Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Южно-Уральский государственный университет»
(Национальный исследовательский университет)
Юридический институт
Кафедра «Уголовное и уголовно-исполнительное право, криминология»

ДОПУСТИТЬ К ЗАЩИТЕ
Руководитель магистерской программы,
д.ю.н., профессор, профессор кафедры
_____Ю.А. Воронин
_____ 2017 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА И ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

ФГАОУ ВО «ЮУрГУ» (НИУ) – 40.04.01.2017.244.М

Направление: «Юриспруденция»
Магистерская программа: «Уголовное право, криминология и уголовно-исполнительное право»

Руководитель магистерской диссертации
Гарбатович Денис Александрович
к.ю.н., доцент _____
_____2017 г.

Автор магистерской диссертации
магистрант группы Юм – 244
Савиновский Артем Николаевич_____
_____2017 г.

Нормоконтролер, преподаватель
Бирюкова Дарья Вячеславовна
_____
_____2017 г.

Челябинск 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы диссертационного исследования. В динамичных условиях 21 века общество постоянно сталкивается с проблемами различного характера, порождение которых зачастую вызвано стремлением общества к созданию более совершенных и эффективных моделей своего существования. Это касается, в том числе и сферы применения компьютерных технологий.

Мы вынуждены констатировать, что процесс информатизации общества и особенно через его компьютеризацию приводит к увеличению количества компьютерных преступлений, их объём в целой доле преступлений.

В РФ в наши времена поражают темпы роста компьютерных преступлений, особенно в Интернете, где по данным Интерпола «преступность растет самыми быстрыми темпами на планете». В этом смысле все реальнее кажутся прогнозы некоторых учёных, согласно которым компьютерные преступления в скором будущем станут генератором преступности во всем мире. Важно уже сейчас понимать личность компьютерного преступника, знать где и как ему противодействовать и какие правовые меры применять. Уже сейчас мы должны признать, что компьютерные преступники ушли намного дальше правоохранительной системы в своих способностях и возможностях вести незаконную деятельность безнаказанно.

Степень научной разработанности проблемы. С преступлениями в сфере компьютерной безопасности мир и, в частности, Российская Федерация, сталкиваются не в первый раз. Эта категория появилась в конце 20 века и с тех пор активно «завоёвывала» своё место среди преступников. Ясно, что для противодействия даже преступникам-любителям в такой сфере необходимо активное взаимодействие с профессионалами своего дела. Рассмотрев работы таких учёных как, например, Щербович, Дворецкий, Ткачев, Батурин и др. мы видим, что некий теоретический базис может и

будет актуален до сих пор, но с практической точки зрения мы едва ли можем опираться на их рекомендации, ввиду слишком быстрого прогресса компьютерных технологий. Портрет преступника с каждым годом также меняется как и орудия с помощью которых он совершает преступления.

В связи с этим есть явная необходимость рассмотреть вопросы касающиеся темы магистерского исследования.

Цель и задачи исследования. Целью проведенного в магистерской работе исследования является анализ и получение конкретных результатов по составлению портрета преступника, занимающегося деятельностью в компьютерной сфере, понять его цели, мотивы, задачи, образы мышления и способы ведения деятельности. Достижение названной цели потребовало решения следующих задач:

- провести анализ действующего уголовного законодательства в области преступлений в сфере компьютерной информации;
- осмысление основных понятий связанных с преступлениями в сфере компьютерной информации;
- анализ состояния и тенденций таких преступлений в России;
- определение основных мероприятий правового, технического, организационного характера с целью предупреждения преступлений в сфере компьютерной информации;

Объектом исследования являются преступность в сфере компьютерной информации.

Предметом исследования являются специальная литература, материалы судебно-следственной практики, статистические данные, отечественный и зарубежный опыт борьбы с компьютерной преступностью.

Методология и методика исследования. Методологической основой исследования послужили общенаучные методы познания, а также частно-научные методы:

– историко-правовой - применительно к изучению исторического опыта по установлению уголовной ответственности за совершение преступлений в сфере компьютерной информации;

– формально-логический, заключающийся в детальном анализе уголовно-правовых и организационно-технических мер противостояния неправомерному доступу к компьютерной информации;

– статистический, включающий сбор и анализ статистических данных о неправомерном доступе к компьютерной информации.

Эмпирическую базу исследования магистерской диссертации составляют материалы, содержащиеся в законах и нормативных правовых актах, работы известных юристов, криминологов и специалистов в сфере компьютерной информации – И.А. Щербович, М.Ю. Дворецкого, А.Ю. Карамнова, А.В. Ткачева, Ю.М. Батурина, А.М. Жодзишского, А.Н. Копырюлина, Е.В. Беспаловой, В.А. Широкова, С.Н. Золотухина и др.

Научная новизна исследования. Автором комплексно проанализирован криминологический аспект преступлений в сфере компьютерной информации, при этом определены теоретические основы и понятия данной сферы криминологии. Выявлены недостатки в нормативных актах и криминологических подходах к данным преступлениям. Рассмотрены актуальные проблемы и пути их решения в преодолении безнаказанности и вездесущности компьютерных преступников.

В диссертации сформулированы и выносятся на защиту следующие выводы и положения, отражающие научную новизну исследования.

1 Преступность в сфере компьютерной информации, и особенно в Интернете, имеет тенденцию к значительному росту в части статей УК РФ, предусматривающих неправомерный доступ к компьютерной информации и создание, использование и распространение вредоносных программ для ЭВМ.

2 С каким бы мотивом и целью не совершался неправомерный доступ к охраняемой законом компьютерной информации, виновное лицо подлежит уголовной ответственности. Однако некоторые мотивы и цели безусловно повышают степень общественной опасности преступления.

3 Компьютерный преступник (хакер) - это, как правило, мужчина в возрасте от 18 до 24 лет с высоким уровнем образования, часто технического.

4 Важным направлением борьбы с преступностью в сфере компьютерной информации должно стать становление и развитие правового фундамента в сфере Интернета путем принятия Закона «О правовом регулировании использования сети Интернет».

5 Преступления в сфере компьютерной информации являются преступлениями с крайне высоким уровнем латентности. Причины как в недостаточной осведомленности граждан, так и в низкой квалификации сотрудников правоохранительных органов.

6 Создание международных круглосуточных онлайн центров по противодействию и отслеживанию киберпреступлений как мера предупреждения преступлений и их расследования.

Теоретическая и практическая значимость исследования. Научное и практическое значение работы состоит в том, что в процессе исследования теоретические положения и выводы, определения ряда понятий и высказанные рекомендации окажутся полезными для дальнейших исследований, посвященных борьбе с преступностью в сфере компьютерной информации.

Сформулированные в магистерской диссертации выводы и предложения могут быть использованы в практической деятельности, в процессе преподавания в высших учебных заведениях.

Апробация результатов исследования. Диссертация подготовлена, рассмотрена и одобрена на кафедре рассмотрена и одобрена на кафедре

уголовного права, криминологии и уголовно-исполнительного права Южно-Уральского государственного университета.

1. Савиновский А. Н., Гарбатович Д.А. Ответственность за преступления в сфере компьютерной информации по зарубежному законодательству / А.Н. Савиновский Д.А. Гарбатович // Научный диалог: вопросы гуманитарных исследований. [Электронный ресурс] URL: https://interactive-plus.ru/ru/article/320927/discussion_platform (дата обращения: 11.06.2017).
2. Савиновский А.Н. Гарбатович Д.А. Преступления в сфере компьютерной информации в законодательстве РФ / А.Н. Савиновский Д.А. Гарбатович // Экономика Социология и Право. № 5 (МАЙ) – С. 65.
3. Савиновский А.Н. Гарбатович Д.А. Понятие и система преступлений в сфере компьютерной информации по Уголовному кодексу Российской Федерации / А.Н. Савиновский Д.А. Гарбатович // Научные исследования: Проблемы науки. – С. 84

Структура и объем диссертации. Работа состоит из введения, трех глав, включающих в себя восемь параграфов, заключения и библиографического списка. Диссертация изложена на 100 страницах машинописного текста, библиография включает 93 наименования.

1 ПРАВОВАЯ ПРИРОДА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1 Понятие и система преступлений в сфере компьютерной информации по Уголовному кодексу Российской Федерации

Для начала раскроем понятие преступления в сфере компьютерной информации, чтобы у нас была возможность их чёткого разграничения в законодательстве.

В Уголовном кодексе РФ отсутствует упоминание термина "компьютерное преступление". Глава 28 «Преступления в сфере компьютерной информации» содержит три статьи: Статья 272. Неправомерный доступ к компьютерной информации.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно–телекоммуникационных сетей. Законодатель подошел к определению характера этих преступлений таким образом, что основным признаком стал не сам компьютер как орудие преступления, а некоторые отношения, а именно информационные отношения хранения, отбора, диссеминации и передаче пользователю виртуальных данных.

С одной стороны, норма определяет их к преступлениям против общественной безопасности. Ввиду этого составы компьютерных преступлений возможно толковать в том смысле, что такие преступления представляют опасность для охраняемых законом интересов неопределенного круга лиц. В то же время, такие преступления совершаются путем незаконного воздействия на компьютерную информацию, что ограничивает объект и уточняет предмет такого преступления.

Общность объекта компьютерных преступлений возникает не по той причине, что социальные отношения по поводу использования компьютерной информации определяются отдельной сферой общественной жизни. В изолированном виде эти отношения не содержат ценностного содержания. Ценность и значение объекта преступления имеет только компьютерная безопасность. Опасность компьютерных преступлений в том, что они образуют возможность вреда жизни и здоровью, имущественным правам и интересам, неприкосновенности частной жизни, иным охраняемым законом интересам личности, общества и государства. Неприемлимо применение к человеку уголовных санкций только за нарушение установленного порядка в сфере использования компьютерной информации, если его деяние не повлекло за собой и не могло повлечь никакого реального вреда. К примеру, использование несовершеннолетним компьютера другого несовершеннолетнего для игр без согласия последнего, даже если это привело к копированию очень большого объема информации, в размере тысяч килобайт, не будет преступлением в силу ч. 2 ст. 14 УК РФ. При этом, изменение даже небольшой части информации в системе обороны или транспорта страны может привезти к серьезным последствиям и, соответственно, повлечь за собой уголовную ответственность при незаконном вмешательстве.

В связи с этим является обоснованными предложение Г.П. Новоселова delegeferenda не рассматривать уничтожение, блокировка информации и т.п. в качестве последствия преступления. Целесообразно было бы определить их в качестве способа посягательства, но это не отражено в действующем законе.

Возвращаясь к предмету данного преступления, вспомним, что им является компьютерная информация. Информационным законодательством России охраняются: сведения, отнесенные (соответствующим федеральным законом) к государственной тайне; сведения, отнесенные к служебной и

коммерческой тайне; сведения, имеющие статус персональных данных. Легальная дефиниция компьютерной информации была введена Федеральным законом от 07.12.2011 № 420–ФЗ «О внесении изменений в Уголовный кодекс РФ и отдельные законодательные акты РФ»3 и содержится в прим. 1 к ст. 272 УК. Так, под компьютерной информацией «понимаются сведения (данные, сообщения), представленные в форме электрических сигналов, вне зависимости от средств их обработки, хранения и передачи». Законодательное закрепление рассматриваемого понятия стало знаковым событием на пути правового обеспечения противодействия компьютерным преступлениям на современном этапе. Исключение из гл. 28 УК РФ перечня средств хранения, обработки и передачи компьютерной информации, по мнению М.Ю. Дворецкого и А.Ю. Карамнова, отныне позволит компьютерной информации выступать как предметом, так и средством совершения компьютерных преступлений.[1]

В ст. 128 ГК РФ информация указана как один из видов объектов гражданских прав; ст. 39 ГК РФ устанавливает меры гражданско–правовой защиты информации, являющейся служебной или коммерческой тайной. Важно понимать, что такие меры не являются правовыми режимами информации в отличие от содержащей государственную тайну или конфиденциальной, поскольку определить принадлежность информации к государственной тайне могут лишь уполномоченные органы в соответствии с Законом РФ «О государственной тайне», к тому же, эти режимы устанавливаются только информации на материальном носителе с идентифицирующими реквизитами. Чтобы отнести информацию к коммерческой или служебной тайне ее не обязательно документировать, достаточно, чтобы эта информация отвечала следующим условиям, установленным в ст. 139 ГК РФ: имеет действительную или потенциальную

[1]Дворецкий М.Ю., Карамнов А.Ю. Оптимизация уголовной ответственности за преступления в сфере компьютерной информации // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2012. – № 11. – С. 387.

коммерческую ценность в силу недоступности ее третьим лицам; отсутствие свободного законного доступа; обладатель информации принимает меры к охране содержащихся сведений; сведения, составляющие служебную и коммерческую тайну, не отнесены законом к сведениям, которые не могут ее составлять.

Отнесение информации к государственной тайне или к конфиденциальной осуществляется в порядке, установленном законодательством Российской Федерации (в частности, Законом РФ от 21 июля 1993 г. «О государственной тайне»).

Конституция РФ в ст. 23 провозглашает право каждого на неприкосновенность частной жизни, личную и семейную тайну. В ч. 1 ст. 24 Конституции РФ указано, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Закон об информации относит сведения о гражданах (персональные данные), т.е. о событиях, фактах и обстоятельствах жизни гражданина, которые позволяют его идентифицировать, к конфиденциальной информации. Законодательством также определены сведения, к которым не может быть ограничено право свободного доступа.

В научной литературе до сих пор отсутствует однозначное понятие информации. В общем смысле информация означает какие–либо сведения. При этом не любые, а только те, которые имеют субъективную ценность для их получателя. Исходя из этого фактора, закон охраняет информацию, составляющую личную, семейную, коммерческую, банковскую, государственную и иные виды тайн. Сведения, имеющие информационную значимость, составляют сообщения и данные. Сообщение представляется в форме графических изображений, схем, символов и т.п. Согласно теории коммуникации, обмен сообщениями предполагает собой определенную деятельность адресанта (отправителя) по передаче по заранее выбранным

каналам связи информации адресату (получателю)[1]. Проще говоря, сообщение можно назвать информацией лишь при наличии реального получателя, субъекта в конце связи. Интересно в связи с этим мнение Г.М. Маклюэна, утверждавшего, что электронная техника (средство) отражает не только форму, но и содержание сообщения[2]. При этом, данные, с точки зрения информатики, представляют собой «информацию, закодированную определенным образом с целью передачи, обработки, хранения, поиска или извлечения»[3]. В общем говоря, данные — это форма представления (хранения) информации на электронном носителе. В отличие от сообщений, данные не подразумевают наличие получателя. Формой представления компьютерной информации являются электрические сигналы. В теории электрической связи под сигналом понимается физический процесс (электрический ток или радиоволны), способный перемещаться в пространстве и нести в себе информацию[4]. Если передаваемая посредством сигналов информация принимается в системе связи, то она приобретает вид сообщения (совокупности знаков–символов). Далее, при поступлении информации в компьютер происходит процесс кодирования, то есть ее представления в виде двоичного кода (бинарное представление), выраженного комбинацией цифр 0 (отсутствие сигнала) и 1 (наличие сигнала). Кодированная информация и есть те самые данные, содержащиеся в компьютере. В свою очередь, для того чтобы эти данные могли быть познаны, восприняты человеком, происходит обратный процесс декодирование, то есть преобразование двоичного кода в доступную для восприятия форму (текстовую, графическую и т.д.).

---

[1]Викулова Л.Г., Шарунов А.И. Основы теории коммуникации: практикум. – М., 2008. – С.42

[2]Маклюэн М.Г. Средство само есть содержание. [Электронный ресурс]. – URL: http://www.uic.unn.ru/pustyn/lib/maclu.ru.html.

[3]Макарова Н.В., Волков В.Б. Информатика: учеб. для вузов. – СПб., 2011. – С. 18.

[4]Романов Б.Н., Краснов С.В. Теория электрической связи. Сообщения, сигналы, помехи, их математические модели: учеб. Пособие. – Ульяновск, 2008. – С. 7.

Таким образом, сообщения и данные становятся информацией в процессе их осмысления человеком, то есть требуют субъективной оценки. Уголовно–правовой охране по УК РФ подлежит компьютерная информация в процессе ее хранения, преобразования и передачи по каналам связи с помощью электрического тока. Однако предлагаемая законодателем дефиниция не учитывает иных технических средств и способов передачи информации. В частности, речь идет о средствах оптоволоконной связи, использующих световые, а не электрические сигналы. Поэтому можно предположить, что неправомерное, вопреки запрету пользователя, снятие информации с оптических каналов связи не будет являться уголовно–наказуемым деянием.

Законодательная неопределенность стала одной из причин неоднородности судебной практики. С одной стороны, средствами–носителями компьютерной информации суды стали признавать широкий круг технических устройств от компьютеров и ноутбуков до банкоматов. Здесь важно отметить, что генерировать информацию, представленную в форме двоичного кода, на сегодняшний день способно множество устройств, включая компьютер. К ним относятся мобильные телефоны, смартфоны, планшетные компьютеры и т.д. В связи с этим понятие «компьютер», используемое в гл. 28, выглядит несколько аморфным и полностью не отражающим суть рассматриваемых преступлений.

Проблема усугубляется и отсутствием унифицированного терминологического аппарата в законодательстве. К примеру, в ст. 1261 ГК используется понятие «программа для ЭВМ», в то время как ст. 273 УК содержит термин «компьютерная программа». Очевидно, что по своему содержанию они идентичны, однако легальная несогласованность способна создать существенные препоны на пути формирования единой судебной практики. Помимо указанных, Федеральным законом от 28 июля 2012 г. № 143–ФЗ в ряд статей УПК РФ было введено понятие «электронный носитель

информации»[1], при этом его содержание не раскрывается. Логично предположить, что к числу таких носителей следует относить все вышеназванные устройства. Однако, по мнению А.В. Ткачева, такая позиция законодателя ляжет бременем на криминалистов, отныне вынужденных проводить дополнительные исследования «по отнесению тех или иных устройств к средствам обработки компьютерной информации или электронным носителям информации»[2]. Выход из сложившейся ситуации предполагает собой конкретизацию понятийного аппарата отраслей права, приведения их в функциональное единство с учётом современных реалий развития науки и техники.

Достаточно лаконичным и интересным видится определение С.В. Бородина, который описывает компьютерное преступление как общественно опасное деяние, направленное против общественных отношений, регулирующих изготовление, использование, распространение и защиту компьютерной информации. Полностью противоположной точки зрения придерживается Ю.М. Батурина, который считает, что компьютерные преступления в качестве индивидуальной группы преступлений не существуют, а верно определять лишь компьютерные аспекты преступлений. При этом компьютер при совершении преступления выступает лишь в качестве объекта, орудия совершения преступления или среды, в которой оно совершается.[3]

Важно понимать также позицию В.Б. Вехова, который утверждает, что термин «компьютерные преступления» не имеет уголовно–правовых границ и может использоваться только в криминологическом и криминалистическом аспектах. Автор объясняет это тем, что, выделяя группу преступлений в сфере компьютерной информации в раздел посягательств на общественную

[1]Федеральный закон «О внесении изменений в Уголовно–процессуальный кодекс РФ» от 28 июля 2012 г. № 143–ФЗ // Российская газета. – 2012. – №5847.
[2]Ткачев А.В. Исследование компьютерной информации в криминалистике // Эксперт–криминалист. – 2012. – № 4. – С. 5.
[3]Батурин Ю.М. Проблемы компьютерного права. – М., 1991. – С.129.

