Содержание:

ВВЕДЕНИЕ

Определенные проблемы в борьбе с преступлениями в сфере высоких технологий вызывают следующие обстоятельства. В первую очередь это высокий уровень латентности указанной группы преступлений, о чем говорилось выше. Здесь основной причиной, на наш взгляд, является отсутствие видимых материальных следов приготовления и совершения преступлений.

Следующее обстоятельство – это, конечно, разнообразие способов совершения данных преступлений. Вызывают также определенные трудности определение самого события преступления, включающего в себя место и время его совершения.

Здесь мест совершения преступлений может быть несколько, при этом располагаться они могут, на разных территориях. Их границы, в свою очередь, могут находится на значительном расстоянии друг от друга.

Также вызывает затруднение определения времени совершения преступлений. Например, вредоносная программа может начать действовать, пока не наступит определенное в ее алгоритме событие. Негативным обстоятельством для данных преступлений является легкость уничтожения следов подготовки и совершения преступлений.

Цель: провести анализ технологий совершения компьютерных преступлений

Задачи:

1. Изучить совершения компьютерных преступлений
2. Рассмотреть особенности совершения компьютерных преступлений

Объектом исследования является компьютерные преступления

Предметом исследования является процесс технологий совершения компьютерных преступлений

Теоретической и методологической основой исследования стали книги и статьи следующих авторов работают А.Р. Алавердов, Е.О. Куроедова, О.В. Нестерова. и др.

Структура данной работы включает в себя: введение, двух глав, заключение и список использованной литературы.

Во введении рассмотрены: актуальность темы, определяются предмет, объект, цели и задачи.

В первой главе будут рассмотрены совершения компьютерных преступлений

Во второй главе показаны сущность компьютерных преступлений

В заключении проведены итоги.

ГЛАВА 1. КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

СОВЕРШЕНСТВОВАНИЕ РАССЛЕДОВАНИЯ И РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Мировой опыт показывает, что конкурентоспособность любой национальной экономики, напрямую связана с развитием информационных технологий.

Информационные технологии в настоящее время являются одной из наиболее динамично развивающихся отраслей не только в мире, но и в России. Например, объем мирового рынка информационных технологий оценивается в 1,7 трлн долл. США.

По прогнозам, до 2016 г. рынок продолжит расти в среднем не менее чем на 5 % в год. При этом средний темп роста российского рынка, за последние 10 лет, превосходит средне- мировой и составляет более 10 % в год [1].

Международный союз электросвязи в отчете за 2015 г. сообщил, что количество пользователей сети Интернет возросло до 3,2 млрд чел. За про- шедшие 15 лет количество людей, пользующихся данной сетью, увеличилось в восемь раз [2].

Однако, не смотря на рост российской отрасли информационных технологий, многие как зарубежные, так и отечественные эксперты отмечают ее отставание в данной области от развитых стран в среднем на 15-20 лет.

Одним из негативных последствий процесса информатизации общества является появление так называемой компьютерной преступности.

Для нашей страны данный вид преступлений является сравнительно новым, о чем также свидетельствует сравнительно-правовой анализ действующих в этой сфере нормативно-правовых актов.

Если в США на сегодняшний день действует более 2000 законов и подзаконных актов, касающихся компьютерных преступлений и связанных с ними явлений, аналогичные нормы действуют в ФРГ, Великобритании и Франции, то в России их число не превышает 10 законов [3].

Данные статистики МВД РФ говорят о том, что, начиная с 2006 и по 2011 гг., в России наблюдалось неуклонное трехкратное снижение преступлений в сфере компьютерной информации.

Например, в 2006 г. в России, было зарегистрировано 8889 таких преступлений (7337 – 272 УК РФ, 1549 – 273 УК РФ, 3 – 274 УК РФ), 2007 г. – 7236, 2008 г. – 9010, 2009 г. – 11636, 2010 г. – 7398, 2011 г. – 2698, 2012 г. – 2820, 2013 г. – 2563, 2014 г. – 1739, 2015 г. – 2382 (1396 – 272 УК РФ, 974 – 273 УК РФ, 12 – 274 УКРФ) [4].

