совершаемые в информационной среде. Ярким представителем данного вида является хищение денежных средств потерпевшего в результате автоматического срабатывания информационной системы (распространенное хищение денежных средств с банковского счета посредством использования сервисов дистанционного

банковского обслуживания). Деяние, которое неоправданно было оценено законодателем как мошенничество, в действительности своей представляет совершенно новую (седьмую)[48] форму хищения.

Примером, пожалуй, также выступают деяния, связанные с требованием о передаче имущества в качестве условия разблокировки программного обеспечения компьютера, возобновления доступа к электронной почте или аккаунту в социальной сети, восстановления модифицированной информации и т. п.

12 мая началась эпидемия трояна-шифровальщика WannaCry — похоже, происходит это по всему миру. Эпидемией мы это называем потому, что очень уж велики масштабы. За один только день мы насчитали более 45000 случаев атаки, но на самом деле их наверняка намного больше[49].

Что именно произошло: о заражениях сообщили сразу несколько крупных организаций, в том числе несколько британских клиник, которым пришлось приостановить работу. По сторонним данным, WannaCry заразил уже более 300000 компьютеров. Собственно, именно поэтому к нему и приковано столько внимания.

Больше всего атак пришлось на Россию, но также от WannaCry серьезно пострадали Украина, Индия, Тайвань, всего же мы обнаружили WannaCry в 74 странах. И это за один только первый день атаки.

В целом WannaCry — это эксплойт, с помощью которого происходит заражение и распространение, плюс шифровальщик, который скачивается на компьютер после того, как заражение произошло.

В этом и состоит важное отличие WannaCry от большинства прочих шифровальщиков. Для того, чтобы заразить свой компьютер, обычным, скажем так, шифровальщиком, пользователь должен совершить некую ошибку — кликнуть на подозрительную ссылку, разрешить исполнять макрос в Word,

---

[48] Шумихин В. Г. Седьмая форма хищения чужого имущества // Вестник Пермского университета. 2014. № 2 (24). С. 229.

[49] https://www.kaspersky.ru/blog/wannacry-ransomware/16147/

скачать сомнительное вложение из письма. Заразиться WannaCry можно, вообще ничего не делая.

WannaCry как шифровальщик (его еще иногда называет WCrypt, а еще, почему-то, порой зовут WannaCry Decryptor, хотя он, по логике вещей, вовсе даже криптор, а не декриптор) делает все то же самое, что и другие шифровальщики — шифрует файлы на компьютере и требует выкуп за их расшифровку. Больше всего он похож на еще одну разновидность печально известного троянца CryptXXX.

Он шифрует файлы различных типов, среди которых, конечно же, есть офисные документы, фотографии, фильмы, архивы и другие форматы файлов, в которых может содержаться потенциально важная для пользователя информация. Зашифрованные файлы получают расширение. WCRY (отсюда и название шифровальщика) и становятся полностью нечитаемыми.

После этого он меняет обои рабочего стола, выводя туда уведомление о заражении и список действий, которые якобы надо произвести, чтобы вернуть файлы. Такие же уведомления в виде текстовых файлов WannaCry раскидывает по папкам на компьютере — чтобы пользователь точно не пропустил. Как всегда, все сводится к тому, что надо перевести некую сумму в биткоин-эквиваленте на кошелек злоумышленников — и тогда они якобы расшифруют файлы. Поначалу киберпреступники требовали $300, но потом решили поднять ставки — в последних версиях WannaCry фигурирует цифра в $600.

Также злоумышленники запугивают пользователя, заявляя, что через 3 дня сумма выкупа увеличится, а через 7 дней файлы невозможно будет расшифровать. Мы не рекомендуем платить злоумышленникам выкуп — никаких гарантий того, что они расшифруют ваши данные, получив выкуп, нет. Более того, в случае других вымогателей исследователи уже показывали, что иногда данные просто удаляют, то есть и возможности расшифровать не остается физически, хотя злоумышленники требуют выкуп, как ни в чем не бывало.