безопасность и общественный порядок, законотворцы не указывают ни в каком составе преступлений на такой квалифицирующий признак, как совершение преступления с использованием компьютерных технологий. И, хотя, с его точкой зрения трудно не согласиться, такая позиция образует еще одну проблему – определение локации норм, определяющих преступления против компьютерной информации в структуре Уголовного кодекса РФ. В данном вопросе учёные также расходятся во мнениях. Определение гл.28 в разд. 9 УК РФ, на первый взгляд, устанавливает его родовой объект как общественные отношения, регулирующие общественную безопасность и общественный порядок. Однако по утверждению некоторых учёных, не согласных с общеопасным характером компьютерных преступлений, такой подход законодателя считается слишком общим.[1] Замечания по поводу определения компьютеров к источникам повышенной опасности обоснованно справедливы. При этом, нельзя отрицать высокую общественную опасность преступлений, предусмотренных статьями 272–274 Уголовного кодекса, степень которой дифференцируется от важности и значимости охраняемой информации, а также от размера вреда, нанесенного государству, гражданину или организации. То есть, преступлениями в сфере компьютерной информации может быть причинен существенный вред общественной безопасности. Вред от такого вида преступлений может быть нанесён также государственной безопасности. По оценкам специалистов стран Восточной и Западной Европы по вопросам борьбы с компьютерной преступностью, выгода преступников от преступлений с использованием компьютерных технологий занимает третье место после доходов от продажи вооружений и наркотических средств, а нанесенный ущерб оценивается

[1]Копырюлин А.Н. Система преступлений в сфере компьютерной информации в структуре РФ//Системность в уголовном праве//Материалы 2–го Российского Конгресса уголовного права. – 2007.

миллиардами долларов.[1] С таким мнением солидарны Ю.А.Батурин и А.М Жодзишский, которые выступают за то, что компьютерные преступления наносят вред отношениям общественной безопасности, призванные «удерживать информационные системы в безопасном цельном состоянии».[2] Вышеуказанное позволяет нам понять позицию законодателя и доказывает рациональность отнесения преступлений, предусмотренных гл.28, к преступлениям против общественной безопасности и общественного порядка и выделения в качестве непосредственного объекта совокупность общественных отношений по правомерному и безопасному использованию компьютерной информации.

Рассмотрим также для лучшего понимания нынешней ситуации в законодательстве фактор субъективной стороны в главе 28 УК РФ.

Субъективная сторона преступления предусматривает две формы вины (умысел и неосторожность). При этом умысел и неосторожность являются обязательными признаками субъективной стороны, а факультативными будут мотив и цели. Изучение трудов учёных в этой сфере позволяет сделать вывод об отсутствии цельного подхода о форме вины при незаконном доступе к компьютерной информации. Рассмотрим различные точки зрения в частном порядке. Например, имеет место быть точка зрения, в соответствии с которой незаконный доступ к компьютерной информации может быть совершен лишь с прямым умыслом[3]. А.И. Абова утверждает, что «неправомерный доступ к охраняемой законом компьютерной информации может быть совершен только с прямым умыслом»[4]. Д.Г. Малышенко

[1]Беспалова Е.В., Широков В.А. Компьютерные преступления: основные тенденции развития// Юрист. – М.: Юрист 2006, № 10. – С.18–21.

[2]Батурин Ю.М., Жодзишский А.М. Компьютерные преступления и компьютерная безопасность. – М., 1991. – С.30–31.

[3]Комментарий к Уголовному кодексу Российской Федерации / под ред. Наумова.– М.: 1996–С. 665; Борчева Н.А. Компьютерные преступления в России (комментарий к Уголовному Кодексу РФ). – М.: 2001.–С.10.

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

убежден, что «умысел может быть только прямым»[1]. С этим утверждением солидарны С.В. Григоренко, С.Н. Ткаченко, А.А. Каспаров, которые считают, что «с субъективной стороны преступление может быть совершено только с прямым умыслом»[2]. Во большей части научных трудов задаётся вопрос о возможности получения незаконного доступа к компьютерной информации не только с умыслом, но и по неосторожности. С.А. Пашин указывает: «... данное преступление может совершаться не только с прямым умыслом, но и по неосторожности»[3]. С ним солидарны С. Н. Золотухин и А. З. Хун, утверждая, что «неосторожная форма вины может проявляться при оценке лицом правомерности своего доступа к компьютерной информации (так называемая «юридическая ошибка»), а также в отношении неблагоприятных последствий»[4]. С.В. Озерский, Ю.Н. Лазарев, А.Ю. Лавров сходятся во мнении, что преступление может быть с прямым или косвенным умыслом, но «неосторожная форма вины может проявляться при неверной оценке лицом правомерности своего доступа к компьютерной информации, а также в отношении различных последствий доступа, предусмотренных диспозицией данной нормы уголовного закона»[5]. А.Е. Шарков согласен с такой позицией, подтверждая ее тем, что «субъект, пытающийся получить незаконный доступ по неосторожности, может осознавать опасность своих действий, но действует легкомысленно, или не предвидит возможных опасных

[1]Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: диссертация... кандидата юридических наук – М.:, 2002.–С.95.
[2]Григоренко С.В., Ткаченко С.Н., Каспаров А.А., Преступления в сфере компьютерной информации.– М.: Полтекс, 2003.–С.11.
[3]Пашин С.А. Преступления в сфере компьютерной информации// Коммент к УК //под ред. Скуратова и Лебедева –М.: 1996.–С. 640.
[4]Золотухин С.Н., Хун А.З. Уголовно–правовые и криминологические аспекты преступлений в сфере компьютерной информации: учебное пособие Краснодар: Краснодарский университет МВД России. – 2008.–С.72.
[5]Озерский С.В., Лазарев Ю.Н., Лавров А.Ю. Компьютерные преступления: методы противодействия и защиты информации: Учебное пособие Саратов: Саратовский юридический институт МВД России. – 2004.– С.24.

последствий, хотя может и должен их предвидеть»[1]. Имеет место мнение, что форма вины зависит от самих последствий, так, к примеру, копирование информации может быть совершено только с прямым умыслом, а уничтожение, улучшение, блокировка компьютерной информации могут быть совершены, как умышленно, так и по неосторожности[2]. Теоретики, согласны с этой позицией и утверждают, что копирование информации направлено именно на достижение определенного результата, а уничтожение, улучшение, блокировка информации могут быть совершены как умышленно, так и по неосторожности. Мы считаем, что нельзя ставить в зависимость форму вины от самих последствий, так как лицо уже осознает неправомерность деяния по характеру его совершения. Изучим также мнение А.Г. Волеводза, он утверждает, что «субъективная сторона данного преступления характеризуется виной в форме прямого умысла. Косвенный умысел и неосторожная форма вины может иметь место по отношению к наступлению вредных последствий неправомерного доступа»[3]. Изучение большей части теоретических материалов позволяют нам сделать вывод, что неправомерный доступ к компьютерной информации совершается либо с прямым, либо с косвенным умыслом. Преступник осознает, что совершает незаконный доступ к компьютерной информации, предвидит неизбежность или возможность наступления различных последствий, предусмотренных законом, желает или сознательно допускает их наступления либо или относится к ним безразлично[4]. Такое мнение учёные подтверждают следующими аргументами: осуществляя неправомерный доступ по мотивам

[1]Шарков А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: диссертация\кандидата юридических наук – Ставрополь, 2004.–С.149.

[2]Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: диссертация кандидата юридических наук.– Красноярск:2002.–С. 134.

[3]Волеводз А.Г. Противодействие к компьютерным преступлениям: правовые основы международного сотрудничества.– М.: 2002.–С. 71.

[4]Сударева Л.А. Правовое и информационное обеспечение деятельности органов внутренних дел по предупреждению компьютерных преступлений: диссертация кандидата юридических наук.– М.: 2008.–С.44.

хулиганских действий преступник, чаще всего, относится к возможным последствиям безразлично. Ю. Ляпунов и В. Максимов полагают, что «субъективная сторона неправомерного доступа к компьютерной информации характеризуется виной в форме умысла, прямого или косвенного: лицо должно осознавать общественную опасность своего действия, предвидеть возможность или неизбежность наступления общественно опасных последствий и желать их наступления, либо допускать их или относиться к ним безразлично»[1]. С. Кочои, Д. Савельев тоже согласны в той части, что преступление совершается умышленно. Индивид, пытающийся получить доступ к информации, должен сознавать, что свободный доступ к информации закрыт, он не имеет законных прав на доступ к этой информации. Об умысле будут говорить меры защиты информации от доступа посторонних (пароли, коды и т.п.), которые необходимо обойти, чтобы достичь желанной информации, визуальные предупреждения на дисплее компьютера, звуковые оповещения о запрете доступа к информации и т.д[2]. При этом по отношениям к последствиям вина может быть, как умышленной, так и неосторожной. В этой части учёные К. Н. Евдокимов[3]. В. А. Мазуров тоже утверждают, что последствия могут быть результатом неосторожного к ним отношения и «следовательно, лицо можно будет привлечь к ответственности только за покушение, либо оно вообще не подпадает под действие уголовного закона»[4]. В данном случае актуально внесение соответствующих изменений в уголовный закон либо появление административной ответственности для вышеуказанных случаев. В соответствии с ч.2 ст.24 УК РФ: «Деяние, совершенное только по

[1]Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления //Законность.– 1997.– №1. – С.12.
[2]Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации. Электронный ресурс.– 1999.
[3]Евдокимов К.Н. Субъективная сторона неправомерного доступа//Вестник Академии Генеральной Прокуратуры РФ. – М.2009. – №12.
[4]Мазуров В.А. Компьютерные преступления: классификация и способы противодействия: учебно–практическое пособие. – М.: 2002.–С.115.

неосторожности, признается преступлением лишь в том случае, когда это специально предусмотрено соответствующей статьей Особенной части настоящего Кодекса». Из этого можно сделать вывод, что если при описании преступления не указана форма вины, то оно может совершаться как умышленно, так и неосторожно. Мы считаем, что преступление может совершаться только умышленно, на это прямо указывает понятие «неправомерность», то есть виновный осознает, что совершает незаконный, закрытый доступ к охраняемой законом компьютерной информации. Помимо этого, на то, что неправомерный доступ к компьютерной информации совершается умышленно, есть ссылка в некоторых источниках информационного права. Так, например, согласно ст.3 Соглашения о сотрудничестве государств–участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации, подписанного в Минске 1 июня 2001 года: «Стороны признают в соответствии с национальным законодательством в качестве уголовно наказуемых следующие деяния, если они совершены умышленно: осуществление неправомерного доступа к компьютерной информации». Проанализировав судебную практику по делам о привлечении к ответственности по статье 272 УК РФ, мы сделали вывод: суды при разбирательстве уголовных дел устанавливают, что преступники имеют умысел на неправомерный доступ к охраняемой законом компьютерной информации и на достижение последствий в виде уничтожения, копирования, блокировки и модификации компьютерной информации. Например: согласно приговору от 13.02.2013г. по делу №1–12/2013, мировой суд судебного участка № 45 Егорьевского судебного района Московской области[1] установил: «Г., имея преступный умысел, направленный на осуществление неправомерного доступа к охраняемой законом

[1]Уголовное дело №1–12/2013 от 14.02.2013 // Арх. Егорьевского городского суда (Московская область). [Электронный ресурс]. – URL: https://rospravosudie.com/act-107303628/

компьютерной информации и ее копирование...»; согласно постановлению о прекращении уголовного дела за примирением сторон от 14.03.2012г. по делу №1–155/12 Первомайского районного суда г. Ижевска Удмуртской Республики[1]: «Х., реализуя свой преступный умысел, осознавая общественную опасность своих действий, предвидев неизбежность наступления общественно опасных последствий в виде блокирования и модификации компьютерной информации...»; согласно приговору от 02.02.2011г. Железнодорожный суд г. Самары: «Д. руководствуясь корыстными мотивами, преследуя цель незаконного личного обогащения, действуя умышленно и осознавая, что без использования абонентской карты и заключения абонентского договора, не обладает правом доступа к компьютерной информации... осуществил неправомерный доступ к компьютерной информации... Д., осуществляя неправомерный доступ к охраняемой законом компьютерной информации, предвидел, что в результате наступят вредные последствия, но относился к ним безразлично...». В условиях ограниченности диссертации проблематично процитировать все проанализированные приговы, но указанные примеры позволяют нам понять основную позицию судов – неправомерный доступ к охраняемой законом информации преступник осуществляет с прямым или косвенным умыслом, при этом умысел направлен и на наступление последствий, перечисленных в ст. 272 УК РФ. Мотивы и цели неправомерного доступа к компьютерной информации не являются обязательным признаком состава преступления. При этом определение цели и мотива позволяют установить причины преступления, определить индивидуальную ответственность, назначить справедливое наказание. Мотивом преступления считается намерение лица совершить преступление, а целью результат, к которому это лицо стремится. Зависть, корысть,

[1] Уголовное дело № 1–155/12 от 14.03.2012 // Арх. Первомайского районного суда г. Ижевска [Электронный ресурс]. – URL: https://rospravosudie.com/act-101676606/

хулиганские побуждения, желание унизить другое лицо, месть являются самыми частыми мотивами к совершению преступления. Иногда определение целей и мотивов могут серьёзным образом повлиять на квалификацию преступления. Так, неправомерный доступ к информации, являющейся государственной тайной, и ее копирование в зависимости от преследуемых преступником целей может быть квалифицирован, как неоконченная государственная измена по ст. ст. 30, 275 УК, если целью была выдача государственной тайны иностранному субъекту, или по ст. 272 УК, если вышеуказанный состав не имеет места. Некоторые учёные предполагают, что отсутствие в уголовном кодексе прямого указания на обязательность анализа целей и мотивов совершения компьютерных преступлений можно рассматривать как недостаток в законе[1]. По нашему мнению, не включение законодателем мотива и цели в диспозицию ст. 272 УК РФ свидетельствует о следующем: не имеет значение цель и мотив совершения неправомерного доступа, виновное лицо подлежит уголовной ответственности. Но, всё же, некоторые цели и мотивы так или иначе повышают степень общественной опасности преступления.

1.2 Ответственность за преступления в сфере компьютерной информации по зарубежному законодательству

Законодательство об уголовной ответственности за преступления в сфере компьютерной информации в сильно дифференцируется в разных странах. Мы считаем, что первопроходцами в сфере защиты компьютерной информации были Шведские законотворцы, когда 4 апреля 1973 годаони приняли «Закон о данных», который ввёл в устаревшее законодательство

[1]Кочои С.М. Ответственность за корыстные преступления против собственности. – М.,1998. – С.132.

новую терминологию — «злоупотребление при помощи компьютера»[1]. В США закон впервые защитил компьютерную информацию в принятом законодательными собраниями американских штатов Флорида и Аризона законе «Computer crime act of 1978»[2], определяющем уголовную ответственность за преступления в сфере компьютерной информации. В этом законе преступлением считались противоправные действия, сопряженные с уничтожением, нарушением целостности, незаконным доступом, кражей содержащейся на ЭВМ информации, программного обеспечения, и наказывались пятью годами лишения свободы, либо денежным штрафом в размере 5000 долларов, либо тем и другим одновременно в зависимости от тяжести причиненного потерпевшему вреда. Те же деяния, но совершенные с целью хищения различного имущества, наказывались пятнадцатью годами лишения свободы, либо штрафом в размере 10 000 долларов, либо совокупностью этих мер. В скором времени почти во всех штатах США были приняты схожие законы и иные нормативно–правовые акты. В федеральном «Законе о компьютерном мошенничестве» 1984 года вводится новая уголовная ответственность за совершение несанкционированного доступа к федеральным компьютерным сетям[3]. К примеру, наказание наступает для лиц, которые путем неправомерного доступа к компьютерной информации:

1 Получают информацию закрытого режима правительства США с намерением или осознанием того факта, что данная информация может быть использована во вред государству либо на пользу иностранному субъекту.

2 Получают информацию финансовой сферы США или информации о клиентах различных финансовых учреждений.

---

[1]Баранов А.А. Права человека и защита персональных данных. – Киев: Государственный комитет связи и информатизации Украины, –2000. – С. 280.

[2]Computer crime act of 1978 USA Law [Электронный ресурс]. – URL: http:// docweb.cns.ufl.edu/docs/d0010/d0010.html (дата обращения: 10.02.2011)

[3]Computer Fraud and Abuse Act [Электронный ресурс]. – URL: http:// www.law.cornell.edu /uscode/18/1030.html (дата обращения: 10.02.2011)

3 Целенаправленно копируют, модифицируют или уничтожают данные на определенных компьютерах. Так, например, в параграфе 33–02 «Breach of computer security» УК штата Техас определено, что лицо совершает преступление, если «сознательно использует компьютер, компьютерную сеть или компьютерную систему без официального согласия владельца или уполномоченного регламентировать доступ лица; при этом лицу, совершающему данное действие, заведомо известно о наличии защитной системы, специально созданной для защиты от потерь, изменения и стирания информации»[1]. Изучив данную норму мы можем сделать вывод, что обязательным и достаточным условием начала уголовного преследования при совершении преступлении в сфере компьютерной информации является обязательное наличие защитного механизма у такой информации. Помимо такой нормы с формальным составом уголовное законодательство Техаса имеет и специальные нормы, устанавливающие ответственность за блокирование в получении услуг отдельным категориям пользователей, т.е. за вмешательство в работу информационных сервисов. Согласно вышеуказанной норме, за преступления, связанные с «доступом с причинением ущерба», законодателем предусмотрено более строгое наказание. К примеру, уголовному преследованию подвергается человек, который «без согласия владельца или доверенного лица» умышлено «нарушает работу системы или вмешивается в стабильную работу системы» либо без согласия указанных выше лиц «изменяет, повреждает или уничтожает начинку этих систем». В США как федеральные, так и субъектные законотворцы, в 80-е гожа приняли не менее 5 различных законопроектов об уголовной ответственности за преступления в сфере компьютерной безопасности. В их числе был закон о противодействии компьютерному мошенничеству, мошенничеству с использованием

[1] Texas Penal Code – Section 33.02. Breach Of Computer Security [Электронныйресурс]. – URL: http://law.onecle.com/texas/penal/33.02.00.html (дата обращения 10.02.2011)

банковских карт, доступу к ограниченной информации и др. В 1983 году Организация экономического сотрудничества и развития Европы (ОЭСР) также приступила к изучению ситуации с компьютерной безопасностью. В 1986 году они опубликовали доклад «Преступления, связанные с применением компьютеров: анализ политики в области права». Таким образом было положено начало созданию единой схемы закона об уголовной ответственности за преступления в сфере использования компьютерной информации в целях установления юридического единства по данному вопросу в Европейских государствах. В основу закона взяли следующее определение: «Компьютерным преступлением считается всякое незаконное, неэтичное и несанкционированное поведение, касающееся автоматизированных процессоров и трансмиссии данных»[1]. Некоторые авторы считают, что в настоящее время правоохранительные органы США испытывают определенные сложности в ситуациях, когда речь ведется о привлечении к уголовной ответственности лиц, совершивших преступления в сфере компьютерной информации будучи не находясь на территории США, даже несмотря на столь детальное описание вопросов уголовной ответственности за данные деяния[2]. Мы считаем, что этого можно было бы избежать при условии включения американским законодателем в законодательные акты, регламентирующие ответственность за компьютерные преступления, квалифицирующих признаков — совершения преступлений с использованием специфичных особенностей компьютерных систем и осуществления несанкционированного доступа при помощи компьютеров, находящихся территориально не в США, в том числе и

[1]Громов Е.В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше) // Вестник ТГПУ. – 2006. – №11 (62). – С. 30–35.