При этом общее количество выявленных лиц, совершивших данные преступления, также снижалось в период с 2010 по 2014 г.

В основном это снижение было характерно для такого преступления как неправомерный доступ к компьютерной информации (ст. 272 УК РФ): число выявленных лиц за данные преступления сократилось с 3973 до 290 человек или в более чем 13 раз [5].

Между тем по данным агентства Интерфакс в России количество пользователей Интернет в 2015 г. составило 84 млн чел., а уровень проникновения Интернет среди населения в России в возрасте 16 лет составил 70,4 % [6].

Вышеприведенные данные подтверждают тот факт, что преступления, совершаемые с использованием компьютерной техники, характеризуются высоким уровнем латентности, в среднем 90 % [7] и низким уровнем раскрываемости, что делает «компьютерную преступность» делом очень прибыльным и достаточно безопасным для преступников.

Вместе с тем, по данным бюро специальных технических мероприятий (БСТМ) МВД России в 2015 г. в России было зарегистрировано 11 тыс. преступлений в сфере компьютерной информации [8]. Расхождение данных БСТМ с данными официальной статистики МВД РФ в первую очередь связано с тем, что они в своей

деятельности относят к категории компьютерных преступлений не только предусмотренных главой 28 УКРФ, но и такие, как кража (ст. 158 УКРФ), мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), неправомерный оборот средств платежей (ст. 187 УК РФ), изготовление и незаконный оборот материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242.1 УК РФ).

По словам начальника БСТМ МВД России Мошкова, в этой сфере наблюдаются две устойчивые тенденции. Первая связана с преступлениями, совершаемыми профессионалами, которые создают мощные вирусные программы, способные парализовать работу целых предприятий и организаций.

Вторая группа – это банальные мошенники, размещающие в интернете объявления о продаже оптом товара по низким ценам. «Многие потребители клюют на это, платят деньги, не задумываясь, кому они платят и получат они товар или не получат. Таких мошенничеств на сегодняшний день очень много».

Вышеуказанные данные также свидетельствуют, что если ранее компьютерные преступления в основном совершались лицами, обладающими определенным уровнем специальных познаний в сфере высоких технологий, то в настоящее время, в связи с появлением в Интернете программ, предназначенных для несанкционируемого доступа к информации и инструкций к ним, их может осуществить обычный пользователь.

Анализ статистики преступлений в сфере компьютерной информации констатирует низкую эффективность их расследования и судебного разбирательства.

Раскрытие компьютерных преступлений – это в основном нетрадиционная и порой дискуссионная проблема – как по причине сложности самого факта доказывания, так и в силу несовершенства действующего законодательства.

При этом с использованием компьютерной техники осуществляется воздействие компьютерной информации на саму компьютерную информацию. В этом случае она может выступать, с одной стороны как носитель следов, а с другой стороны – быть следами совершенных преступлений.

Характеризуя следы рассматриваемых, сравнительно новых в практике криминалистики преступлений, необходимо отметить, что в настоящее время среди ученых не сложилось единого мнения в определении их понятия и сущности.

Традиционно, в частной криминалистической теории следообразования, считается, что следами преступления являются любые изменения среды, возникшие в результате совершения в этой среде преступления [9].

При этом все следы преступления, согласно данной теории, классифицируются на материальные и идеальные. К первым, обычно относятся «отпечатки» события на любых материальных объектах: предметах, документах, теле потерпевшего и т. д.

Под идеальными следами понимают отпечатки события в сознании, памяти преступника, потерпевшего, свидетелей и других людей. Однако анализ особенностей формирования следовой картины при совершении преступления в сфере компьютерной информации показывает, что данные следы не вписываются в вышеуказанную классификацию следов.

Поэтому в настоящее время ряд ученых (В. А. Мещеряков и др.), пришли к выводу, о необходимости введения понятия «виртуальные следы», как промежуточных в классификации между материальными и идеальными следами [10].

Данной позиции также придерживается А. К. Шеметов [11]. В свою очередь, Ю. В. Гаврилин, разрабатывая методику расследования преступлений в сфере компьютерной информации, использует термин «информационные следы преступления» [12].