К сожалению, на данный момент способов расшифровать файлы, зашифрованные WannaCry, нет. То есть с заражением можно бороться единственным способом — не допускать его.

Конечно же никогда не скачивать файлы с подозрительных ресурсов и не открывать вложения в письмах от незнакомых вам людей. Всегда можно уточнить, например, ответив на письмо, откуда автор - отправитель узнал адрес вашей электронной почты. Ни в коем случае не открывайте файлы во вложении. Проще попросить отправителя выслать файлы в другом формате. Необходимо помнить, в большинстве случаев отправитель даже не подозревает, что от его имени отправлялись файлы шифровальщика, и скорее всего он ответит Вам, что ничего Вам не отправлял.

Обращаем Ваше внимание, что 100% защиты от антивируса ждать не стоит, так как подобные шифровальщики живут 2-3 дня, и после добавления их в базу антивирусов, код их переписывается.

Как представляется, значительный потенциал расширения преступлений данного вида содержится в регламентации средств уголовно-правового противодействия посягательствам на объекты «виртуальной собственности». Следует отметить, что правовая природа подобного рода объектов до настоящего времени четко в науке не определена. Юристы спорят о том, могут ли такие объекты как электронные книги, библиотеки itunes, аккаунт в социальной сети или многопользовательской игре переходить в порядке наследования, а равно возможно ли возложить на подобное цифровое имущество обременение или использовать его в порядке исполнительного производства[50]. Разумеется, в решении этого вопроса доктрина уголовного права зависит от развития науки цивилистической, которая, думается, должна выделить такие объекты в качестве особой категории объектов гражданских

[50] См., например: Архипов В.В. Виртуальное право: основные проблемы нового направления юридических исследований // Известия высших учебных заведений. Правоведение. №2. 2013; Дюранске Б.Т., Кейн Ш.Ф. Виртуальные миры, реальные проблемы // Известия высших учебных заведений. Правоведение. №2. 2013; Семенюта Б. Онлайн-игры: правовая природа отношений // Интеллектуальная собственность. Авторское право и смежные права. № 8. 2014; Лисаченко А.В. Право виртуальных миров: новые объекты гражданских прав // Российский юридический журнал. №2. 2014 и др.

прав с использованием отдельных элементов правового режима вещей, как это сделано, например, в отношении бездокументарных ценных бумаг.

И наконец, значительно большую группу образуют традиционные преступления, объективная сторона которых может быть выполнена посредством программно-технических средств обработки информации. Особенностью данных преступлений является то, что в целом они не предполагают обязательного использования методов или процессов обработки информации, однако их совершение с использованием ИКТ является не только возможным, но и нередко встречающимся на практике. Так, например, использование «сайта-двойника» или электронной торговой площадки, смс-рассылка по типу: «Мама, отправь 1000 рублей на этот номер! Позже все объясню!», являются всего лишь новыми формами обмана как традиционного способа мошенничества.

Несмотря на масштаб и сложность проблемы эффективного противодействия преступлениям, совершаемым с использованием ИКТ, полагаю, что модернизация уголовного закона должна осуществляться крайне осторожно, по принципу минимизации вносимых поправок. Нет никакой необходимости сплошного «насыщения» диспозиций уголовно-правовых норм указанием на возможность их совершения посредством ИКТ. Такие оговорки должны иметь место только в случаях коллизий, либо пробелов уголовного закона, его очевидного несоответствия современным угрозам. Так, например, действующая уголовно-правовая норма об ответственности за вымогательство не позволяет должным образом оценить встречающиеся на практике случаи требования передачи денежных средств или иного имущества под угрозой совершения DDOS-атаки[51]. В связи с этим, думается, что ст. 163 УК РФ нуждается в изменениях.

[51] Атаки на вычислительную систему (сайт) с целью создания условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён.