[2]RobertJ. Sciglimpaglia. Computer Hacking: A Global Offense, 3 Pace Y.B. Int'l L.199, 231 (1991); Keith Nicholson. International computer crime: a global village under siege // New England International & Comparative Law Annual. – 1997. – № 2. New England School of Law, Boston, Massachusetts. [Электронный ресурс]. – URL: http://www.nesl.edu /annual/vol2/computer.htm (дата обращения: 10.02.2011)

прокси–серверов[1]. В ФРГ в 1986 г. был принят закон о борьбе с экономической преступностью, дополнивший законодательство нормами о преступлениях в сфере компьютерной безопасности, в 1994 году — Федеральный закон «О защите информации». В параграфах 43, 44 данного акта определена уголовная ответственность за «неправомерное получение информации для себя или иного лица, если она была защищена от несанкционированного доступа», в виде лишения свободы на срок от 1 до 2 лет или денежного штрафа до 50 тысяч марок. В наши дни законодательство Германии включает в себя различные нормы, предусматривающих уголовную ответственность, за различные преступления, совершаемые с с помощью различных девайсов на внутрисетевом уровне. Например, «компьютерное мошенничество» (ст. 263a), «Подделка используемых данных» (ст. 269), «Обман в официальных научных работах в совокупности с обработкой данных» (ст. 270), «Замена данных» (ст. 303a), «Компьютерный саботаж» (ст. 303b), «Информационный шпионаж» (ст. 202a) и др. Мы считаем, что необходимо учитывать в перспективе положительный опыт немецких коллег. Великобританские законотворцы же, впервые, приняли Computer Misuse Act — Закон о неправомерном использовании компьютерных технологий, принятый в 1990 году. В данном законе были выделены три вида преступлений: 1) несанкционированный доступ к компьютерной информации; 2) несанкционированный доступ к компьютерным данным с намерением совершить или способствовать совершению дальнейших преступлений; 3) несанкционированное изменение компьютерных данных[2]. Мы считаем, эта мера в полной мере позволила встать британским правоохранительным органам на путь борьбы с компьютерной преступностью, так как до этого имела место проблема, когда,

[1]Определение Прокси–сервер. [Электронный ресурс]. – URL: http://ru.wikipedia.org/wiki/Прокси–сервер (дата обращения: 10.02.2011)

[2]Computer Misuse Act Law of Great Britain [Электронный ресурс]. – URL: http://www.legislation.gov.uk/ukpga/1990/18/contents (дата обращения: 10.02.2011)

например, не удалось добиться в суде обвинительного заключения по делу Стивена Гоулда и Роберта Шифрина, которые в 1984 году получили несанкционированный доступ к принадлежащему компании British Telecom сервису Prestel. Обвинение против них было выдвинуто в соответствии с Законом о подлоге и подделках 1981 года. В апелляционном суде обвиняемые были оправданы, и оправдательный приговор был утвержден палатой лордов [1]. Максимальный срок тюремного заключения, предусмотренный законом за эти преступления, составлял соответственно шесть месяцев, пять лет и пять лет.

В законах зарубежных стран отсутствует специальная уголовная ответственность за нарушение правил эксплуатации компьютерных систем и распространение вирусов с негативными эффектами. Подобные действия рассматриваются как разновидность диверсий, наносящих значительный ущерб компьютерной информации посредством разрушительных воздействий в отношении материальных носителей и зафиксированных на них данных[2]. Способы совершения действий, направленных на нарушение работоспособности компьютерных систем, могут быть как самыми простыми, например, физическое уничтожение частей компьютерных систем и сетей, так и более сложными, такими как воздействие на программное обеспечение, использующее как физическое разрушение частей информационных систем, так и деструктивные программы. Так, о первом случае заражения китайских компьютеров программными вирусами сообщалось в начале 1989 года, когда компьютеры алюминиевого завода Синань оказались поражены вирусом неизвестного преступника, названным «хлореллой» (либо «пятнами»). К концу 1989 года была проведена профилактика более чем 13600 компьютеров, в результате чего пятая часть

[1]ЭммД. Киберпреступность и закон [Электронный ресурс]. – URL: http:// cybercrime.zp.ua/ viewtopic.php?f=3&t=4776 (дата обращения: 10.02.2011).
[2]Смирнова Т.Г. Уголовно–правовая борьба с преступлениями в сфере компьютерной информации: дис. … канд. юрид. наук. – М., 1999. – С. 230.

оказалась зараженной этим вирусом. В Канаде в 1985 году был принят «Закон о поправках к Уголовному кодексу», в который добавили условности для лица, которое «1) изменяет или уничтожает данные, 2) уничтожает значимость данных, делая их бесполезными, в) препятствует их законному использованию или лишает собственника доступа к ним».

Одной из самых активных стран, ведущих борьбу с компьютерными преступлениями являются Нидерланды. В Нидерландах был создан Консультативный комитет по компьютерным преступлениям, который сформировал определенные предложения по внесению изменений в Уголовный кодекс и Уголовно–процессуальный кодекс Нидерландов. Консультативный комитет не дал определения компьютерных преступлений, но дифференцировал их. При этом полицейская разведка Нидерландов, которая занимается регистрацией всех случаев компьютерных преступлений, использует в своей работе следующее определение компьютерного преступления: это потенциально вредное поведение, связанное с компьютерными устройствами и предполагающее хранение, изъятие и распоряжение данными. Они различают преступления, в которых компьютер является объектом преступления, и те, 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 технических средств поддержки;

– компьютерное мошенничество;

– компьютерный террор (совершение преступлений с целью повреждения компьютерных систем): использование незаконного доступа; использование вредоносных программ, типа компьютерных вирусов; 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 рекомендациям Совета Европы, но отличается простотой и понятной формулировкой. Причина же единого определения компьютерных преступлений в Нидерландах заключается в том, что, по мнению голландских теоретиков, существует множество трудностей при формулировании определения, которое стало бы и ёмким и точным и достаточно специфичным в плане терминологии. Применяется два понятия компьютерного преступления – в узком и широком смысле. В узком смысле – это совершение преступления, которое возможно выполнить только с помощью использования компьютерных систем.

Нидерланды, тем временем, в 1993 г. приняли Закон о компьютерных преступлениях, который дополнил УК Голландии[1]:

- 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), 350b);
- компьютерный шпионаж (ст. 273 (2)).

В ряд статей УК Голландии, предусматривающих ответственность за совершение традиционных преступлений (вымогательство (ст. 317, 318), запись (копирование, прослушивание) 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

[1]Уголовный кодекс Голландии / Науч. ред. д.ю.н., проф. Б.В. Волженкин, пер. с англ. И.В. Мироновой. – СПб, 2000.

данные составы преступлений, в соответствующих случаях, и для борьбы с компьютерными преступлениями.

Как мы видим, 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. В модельном Уголовном кодексе Союза Независимых Государств компьютерные преступления помещены в XII раздел «Преступления против информационной безопасности», состоящей из одной главы с таким же названием и семи статей – ст. 286– 292 УК СНГ. На первый взгляд УК РФ и СНГ очень похожи, но есть и различия. В УК СНГ выделено больше статьей за счёт включения фактора субъективной стороны. Например, несанкционированный доступ к компьютерной информации, повлекший неосторожные последствия (ст. 286 УК СНГ, аналог ст. 272 УК РФ), дополняется отдельно предусмотренной ответственностью за изменение компьютерной информации, компьютерный саботаж. УК СНГ в лучшую сторону ушёл от УК РФ. В УК СНГ даются определения ряда понятий, например, модификация компьютерной информации, компьютерный саботаж, неправомерное завладение компьютерной информацией. К сожалению, санкции, предусмотренные в нормах УК СНГ, также нуждаются в доработках, так как имеются несоответствия между общественной опасностью деяний и санкциями. Отдельно в УК СНГ (ст. 290) предусмотрена уголовная ответственность за изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной информации, к компьютерной системе или их сети, что также выгодно выделяет СНГ на фоне кодекса РФ. В ст. 287 УК СНГ закладываются основы для более чёткой дифференциации компьютерных и иных смежных составов преступлений, что также хорошо влияет на квалификацию. Отдельно стоит обратить внимание на системное изложение

квалифицирующих признаков компьютерных преступлений. Законотворцы в РФ чаще всего используют именно системный метод для квалифицирующих признаков, однако в главе 28 законодатель ограничился простым перечислением таких признаков. Санкции, утвержденные в УК СНГ за компьютерные преступления, не строже наказаний за преступления средней тяжести, но, неправомерное завладение информацией, совершенное при квалифицирующих обстоятельствах (сопряженное с насилием, совершенное с целью получения особо важной информации), наказывается как тяжкое преступление (ч. 3 ст. 289 УК СНГ). За особо квалифицированный вид такого преступления (совершение преступления организованной группой, сопряженное с причинением тяжкого вреда здоровью или по неосторожности смерти либо иных тяжких последствий) – наказание назначается как за особо тяжкое преступление (ч. 4 ст. 289 УК СНГ).[1] Это обосновывается тем, что помимо причинения вреда сопряженного с компьютерной информацией, причиняется также вред здоровью и имуществу, нарушается целостное функционирование общественных отношений. Естественно, что совершение преступления группой лиц по предварительному сговору или организованной группой, автоматически повышается характер и степень общественной опасности преступления. Тем не менее нам видится спорным введение дополнительно квалифицирующего признака – совершение преступления с целью получения особо важной информации. Важно понимать, что ценная информация имеет место быть, однако данная категория является оценочной и зависит от субъективного восприятия причинённого вреда каждым лицом. С таким квалифицирующим признаком обязательно наличие ориентиров для законоприменителя. Рассмотрим также Польшу, в УК которой имеется глава 33 «Преступления против охраны информации», содержащая 6 статей, объектом которых являются

[1]Модельный уголовный кодекс для государств СНГ // Панфилов Е.И. Попов А.С. Компьютерные преступления. – СПб., 1998.

общественные отношения касающиеся информации, в целом. [1]Общественные отношения в сфере компьютерной информации являют собой лишь часть объекта. Для нас важны только 2 статьи – ст. 267 и 268 УК Польши. В ст. 267 УК устанавливается уголовная ответственность за неправомерный доступ к информации, в том числе путем повреждения средств, обеспечивающих безопасность информации. В ст. 268 УК Польши предусматривается уголовная ответственность лиц, не имеющих на то уполномочия уничтожения, повреждения удаления или изменение записи на компьютерном носителе информации, важной для обороны государства, безопасности узлов связи, стабильного функционирования государственного аппарата. При этом такое преступления может квалифицироваться как посягательство на государственную тайну. Статьи 278, 287 УК Польши, расположенные в главе 35 «Преступления против имущества», также можно отнести к «компьютерным» составам преступлений. Нормы в данном случае устанавливают следующую ответственность: – приобретение без ведома управомоченного лица чужой компьютерной программы с целью извлечения имущественной выгоды (ст. 278); – воздействие неуправомоченным на то лицом на автоматизированное изменение, кражу или изъятие информации, или изменение, удаление, введение иной информации на материальный носитель с целью получения материальной выгоды или причинения вреда другому лицу (ст. 287). Интересный факт, что если вред причинён родственнику преступника, то возбудится преследование может только по заявлению потерпевшей стороны. Польские законодатели разделили преступления в сфере компьютерной информации на 2 группы и так их и расположили в УК Польши, дифференцируя по направленности деяния субъекта либо на получение информации, либо на получение материальной выгоды. Нам это кажется довольно таки спорным решением, ведь и в первом

[1]Уголовный кодекс Республики Польша / Отв. ред. Э.А. Саркисова, А.И. Лукашов. Пер. с польск. Д.А. Бариловича. – Минск, 1998.

и во втором случаях субъект получает доступ к определенному объему информации; и в первом, и во втором случаях лицо может получить личную выгоду, например через вознаграждение от третьего лица. 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 Компьютерные преступления в сфере экономики, например, компьютерное мошенничество в УК ФРГ.

2 Компьютерные преступления против прав и свобод граждан и организаций, нарушающие неприкосновенность частной жизни, такие как, неправомерные использование информации, находящейся на различных носителях, разглашение сведений, имеющих частную, коммерческую тайну.

3 Компьютерные преступления против интересов государства и общества в целом, такие как влияние на обороноспособность страны, подделка результатов выборов и т.д.

2 КРИМИНОЛОГИЧЕСКИЙ АСПЕКТ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

2.1 Криминологическая характеристика личности преступника

Обратим наше внимание на то, что преступления в сфере компьютерной информации, преимущественно являются латентными. Чаще всего для установления индивида, совершившего преступление данной области, и доказывания факта его причастности кроме следственных действий требуется большое количество оперативно–розыскных мероприятий, осуществляемых правоохранительными органами. При этом в п. 24 ст. 5 и ч. 1 ст. 40 УПК РФ к числу органов дознания среди прочих отнесены органы внутренних дел РФ и входящие в их состав подразделения, а также иные органы исполнительной власти, наделенные в соответствии с законодательством полномочиями по ведению оперативно–розыскной деятельности. Кроме того, положения ст. 11 федерального закона «Об оперативно–розыскной деятельности» от 12.10.1995 г. № 144–ФЗ указывают на возможность использования итогов такой деятельности в качестве не только базы доказательств, но и повода для возбуждения уголовного дела. Таким образом мы можем сделать вывод, что сведения о портрете преступника являются крайне важной частью оперативно-розыскной и криминалистической характеристик различного рода преступлений. Нельзя исключать и преступления в сфере компьютерной информации. Внимательно изучим содержание и природу свойств личности, являющихся социально значимыми, а также обратим внимание на условия, влияющие с внешней стороны на поведение лиц, потенциально являющихся преступниками.

Что такое личность преступника? Можно, например, описать это как совокупность значительных в социальной сфере свойств, а также внешних условий, влияющих на индивида. Мы считаем, что необходимо тщательно анализировать портрет преступника, совершающего преступления,

предусмотренные в гл. 28 УК РФ. Нужно определить главные признаки, которые определяют противоправное поведение лица и его преступный выбор, в целом. Типовая классификация лиц, совершающих правонарушения в сфере компьютерной информации, рассматривалась многими известными учеными. Например, учёный В.В. Крылов выделяет четыре распространённых вида преступников:

1 Простые нарушители правил эксплуатации компьютерных систем.

2 «Белые воротнички» – респектабельные преступники.

3 Профессиональные компьютерные шпионы.

4 Хакеры, или «одержимые программисты»[1].

При этом в трудах иностранных учёных мы увидим иную классификацию. К примеру, Д. Паркер определяет семь видов индивидов, связанных со сферой компьютерной информации:

1 «Pranksters» – лиц, совершающие преступления на развлекательной почве, без преступного умысла.

2 «Hucksters» – лица с корыстными преступными намерениями.

3 «Malicioushackers» – лица с корыстным умыслом на причинение вреда.

4 «Personalproblemsolvers» – категория лиц, решающих личные проблемы.

5 «Careercriminals» – профессионалы в преступной сфере.

6 «Extremeadvocates» – лица, совершающие преступления ради риска.

7 «Irrationalpeople» – лица с ярко выраженным иррациональным мышлением[2].

Рассматривая данные категории с точки зрения криминологического портрета преступника мы должны учитывать различные факторы: социально-демографические, психологические, биологические, нравственные, социально–ролевые, криминологические и уголовно-правовые. В наше время

[1] Крылов В.В. Информационные компьютерные преступления. – М., 1997..– С. 64.
[2] Parker D. Fighting computer crime. – N. Y., 1998. – P. 248.

очевидно преобладание общения и социальной адаптации в социальных сетях, поэтому люди зачастую пытаются самореализоваться на просторах этих сетей. Естественно, реализуют свои амбиции они, в том числе, незаконными путями. В ситуации, когда человек не является визуально привлекательным по оценкам своего окружения и имеющий в связи с этим определенные проблемы психологического характера с самооценкой и взаимодействием с другими людьми, постоянно сталкивающийся с агрессивным отношением со стороны окружающих и непониманием, будет пытаться проявить себя на просторах интернета и будет пытаться добиться определенных успехов на этом поприще. Таким образом он и будет самоутверждаться, совершая различного рода преступления, используя свои навыки в компьютерной и сетевой сферах. Это позволяет таким индивидам чувствовать себя лучше интеллектуально, увеличивает их собственную значимость и самомнение. Для примера рассмотрим уголовное дело, имевшее место в Иркутской области. Гражданин Н., был трудоустроен в аптеке г. Ангарска программистом, после своего увольнения он принял решение отомстить обидчикам и, получив несанкционированный доступ к внутренней сети организации, воспользовался конфиденциальной информацией предприятия и уничтожил изнутри целостность сети. После этого гражданин Н был пойман на попытке продажи конфиденциальных сведений конкурентам вышеуказанной организации. По итогам его действий ООО «Аптека» потерпела ущерб на сумму 54 814 р. 90 коп[1]. Потенциальный преступник может как тщательно изучать и прорабатывать план действий, так и действовать на эмоциях, импульсивно. Вероятно, что некоторые люди становятся киберпреступниками, противопоставляя себя обществу и социальным отношениям в нём. Конечно есть преступники, которые не поддаются эмоциям, действуют хладнокровно, долго и тщательно планируя

[1]Уголовное дело № 1–158 от 2003 г. // Арх. Ангарского районного суда Иркутской области. [Электронный ресурс]. – URL: https://rospravosudie.com/act-507626283/

каждый шаг преступления, выжидая удобного момента, учитывая все варианты развития событий, способы скрыть совершение преступления и только потом совершать непосредственно преступные действия. Часто бывает так, что киберпреступления связаны с личными интересом или желанием обогатиться. Но при этом корысть у таких преступников может быть гипертрофированной, характеризуясь стремлениями к так называемой «лёгкой наживе». Большая часть преступников в сфере компьютерной информации в РФ это молодёжь, а они зачастую характеризуются сильно развитыми потребностями получения статуса в социуме и проблемы с получением такого статуса ведут к агрессивному поведению. Исследования криминологов показывают, что ценностные приоритеты у таких людей сконцентрированы на своей индивидуальности или группе единомышленников. В вышеуказанных примерах основное желание — это улучшение своего материального положения, окружение себя зоной комфорта, активная реализация своего внутреннего эго или эго группировки[1]. Важно понимать, что таких преступников также воодушевляет свобода их действий на просторах сети интернет и лёгкий доступ к высоким технологиям, что позволяет им без проблем получать большую часть информации и объединяться в сильные группировки и объединения, даже на международном уровне. Естественно, что у таких преступников деформировано нравственное развитие и имеет сильное влияние правовой нигилизм. Учёные А.Р. Ратинов и И.И. Карпец ещё 30 лет назад сделали вывод о том, что сама по себе нестабильность правосознания может привести к выбору противозаконного поведения[2]. Конечно, в наше время имеет место и обратная тенденция. Например, различные политические группы хакеров

[1]Криминология : учебник / под ред. А.И. Долговой. – М., 1997. – С. 292.
[2]Карпец И.И., Ратинов А.Р. Правосознание как элемент правовой культуры // Правовая культура и вопросы правового воспитания: сборник научных трудов. – М., 1974. – С. 55 – 57.