В. А. Милашев в контексте рассмотрения проблем тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ вводит понятие «бинарных следов» [13].

В связи с изложенным, следует констатировать, что в настоящее время возникла необходимости пересмотра в этом отношении, частной криминалистической теории следообразования.

Нельзя не заметить, что при раскрытии и расследовании преступлений в сфере компьютерной информации данные следы имеют решающее значение, поскольку нередко являются единственными и играют важную роль в диагностических исследованиях, позволяющих восстановить механизм совершения преступления.

Как показывает практика, наиболее сложные преступления в сфере компьютерной информации совершаются с использованием возможностей, предоставляемых глобальными компьютерными сетями.

Поэтому при раскрытии и расследовании данных преступлений исследуются следы, которые создаются не только в технических средствах пользователя, но формируются в результате про- хождения информации по самим техническим каналам связи.

Передаваемая по этим каналам информация обычно состоит их двух частей: служебной (задающей маршрут передачи) и содержательной. Для решения задач раскрытия и расследования преступлений основной интерес, несомненно, представляет доступ к содержательной части сообщений, передаваемых с определенного адреса и потенциально включающих сведения о преступной деятельности, однако часто самостоятельную ценность также имеет и служебная часть сообщений, несущая в себе диагностическую информацию о месте, времени и связей преступника.

Если рассматривать следы, образуемые в технических каналах связи, то обычно они представляют собой сведения о сообщениях, передаваемых по данным сетям, которые содержатся в техническом оборудовании оператора связи, и аккумулируются в специальных файлах регистрации, так называемых LOG-файлах.

Например, в этих LOG-файлах могут находится данные о том, кто инициировал данное сообщение, когда и в какое время оно произошло и какие файлы затронуло. По существу в них протоколируется техническая информация, содержащая данные о информационно-технологических процессах обработки информации и представления ее потребителю.

При этом обычно выделяют две основных категории «служебных данных»: данные о пользователе и сведения о сообщении.

Их анализ показывает, что они зачастую имеют разное доказательственное значение в раскрытии и расследовании рассматриваемых преступлений. Например, данные о пользователе могут включать в себя сведения о имени, адресе, дате рождения, номере телефона, адресе поставщика услуг в Интернет, адресе электронной почты, о номере или счете, используемого для осуществления платежных операций по расчетам за услуги провайдера, справочных данных, данных юридического лица, перечне предоставляемых услуг, на которые подписался клиент, IP-адресе, предыдущем IP-адресе пользователя, дополнительном адресе электронной почты и т. д. Тогда как сведения о сообщении содержат уже качественно иную информацию.

Например, это могут быть данные первоначального номера телефона, используемого для связи с LOG- файлом регистрации; даты сеанса связи; информации о времени связи; статических или динамических IP-адресных журналов регистрации провайдера в Интернет и соответствующих телефонных номеров; скорости передачи сообщения; исходящих журналов сеансов связи, включающих тип использованных протоколов, самих протоколов и т. д.

Как указывалось ранее для решения задач раскрытия и расследования преступлений, кроме следов оставляемых служебной частью сообщений, так называемых LOG-файлах рассмотренных выше, особое значение представляют следы преступлений, имеющиеся в содержательной части этих сообщений. Например, файлы, содержащие тексты документов, фотоизображения, видео- и аудио- фрагменты, программное обеспечение и т. п.

Все рассмотренные объекты в свою очередь могут:

а) быть орудиями преступлений (программное обеспечение);

б) сохранять следы преступления (журналы регистрации событий в компьютерной системе);

в) содержать информацию, запрещенную законом к распространению (например, детскую порнографию);

г) относиться к иным объектам, имеющим доказательственное значение (файлы электронной переписки, интернет-адреса посещенных сайтов и т. д.).

Так как до настоящего времени на законодательном уровне вопросы хранения провайдерами вышеуказанных объектов компьютерной информации были не закреплены, то каждый из них регулировал эту деятельность самостоятельно.

Практика показывает, что операторы, являющиеся собственниками указанных сведений, обычно оптимизируют их по-своему усмотрению и сохраняют лишь для обеспечения контроля поступающих за эти услуги платежей.