Пожалуй, в качестве примера успешной модернизации уголовного закона к условиям информатизации преступности можно привести дополнение диспозиции ст. 187 УК РФ такой альтернативной формой совершения преступления как изготовление, приобретение, хранение, транспортировка в целях использования или сбыта, а равно сбыт компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи или перевода денежных средств.

Выборочным, социально и криминологически обоснованным должно быть также признание использования ИКТ квалифицирующим признаком преступления. Очевидно, что далеко не всякое применение информационных технологий (сети Интернет, например) влияет на степень общественной опасности деяния. Так, не имеет принципиального значения, состоялось ли разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, путем передачи документов, либо посредством отправки письма по электронной почте. Мошенник, обманывающий потерпевших через «Skype», вымогатель, отправляющий свои угрозы посредством сервиса «What's up!», вряд ли совершает более тяжкое преступление в сравнении с классическими его формами. Таким образом, использование ИКТ имеет неравнозначный характер с точки зрения влияния на характер и степень общественной опасности преступления. Данный факт является насколько очевидным, настолько и теоретически непроработанным. Специалисты обходят стороной эту проблему, не опираясь на какие-либо критерии, нередко почти интуитивно предлагают предусмотреть использование ИКТ квалифицирующим признаком того или иного преступления.

Включение квалифицирующего признака в состав преступления необходимо в случаях, когда он объективно повышает вероятность наступления вредных последствий, что является важнейшим показателем опасности действия. Как справедливо писал по этому поводу В.Н. Кудрявцев, «опасность действия заключается в том, что оно может вызвать определенные вредные

последствия. Однако эти последствия наступают не во всех случаях. Естественно, что действия будут сравнительно тем опаснее, чем выше степень вероятности наступления вредных последствий»[52].

Например, Федеральным законом от 01.03.2012 г. № 18-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» система квалифицирующих признаков сбыта наркотических средств, психотропных веществ или их аналогов была обоснованно дополнена указанием на использование электронных или информационно-телекоммуникационных сетей (включая сеть Интернет). Дело здесь не только в том, что использование информационно-телекоммуникационных сетей существенно осложняет выявление и раскрытие сбыта наркотических средств, но, что более важно, оно существенно облегчает его совершение (предоставляет неограниченные возможности для формирования клиентской базы, гарантирует анонимность, упрощает расчеты и т. д.).

Соглашаясь с приведенным решением, закономерно возникает вопрос о последовательной реализации уголовно-политического курса и распространении такого подхода к дифференциации ответственности за сбыт оружия (ст. 223 УК РФ), сильнодействующих или ядовитых веществ (ст. 234 УК РФ), новых потенциально опасных психоактивных веществ (ст. 234.1 УК РФ), недоброкачественных лекарственных средств или медицинских изделий (ст. 238.1 УК РФ) и др. Очевидно, что для упорядочения и унификации в этой области недостаточно только устранения погрешностей в отдельных статьях и даже главах уголовного закона, для этого потребуется ревизия всего Уголовного кодекса Российской Федерации.

Вывод:

Руководствуясь приведенным выше критерием оценки опасности действия в зависимости от вероятности наступления общественно опасных последствий, следует сделать вывод, что использование ИКТ должно

[52] Кудрявцев В. Н. Объективная сторона преступления. М., 1960. С. 102.

признаваться квалифицирующим признаком составов преступлений, объективная сторона которых связана с распространением деструктивной информации: ст. 230 «Склонение к потреблению наркотических средств, психотропных веществ или их аналогов», ст. 354 «Публичные призывы к развязыванию агрессивной войны, ст. 354.1 «Реабилитация нацизма» и др. Использование ИКТ является нередкой практикой по делам о распространении клеветнических сведений в отношении судьи, работников прокуратуры или следователей (ст. 298.1 УК РФ).