совершают явные незаконные деяния, мотивируя свою деятельность высшими идеалами.

В.Н. Кудрявцев предлагает наиболее полноценную по своему содержанию структуру личности правонарушителя: социально–демографическая и правовая характеристика, которая охватывает пол, возраст, образование, семейное положение, профессию, социальное положение, характер совершенного правонарушения и прежнюю судимость; нравственно–психологическая характеристика, включающая социальную и антисоциальную направленность личности, систему ценностных ориентаций, основные потребности и интересы, отношение к нормам морали, уровень правосознания; основные психические и психофизиологические особенности; социальное поведение, заключающееся в отношениях в производственном коллективе, семье, учебном заведении, ближайшем окружении, а также в связях с антиобщественными элементами и в самооценке[1].

Такая структура личности в процессе изучения лиц, совершивших преступления в сфере компьютерной информации, на наш взгляд, является предпочтительной. Компьютерная информация обладает целым комплексом отличительных свойств и признаков. В связи с этим необходимо сразу же обратить внимание на тот факт, что лицо, совершающее преступление в сфере компьютерной информации, обладает определенной совокупностью знаний, умений и навыков обращения с компьютером, программным обеспечением, компьютерными системами и сетями. С учетом данного тезиса важно подметить то, что навыки в общении с компьютерной техникой может в настоящее время приобрести практически каждый. Однако в зависимости от типа компьютерной информации (открытой, ограниченной либо конфиденциальной) доступ к ней может быть предоставлен различному по широте охвата кругу субъектов. Если доступ к открытой информации

[1] Кудрявцев В.Н. Причины правонарушений. – М., 1976. – С. 35.

рассчитан на любого пользователя, то ограниченную либо конфиденциальную информация может получить только тот, кто знает соответствующие пароли, шифры, криптографические ключи, обеспечивающие защиту самой информации. Наличие у индивида специальных знаний и навыков уже предполагает возможность совершения им действий, направленных на преодоление защитных механизмов на пути к получению информации. В то же время, лицо, совершающее компьютерное преступление, обладает специальными, глубокими по уровню знаниями, прочными навыками, позволяющими ему искать пути вскрытия ограниченной или конфиденциальной информации, раскрывая секреты ее защиты. Исследование показывает, что представление характерологических особенностей личности преступника, совершающего противоправные посягательства в сфере компьютерной информации, целесообразно осуществить через типологию соответствующих лиц, применительно к тому или иному виду преступного деяния, определенного ст. 272–274 Уголовного кодекса РФ. Оценивая удельный вес этих преступлений в структуре противоправных деяний в сфере компьютерной информации, необходимо указать, что доля неправомерного до –ступа к компьютерной информации составляет три четверти от всех деяний данного вида. Доля преступлений, заключающихся в распространении вредоносных программ для электронно–вычислительной техники, составляет 22% от общей численности компьютерных преступлений. Распространение носителей, содержащих вредные программы, совершается преимущественно при реализации пиратского программного обеспечения. Остальные 3% приходится на долю нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети. Предпосылками такого факта являются следующие объективные и субъективные обстоятельства: широкое развитие сферы высоких технологий и значительная распространенность компьютерной техники среди населения; наличие специальностей в высших образовательных учреждениях, по

которым ведется подготовка обучающихся с привитием им профессиональных знаний, умений и навыков программирования; влияние семейного и внесемейного окружения на процесс становления личности правонарушителя в сфере компьютерной информации; фактическая безнаказанность лиц, совершивших компьютерные преступления, из–за высокой латентности данных противоправных деяний, отсутствие надлежащей подготовки сотрудников правоохранительных органов, осуществляющих производство по уголовным делам данной категории преступлений. В литературе выделяются различные группы компьютерных преступников. Наиболее многочисленными среди них являются так называемые «хакеры» и «кракеры». Фактически и те, и другие занимаются поиском уязвимых мест в вычислительных системах и осуществлением атак на данные системы[1]. Однако основная задача хакера состоит в том, чтобы, исследуя вычислительную систему, обнаружить слабые места в ее системе безопасности и информировать пользователей и разработчиков системы с целью последующего устранения найденных недостатков, внести предложения по ее усовершенствованию. Вообще же, слово «хакер», согласно специальным источникам, обозначает талантливого законопослушного программиста[2]. В какой–то степени с этим можно согласиться, так как в любом деле высоко оценивается профессионализм. Действительно, тот же системный администратор (даже если в системе всего два–три компьютера) обязан детально изучить операционные системы, особенности языков программирования и тонкости прикладных пакетов. Тем самым он, прежде всего, выявляет слабые и сильные стороны компьютерных систем и использует полученные знания. Эти знания позволяют не только «защищать» системы от взлома, но и наоборот – «ломать» их. Таким образом, термин «хакер» совмещает в себе, по крайней мере, два значения: с

[1]Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на INTERNET. – М., 2000. – С. 11.
[2]Айков Д., Сейгер К., Фонстрох У. Компьютерные преступления. – М., 1999. – С.18.

одной стороны, это взломщик, а с другой – асс, мастер. С точки зрения психофизиологических характеристик – это, как правило, творческая личность, способная идти на технический вызов, риск. В настоящее время крупные компании стремятся привлечь наиболее опытных хакеров на работу с целью создания систем защиты информации и компьютерных систем. Кракер же, осуществляя взлом компьютерной системы, действует с целью получения несанкционированного доступа к чужой информации. Мотивы этого могут быть различными: от озорства до промышленного шпионажа. Среди субъектов неправомерного доступа к компьютерной информации в зависимости от вида их деятельности выделяют еще: фрикеров – людей, специализирующихся на использовании телефонных систем с целью уклонения от оплаты телекоммуникационных услуг; кардеров, оплачивающих свои расходы с чужих кредитных карточек; коллекционеров, использующих компьютерные программные продукты, перехватывающих различные пароли, а также коды телефонного вызова и номера телефонных компаний, имеющих выход к компьютерным сетям общего использования, например, Интернет; киберворонов – злоумышленников, которые специализируются на несанкционированном проникновении в компьютерные системы финансовых, банковских расчетов. Обычно они используют компьютерные технологии для получения номеров кредитных карточек и другой ценной информации с целью наживы. Нередко полученную информацию они продают другим лицам; компьютерных пиратов, специализирующихся на незаконном взломе систем защиты лицензионных компьютерных программных продуктов, которые потом распространяют за деньги по ценам, которые значительно ниже цен законных изготовителей. Анализ публикаций отечественных и зарубежных авторов, касающихся проблемы характеристики личности компьютерного преступника свидетельствует о том, что криминолого–психологический портрет того же хакера, как правило, весьма абстрактен. В частности, указывается, что он

рано знакомится с компьютером, компьютерная система и соответствующие технологии для него – смысл жизни, он социальный отщепенец, не обращающий внимания на окружающий мир, часто закомплексован, для большинства хакерство является первым настоящим достижением в реализации своих творческих начал и т. д[1]. Исследование показывает, что возрастной диапазон компьютерных правонарушителей колеблется в пределах от 14 до 45 лет. 54% преступников – это лица в возрасте от 18 до 25 лет; 13% – от 26 до 40 лет. Таким образом, свыше 75% выявленных преступников составляет молодежь и есть основания для опровержения многих устоявшихся в обществе стереотипах о возрастных особенностях личности хакера. Преступления в сфере компьютерной информации мужчинами совершаются в 5 раз чаще, нежели лицами женского пола. Большинство субъектов таких преступлений имеют высшее или неоконченное высшее техническое образование (54%), а также другое высшее либо неоконченное высшее образование (19%). Однако в последние несколько лет наметилась отчетливая тенденция к увеличению доли женщин в структуре компьютерных преступников. Во многом это обусловлено профессиональной ориентацией некоторых специальностей и должностей, оборудованных автоматизированными компьютерными рабочими местами, которые чаще занимают женщины. По нашим данным, полученным в ходе проведения соответствующего исследования, 52% правонарушителей имели специальную подготовку в области автоматизированной компьютерной обработки информации; 97% являлись сотрудниками государственных учреждений и организаций, которые использовали компьютерные системы и информационные технологии в своей повседневной деятельности, причем 30% из них имели непосредственное отношение к эксплуатации средств компьютерной техники. На сегодняшний день имеют место факты совершения компьютерных преступлений и сотрудниками, занимающими в

[1]SurgeonB. Хакеры //Компьютерра. – 1996. – № 43. – С. 22.

организации ответственные посты. Так, каждое четвертое из компьютерных преступлений совершаются руководителями организаций.

Современные руководители, как правило, специалисты высокого уровня, владеют достаточной компьютерной подготовкой и профессиональными знаниями, имеют доступ к информации широкого круга и могут отдавать распоряжения, хотя непосредственно за работу компьютерной системы не отве –чают. Следует иметь в виду, что в совершение компьютерных преступлений в нынешний период времени втянут широкий круг лиц, среди которых есть как дилетанты, так и высококвалифицированные специалисты. При этом все они имеют разный социальный статус и уровень образования, что уже позволяет всех их классифицировать на две большие группы – это как лица, состоящие с потерпевшим в трудовых или иных служебных отношениях, так и лица, не связанные с потерпевшим соответствующими деловыми контактами. К первой группе следует отнести сотрудников, которые злоупотребляют своим положением. Ими являются клерки из различных сфер деятельности, сотрудники служб по контролю безопасности организации, работники контроля, лица из организационной группы, инженерно–технический персонал.

По результатам социального исследования, доля инженеров, программистов, операторов ЭВМ и других различных сотрудников организаций, которые совершают деяния по несанкционированному доступу к информационным системам, составила 42%. В 20% случаев это иной спец. персонал и ещё 8% составляют обычные работники. В целом, угрозу составляют и сотрудники других организаций, которые также работают в информационном сервисном обслуживании. Отдельно выделим группу, в которую входят лица с высоким уровнем знаний в сфере компьютерных технологий. Эти лица, чаще всего, имеют корыстный умысел. К ним также отнесём специалистов, работающих в данной сфере и совершающих проникновение в чужие системы как будто преодолевая собственные

возможности. Часть из них со временем уже привыкают к такой деятельности и понимают, что для них это становится обыденностью. Практически каждый второй из числа лиц, относящихся к той или иной группе, – это все же дилетант, не обладающий глубокими познаниями в сфере компьютерных технологий, недостаточно уверенно владеющий навыками обращения с электронно– вычислительной техникой и компьютерными сетями. Специалисты в области компьютерной безопасности считают, что наиболее многочисленны, но наименее опасны именно хакеры–дилетанты. На их долю приходится до 80% всех компьютерных атак. Но этих людей интересует не некая цель, а сам процесс атаки. Они испытывают удовольствие от преодоления систем защиты. Чаще всего их действия удается легко пресечь, поскольку хакеры–любители предпочитают не рисковать и не вступать в конфликт с законом[1]. Большинство из лиц такого рода приобщились к компьютеру еще в школе. Знание компьютерных технологий ограничивается одним–двумя языками программирования. Наряду с хорошим уровнем технического образования или самообразования, общая образованность явно недостаточна (в текстах переписки «невооруженным» глазом виден «корявый» стиль и масса грамматических ошибок). Установка на преступное поведение среди дилетантов формируется стихийно, в основном под влиянием случайной цепи удачных и неудачных «взломов» защитных программ на других компьютерах. Закрепление такой установки происходит под влиянием «авторитетного мнения старших товарищей», высказанное ими после общения с «новичком» в сетевых «кулуарах». С повышением уровня профессионализма, связанного с фактическим получением высшего технического образования, дилетанты приобретают более глубокие, систематизированные знания в области компьютерных технологий, языков

[1] Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. – М., 2002. – С. 131.

программирования, прочные умения и навыки работы с сетями, программным обеспечением и т. д. Они уже являются специалистами. Психологически люди данной группы более уравновешенны, имеют отчетливо сформированную систему взглядов и ценностей, однако высокий уровень амбициозности им все же пока не присущ [3, с. 55–56]. В большинстве случаев, преступная «карьера» такого круга лиц трансформируется из «карьеры» любителя, либо складывается в результате вхождения в криминальную среду, например, при содействии и протекции друзей–«профессионалов». Основной сферой преступной деятельности «специалистов» являются сетевой взлом, действия в операциях по получению конфиденциальной информации, обладающей мощными системами защиты данных, промышленный и интеллектуальный шпионаж. Наиболее опасную группу составляют все же профессиональные компьютерные преступники. Так, на долю этих лиц приходится порядка 80% всех преступлений, которые связаны с хищением материальных ценностей в особо крупных размерах с использованием компьютера. Лица этой группы характеризуются тем, что это высококвалифицированные специалисты с высшим юридическим, техническим или экономическим образованием. Они прекрасно разбираются в электронно–вычислительной технике, мастерски владеют программированием, их действия сопровождаются продуманной маскировкой поступков и сокрытием «следов» преступления. Знания этих людей в области компьютерных технологий обширны и глубоки: они владеют несколькими языками программирования, в совершенстве знают особенности аппаратной части современных компьютерных систем, имеют навыки профессиональной работы с несколькими компьютерными платформа ми, основными операционными системами и большинством пакетов прикладного программного обеспечения специализированного назначения, прекрасно информированы об основных системах электронных транзакций, системах сотовой связи, методах криптографии. Психологически

они уравновешенны, стойки к внешним воздействиям, крайне амбициозны, дальновидны, реально оценивают свои возможности, имеют связи с чиновниками из властных структур, которые нередко прибегают к их помощи для получения информации различного рода (в том числе и компрометирующей). Профессиональные компьютерные преступники работают в основном «для прикрытия» чаще всего руководителями подразделений информационных технологий в банках, иностранных компаниях, государственных учреждениях либо их заместителями, причем основная их деятельность связана с нелегальной и полулегальной деятельностью. Для подавляющего большинства лиц, совершающих преступления в сфере компьютерной информации, характерны корыстные мотивы (67% лиц). Однако наряду и с корыстью выделяются и иные виды мотивов, определяющих соответствующее преступное поведение. В частности, мотивами рассматриваемой категории деяний являются политические мотивы (17%), так как глобальные компьютерные системы являются эффективным инструментом политических акций, мотивы мести (4%), озорство и хулиганские побуждения (5%), а также исследовательские интересы (7%), направленные для получения информации для собственных нужд или для осуществления соответствующей деятельности из–за мотивов самоутверждения. Исследование мотивообразующих факторов, детерминирующих преступное поведение компьютерных преступников, свидетельствует о том, что все они могут быть сведены в три основные группы применительно к лицам, совершающим данные противоправные посягательства: лица с ярко выраженным корыстным мотивом; лица с отличительной особенностью устойчивого сочетания профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности; лица, страдающие новым видом психических заболеваний – информационными болезнями или компьютерными маниями. Если удельный вес первой группы лиц, чье

поведение обусловлено жаждой наживы, составляет около 72%, то на долю второй и третьей групп приходится 24% и 4% соответственно. Необходимо отметить, что правоохранительные органы, изучая природу рассматриваемых преступлений, осуществляют борьбу со злоумышленниками их же оружием – через Интернет. Преступность в сфере использования компьютерных технологий не признает границ, поэтому традиционные приемы обнаружения и борьбы с преступлениями данного вида пока недостаточно эффективны. В этом контексте актуальными являются комплексное исследование проблемы компьютерных преступлений, научный поиск эффективных путей повышения уровня информационной безопасности посредством совершенствования организационно–правовой защиты информации в компьютерных системах, решения проблем предупреждения компьютерных преступлений, подготовки специалистов–юристов в этой сфере, осуществляющих практику раскрытия и расследования соответствующих преступлений.

Экспертами криминалистами МВД в 1998 г. Был проведен анализ лиц, занимающихся определенной преступной деятельностью с использованием компьютерных устройств с целью их классификации[1]. Мы можем с уверенностью сказать, что общая криминологическая характеристика преступника с тех времён сильно изменилась и по большей части разнится с ныне существующей. Это связывают с различными факторами. К примеру, в последние 5 лет доступность различной компьютерной техники стала в разы выше, в этот список входят и компьютеры, и планшеты/смартфоны. Также практически повсеместно распространён беспроводной доступ по сетям Wi-Fi и 3G/4G, что существенно повышает мобильность преступлений и их локальное многообразие. В связи с этим, мы можем констатировать, что массовая глобализация и информатизация нашего общества привела к

[1]Ушаков С.И. Преступления в сфере обращения компьютерной информации (теория, законодательство, практика) : дис. … канд. юрид. наук. – Ростов н/Д., 2000. – С. 144.

понижению возраста киберпреступников. Это связывают как с общим информационно-культурным воспитанием, в том числе по причине информационной неграмотности внутри семьи, но также и с тем, что молодые преступники чувствуют себя защищёнными, ощущают свою безнаказанность, в силу возраста уголовной ответственности.[1] Необходимо тщательно изучать свойства индивидуальности лиц, совершающих киберпреступления для того, чтобы сформировать работающую базу доказательств по уголовным делам в этой сфере. Это даст возможность следователям (суду) в процессе производства по уголовному делу выявлять обстоятельства, способствовавшие совершению преступления, а также сотрудникам оперативных аппаратов в рамках повседневной деятельности определять основные направления поиска и предполагаемые источники оперативно значимой информации, необходимой для решения стоящих перед ними задач.