Из-за разнообразия услуг, предоставляемых компаниями, и связанных с ними разнообразных данных, которые могут быть доступными для сохранения, весьма трудно выделить те их них, которые каждое частное лицо или поставщик услуг должны сохранять.

При этом форматы и объемы этих данных в регистрационных файлах напрямую зависят от технических возможностей самого оператора связи. Высокая конкуренция и сложная экономическая обстановка заставляет их сокращать свои расходы, в частности, и на хранение вышеуказанных данных, что неблагоприятно влияет на раскрытие и рас- следование преступлений в сфере компьютерной информации.

Как указывалось выше, уголовные дела по данным преступлениям в основном возбуждаются либо по сведениям, полученным в ходе осуществления ОРД, либо по факту уже совершенного преступления. Так как расследование преступления по факту его совершения носит ретроспективный характер и в основном производится через сравнительно длительное время после его совершения, то возможность восстановления следователем механизма его совершения и получения при этом доказательств, ввиду не сохранения провайдером вышеуказанных следов, является ничтожной.

Аналогичные сложности возникают у следователя и при расследовании преступлений, возбужденных по данным, полученным в ходе осуществления ОРД [14]. Например, оперативные сотрудники, работая в реальном времени, задокументировали преступную деятельность разрабатываемых лиц, но так как по сложным преступлениям их оперативная разработка осуществляется достаточно продолжительный период времени, то эти данные могут быть не сохранены провайдером и поэтому в ходе проведения уже процессуальных следственных действий не могут быть получены в качестве доказательств по уголовному делу.

Относительно данных случаев судебная практика показывает, что суды не всегда признают копию, даже соответствующим образом документированной компьютерной информации, в данном случае оперативными подразделениями, в качестве доказательств по уголовным делам,

В настоящее время предпринята попытка разрешения данной проблемы в связи с принятием дополнений в Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (в ред. Федерального закона от 06.07.2016 № 374-ФЗ), где в ст. 64 «Обязанности операторов связи и ограничение прав пользователей услугами связи при проведении оперативно- розыскных мероприятий, мероприятий по обеспечению безопасности Российской Федерации и осуществлении следственных действий» введена новелла о том, что операторы связи, обязаны хранить информацию о фактах приема, передачи, доставки и обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей

услугами связи – в течение трех лет.

Из содержания данной нормы следует предположить, что «информация о фактах» – это, по сути, так называемые LOG-файлы рассматриваемые выше и характеризующие следы, оставляемые служебной частью сообщений образуемых в технических каналах связи.

В отношении информации, находящейся в содержательной части этих сообщений – текстовых сообщений, голосовой информации, изображений, звуков, видео-, иных сообщений пользователей услугами связи – законодателем установлен срок их хранения до шести месяцев.

При этом необходимо учесть, что порядок, сроки и объем хранения данной информации будет дополнительно установлен Правительством РФ.

Представляется, что в данном правовом акте заинтересованным компетентным органам необходимо разрешить следующие проблемные вопросы, рассмотренные выше: о единых стандартах сведений о сообщениях, подлежащих хранению, передаваемых по техническим каналам связи; разработать единые требования к объему и номенклатуре, под- лежащей обязательному сохранению компьютерной информации; определить окончательный срок ее хранения; установить порядок ее документирования и передачи правоохранительным органам; разработать правила и порядок их уничтожения при отсутствии надобности.

До того, как Правительство РФ нормативно не урегулирует этот порядок, данная норма, касающаяся информации, находящейся в содержательной части этих сообщений, фактически не будет действовать. Для нее предусмотрена отсрочка вступления в силу на два года: она начнет действовать с 1 июля 2018 г.

Аналогичные правила хранения информации, с теми же оговорками, вводятся в отношении организаторов распространения информации в сети Интернет. Только здесь закон предписывает им хранить информацию о фактах коммуникации сообщений в течение одного года, а их содержании – до полугода.