Нельзя не отметить, что при решении вопроса о закреплении использования ИКТ в качестве квалифицирующего признака необходимо также учитывать степень его распространенности. При этом требуется оценка не только фактической распространенности, но и анализ реальной опасности эскалации такого поведения в случае непринятия уголовно-политического решения. Так, отмечая, что современное медицинское оборудование зачастую имеет беспроводной интерфейс доступа, специалисты обсуждают угрозу совершения убийства посредством дистанционного управления имплантируемым электрокардиостимулятором или дефибриллятором-кардиовертером[53]. Нельзя признать основательность таких угроз, возможность их реального воплощения в будущем. Вместе с тем, вряд ли следует утверждать, что такие формы посягательства на жизнь человека будут иметь типичный характер и потребуют своего определения в ряду квалифицирующих признаков убийства.

В качестве общего вывода следует отметить, что правовые проблемы, связанные с преступлениями, совершаемыми с использованием ИКТ, со временем будут лишь актуализироваться. Стремительно развивающаяся информационно-коммуникационная инфраструктура содержит большой

[53] На конференции по безопасности Breakpoint в Мельбурне (17.10.2012 г.) исследователь Барнаби Джек выступил с заявлением о том, что из-за недоработок в программном обеспечении имплантируемые кардиостимуляторы можно заставить нанести смертоносный удар током напряжением 830 вольт путем отправки команды с ноутбука, находящегося на расстоянии до 15 метров // URL: http://hitech.newsru.com/article/17Oct2012/cardio (дата обращения: 08.08.2016 г.).

методологический потенциал для юриспруденции, что и является залогом последующего интереса к этой теме, в том числе в аспекте науки уголовного права.

ЗАКЛЮЧЕНИЕ

Современный этап характеризуется устойчивой тенденцией роста компьютерных преступлений, как в России, так и во всем мировом информационном пространстве.

Рассмотрение исследованных в выпускной квалификационной работе аспектов уголовно-правового противодействия преступлениям в сфере компьютерной информации, основанное на нормах российского законодательства и правоприменительной практики, позволяет сформулировать основные теоретические выводы и предложения, которые выразились в следующем.

Под компьютерным преступлением понимается - предусмотренное уголовным законом, противоправное, виновное нарушение чужих прав и интересов, связанное с использованием, модификацией, уничтожением компьютерной информации, причинившее вред либо создавшее угрозу причинения вреда подлежащим уголовно-правовой охране правам и интересам физических и юридических лиц, общества и государства (личным правам и неприкосновенности частной сферы, имущественным правам и интересам, общественной и государственной безопасности в области высоких технологий и конституционному строю).

Под понятие компьютерного преступления подпадают как преступления в сфере компьютерной информации, так и преступления, совершаемые с использованием компьютерных технологий. Последние в зависимости от характера использования компьютеров (или их систем) подразделяются:

– на преступления, в которых компьютерная информация является предметом преступления;

– преступления, в которых компьютерная информация используется как орудие преступления;

– преступления, в которых компьютер играет роль интеллектуального средства.

Новый Федеральный закон РФ от 07.12.2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» внес значительные изменения в главу 28 УК РФ о преступлениях в сфере компьютерной информации. Данный закон позволил внести ясность в некоторые дефиниции ст. ст. 272–274 УК РФ, однако трактовка некоторых ряда понятий и положений указанных статей остается весьма спорной.

Предметом рассматриваемой группы преступлений выступает компьютерная информация, т.е. сведения (сообщения, данные) представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Однако понятие информация далеко не тождественно понятиям сведения, данные. Прежде всего, если сведения существуют объективно, то информация возникает только у субъекта, анализирующего и сопоставляющего эти сведения, а также свои знания об этом объекте – и все это используется субъектом для принятия управленческого решения. Т.е., с точки зрения науки информатики, применение термина информация в данном случае, как минимум, не совсем корректно.

Рассматриваемые составы преступлений относятся к числу материальных составов. Уголовная ответственность наступает только в том случае, если наступили указанные в законе вредные последствия.