2.2 Факторы, способствующие совершению преступлений в сфере компьютерной информации

Проблематика понимания причин определенной преступности является одной из важнейших в криминологии[2]. Причинный комплекс преступности включает ее условия и, собственно, причины, которые в совокупности составляют факторы преступности. Причины — это социально–психологические детерминанты, которые непосредственно порождают, воспроизводят преступность и преступления как свое закономерное следствие; условия — это такие социальные явления, которые сами не порождают преступность и преступления, а способствуют, облегчают,

[1]Ходякова Н.В. Личностный подход к формированию информационной культуры выпускников вузов : дис. … канд. юрид. наук. – Волгоград, 1996. – С. 63.
[2]Криминология / под ред. В. Н. Бурлакова, Н. М. Кропачева. – СПб, 2004. – С. 85.

интенсифицируют формирование и действие причины[1]. А.И. Долговой, считает, что изменения в социуме, касательно непосредственно компьютерных технологий характеризуются следующими обстоятельствами:

1 Всеобъемлющее и повсеместное внедрение инновационных технологий привело к повышению уровня технологий у преступников.

2 Появление новых технологий совершения преступлений. В наше время для многих преступников стало проблематичным или почти невозможным совершать некоторые преступления без определенных рисков, если не использовать новейшие технологии. В связи с этим, например, получают всё большее распространение мошеннические преступления, связанные с банковскими карточками и безналичным оборотом денежных средств

3 Образование нового информационно-социального пространства, основанного на использовании сети Интернет, а также связанные с этим процессы с этим процессы развития социума внутри таких сетей, что приводит к появлению новых видов преступлений.

Обычно выделяют два вида причинного комплекса киберпреступности[2]. Первый тип – это причинный комплекс, в целом, без специфики компьютерных преступлений. Отличается он только тем, что преступники применяют компьютерные технологии. В связи с этим изменяются условия совершения преступлений, ее масштабы, последствия и формы. Второй тип уже определяет специальный комплекс причин. Он предполагает, что мотивация лица совершить преступление выстроена в связи с появлением новых технологий, позволяющих этому лицу эффективно применять их. Учёные В.А. Минаев и В.Д. Курушин определяют следующие причины компьютерной преступности:

1 Слабая защита и зависимость компьютерных систем друг от друга.

[1]Криминология : учебник / под ред. Н. Ф. Кузнецовой, В. В. Лунеева. 2–е изд., перераб. и доп. – М. :ВолтерсКлувер, 2005. – С. 167–168.
[2]Долгова, А. И. Криминология. М. : ИНФРА – М, 2002. – С. 684–685.

2 Несовершенство юридических, политических и социальных сфер, которые сильно отстают от уровня развития технологий

3 Актуальность проблемы для развитых и развивающихся стран. [1].

4 Отсутствие проработанной ответственности. Многие аспекты компьютерной преступности в большей степени являются следствием слабого обеспечения безопасности информации, чем результатом действий злоумышленников. Отсюда появляется необходимость расширения осведомленности общества об уязвимости компьютерных систем и необходимость осуществления действенных мер безопасности.

5 Классическое несовершенство уголовного законодательства, в котором либо отсутствуют соответствующие составы преступлений, либо имеются проблемы с толкованием уже существующих норм.

6 Отсутствие согласованности законов и взаимодействия между правоохранительными органами как на государственном, так и на международном уровнях.

7 Слабое развитие межгосударственных соглашений по процедурным вопросам, что самым серьезным образом влияет на нормальное функционирование органов правопорядка.

8 Правовой нигилизм и низкий уровень обслуживания в организациях, занимающихся тех.обслуживанием и сетями интернет.

9 Компьютерные технологии уходят далеко вперед международных и внутригосударственных стандартов.

10 Низкий уровень грамотности пользователей компьютерных технологий и сети интернет, как на государственном, так и на частном уровнях.

Т.П. Кесареева выделяет следующие группы причин киберпреступности:: экономические, правовые, политические, нравственно–психологические,

[1]Курушин, В. Д. Компьютерные преступления и информационная безопасность / В. Д. Курушин, В. А. Минаев. М. : Новый юрист, – 1998. – С. 18–21.

низкий уровень квалификации органов правозащиты в борьбе с новыми видами преступлений, самодетерминация преступников, слабый социальный контроль[1]. В.Ю. Максимовым проводил опрос в органах внутренних дел, который показал, что сотрудники чаще всего называют следующие причины преступности: различные экономические факторы назвали 87 % респондентов, социальные — 35 %, правовые — 30 %, политические — 10 %. Такие причины, конечно, одинаково влияют на большую часть социальных групп, хоть и не все из них совершают преступления. Несомненно, что крайне высокий уровень латентности киберпреступлений свидетельствует о безнаказанности преступников, что также работает как фактор повышения преступности. Низкая квалификация сотрудников органов внутренних дел, игнорирование общественной опасности и в целом пассивность в отношении киберпреступлений вызывает стойкое ощущение безнаказанности и уверенность в своих силах, что приводит к совершению новых преступлений.

Важно также понимать, что, иногда факторы для совершения преступлений создаёт потерпевшая сторона. Зачастую с компьютерными преступлениями таким фактором является неосторожность, неграмотность. Чаще всего, компьютерные программы не защищены от внешнего доступа, поэтому киберпреступники легко перехватывают информацию. В.А. Бессонов проводил исследование, согласно которому 16,6 % респондентов утверждают, что преступность в сфере компьютерных технологий может существовать и без фактора неосмотрительности потерпевших. При этом, у 82,3 % людей вызывает интерес информация на чужих компьютерах и присутствует желание изучить её[2]. Соответственно, мы можем также считать это часть причинного комплекса. Мы также не согласны с мнением автора о введении в криминологию термина «виктимность компьютера».

[1]Кесареева, Т. П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет :дис. ... канд. юрид. наук. – М., 2002. – С. 122.

[2]Бессонов, В. А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации :дис. ... канд. юрид. наук. – Н. Новгород, 2000. – С. 122.

Виктимность — это свойство, присущее только человеку как личности. В данном случае можно указать на виктимность владельца компьютера, но никак не на компьютер и информацию в нём. Сам компьютер следует определять только как предмет, интересный для преступников, либо как источник повышенной опасности, если говорить о нём со стороны преступников. Исследуя причины и условия совершения преступлений, предусмотренных ст. 272 Уголовного кодекса (УК) РФ, суды, в частности, отмечали превышение стоимости лицензионного программного обеспечения в десятки, а порой и в сотни раз над стоимостью контрафакта и соответственно высокий спрос населения именно на контрафакт. По ряду дел лица, привлекаемые к ответственности, признавались, что материалы для записи скачивали из сети Интернет. В приговоре Калининского районного суда г. Челябинска от 19 июля 2012 г. по делу № 1–483/2012[1] отмечается, что С., реализуя преступный умысел, направленный на незаконное использование, приобретение, хранение, перевозку контрафактных экземпляров программных продуктов в целях сбыта, действуя умышленно, с целью извлечения прибыли из корыстных побуждений при помощи персонального компьютера скачивал из сети Интернет заведомо контрафактные, то есть изготовленные нелегально экземпляры программных продуктов. Общий ущерб правообладателям программных продуктов AdobePhotoshop CS5 Extended, AutoCAD 2010, Windows 7 Ultimat составил 108 737 р. 72 к., в то время как в сети Интернет контрафактные экземпляры были размещены в свободном доступе неустановленными лицами. Однако следует отметить индивидуальность причин, детерминирующих преступное поведение для каждого субъекта. Центральным районным судом г. Челябинска в постановлении о прекращении уголовного дела от 14 сентября

[1] Уголовное дело №1–483/2012 от 19.07.2017 // Архив Калининского районного суда г. Челябинска

2009 г. по делу № 1–356/2010[1] было установлено следующее. И., являясь заместителем начальника отдела технического обслуживания ООО «А.», в связи со служебной необходимостью получил доступ к имени пользователя и паролю почтового сервера ООО «А.». Позднее, будучи уволенным в связи со сложившимися неприязненными отношениями с руководством фирмы, И. совершил неправомерный доступ к охраняемой законом компьютерной информации, подключившись к серверу ООО «А.» и удалив компьютерную информацию с сервера, что привело к уничтожению, блокированию, модификации информации. Данный пример наглядно показывает ненадлежащее отношение к вопросу информационной безопасности со стороны потерпевшего.

2.3 Меры по предупреждению преступлений в сфере компьютерной информации

К организационным мерам предупреждения преступлений в сфере компьютерной информации можно отнести следующую совокупность мероприятий:

– совершенствование научно–технических средств, тактических приемов и методов расследования неправомерного доступа к компьютерной информации;

– своевременное явление и пресечение как начавшихся преступлений, так и неправомерного доступа к компьютерной информации на стадии покушения или подготовки к нему;

– установление обстоятельств, способствовавших совершению каждого преступления, разработка и совершенствование методов и приемов выявления таких образов;

[1] Уголовное дело №1–356/2010 от 14.09.2009 // Арх. Центрального районного суда г. Челябинска

– создание подразделений в МВД, ФСБ и прокуратуре, специализирующихся на расследовании высокотехнологичных преступлений, в частности неправомерного доступа к компьютерной информации, а также экспертно – криминалистических подразделений, способных отвечать на все вопросы компьютерно–технических и компьютерно–информационных экспертиз;

– своевременная регистрация и надлежащий учет этих преступлений;

– переподготовка и повышение квалификации работников правоохранительных органов, расследующих неправомерный доступ к компьютерной информации;

– информационное обеспечение деятельности органов внутренних дел[1];

– разработка и внедрение политики безопасности компьютерной информации, включающий подбор, проверку и инструктаж персонала, участвующего во всех стадиях информационного процесса.

В настоящее время основными задачами отделов по борьбе с преступлениями в сфере высоких технологий (ОБПСВТ) являются:

1 Выявление преступлений в сфере компьютерной информации когда объектом преступного посягательства является ЭВМ, их системы м сети права собственника информации, в сфере телекоммуникаций ЭВМ их системы и сети являются орудием совершения преступления, а также посягательств на конституционные права граждан – неприкосновенность личной жизни, тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, совершенных путем неправомерного прослушивания сообщений и снятия информации с технических каналов связи.

2 Возбуждение уголовных дел и производство неотложных следственных действий, при необходимости пресечение указанных преступлений.

[1]Котухов М.М., Марков А.С. Законодательно–правовое и организационно–техническое обеспечение информационной безопасности автоматизированных систем / М.М. Котухов, А.С.Марков– СПб.: ВУС, 2004. – С. 190.

3 Выявление лиц, групп и сообществ, занимающихся противоправной деятельностью в данной области, документирование их преступной деятельности, проведение мероприятий по предупреждению таких преступлений.

4 Выполнение поручений следователей по расследованию указанных преступлений, производство оперативно – розыскных мероприятий, а также участие в расследовании в составе следственно – оперативных групп.

Аналогичные подразделения созданы и в других российских правоохранительных органах – Генеральной прокуратуре и Федеральной службе безопасности.

1 Аналитическую разведку совершенствование информационного – аналитического обеспечения деятельности подразделении криминальной милиции, изучение перспективных средств и методов поиска и сопоставительного анализа самой разнообразной, имеющей значение для борьбы с данным компьютерным преступлением информации от материалов средств массовой информации в электронных библиотеках сети Интернет до конкретных оперативных данных. Целью такого анализа является формирование новых знаний о способах совершения неправомерного доступа к компьютерной информации, способах его сокрытия, выявления фактов несанкционированного доступа о которых не поступило заявлений в правоохранительные органы и.т.п.

2 Компьютерную разведку – применение средств и методов организации гласного и негласного получения информации, хранимой и обрабатываемой компьютерными системами для получения сведений о готовящихся преступлениях. Деятельность по скрытому получению компьютерной информации может предусматривать как непосредственный доступ к интересующим информационным ресурсам, так и перехват электронных сообщений, передаваемых по компьютерным проводам и радиосетям.

3 Обеспечение информационной безопасности органов внутренних дел которое распространяется от защиты субъектов и интересов органов внутренних дел от недоброкачественной информации до защиты ведомственной информации ограниченного доступа, информационных технологий и средств их обеспечения. Информационная безопасность ОВД определяется надежностью систем ее обеспечения включая надежность аппаратных средств и программного обеспечения[1].

Международное сотрудничество при расследовании рассматриваемого преступления осуществляется в формах:

а) обмена информацией, в том числе:

– о готовящемся или совершенном неправомерном доступе к компьютерной информации и причастных к нему физических и юридических лицах;

– о формах и методах предупреждения, выявления, пресечения, раскрытия и расследования данного преступления;

– о способах его совершения;

– о национальном законодательстве и международных договорах, регулирующих вопросы предупреждения выявления пресечения, раскрытия и расследования как рассматриваемого преступления, так и других преступлений в сфере компьютерной информации.

б) исполнения запросов о провидении оперативно – розыскных мероприятий, а также процессуальных действий, в соответствии с международными договорами о правовой помощи.

в) планирования и проведения скоординированных мероприятий и операций по предупреждению, выявлению, пресечению, раскрытию и расследованию неправомерного доступа к компьютерной информации.

[1]Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М.: Изд–во Юрлитиформ, 2000.– С.495.

г) оказания содействия ив подготовке и повышении квалификации кадров, в том числе путем стажировки специалистов, организации конференций, семинаров, и учебных курсов.

д) создания информационных систем, обеспечивающих выполнение задач по предупреждению, выявлению, пресечению, раскрытию и расследованию данного преступления.

е) проведения совместных научных исследований по представляющим взаимный интерес проблемам борьбы с рассматриваемым преступлениями, а с другой стороны– увеличить объем информации, проходящей через государственные СМИ, направленной на повышение уровня правовой, информационной и компьютерной культуры общества.

Организационные мероприятия по предупреждению неправомерного доступа к компьютерной информации рассматриваются многими специалистами, занимающимися вопросами безопасности компьютерных систем как наиболее важные и эффективные. Это связано с тем что они являются фундаментом на котором строится вся система защиты компьютерной информации от неправомерного доступа.

Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно– технических средств защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти. Правительство Российской Федерации определяет порядок осуществления такого контроля. В организациях обрабатывающих государственную информацию с ограниченным доступом создается специальные службы обеспечивающие защиту такой информации[1].

Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите

[1]Борзенков Г.Н., Комиссаров В.С. Уголовное право Российской Федерации / Г.Н. Борзенков, В.С. Комисаров. – М.: Олимп, 1997. – С.56.

информации и запрещать или приостанавливать обработку информации, в случае невыполнения этих требований. Он также вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах. Соответствующие органы определяет Правительство Российской Федерации. Эти органы соблюдают условия конфиденциальности самой информации и результатов проверки. Субъектами, осуществляющими профилактику неправомерного доступа к компьютерной информации являются правоохранительные органы, поскольку профилактическая деятельность составляет обязательную составную часть правоохранительной деятельности: органы межведомственного контроля, отраслевые органы управления, международные органы и общественные организации, а так же непосредственные руководители предприятий и организаций в которых обращается конфиденциальная компьютерная информация ответственные сотрудники по информационной безопасности. Практика борьбы с преступлениями в сфере компьютерной информации показывает, что положительный результат можно получить только при использовании комплекса правовых, организационных и технических мер предупреждения неправомерного доступа к компьютерной информации, причем все они одинаково важны и лишь дополняя друг друга образуют целенаправленную систему предупреждения и профилактики исследуемого преступления.

2.4 Международное сотрудничество в борьбе с преступлениями в сфере компьютерной информации

В рамках СНГ предприняты определенные меры в целях усиления международного сотрудничества в борьбе с преступлениями в сфере высоких технологий. Тем не менее средства и способы совершения таких преступлений постоянно совершенствуются. В актах многих международных организаций рост транснациональной преступности в сфере высоких

технологий рассматривается в качестве угрозы информационной безопасности. В связи с этим анализ существующих правовых и институционных инструментов, которыми располагает СНГ в рассматриваемой области, является актуальным.

Договорно–правовое сотрудничество в борьбе с преступностью в сфере высоких технологий в рамках СНГ базируется на Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. (далее – СПКИ).

СПКИ состоит из 17 статей. В нем определены четыре состава преступления, которые государства – участники Соглашения обязуются закрепить в своем уголовном законодательстве, если они совершены умышленно:

1 Неправомерный доступ к охраняемой законом компьютерной информации.

2 Создание, использование или распространение вредоносных программ.

3 Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

4 Незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права.

Наиболее детальную регламентацию в СПКИ получила процедура направления и исполнения запроса об оказании содействия (ст. 6 – 8). В Соглашении также закреплены нормы, касающиеся использования конфиденциальной информации, полученной от компетентного органа другого государства – участника СПКИ (ст. 9).

На наш взгляд, СПКИ имеет ряд неточностей:

1 Название договора представляется не вполне удачным. Понятие "преступление в сфере компьютерной информации" не включает в себя ряд противоправных деяний, предметом которых не является компьютерная информация, однако которые совершаются с помощью компьютерных технологий.

Если оценить статистические данные Министерства внутренних дел Республики Беларусь, то доля хищений путем использования компьютерной техники среди всех совершенных преступлений в сфере высоких технологий составила: в 2011 г. – 95,6%, в 2012 г. – 94,5%, в 2013 г. – 89%, в 2014 г. – 88,8%. Это свидетельствует о том, что объектом подавляющего количества преступлений в сфере высоких технологий является не информационная безопасность (раздел XII Уголовного кодекса Республики Беларусь), а иные охраняемые законом общественные отношения. Таким образом, в случае совершения подобного противоправного деяния с иностранным элементом сотрудничество по его расследованию не будет подпадать под сферу регулирования СПКИ.

2 СПКИ основано на традиционном представлении о правовой помощи. В.П. Талимончик, справедливо критикуя Соглашение, говорит следующее: «Вызывает удивление, что система электронных запросов на оказание правовой помощи не нашла своего применения в рамках СНГ. Поразительным является тот факт, что СПКИ... основано также на традиционном представлении о правовой помощи. Оно вкратце упоминает о новых технологиях при направлении запроса о правовой помощи, не упоминая о них при ответе»[1]

Действительно, в договоре, координирующем международное сотрудничество в борьбе с преступлениями в сфере компьютерной информации, должна как минимум учитываться природа данного вида преступлений. В связи с этим такой международный договор должен содержать нормы, закрепляющие специальные процессуальные формы сотрудничества.[2]

[1]Талимончик В.П. Конвенции о киберпреступности и унификация законодательства // Информационное право. – 2008. – № 2. – С. 29.

[2]Мороз Н.О. Принципы международно–правового сотрудничества в борьбе с преступностью в сфере высоких технологий // Российская юстиция. – 2012. – № 3. – С. 29 – 30.

3 В документе не называются компетентные органы для работы с запросами. В части 1 ст. 4 СПКИ говорится, что сотрудничество между сторонами в рамках настоящего Соглашения осуществляется между компетентными органами непосредственно.