Кроме того, провайдеры обязаны при использовании в электронных сообщениях пользователей сети Интернет дополнительного кодирования электронных сообщений представлять в ФСБ Российской Федерации информацию, необходимую для декодирования принимаемых, передаваемых электронных сообщений.

В настоящее время этот порядок представления ими в данный орган информации, необходимой для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений пользователей информационно-телекоммуникационной сети Интернет, уже существует и регулируется приказом ФСБ России от 19.07. 2016 г. № 432 [15].

Конечно, в первую очередь отсрочка исполнения данного закона напрямую связана с проблема- ми, возникающими в плане его технического исполнения операторами связи. Например. В сводных материалах по всем операторам связи говорится, что «большой тройке» (МТС, Мегафон, Билайн), Ростелекому и всем остальным суммарно потребуется 40,6 млн накопите- лей HDD объемом 10 ТБ и 30,5 млн SSD-накопителей объемом 1,6 ТБ.

Кроме того, компаниям будут необходимы 565 тыс. штук различного сетевого оборудования: коммутаторов, маршрутизаторов и межсетевых экранов [16].

«Коммерсант» ознакомился с техническими требованиями для съема и хранения в течение полугода всех телефонных разговоров, текстовых сообщений, видео, изображений и другой информации, подготовленными ведущими операторами связи накануне внесения доклада президенту.

Суммарные инвестиции компаний в модернизацию своей инфраструктуры могут, по экспертным оценкам, обойтись не в 2 трлн руб., как полагали операторы, а в несколько раз больше [17].

Определенные операторы в связи с этим предлагают государству самостоятельно создать центр обработки и хранения необходимых данных, ссылаясь на то, что это не их задача.

В связи с этим Президент подписал перечень поручений правительству, который позволит осуществлять мониторинг исполнения закона.

Из него следует, что правительство и ФСБ России в целях «минимизации рисков» должны будут подготовить необходимые нормативно-правовые акты, обращая внимание на уточнение этапов применения норм, «требующих существенных финансовых ресурсов и модернизации технических средств ... с учетом не-обходимости использования отечественного оборудования»; уточнение полномочий правительства и федеральных органов исполнительной власти; при- менение норм об ответственности за использование несертифицированных средств шифрования; разработку и ведение Роскомнадзором реестра сервисов, предоставляющих

средства шифрования; применение норм о расторжении договоров провайдером в случае неподтверждения персональных данных абонентов. Минпромторг и Минкомсвязи должны проанализировать затраты, необходимые для хранения информации пользователей Интернет, а ФСБ к моменту вступления закона в силу должна утвердить порядок сертификации средств шифрования и порядок передачи ключей [18].

На наш взгляд, ссылкам заинтересованных лиц на затратность подлежащих использованию для этого технических средств, не должно придаваться первостепенное значение.

Так как экономический эффект от пресечения и раскрытия преступной деятельности в сфере компьютерной информации будет многократно выше затрат, связанных с сохранением сведений о сообщениях, передаваемых по техническим каналам связи.

Так, по данным ООН, уже сегодня ущерб, на- носимый компьютерными преступлениями, сопоставим с доходами от незаконного оборота наркотиков и оружия.

Только в США ежегодный экономический ущерб от такого рода преступлений составляет около 100 млрд долл. Причем многие потери не обнаруживаются или о них не сообщают [19].

КОМПЬЮЕРНАЯ ПРЕСТУПНОСТЬ

В современном обществе компьютерные технологии используются практически во всех отраслях. Но это не только упрощает нашу жизнь, делает ее более комфортной, но и создает проблемы, связанные, прежде всего с обеспечением информационной безопасности.

Компьютерная преступность впервые появилась в 70-х гг. XX века в США, в России она стала распространять лишь с 90-х гг. XX в.

Она представляет собой любое незаконное, неразрешенное поведение, затрагивающее автоматизированную обработку данных.

С экономической точки зрения, компьютерная преступность довольно выгодное занятие.

Взлом баз данных, банковских систем, доступ к закрытой информации, создание и распространение вредоносных программ, компьютерное хулиганство может принести огромную прибыль взломщику, но и нанести ущерб как человеку, так и государству в целом.