Однако в ряде случаев являются общественно опасными и такие действия лица, когда неправомерный доступ к компьютерной информации осуществляется только с одной целью – ознакомиться с той или иной информацией. Получается, что от таких деяний компьютерную информацию закон в настоящее время никак не защищает. Вряд ли это правильно. Поэтому

полагаю, что в ч. 1 ст. 272 УК РФ в новой редакции нового закона следует после слова «повлекло» добавить такие слова: «несанкционированное ознакомление» и далее по тексту закона. Уголовный закон должен пресекать незаконное любопытство некоторых лиц, тем более, что это может иметь общественно опасные последствия для владельца той или и иной информации.

Чёткие критерии, по которым программные продукты (модули) могут быть отнесены к категории вредоносных программ, до настоящего времени нигде четко не оговорены в уголовном законе и не выработаны пока еще судебной практикой. Для того, чтобы утверждение о вредоносности программы было обоснованным и имело бы юридические последствия, необходимо проведение программно-технической экспертизы с соблюдением всех установленных в уголовном судопроизводстве правил.

По ст. 274 УК РФ в новой редакции самым спорным является термин – правила эксплуатации. Для привлечения лица к уголовной ответственности по ч. 1 ст. 274 УК РФ следует установить, какие конкретно были нарушены правила эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации.

Это и является самой большой сложностью в трактовке и применении данной статьи. Правила могут быть самыми различными: начиная от тех, которые создаются самими разработчиками электронно-вычислительной техники, до правил, которые действуют только на конкретных предприятиях и фирмах, а также, разрабатываемых и утвержденных соответствующими министерствами и ведомствами, законодательными актами субъектов Российской Федерации. Рассматриваемые правила могут также содержаться в некоторых международных договорах и соглашений, заключенных Российской Федерации с другими иностранными государствами.

Думается, что количество всевозможных правил и инструкций (и их трактовок) неисчерпаемо, и устанавливать уголовную ответственность за их нарушения вряд ли правомерно.

В вопросе повышения уровня расследования киберпреступлений необходимым этапом является совершенствование координационной деятельности правоохранительных органов, что требует изменения и дополнения рабочих процессов различных государственных служб и подконтрольных организаций.

Эффективным разрешением данной проблемы представляется разработка и введение единого, для всех государственных служб и подконтрольных подразделений (а также лиц, взаимодействующих с ними в силу своей деятельности), ресурса (с применением блокчейн технологий), представленного в виде «гибрида» централизованной и децентрализованных систем, обеспечивающего электронный документооборот и хранение информации. При этом, на основе указанного ресурса необходимо объединить имеющиеся базы данных и создать новую, единую электронную базу данных. В части правоохранительных органов включить, в том числе следующие сведения:

– о заявителе/потерпевшем (в том числе организации или учреждении ими представляемых), в том числе с указанием контактного телефона;

– о скомпрометированных сетевых узлах (электронных носителях информации) с указанием: наименования и серийного номера, даты, времени, адресного указателя источника инфицирования, полученных данных о точках доступа;

– о выявленных вредоносных объектах (указание сигнатуры или вердикта, по которому детектируется вредоносное программное обеспечение), с учетом предыдущего пункта (по образцу АДИС «Папилон») в том числе с указанием специалиста/эксперта их установившего и его контактного телефона;

– о последствиях, возникших в результате атаки;

– о способе вывода денежных средств (обналичивания);

– о счетах, банковских картах, фирм «однодневок» и дропов (возможно номера операторов мобильной связи) на счета которых переведены денежные средства, данные о номинальных и фактических руководителях юридических

лиц, а также данные оперативных сотрудников правоохранительных органов их установивших, с указанием контактных телефонов;

– о ключевых данных совершенного преступления, т.е. переход на единый электронный учет сообщений о преступлениях.