Представляется, что установление четкого списка уполномоченных для сотрудничества органов поможет упростить применение Соглашения. Подобная практика получила распространение в Соглашении о сотрудничестве государств – участников СНГ в борьбе с незаконным оборотом наркотических средств, психотропных веществ и прекурсоров от 30 ноября 2000 г., Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступностью от 25 ноября 1998 г.

4 В статье 7 СПКИ, которая посвящена процедуре исполнения запросов, во–первых, не содержится четко определенных случаев, когда исполнение запроса может быть приостановлено. Во–вторых, несмотря на специфику преступлений в сфере высоких технологий, ст. 6 требует обязательного письменного подтверждения запроса.

5 Соглашением не рассматривается такая перспективная процессуальная форма сотрудничества, как создание совместных следственных групп.

6 СПКИ не предусматривает таких важных положений, как решение вопросов, затрагивающих суверенитет государства (вопросы конкурирующей юрисдикции, передачи уголовного производства).

7 СПКИ не обеспечивает должной защиты персональных данных.

Таким образом, договорно–правовое сотрудничество в борьбе с преступностью в сфере высоких технологий в рамках СНГ нуждается в совершенствовании. Это обусловлено узким объектом правового регулирования СПКИ 2001 г., а также рядом неточностей, которые в нем содержатся. Необходим полный пересмотр СПКИ 2001 г., а не внесение в него поправок, поскольку предполагается изменение объекта данного международного Соглашения.

В договоре, пересматривающем СПКИ, – Соглашении о сотрудничестве государств – участников СНГ в противодействии преступности в сфере высоких технологий необходимо предусмотреть: цель Соглашения; определения всех значимых терминов; направления и процессуальные формы сотрудничества; компетентные органы для работы с запросами; порядок установления юрисдикции, а также разрешения конкуренции юрисдикций; нормы, направленные на согласование норм материального и процессуального права государств – участников СНГ в рассматриваемой сфере; положения об информационном взаимодействии, исполнении запросов, поручений, совместных расследованиях, передаче уголовного производства и защите информации, включая персональные данные; заключительные положения, касающиеся вступления в силу данного Соглашения, присоединения к нему, отношения к другим международным договорам.

В целях выявления особенностей институционной формы сотрудничества в борьбе с преступностью в сфере высоких технологий в рамках СНГ считаем необходимым рассмотреть две основные области деятельности органов СНГ в данной сфере: принятие актов и практическая деятельность специальных органов.

Документы, касающиеся регулирования противодействия преступности в сфере высоких технологий, утверждаемые органами СНГ, можно разделить на следующие категории: модельные акты (Модельный уголовный кодекс СНГ от 17 февраля 1996 г., Модельный уголовно–процессуальный кодекс СНГ от 17 февраля 1996 г.), концепции (Концепция сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий), рекомендации (например, Постановление Межпарламентской ассамблеи СНГ от 28 сентября 2010 г. N 35–8 "О Рекомендациях по гармонизации и унификации законодательства государств – участников СНГ в сфере защиты детей от информации,

причиняющей вред их здоровью и развитию") и межгосударственные программы. Кроме того, в рамках СНГ планируется принять стратегию обеспечения информационной безопасности. Проект документа был одобрен Межпарламентской ассамблеей государств – участников СНГ 28 ноября 2014г.

Межгосударственные программы совместных мер борьбы с преступностью являются действенным правовым инструментом координации сотрудничества в борьбе с преступностью в рамках СНГ. Решение о действующей в настоящее время Межгосударственной программе совместных мер борьбы с преступностью на 2014 – 2018 гг. было утверждено Советом глав государств СНГ 25 октября 2013 г. (далее – Программа).

Среди организационно–правовых мероприятий, закрепленных Программой, – подготовка и внесение на рассмотрение Совета глав государств проекта Соглашения о сотрудничестве государств – участников СНГ в противодействии преступности в сфере информационных технологий.

Полагаем не вполне обоснованным использование термина "преступность в сфере информационных технологий" для целей международного Соглашения. Это обусловлено тем, что понятие "информационные технологии":

1 Является очень широким и многозначным.

2 Включает в строгом смысле технические средства работы только с информацией, но не с данными.

3 Не получило достаточного распространения в международной договорной практике государств, а также в актах органов ООН.

Полагаем, что понятие "преступление в СВТ" наиболее точно охватывает и отражает специфику средств осуществления преступных посягательств в рассматриваемой области.

В целях совершенствования и сближения национального законодательства в Программе предусмотрено разработать изменения и

дополнения в Модельный уголовный кодекс по вопросам борьбы с преступлениями в информационной сфере.

Следует с сожалением отметить, что Программой не запланировано внесение изменений и дополнений в модельные уголовно–процессуальные нормы (например, урегулирование обыска и выемки в компьютерных сетях).

Обеспечение взаимодействия государств – участников СНГ в борьбе с преступностью является полномочием ряда органов СНГ: Координационного совета генеральных прокуроров государств – участников СНГ, Совета министров внутренних дел государств – участников СНГ; Совета руководителей органов безопасности и специальных служб государств – участников СНГ (в отношении организованной преступности международного характера). В рамках СНГ также действует специальный орган по борьбе с организованной преступностью – Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств – участников СНГ, действующее с 1993 г. (далее – Бюро СНГ)[1]. Тем не менее в СНГ не было создано специальных структурных единиц для координации сотрудничества в борьбе с преступностью в сфере высоких технологий.

Полагаем, что в целях повышения эффективности международного сотрудничества в борьбе с преступностью в сфере высоких технологий в рамках СНГ необходимо расширение компетенции Бюро СНГ.

В частности, считаем целесообразным наделить Бюро СНГ функцией содействия государствам – участникам СНГ в проведении судебных компьютерных экспертиз, поскольку: а) в рамках СНГ не существует органа, компетентного осуществлять такое содействие; б) осуществление данной функции будет обеспечено коллективными экспертно–криминалистическими

[1]Положение о Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств – участников Содружества Независимых Государств [принято в г. Москве 25.11.2005]: в ред. решения Совета глав правительств СНГ от 18.10.2011 // Доступ из СПС «КонсультантПлюс».

ресурсами, что позволит более эффективно противодействовать преступности в сфере высоких технологий; в) государства – участники СНГ с различным потенциалом в области проведения судебных компьютерных экспертиз смогут обеспечить надлежащее уголовное преследование лиц, совершивших преступления в сфере высоких технологий.

Считаем целесообразным также ограничить сферу деятельности Бюро СНГ в рассматриваемой области наиболее серьезными преступлениями: а) совершенными организованными группами; б) связанными с детской порнографией в Интернете; в) наносящими ущерб критическим объектам и государственным информационным системам.

При этом для определения "серьезности" преступления может использоваться критерий, применяемый в Конвенции ООН против транснациональной организованной преступности от 15 ноября 2000 г. Так, в п. b ст. 2 данной Конвенции под серьезным понимается преступление, наказуемое лишением свободы на максимальный срок не менее четырех лет или более строгой мерой наказания.

Указанные выше предложения по расширению компетенции Бюро СНГ основаны на изучении опыта правового регулирования Европейского центра киберпреступности (Европол, Европейский союз) и Межамериканского комитета против терроризма (Организация американских государств). Полагаем, что этот опыт может быть использован применительно к СНГ по следующим причинам:

а) Межамериканский комитет против терроризма, так же как и Бюро СНГ, не является специально созданным органом для координации сотрудничества в борьбе с преступностью в сфере высоких технологий. Такие полномочия были возложены на Межамериканский комитет против терроризма дополнительно и успешно им реализуются.[1]

[1] Work Plan of the Inter–American Committee against terrorism: approved at the Fourth Plenary Session, 7 March 2012 [Electronic resource]. URL:

б) Европейский центр является подразделением Европола, созданным для противодействия новейшим вызовам информационной безопасности, которое не имеет аналогов в региональных международных организациях, в связи с чем его опыт уникален.

в) Компетенция Европейского центра киберпреступности, так же как и Бюро СНГ, ограничена наиболее серьезными преступлениями и носит координационно–операционный характер.[1]

Подводя краткие итоги, можем сделать два основных вывода:

1 СПКИ имеет узкий объект правового регулирования, а также ряд неточностей. Необходим полный пересмотр СПКИ 2001 г., а не внесение в него поправок, поскольку предполагается изменение объекта данного международного Соглашения.

2 Необходимо наделить Бюро СНГ полномочиями по содействию государствам – участникам СНГ в проведении судебных компьютерных экспертиз. Сферу деятельности Бюро СНГ в рассматриваемой области следует ограничить наиболее опасными преступлениями в СВТ.

В настоящее время, базой для международного взаимодействия в борьбе с компьютерными преступниками является «Конвенция о преступности в сфере компьютерной информации». Изучив документ, мы увидим, что в нём определены основные обеспечительные меры по противодействию преступникам киберпространства на государственной и интернациональной арене. Сотрудничество между различными государствами решает такие проблемы как, например, экстрадиция лиц, виновных в компьютерных преступлениях, определяет в систему способы взаимопомощи, в плане распределения и защиты информации, обеспечивает конфиденциальность

---

http://www.cicte.oas.org/rev/en/meetings/sessions/12/2012%20WORK%20PLAN/DOC%205%20rev%201%202012%20WORK%20PLAN%20CICTE00752E04.pdf.

[1] Tackling crime in our digital age: establishing a European Cybercrime Centre: communication from the Commiss. to the Council a. the Europ. Parliament, COM/2012/0140 [Electronic resource]. URL: http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:HTML.

международной информации, межгосударственную доступность и т.д[1]. Основываясь на данной конвенции, экстрадиция предполагается за такие киберпреступления как: незаконный доступ, несогласованная передача информации, влияние на нормальное функционирование сетей, противоправный доступ к сетям, мошенничество и подлог при помощи информационных сервисов, преступления, основанные на распространении порнографии с участием несовершеннолетних, нарушения различных авторских прав. Возможна также экстрадиция индивидов между государствами, если имеет место покушение, элемент соучастия или подстрекательства к совершению указанных правонарушений. Также, экстрадиция индивидов, совершивших преступления, может быть осуществлена, если у потерпевших государств имеются санкции в виде лишение свободы не менее года. Интересно, что в 2005 издан документ Президента РФ «О подписании конвенции о киберпреступности». Документ содержит условие, что Российская Федерация участвует в конвенции на условиях, что будет переиначен пункта «b» статьи 32[2]. В данном пункте указана возможность доступа и получения интернациональных компьютерных данных правоохранительным органам сторон, подписавших конвенцию, при условии, что уполномоченное лицо добровольно даёт согласие на распространение таких данных. Этот пункт был оставлен без изменений, и в 2008 году Президент РФ утвердил новое распоряжение, по которому предыдущее утратило силу[3]. Вследствие этого Конвенция не была ратифицирована, и в наше время не действует на территории Российской Федерации. Международное взаимодействие по противодействию преступлениям в сфере киберпреступности должно реализовываться за счёт:

[1]Международное право [Электронный ресурс]. – URL: www.pravo.ru/interpravo/legislative/view/27/?page=20

[2]Распоряжение Президента РФ от 15.11.2005 N 557–рп «О подписании Конвенции о киберпреступности»// Доступ из СПС Консультант плюс

[3]Распоряжение Президента РФ от 22.03.2008 N 144–рп «О признании утратившим силу Распоряжения Президента Российской Федерации от 15 ноября 2005 г. N 557–рп «О подписании Конвенции о киберпреступности»// Доступ из СПС Консультант плюс

законодательного утверждения ответственности за киберпреступления, международной кооперации различных органов правопорядка, интернационального обмена сведениями тезисов о противодействии киберпреступникам, обязательного повышения квалификации сотрудников органов правопорядка, улучшения системной защиты от незаконного доступа, обеспечения целостности закрытых систем данных и оперативного сбора базы доказательств при расследовании преступлений. В частности, отметим п 1. j) Резолюции. В нём указано, что разработка информационных технологий должна изначально предусматривать предупреждение и своевременное обнаружение незаконного доступа, вести слежку за предполагаемыми преступниками и автоматически собирать актуальную доказательную базу[1]. В теории, вышеуказанное уточнение позволяет правозащитным органам определенного государства оперативно реагировать на преступления в кратчайшие сроки и действовать эффективно. Однако существует возможность незаконного получения доступа к вышеуказанным технологиям киберпреступникам, что позволит им также использовать эти же технологии против их владельцев. Страны G8 в 1996 году была создана группа спец.подразделений по противодействию международным киберпреступлениям — «Лионская группа». После этого главу государств одобрили план из 10 пунктов, по борьбе с так называемыми хакерскими группировками. Для нас важны следующие пункты соглашения: формирование на национальном уровне оперативного центра для международного сотрудничества, функционирующего в режиме онлайн для борьбы с киберпреступностью, специальные уполномоченные сотрудники правозащитных органов должны оказывать помощь другим странам, важна постоянная разработка актуальных баз данных и программ для анализа электронных сведений на предмет их законности в досудебном и судебном

[1]Резолюция, принятая Генеральной Ассамблеей 55/63. Борьба с преступным использованием информационных технологий

разбирательствах, информирование государств-участников об актуальных методах борьбы с киберпреступностью на законодательном уровне[1]. В 2009 году государства-участники НАТО утвердили документ «НАТО и Кибер защита». В нём были утверждены основные принципы по защите от киберпреступности от различного вида компьютерных угроз. Было внесено предложение актуализировать законодательства государств заполнив их такими терминами как: «кибер–война», «кибер–атака», «кибертерроризм». Была оглашена важнейшая необходимость более плотного взаимодействия государств с интернет организациями частными правозащитниками для улучшения защитных качеств государств. Также, для улучшения обороноспособности стран НАТО, было рекомендовано помогать Индии, Бразилии, Китаю и России, для их присоединения к «Конвенции о преступности в сфере компьютерной информации». В 2008 всё теми же государствами-участникам НАТО в Эстонии, был открыт информационный центр обучения сотрудников в сфере противодействия киберпреступлениям и даже военного противодействия на киберпространстве. Законодательство стран ООН и НАТО, в целом, имеет большое значение в противодействии киберпреступлениям. Онлайн центры, работающие в круглосуточном режиме, утверждение актуальных определений и терминов на законодательном уровне в сфере киберпреступности, международная экстрадиция граждан, интернациональная работа сотрудников органов правозащиты, участие в международных обучениях и семинарах, обмен сведениями без сомнений помогают в оперативном и эффективном реагировании на киберпространственные преступления.[2]

[1]Киберпреступность [Электронный ресурс]. – URL: http://news.bbc.co.uk/2/hi/science/nature/38671.stm

[2]Кривогин М. С. Международно–правовые аспекты борьбы с кибернетическими преступлениями [Текст] // Государство и право: теория и практика: материалы II Междунар. науч. конф. (г. Чита, март 2013 г.). – Чита: Издательство Молодой ученый, 2013. – С. 77–79.

3 ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

3.1 Особенности ответственности за преступления в сфере компьютерной информации по законодательству РФ

Когда были сделаны первые шаги на пути к формированию новых статей, в отношение уголовного законодательства в сфере компьютерных технологий, непосредственно в Российской научной среде, они в первую очередь старались усовершенствовать уже существующее законодательство. Учёные А.М. Жодзишский и Ю.М. Батурин тщательно изучали преступления в сфере компьютерной информации. По итогам исследований они удалось выявить базовые два вида — первый был связан с вмешательством в нормальное функционирование системы и второй связан с использованием компьютера как средства достижения преступных целей[1]. Первый характеризуется следующими тезисами:

1 Получение неправомерного доступа к сведениям на компьютере потерпевшего.

2 Введение в компьютерную систему потерпевшего вредоносных программ, которые могли полностью или частями нарушить её функционирование.

3 Незаконное распространение и формирование программ для компьютера, которые могли нанести ему разрушительный урон – вирусов.

4 Создание и использование некачественных программ для компьютерных систем, которые могли нарушить нормальную работу.

5 Несанкционированное изменение сведений в компьютере.

6 Хищение сведений с материальных носителей.

[1]Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М., 1991. – С. 111.

Изучив зарубежное законодательство, мы увидим, что в нём отсутствует уголовная ответственность за создание вирусов и нарушение правил работы с ЭВМ. Нельзя не согласиться с Т.Г. Смирновой в части того, что такие деяния стоит рассматривать как один из видов диверсий, которые могут нанести вред сведениям, содержащимся на компьютерах[1].

Российское законодательство, практически, не регулирует отношения в сфере компьютерных отношений, помимо главы 28 УК РФ. Интересно, что по статье 273 этой главы мы можем квалифицировать деяние по неосторожности и за него будет предусмотрена санкция в виде лишения свободы. Нам видится такая ситуация неоднозначной, так как неясно, каким образом оценивать и квалифицировать действия киберпреступника, с точки зрения субъективной стороны. На основании изученного мы можем определить термин киберпреступлений в виде следующего: это предусмотренное уголовным законом, противоправное, виновное нарушение чужих прав и интересов, связанное с уничтожением, использованием, модификацией виртуальных информационных сведений, причинившее ущерб или создавшее угрозу причинения такого ущерба подлежащим уголовно–правовой охране правам и интересам физических и юридических лиц, общества и государства (личным правам и интересам, частной неприкосновенности, общественной и государственной безопасности, конституционному строю, имущественным правам).

Очевидно, что такие законодательные недоработки способствуют развитию киберпреступности в РФ. У правоохранительных органов нет специальных центров по слежению за активностью киберпреступников в сети интернет и на локальных сервисах. Сеть Интернет растёт с каждым днём и вместе с ней растёт количество пользователей, в свою очередь это ведёт к росту опасности преступлений в сфере компьютерной информации и к их

[1]Смирнова Т.Г. Уголовно–правовая борьба с преступлениями в сфере компьютерной информации: дис. … канд. юрид. наук. – М., 1999. – С. 230.

распространённости, а значит необходим и рост в сфере защиты сетевой информации. Помимо этого, мы считаем, что отечественному уголовному законодательству и другим государствам, которые могут быть подвержены кибератакам, требуется унификация и систематизация. Мы также считаем необходимым провести имплементацию норм международного уголовного права в отечественное законодательство, ведь, как мы уже убедились на примере предыдущих глав, те же Европейские законодательства имеют обширные нормы ответственности за компьютерные преступления.

Мы вынуждены также констатировать, что в Российском законодательстве не отражены в материальном виде преступления киберхарактера, посягающие на информационные ресурсы собственности граждан и организаций. Изучив практику, мы увидим, что сейчас эти деяния квалифицируются самым различным образом, в зависимости от обстоятельств. К примеру, имеют место случаи информационно-компьютерного хищения данных, содержащих сведения государственной тайны с последующей передачей иностранному государству, организации или гражданам, это могут квалифицировать по ст. 175, 276 или 283 УК РФ, но при этом будут иметь место 272 – 274 УК РФ. В данном случае важно отметить, такая ситуация требует устранения законодательного пробела, чтобы исключить проблемы с квалификацией преступлений. Компьютерные базы данных, в которых содержатся конфиденциальные сведения различного характера стоят больших денег, при этом, если ими будут пользоваться некомпетентные лица, это может принести ущерб правам и свободам человека и гражданина, безопасности общества и государства, привести к совершению новых преступлений. В наше время мы можем видеть активный переход многих баз данных государственных и коммерческих структур на электронные носители. Так как зачастую держатели таких баз данных являются недобросовестными гражданами, это привело к контролю вышеуказанных баз данных в руках лиц, которые впоследствии реализуют их

на «чёрном рынке». Такая ситуация приводит к потере контроля над достоверной и важной информацией. При этом сам факт того, что такие сведения могут свободно продаваться в определенных кругах или распространяться иным образом, представляет собой опасный фактор для общества, так как конфиденциальные сведения будут использоваться не во благо, а во вред. Мы считаем, что сам факт неправомерной торговли такими данными, а также их хранения, сбыта, перемещения и т.д. должен иметь отражение в уголовном законе. Сами способы и содержание информации должны быть запрещены законодательно и должны влечь за собой уголовную ответственность. Нельзя законодательно допускать свободный оборот такой важной информации. В настоящее время в законодательстве РФ подобным образом описаны меры по противодействию незаконного оборота оружия, что является хорошей аналогией в случае с компьютерной информацией. Также не нужно забывать об уже упоминаемой имплементации норм европейского и других законодательств. В отечественном законодательстве, действительно, не отражены многие моменты, связанные с неправомерным использованием компьютерной информации или её элементов. Мы считаем, что это не улучшает ситуацию с назначением наказания за смежные с киберпреступностью деяния и иной раз правоохранительные органы не получают возможности верно оценить характер повышенной опасности совершенного деяния.

Также интересно, что в 2000 г. Открыт для подписания Факультативный протокол к Конвенции о правах ребенка, о детской проституции, торговле детьми и порнографией с участием несовершеннолетних. В вышеуказанном протоколе отражена уголовная ответственность как за действия, связанные с созданием, реализацией, импортом, экспортом, иными видами распространения информации и продукции, предложения о продаже или хранению порнографии с участием несовершеннолетних, вне зависимости от применения или не применения специальных средств (ст. ст. 2 и 3). Само

собой, что в данный момент проблематично согласовать предписания в ст. 242 УК РФ и ситуацию с повышенной общественной опасностью преступлений, связанных с распространением детской порнографии по сетям интернет. Требуется либо внесение новой части в эту статью, либо формирование новой индивидуальной статьи в УК РФ. Таким же образом необходимо поступить и в некоторых других случаях.

3.2 Совершенствование уголовного законодательства России об ответственности за преступления в сфере компьютерной информации

Применение современных информационных технологий в банковской, торговой, промышленной, научной, образовательной, культурной и других сферах общественной жизни детерминировали существование компьютерной преступности в Российской Федерации, ее динамический рост и качественное обновление, что создает новые угрозы для развития российского общества и государства. Так, согласно последнему отчету международной компании «Лаборатория Касперского», в 2014 году ее программные продукты заблокировали 6 167 233 068 вредоносных атак на компьютеры и мобильные устройства пользователей. Кроме того, решения «Лаборатории Касперского» отразили 1 432 660 467 атак, проводившихся с 9 766 119 хостов (интернет–ресурсов), размещенных в разных странах мира. При этом 44% атак проводились с веб–ресурсов, расположенных в США и Германии. Также в 2014 году было задетектировано 123 054 503 новых уникальных вредоносных объектов (скрипты, эксплойты, исполняемые файлы и т.д.). Вместе с тем, по данным «Лаборатории Касперского», Российская Федерация занимает 1–е место в мире по количеству атакованных вредоносными программами пользователей мобильных устройств (45,7%); банковских пользователей, атакованных вирусами–троянцами (87,75%); количеству инфицированных через сеть «Интернет»

компьютеров (53,81% пользователей)[1]. Кроме того, компьютерные преступления наносят колоссальный ущерб российской экономике.

По оценкам аналитиков международной компании Group–IB, объем рынка киберпреступности в РФ и странах СНГ за второе полугодие 2014 – первое полугодие 2015 года составил почти 4 млрд рублей. В том числе, хищения в интернет–банкинге у юридических лиц – 1 912 320 000 рублей, целевые атаки на банки – 638 000 000 рублей, обналичивание похищаемых средств – 1 192 239 900 рублей. Примерный ущерб от одного хищения в интернет–банкинге у юридических лиц составил 480 000 рублей, а у физических лиц – 76 500 рублей[2]. По данным исследования «2014 CostofCyberCrimeStudy», проведенного компанией PonemonInstitute при поддержке HP EnterpriseSecurity, среднегодовой ущерб российской организации от киберпреступлений в 2014 году достиг $3,3 млн[3]. Между тем, по данным ГИАЦ МВД России, общее количество преступлений в сфере компьютерной информации (зарегистрированных в текущем периоде), предусмотренных ст. 272 и ст. 273, 274 УК РФ, в 2009г. составило соответственно 9489 и 2097, 4; в 2010 г. – 6132 и 1010, 0; в 2011 г. – 2005 и 693, 0; в 2012 г. – 1930 и 889, 1; в 2013 г. – 1799 и 764, 0; в 2014 г. – 1151 и 585, 3 [4]. Таким образом, за последние шесть лет количество выявленных преступлений в сфере компьютерной информации сократилось более чем в 6,5 раз, с 11590 до 1739 уголовных дел, что не может не настораживать. Поскольку аналитические отчеты экспертов в сфере информационной безопасности («Доктор Web», «Лаборатория Касперского», Symantec, Group–IB и др.) говорят не столько об улучшении и усилении борьбы

[1]KasperskySecurityBulletin 2014. Основная статистика за 2014 год. [Electronic resource]. – URL: https://securelist.ru/ files/2014/12/Kaspersky–Security–Bulletin–2014–RU.pdf (дата обращения: 30.10.2015).

[2]Тенденции развития преступности в области высоких технологий 2015. URL: http://report2015.groupib.ru/ (дата обращения: 30.10.2015).

[3]2014 Global Report on the Cost of Cyber Crime. [Electronic resource]. – URL: http://www.octree.co.uk/Documents/2014–Global–Report–on–the–Cost–of–Cybercrime.pdf (дата обращения: 05.05.2015).

правоохранительных органов с преступлениями данного вида, сколько о том, что в данной сфере наблюдается качественная трансформация компьютерной преступности, выраженная в приобретении последней высоколатентного и организованного характера. Это в свою очередь, по мнению автора, значительно затрудняет эффективное выявление и расследование указанных преступных деяний, а также определяет тенденцию к снижению количества зарегистрированных в РФ уголовных дел о компьютерных преступлениях. Следует также отметить, что сокращается количество не только выявленных, но и раскрытых преступлений. Так, например, если из находившихся в производстве в 2010 году 1066 уголовных дел (возбужденных по ст. 273 УК РФ) направлено в суд 914, то в 2011 году из 754 уголовных дел в суд направлено 558; в 2012 году соответственно из 953 уголовных дел направлено в суд только 664, а в 2013 году из 860 уголовных дел направлено в суд 575; в 2014 году из 665 уголовных дел в суд направлено 344[1]. По мнению автора, основной причиной сокращения количества направленных в суд уголовных дел по преступлениям в сфере компьютерной информации является снижение качества предварительного следствия, в т.ч. ошибки следователей при уголовно–правовой квалификации преступного деяния на стадии возбуждения уголовного дела[2]. Вместе с тем вопросы уголовно–правовой квалификации компьютерных преступлений в последнее время стали предметом обсуждения российского научного сообщества[3]. Однако, несмотря на научную разработанность данной проблемы, на практике, при квалификации преступлений в сфере компьютерной информации

[1]Ф–615 кн.1. Преступления в сфере компьютерной информации. Сводный и сборник по России за январь–декабрь 2010–2014 гг. URL: http://mvd.ru (дата обращения: 09.03.2015).
[2]Евдокимов К.Н. Актуальные вопросы совершенствования уголовной ответственности за совершение преступлений в сфере компьютерной информации // Проблемы современного российского законодательства: материалы III Всероссийской научно–практической конференции (Иркутск, 3 декабря 2014 г.). – Иркутск; М.: РПА Минюста России, 2015. – С. 255.
[3]Степановегиянц В.Г. Проблемы разграничения неправомерного доступа к компьютерной информации со смежными составами // Право и кибербезопасность. – 2014. – № 2. – С. 6.

правоприменитель часто сталкивается с затруднениями технико–юридического характера. Так, например, у следователя или судьи возникает проблема при уяснении некоторых понятий, содержащихся в диспозициях ст. 272–274 УК РФ, а именно: «компьютерная программа», «несанкционированное уничтожение, блокирование, модификация, копирование компьютерной информации», «нейтрализация средств защиты компьютерной информации», «средства хранения, обработки или передачи охраняемой компьютерной информации». Это связано с тем, что указанные технико–юридические термины законодательно нигде не определены. Поэтому, как правило, судьи, прокуроры, следователи вынуждены обращаться к текстам комментариев Уголовного кодекса РФ. Однако в отсутствие разъяснений пленума Верховного Суда РФ выводы авторов комментариев УК РФ носят часто субъективный и взаимопротиворечивый характер. Это, к сожалению, негативно влияет на единообразие судебной практики по уголовным делам о преступлениях в сфере компьютерной информации. Кроме того, при квалификации деяний, предусмотренных ст. 272–274 УК РФ возникает ряд вопросов, требующих конкретного толкования для правоприменителя Верховным Судом Российской Федерации. Например, будет ли являться уничтожением компьютерной информации деяние, при котором информация была изначально уничтожена, но спустя определенное время частично или полностью восстановлена специалистами? Как квалифицировать уничтожение компьютерной информации сильным электромагнитным или высокочастотным излучением, не повлекшим уничтожение самого носителя информации? Будут ли являться незаконным копированием компьютерной информации действия преступника при получении копии путем распечатывания информации на принтере, фотографирования или видеосъемки изображения монитора компьютера? Будет ли являться созданием вредоносной компьютерной программы написание вредоносного кода «вирусмейкером» на бумажном носителе?

Наконец, как квалифицировать несанкционированное ознакомление с компьютерной информацией, когда преступник, визуально запомнив конфиденциальные сведения (например, персональные данные лица; информацию о содержании коммерческой сделки и сторонах договора; сведения об усыновлении (удочерении), врачебную тайну и т.д.), впоследствии переносит их на другой материальный носитель информации, создав ее копию (написав на листе бумаги, введя информацию в память своего компьютера или иного компьютерного устройства: айфона, смартфона, планшетного компьютера, коммуникатора и т.п.). По мнению автора, описанные деяния и последствия носят противоправный характер и должны учитываться при квалификации преступлений в сфере компьютерной информации. Кроме того, полагаем целесообразным дополнить главу № 28 УК РФ статьей 272. 1 «Незаконное завладение носителем компьютерной информации с целью осуществления неправомерного доступа к компьютерной информации», предусмотрев наказание до двух лет лишения свободы. Данное авторское предложение основано на том, что преступник, тайно, открыто или обманным путем завладев носителем компьютерной информации, например, флэш–картой или DVD–диском, для последующего извлечения и использования информации, избегает уголовной ответственности в силу малозначительности совершенного деяния. Учитывая, что стоимость вышеуказанных носителей информации не превышает тысячи рублей, это грозит виновному (в лучшем случае) наступлением административной ответственности по ст. 7. 27 КоАП РФ (мелкое хищение) и наказанием до 15 суток административного ареста. При этом виновное лицо получает доступ к компьютерной информации, представляющей большую ценность для ее обладателя, чем сам носитель информации. При квалификации преступных действий, предусмотренных ст. 273 УК РФ, следует отметить неудачную юридическую конструкцию ч. 1 ст. 273 УК РФ, в диспозиции которой указывается на «создание,

распространение или использование компьютерных программ … заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации». Указание законодателем на создание, использование и распространение вредоносных компьютерных программ во множественном числе по смыслу статьи можно трактовать как то, что правоприменитель не вправе привлекать к уголовной ответственности лицо, которое создало, использовало или распространило одну вредоносную компьютерную программу. Также, по мнению автора, нецелесообразным является исключение из диспозиции ст. 273 УК РФ такого преступного действия, как «внесение изменений в существующие программы». Данный вопрос приобретает актуальность в связи с тем, что в последние годы создаются уже не отдельные вредоносные программы, а целые семейства компьютерных вирусов, имеющих в основе однотипный цифровой код, либо лицензионные программы в результате модификаций приобретают вредоносный характер. Так, например, вирусмейкеры Джеффри Ли Парсон (США) и Димитрий Чобан (Румыния) модифицировали компьютерный вирус «Blaster», который нанес в 2003–2005 годах ущерб от 2 до10 млрд долларов владельцам и пользователям компьютеров в США и странах Европы. Однако, по их признанию, они не создавали вредоносную компьютерную программу «Blaster», а произвели ее модификацию, внеся изменения в существующую вредоносную компьютерную программу, получив тем самым компьютерные вирусы «Blaster.B» и «Blaster.F»[1]. Думается, что с уголовно–правовой точки зрения, постановление пленума Верховного Суда РФ могло бы устранить сомнения в части, считать ли подобные действия модификацией, т.е. внесением изменений в существующую вредоносную компьютерную программу (информацию), либо созданием новой вредоносной

[1]Компьютерный червь [Электронный ресурс]. – URL: www.ru.wikipedia.org/wiki/Blaster (дата обращения: 07.10.2014).

компьютерной программы (информации). По нашему мнению, в данном случае виновное лицо должно нести ответственность в равной степени как за модификацию, так и за создание новой разновидности вредоносной программы. Кроме того, считаем логичным в число преступных действий, закрепленных в ч. 1 ст. 273 УК РФ, включить такое деяние, как приобретение компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Свою позицию обосновываем тем фактом, что подавляющее большинство преступников, использующих вредоносные компьютерные программы, не являются их создателями, а приобретают их для преступных целей у представителей хакерского сообщества на специализированных сайтах, форумах или веб–страницах. При этом вредоносные компьютерные программы опасны для общества так же, как и оружие, наркотики, сильнодействующие или психотропные вещества, взрывчатые вещества, за приобретение которых предусмотрена уголовная ответственность. Поэтому, по мнению автора, лица, приобретающие компьютерные вирусы, должны нести уголовную ответственность наравне с лицами, их создающими и распространяющими. Данная точка зрения ранее уже высказывалась рядом авторов[1], но законодательного закрепления не нашла. Вызывает определенное недоумение также установление законодателем в ч. 2 ст. 272, 273, ч. 1 ст. 274 УК РФ уголовной ответственности за причинение крупного ущерба в сумме, превышающей один миллион рублей. При этом, например, размер крупного ущерба в ч. 1, 2 ст. 146 за причинение вреда авторским или смежным правам установлен в сто тысяч рублей, а за преступления против собственности (ст. 158, 159, 163, 167 УК РФ) в размере, превышающем двести пятьдесят тысяч рублей. Таким

[1]Родивилин И.П. Проблемы квалификации преступлений в сфере компьютерной информации, совершаемых с использованием дистанционного управления банковским счетом и их предупреждение // Пролог. – 2014. – № 2 (6). – С. 144.

образом, по мнению автора, размер крупного ущерба при совершении преступлений в сфере компьютерной информации явно завышен, что также негативно влияет на борьбу с преступлениями в сфере компьютерной информации. Кроме того, компьютерная информация, технические средства ее обработки, носители информации могут находиться в собственности физических лиц. Поэтому, по нашему мнению, представляется целесообразным учесть имущественные права и интересы потерпевшего, дополнив диспозицию ст. 272, 273 УК РФ новым квалифицирующим признаком: «с причинением значительного ущерба гражданину...». С учетом вышесказанного, считаем целесообразным снизить крупный размер вреда, причиненного преступлением в сфере компьютерной информации, и изложить примечание к ст. 272 УК РФ в следующей редакции: «1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. 2. Значительный ущерб гражданину в статьях настоящей главы определяется с учетом его имущественного положения, но не может составлять менее двух тысяч пятисот рублей. 3. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает сто тысяч рублей». Это позволит привести ст. 272–274 УК РФ в соответствие с остальными уголовно–правовыми нормами по вопросу о сумме ущерба, причиненного преступным деянием, устранив в данном случае возникшую коллизию в размерах причиненного вреда. Продолжая анализ проблем при квалификации преступлений в сфере компьютерной информации, нельзя не остановиться на мотивах и целях преступления. Необходимо отметить, что в действующей редакции ч. 3 ст. 272 УК РФ и ч. 2 ст. 273 УК РФ в качестве квалифицирующего признака преступления закреплен корыстный мотив: «Деяния, … совершенные из корыстной заинтересованности». Это положительный шаг в совершенствовании уголовной ответственности за преступные деяния

данного вида, т.к., по мнению большинства опрошенных работников правоохранительных органов (74%), корыстный мотив присутствует не менее чем в 90% случаев совершения преступлений в сфере компьютерной информации[1]. Однако считаем целесообразным дополнить диспозиции статей 272, 273 УК РФ новым квалифицирующим признаком: «С целью скрыть другое преступление или облегчить его совершение», поскольку преступления в сфере компьютерной информации часто выступают способом совершения множества других преступных деяний (хищений денежных средств, нарушения авторских и смежных прав, сбыта наркотических веществ, умышленного уничтожения или повреждения имущества, шпионажа, государственной измены и т.д.). Анализ научных трудов[2], посвященных совершенствованию уголовной ответственности за преступления в сфере компьютерной информации, подтверждает позицию автора об учете вышеуказанных целей для всесторонней и полной квалификации рассматриваемых преступных деяний. Нельзя не учитывать и политические мотивы (цели) совершения преступлений в сфере компьютерной информации, которые, по мнению автора, вызваны: 1) развитием хактивистского движения как политического протестного движения против государственного контроля в глобальной информационной сети «Интернет»; 2) причинением вреда государственным интересам, деятельности механизма государственной власти Российской Федерации вооруженными силами враждебных стран путем использования вредоносных компьютерных программ в качестве информационного оружия; 3) деятельностью спецслужб иностранных государств в отношении российских органов власти, учреждений, предприятий для получения информации геополитического, военно–технического, дипломатического и иного

[1]Чекунов И.Г. Некоторые особенности квалификации преступлений в сфере компьютерной информации // Российский следователь. – 2012. – № 3. – С. 111.
[2]Менжега М.М. Криминалистические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ: дис. ... канд. юрид. наук. – Саратов: РГБ, 2013. – С. 238.