В целях реализации данного проекта так же потребуется организовать доступ к указанной базе каждому государственному служащему, в том числе сотрудникам правоохранительных органов, в части их должностных обязанностей и в соответствии с установленным режимом секретности. А в процессе разработки и использования на постоянной основе обеспечивать безопасность и секретность хранения, обработки и передачи цифровых данных.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты федерального уровня

1. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 года (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30 декабря 2008 года № 6-ФКЗ, от 30 декабря 2008 года № 7-ФКЗ, от 5 февраля 2014 года № 2-ФКЗ, от 21 июля 2014 года № 11-ФКЗ) // СЗ РФ. 2014. № 31. Ст. 4398.

2. Кодекс административного судопроизводства Российской Федерации от 8 марта 2015 № 21-ФЗ // СЗ РФ. 2015. № 10. Ст. 1391.

3. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 года № 195-ФЗ // СЗ РФ.2002. № 1 (ч. 1). Ст. 1.

4. Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

5. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 01.05.2016) / Собрание законодательства РФ, 24.12.2001, N 52 (ч. I). –ст. 4921.

6. Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СЗ РФ. 2016. № 28. Ст. 4558.

7. Федеральный закон от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления

дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СЗ РФ. 2016. № 28. Ст. 4559.

8. Федеральный закон от 07.02.2011 N 3-ФЗ «О полиции» // СЗ РФ. 2011. N 7. ст. 900.

9. Федеральный закон от 17.01.1992 N 2202-1-ФЗ «О прокуратуре Российской Федерации» // СПС КонсультантПлюс.

10. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (ч. 1). Ст. 3451.

11. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. N 31.

12. Федеральный закон от 12.07.1995 N 144-ФЗ (ред. от 29.06.2015) «Об оперативно-розыскной деятельности» / Собрание законодательства РФ, 14.08.1995, N 33. – ст. 3349.

13. Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС КонсультантПлюс.

14. Федеральный закон от 13.07.2015 N 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» // СПС КонсультантПлюс.

15. ГОСТ Р 7.0.97-2016. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов (утв. Приказом Росстандарта от 08.12.2016 N 2004-ст) (ред. от 14.05.2018) // СПС КонсультантПлюс.

Научная литература

1. Александрова И.А. Новое уголовное законодательство о мошенничестве // Юридическая наука и практика. Вестник Нижегородской академии МВД России. 2013. № 21. С. 54-62.

2. Архипов В.В. Виртуальное право: основные проблемы нового направления юридических исследований // Известия высших учебных заведений. Правоведение. №2. 2013; Дюранске Б.Т., Кейн Ш.Ф. Виртуальные миры, реальные проблемы // Известия высших учебных заведений. Правоведение. №2. 2013;

3. Бабаев М. М., Пудовочкин Ю. Е. Проблемы российской уголовной политики. М., 2014. С. 93.

4. Батурин Ю.М., Жодзишский А.М., Б28 Компьютерная преступность и компьютерная безопасность. – М.: Юрид, лит. 1991.- 160 с.

5. Воронцова С.В. К вопросу о квалификации преступлений в сфере электронных платежей // Банковское право. 2009. № 1.

6. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: Инкомбук, 1997.

7. Гилинский Я. И. Криминологические основы уголовного права в эпоху постмодерна // Криминологические основы уголовного права // Материалы X Российского конгресса уголовного права, состоявшегося 26-27 мая 2016 г. / отв. ред., докт. юрид. наук, проф. В.С. Комиссаров. М., 2016. С. 296.

8. Гуров А.И. Криминогенная ситуация в России на рубеже XXI века. М., 2000. – 96 с

9. Евдокимов К.Н. Проблемы квалификации и предупреждения компьютерных преступлений. Иркутск: Иркутский юридический институт (филиал) Академии Генеральной прокуратуры РФ, 2009.

10. Елин В.М. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. 2013. № 2 (24). С. 70-76.

11. Козаев Н.Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): / под. ред. А.В. Наумова. М., 2015.

12. Крылов В.В. Расследование преступлений в сфере информации. М., 2005. – 180 с.