стратегического характера, т.е. «кибершпионаж»; 4) неправомерным использованием вредоносных компьютерных программ и компьютерных технологий в период предвыборных компаний для дискредитации кандидатов на выборные должности в органы государственной власти и местного самоуправления. Поэтому для более эффективного противодействия преступлениям в сфере компьютерной информации автор предлагает дополнить диспозиции ч. 3 ст. 272, ч. 2 ст. 273, ч. 2 ст. 274 УК РФ новым квалифицирующим признаком: «То же деяние, совершенное по политическим мотивам либо с целью устрашения населения или воздействия на принятие решения органами государственной власти и (или) местного самоуправления, воспрепятствования нормальной деятельности средств массовой информации, органов государственной власти и (или) местного самоуправления, государственных и (или) муниципальных предприятий, учреждений», установив уголовное наказание до 10 лет лишения свободы. Данное предложение, по мнению автора, обусловлено повышенной общественной опасностью «киберсаботажа», «кибершпионажа», «кибертерроризма», «кибервандализма» и прочих компьютерных преступлений политической направленности. При этом автор полагает необходимым также внести изменения в ст. 151 УПК РФ и отнести преступления, предусмотренные ч. 3, 4 ст. 272, ч. 2, 3 ст. 273, ч. 2 ст. 274 УК РФ, к подследственности органов ФСБ РФ, поскольку данные составы преступлений угрожают национальной безопасности России.

ЗАКЛЮЧЕНИЕ

Итак, криминологическая характеристика даёт нам, по крайней мере, возможность в определённой степени предвидеть, что может «принести» конкретное правонарушение с точки зрения личности преступника и его действий, на что надо обращать внимание в первую очередь, какие меры планировать, какую реакцию преступника ожидать. Разработка проблемы компьютерной преступности и поиск методов борьбы с нею задача относительно новая и с каждым годом набирает свои обороты.

Новизна и специфичность преступлений в сфере компьютерной информации, многообразие предметов и способов преступных посягательств, их высокая латентность создают для правоохранительных органов серьёзные преграды на пути к защите прав и интересов общества и государства. Положение усугубляется общим снижением эффективности деятельности в сфере раскрытия и расследования преступлений. Российские правоохранительные органы крайне медленно адаптируются к новым условиям борьбы с преступностью.

Классификация лиц, совершающих преступления в сфере компьютерной информации, уже неоднократно рассматривалась различными криминологами. В основном выделяют таких лиц как «хакеры». Эти лица характеризуется в криминалистической литературе как профессионалы высокого класса, использующие свои интеллектуальные способности для разработки способов преступных посягательств на компьютерную информацию (преимущественно «взломов» систем компьютерной защиты и безопасности). Мотивы этого могут быть различными: хулиганские побуждения, озорство, месть, корыстные побуждения, промышленный и иной шпионаж и пр.

Проанализировав актуальное Российское уголовное законодательство в сфере компьютерной информации мы можем сделать вывод о необходимости

решения различных правовых проблем. В целом, их можно рассмотреть, как составные части механизма защиты компьютерной информации.

Это необходимо сделать путём контролирования противоправного доступа к компьютерным информационным данным различных систем. Борьба с преступностью в сфере компьютерной информации осложняется также из–за высокого уровня её латентности. В среднем, 80–90% преступлений в сфере компьютерной информации остаются «невидимыми» для зарубежных правоохранительных органов. Такая ситуация возникает чаще всего из–за отсутствия стремления самих жертв информировать правоохранительные органы, им не нужна лишняя публичная огласка, привлечение к уголовной ответственности собственных сотрудников, простая юридическая неграмотность и правовой нигилизм. Выделим следующие пути устранения такой латентности:

– социальные опросы граждан, анкетирование, привлечение экспертов, анализ СМИ на предмет их содержания;

– преодоление правового нигилизма руководителей различных организаций и отдельных граждан путем освещения проблем компьютерной преступности в СМИ; – повышение качества работы правоохранительных органов путём улучшения квалификации их работников, повышение требований к уровню профессионализма сотрудников вышеуказанных органов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Раздел 1 Нормативные правовые акты и иные официальные акты

1. Резолюция, принятая Генеральной Ассамблеей 55/63. Борьба с преступным использованием информационных технологий// Сборник международных правовых источников. – 2012. – № 4.
2. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации// Сборник международных правовых источников. – 2013. – № 11.
3. Положение о Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств – участников Содружества Независимых Государств [принято в г. Москве 25.11.2005]: в ред. решения Совета глав правительств СНГ от 18.10.2011 //Доступ из СПС «КонсультантПлюс».
4. Распоряжение Президента РФ от 15.11.2005 N 557–рп «О подписании Конвенции о киберпреступности»// Сборник международных правовых источников. – 2013. – № 10.
5. Распоряжение Президента РФ от 22.03.2008 N 144–рп «О признании утратившим силу Распоряжения Президента Российской Федерации от 15 ноября 2005 г. N 557–рп «О подписании Конвенции о киберпреступности»// Сборник международных правовых источников. – 2013. – № 10.
6. Федеральный закон «О внесении изменений в Уголовно–процессуальный кодекс РФ» от 28 июля 2012 г. № 143–ФЗ // Российская газета. – 2012 – №5847.
7. Федеральный закон «О ратификации Соглашения о сотрудничестве государств–участников Содружества Независимых Государств в

борьбе с преступлениями в сфере компьютерной информации» от 01.10.2008 № 164–ФЗ // Российская газета. – 2016 – № 6989.

8. Ф–615 кн.1. Преступления в сфере компьютерной информации. Сводный и сборник по России за январь–декабрь 2010–2014 г. – URL: http://mvd.ru (дата обращения: 09.03.2015).

Раздел 2 Использованная литература

1. Абов А.И. Преступления в сфере компьютерной информации: неправомерный доступ к компьютерной информации. – М.: Прима–Пресс, 2002.–С.160.
2. Айков Д., Сейгер К., Фонстрох У. Компьютерные преступления. – М., 1999. – 185с.
3. Баранов А.А. Права человека и защита персональных данных. – Киев: Государственный комитет связи и информатизации Украины, –2000. – 280 с.
4. Батурин Ю.М. Проблемы компьютерного права. – М., 1991. – С.229.
5. Батурин Ю.М., Жодзишский А.М. Компьютерные преступления и компьютерная безопасность. – М., 1991. – С.301.
6. Будаковский Д.С. Способы совершения преступлений в сфере компьютерной информации // Российский следователь. – 2011. – № 4. С. 245.
7. Беспалова Е.В., Широков В.А. Компьютерные преступления: основные тенденции развития// Юрист. – М.: Юрист 2006. – № 10. – С.219.
8. Борзенков Г.Н., Комиссаров В.С. Уголовное право Российской Федерации / Г.Н. Борзенков, В.С. Комисаров. – М.: Олимп, – 1997. – 382с.
9. Вехов, В. Б. Компьютерные преступления: Способы совершения, методики расследования. М. : Право и закон. – 1996. – С. 214.

10. Викулова Л.Г., Шарунов А.И. Основы теории коммуникации: практикум. – М., 2008. – С.420.
11. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М.: Изд–во Юрлитиформ. – 2000.–С.495.
12. Григоренко С.В., Ткаченко С.Н., Каспаров А.А., Преступления в сфере компьютерной информации. – М.: Полтекс, 2003.–С.211.
13. Громов Е.В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше) // Вестник ТГПУ. – 2006. – №11 (62). – С. 309.
14. Дворецкий М.Ю., Карамнов А.Ю. Оптимизация уголовной ответственности за преступления в сфере компьютерной информации // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2012. – № 11. – С. 387.
15. Долгова, А. И. Криминология. М. : ИНФРА–М, 2002. – С. 684–685.
16. Евдокимов К.Н. Актуальные вопросы совершенствования уголовной ответственности за совершение преступлений в сфере компьютерной информации // Проблемы современного российского законодательства: материалы III Всероссийской научно–практической конференции (Иркутск, 3 декабря 2014 г.). Иркутск; М.: РПА Минюста России. – 2015. – С. 255.
17. Евдокимов К.Н. Субъективная сторона неправомерного доступа//Вестник Академии Генеральной Прокуратуры РФ. – М,2009 – №12. – С. 56.
18. Золотухин С.Н., Хун А.З. Уголовно–правовые и криминологические аспекты преступлений в сфере компьютерной информации: учебное пособие Краснодар: Краснодарский университет МВД России: – 2008.– С.232.

19. Карпец И.И., Ратинов А.Р. Правосознание как элемент правовой культуры // Правовая культура и вопросы правового воспитания : сборник научных трудов. – М., 1974. – С. 307.
20. Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: диссертация кандидата юридических наук.– Красноярск:2002.–С. 334.
21. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. – М., 2002. – С. 231.
22. Комментарий к Уголовному кодексу Российской Федерации / под ред. Наумова.– М.: 1996–С. 665; Борчева Н.А. Компьютерные преступления в России (комментарий к Уголовному Кодексу РФ).– М.: 2001.–С.10.
23. Копырюлин А.Н. Система преступлений в сфере компьютерной информации в структуре РФ//Системность в уголовном праве//Материалы 2–го Российского Конгресса уголовного права – 2007 – С. 153.
24. Котухов М.М., Марков А.С. Законодательно–правовое и организационно–техническое обеспечение информационной безопасности автоматизированных систем / М.М. Котухов, А.С.Марков– СПб.: ВУС, 2004. – 190 с.
25. Кочои С.М. Ответственность за корыстные преступления против собственности. – М.,1998. – С.232.
26. Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации. – 1999. – 215с.
27. Кривогин М. С. Международно–правовые аспекты борьбы с кибернетическими преступлениями [Текст] // Государство и право: теория и практика: материалы II Междунар. науч. конф. (г. Чита, март 2013 г.). – Чита: Издательство Молодой ученый. – 2013. – С. 177.
28. Криминология : учебник / под ред. А.И. Долговой. – М., 1997. – С. 292.

29. Криминология / под ред. В. Н. Бурлакова, Н. М. Кропачева. – СПб, 2004. – С. 285.
30. Криминология : учебник / под ред. Н. Ф. Кузнецовой, В. В. Лунеева. 2–е изд., перераб. и доп. – М. :ВолтерсКлувер, 2005. – С. 168.
31. Крылов В.В. Информационные компьютерные преступления. – М., 1997. – С. 264.
32. Кудрявцев В.Н. Причины правонарушений. – М., 1976 – 196с.
33. Курушин, В. Д. Компьютерные преступления и информационная безопасность / В. Д. Курушин, В. А. Минаев. М. : Новый юрист, 1998. С. 221.
34. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления //Законность. – 1997. – №1. – С.312.
35. Мазуров В.А. Компьютерные преступления: классификация и способы противодействия: учебно–практическое пособие. – М.: 2002.–С.115.
36. Макарова Н.В., Волков В.Б. Информатика: учеб. для вузов. – СПб., 2011. – С. 318.
37. Маклюэн М.Г. Средство само есть содержание. [Электронный ресурс]. – URL: http://www.uic.unn.ru/pustyn/lib/maclu.ru.html
38. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на INTERNET. – М., 2000. – С. 311.
39. Модельный уголовный кодекс для государств СНГ // Панфилов Е.И. Попов А.С. Компьютерные преступления. – СПб., 1998.
40. Мороз Н.О. Принципы международно–правового сотрудничества в борьбе с преступностью в сфере высоких технологий // Российская юстиция. – 2012. – № 3. – С. 290.
41. Озерский С.В., Лазарев Ю.Н., Лавров А.Ю. Компьютерные преступления: методы противодействия и защиты информации: Учебное пособие Саратов: Саратовский юридический институт МВД России. – 2004.– С.324.

42. Определение Прокси–сервер. [Электронный ресурс]. – URL: http://ru.wikipedia.org/ wiki/Прокси–сервер (дата обращения: 10.02.2011)
43. Пашин С.А. Преступления в сфере компьютерной информации// Коммент к УК //под ред. Скуратова и Лебедева .–М.: 1996.–С. 640.
44. Родивилин И.П. Проблемы квалификации преступлений в сфере компьютерной информации, совершаемых с использованием дистанционного управления банковским счетом и их предупреждение // Пролог. – 2014. – № 2 (6). – С. 244.
45. Романов Б.Н., Краснов С.В. Теория электрической связи. Сообщения, сигналы, помехи, их математические модели: учеб. пособие. – Ульяновск, 2008. – С. 274.
46. Степановегиянц В.Г. Проблемы разграничения неправомерного доступа к компьютерной информации со смежными составами // Право и кибербезопасность. – 2014. – № 2. – С. 316.
47. Сударева Л.А. Правовое и информационное обеспечение деятельности органов внутренних дел по предупреждению компьютерных преступлений: диссертация кандидата юридических наук. – М.: 2008.– С.244.
48. Талимончик В.П. Конвенции о киберпреступности и унификация законодательства // Информационное право. – 2008. – № 2. – С. 270.
49. Тенденции развития преступности в области высоких технологий 2015. [Электронный ресурс]. – URL: http://report2015.groupib.ru/ (дата обращения: 30.10.2015).
50. Ткачев А.В. Исследование компьютерной информации в криминалистике // Эксперт–криминалист. – 2012. – № 4. – С. 295.
51. Уголовный кодекс Голландии / Науч. ред. д.ю.н., проф. Б.В. Волженкин, пер. с англ. И.В. Мироновой. СПб, 2000. – 430с.
52. Уголовный кодекс Республики Польша / Отв. ред. Э.А. Саркисова, А.И. Лукашов. Пер. с польск. Д.А. Бариловича. Минск, 1998 – 510 с.

53. Хакеров впервые официально приравняли к террористам // Компьютерра. – 2001. – № 7. – С. 3.
54. Чекунов И.Г. Некоторые особенности квалификации преступлений в сфере компьютерной информации // Российский следователь. – 2012. – № 3. – С. 211.
55. Щербович И.А. Проблемы совершенствования правового регулирования в информационной сфере и условия формирования информационного общества // Правовые вопросы связи. – М.: Юрист, 2007, – №1. – С.316.
56. ЭммД. Кибер преступность и закон [Электронный ресурс]. – URL: http:// cybercrime.zp.ua/ viewtopic.php?f=3&t=4776 (дата обращения: 10.02.2011).
57. Computercrimeactof 1978 USA Law [Электронный ресурс]. – URL: http:// docweb.cns.ufl.edu/docs/d0010/d0010.html (дата обращения: 10.02.2011)
58. ComputerFraudandAbuseAct [Электронный ресурс]. – URL:http:// www.law.cornell.edu /uscode/18/1030.html (дата обращения: 10.02.2011)
59. Computer Misuse Act Law of Great Britain. [Электронный ресурс]. – URL: http:// www.legislation.gov.uk/ukpga/1990/18/contents (датаобращения: 10.02.2011)
60. Federal Criminal Code and Rules / Title 18 – Crime and Criminal Procedure – § 1030 Fraud and related activity in connection with computers – (amendment received to February 15, 1999), West Group, St. Paul. Minn, 1999.
61. KasperskySecurityBulletin 2014. Основная статистика за 2014 год. [Электронный ресурс]. – URL: https://securelist.ru/ files/2014/12/Kaspersky–Security–Bulletin–2014–RU.pdf (дата обращения: 30.10.2015)
62. RobertJ. Sciglimpaglia. Computer Hacking: A Global Offense, 3 Pace Y.B. Int'l L.199, 231 (1991); Keith Nicholson. International computer crime: a

global village under siege // New England International & Comparative Law Annual. – 1997. – № 2. New England School of Law, Boston, Massachusetts. [Электронный ресурс]. – URL:http://www.nesl.edu /annual/vol2/computer.htm (дата обращения: 10.02.2011)

63. Robert J. Sciglimpaglia. Computer Hacking: A Global Offense, 3 Pace Y.B. Int'l L.199, 231 (1991); Keith Nicholson. International computer crime: a global village under siege / New England International & Comparative Law Annual. № 2. 1997. New England School of Law, Boston, Massachusetts. [Электронный ресурс]. – URL:http://www.nesl.edu/annual/vol2/computer.htm

64. SurgeonB. Хакеры //Компьютера. – 1996. – № 43. – С. 22.

65. Tackling crime in our digital age: establishing a European Cybercrime Centre: communication from the Commiss. to the Council a. the Europ. Parliament, COM/2012/0140 [Electronic resource]. – URL: http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:HTML.

66. Texas Penal Code – Section 33.02. Breach Of Computer Security [Электронный ресурс]. – URL: http://law.onecle.com/texas/penal/33.02.00.html (дата обращения 10.02.2011)

67. Work Plan of the Inter–American Committee against terrorism: approved at the Fourth Plenary Session, 7 March 2012 [Electronic resource]. – URL: http://www.cicte.oas.org/rev/en/meetings/sessions/12/2012%20WORK%20PLAN/DOC%205%20rev%201%202012%20WORK%20PLAN%20CICTE00752E04.pdf.

68. Международное право. [Электронный ресурс]. – URL: www.pravo.ru/interpravo/legislative/view/27/?page=20

69. Компьютерный червь. [Электронный ресурс]. – URL: www.ru.wikipedia.org/wiki/Blaster (дата обращения: 07.10.2014).

Раздел3 Диссертации и авторефераты на соискание ученной степени

1. Бессонов, В. А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации :дис. ... канд. юрид. наук. – Н. Новгород, 2000. – С. 192.
2. Кесареева, Т. П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет :дис. ... канд. юрид. наук. – М., 2002. – С. 322.
3. Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: диссертация... кандидата юридических наук. – М.:, 2002. – С.295
4. Менжега М.М. Криминалистические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ: дис. ... канд. юрид. наук. – Саратов: РГБ, 2013. – 238 с.
5. Смирнова Т.Г. Уголовно–правовая борьба с преступлениями в сфере компьютерной информации: дис. … канд. юрид. наук. – М., 1999. – 230 с.
6. Ушаков С.И. Преступления в сфере обращения компьютерной информации (теория, законодательство, практика) : дис. … канд. юрид. наук. – Ростов н/Д., 2000. – С. 344.
7. Ходякова Н.В. Личностный подход к формированию информационной культуры выпускников вузов : дис. … канд. юрид. наук. – Волгоград, 1996.
8. Шарков А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: диссертация\кандидата юридических наук Ставрополь: 2004.–С.249

Раздел 4 Постановление высших судебных инстанций и материалы судебной практики

1. Уголовное дело № 1–158 от 2003 г. // Арх. Ангарского районного суда Иркутской области. [Электронный ресурс]. – URL: https://rospravosudie.com/act-507626283/
2. Уголовное дело №1–12/2013 от 14.02.2013 // Арх. Егорьевского городского суда (Московская область). [Электронный ресурс]. – URL: https://rospravosudie.com/act-107303628/
3. Уголовное дело № 1–155/12 от 14.03.2012 // Арх. Первомайского районного суда г. Ижевска [Электронный ресурс]. – URL: https://rospravosudie.com/act-101676606/
4. Уголовное дело №1–483/2012 от 19.07.2017 // Арх. Калининского районного суда г. Челябинска
5. Уголовное дело №1–356/2010 от 14.09.2009 // Арх. Центрального районного суда г. Челябинска