13. Кудрявцев В. Н. Объективная сторона преступления. М., 1960. С. 102.

14. Маленкин А.С. Вопросы разграничения мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) и неправомерного доступа к компьютерной информации, совершенного из корыстной заинтересованности (ч. 2 ст. 272 УК РФ) // Противодействие преступности: от теории к практике день за днем: научно-практическая интернет-конференция Омской юридической академии. Омск, 2013.

15. Мочагин П. В. Новые формы следообразований в криминалистике и судебной экспертизе / П. В. Мочагин // Судебная экспертиза в парадигме российской науки (к 85-летию Ю. Г. Корухова) : сб. материалов 54-х кримин. чтений : в 2 ч. — М. : Академия управления МВД России, 2013. — Ч. 2. — С. 97–101.

16. Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации. Дис… канд. юрид. наук. М., 1999. – 230 с. Степанов-Егинянц В. Ответственность за компьютерные преступления // Законность. – 2005. – №12. – С. 49.

17. Смушкин А. Виртуальные следы в криминалистике / А. Смушкин // Законность. — 2012. — № 8. — С. 43–45.

18. Хилюта В.В. Уголовная ответственность за хищения с использованием компьютерной техники // Журн. рос. права. 2014. № 3.

19. Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 201 № 1. С. 9 - 22.

20. Шумилов Н.И. Информационная безопасность: методическое пособие для сотрудников, правоохранительных органов / Под ред. И.А. Возгрина. СПб: СПб. Академия МВД России, 1997, 26с.

21. Шумихин В. Г. Седьмая форма хищения чужого имущества // Вестник Пермского университета. 2014. № 2 (24). С. 229.

22. Экономическая информатика / под ред. В. П. Косарева, Л. В. Еремина. — М.: Финансы и статистика, 2001. — 592 с.

23. Яни П.С. Специальные виды мошенничества // Законность. 2015. № 8. С. 35–40.

Иные нормативно-правовые источники

1. Доклад 10 Конгресса ООН по предупреждению преступности и обращению с правонарушителями // 10 Конгресс ООН по предупреждению преступности и обращению с правонарушителями: сборник документов / сост. А.Г. Волеводев. М., 2001.

2. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А.И. Чучаева. М., 2013.

3. Приказ Генпрокуратуры России № 39, МВД России № 1070, МЧС России № 1021, Минюста России № 253, ФСБ России № 780, Минэкономразвития России № 353, ФСКН России № 399 от 29.12.2005 (ред. от 20.02.2014) «О едином учете преступлений».

4. Постановление Пленума ВС РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате».

5. Указ Президента РФ от 15.01.2013 г. N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

6. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

7. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы».

8. Письмо МВД РФ от 13.07.2015 № 1/5562 «Об организации работы по противодействию отдельным видам мошенничества».

9. Информационное письмо Генеральной прокуратуры РФ от 03.11.2015 № 36-11-2015 «Об определении места производства предварительного расследования мошенничеств, совершаемых с использованием телефонной (сотовой) связи».

Источники на иностранном языке

1. Shannon C.E. A Mathematical Theory of Communication. Bell Systems Technical Journal. July and Oct. 1948 //Claude Elwood Shannon. Collected Papers. N. Y., 1993. P. 8-111.

Интернет-ресурсы

1. http//genproc.gov.ru/smi/news/archive/news-112274.
2. http://hitech.newsru.com/article/ 17Oct2012/cardio.
3. http://itsec.ru/newstext.php?news_id=106860.
4. http://www.kremlin.ru/events/president/news/55495.
5. https://megalektsii.ru/s21781t1.html.
6. https://ria.ru/20130809/955198703.html.
7. https://ru.wikipedia.org/wiki/Petya.
8. https://threatpost.ru.
9. https://www.kaspersky.ru/blog/wannacry-ransomware/16147.
10. https://мвд.рф url:www.threatpost.ru.