Чтобы минимизировать рост компьютерной преступности, программистами были разработаны различные способы защиты личной информации: технические меры, обеспечивающие защиту от несанкционированного доступа к системе, организационные меры, правовые меры, связанные с разработкой правовых норм, устанавливающих уголовную ответственность за компьютерные преступления.

Сформулировано три принципа информационной безопасности, которая должна обеспечивать:

- целостность данных - защиту от сбоев, ведущих к потере информации.

- конфиденциальность информации.

- доступность для всех авторизованных пользователей.

Ситуация, сложившаяся в обществе, потребовала разработки норм уголовного права, которые предусматривают ответственность за совершение компьютерных преступлений.

Компьютерные преступления, особенно это касается взлома удаленных компьютеров, являются практически идеальной возможностью для преступников совершать свои действия безнаказанно.

Доказать совершение этих преступлений на практике очень сложно, поэтому целесообразно совершенствование законов и более активное применение в России позитивного опыта зарубежных стран в противодействии компьютерной преступности

Компьютерная преступность - совокупность компьютерных преступлений, где компьютерная информация является предметом преступных посягательств, преступлений, которые совершаются посредством общественно опасных деяний, предметом которых является компьютерная информация.

Эти деяния посягают на безопасность сферы компьютерной информации, являются одним из наиболее опасных и вредоносных явлений современного мира, ввиду распространенности на сегодняшний день компьютерных технологий.

I. Хищение денежных средств из финансовых учреждений путем несанкционированного проникновения в компьютерные системы.

II. Скрытый перехват паролей пользователей во время их регистрации.

III. Хищение услуг. Компьютер как орудие преступления:

I. Валютное мошенничество.

II. Кредит на выгодных условиях.

III. Мошенничество со страховками.

IV. Мошенничество с инвестициями.

V. "Восстановление" кредитной карточки.

VI. Хищения с использованием генерированных номеров кредитных карточек.

VII. Извещение о выигрыше.

VIII. Мошенничество с предоплатой.

IX. Злоупотребления на рынке ценных бумаг.

В России контролем над преступностью в Сети занимается специально созданное в ФСБ Управление компьютерной и информационной безопасности. Его задачей является предупреждение, выявление и пресечение преступлений в сфере телекоммуникаций, в том числе в Интернете.

Таким образом, компьютерная преступность непосредственно влияет на экономику, порождая новые виды экономических преступлений.

ГЛАВА 2. СУЩНОСТЬ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

2.1. СОВРЕМЕННЫЕ ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ПОНЯТИЯ, СТРУКТУРЫ И СУЩНОСТИ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Т.М. Лопатина считает, что под компьютерной преступностью следует понимать совокупность совершенных на определенной территории за конкретный период

преступлений (лиц, их совершивших), непосредственно посягающих на отношения по сбору, обработке, накоплению, хранению, поиску и распространению компьютерной информации, а также преступлений, совершенных с использованием компьютера в целях извлечения материальной выгоды или иной личной заинтересованности [11].

Д.В. Добровольский определяет компьютерную преступность как совокупность всех преступлений в сфере информационных технологий, а не только общественно опасных деяний, предметом которых является компьютерная ин- формация [12].

По мнению А.А. Жмыхова, компьютерная преступность — это совокупность преступлений, совершаемых с помощью компьютерной системы или сети, в рамках компьютерной системы или сети и против компьютерной системы или сети.

Таким образом, он относит к компьютерным преступлениям не только преступления в сфере компьютерной информации, но и преступления, связанные с компьютерами, т.е. такие традиционные по характеру преступные деяния, совершенные с помощью вычислительной техники, как кража, мошенничество, причинение вреда и др. [13].

В ряде научных работ встречается упоминание о киберпреступности — юридическом понятии, которое часто употребляется в научном обороте за рубежом и наиболее полно, по мнению авторов данных работ, отражает преступные деяния в сфере компьютерной информации, а также преступления, совершенные с помощью компьютерных устройств, информационно-телекоммуникационных сетей и информационных технологий [14; 15].

Такой подход предполагает, что компьютерная преступность является только частью киберпреступности как более широкого понятия. Отдельные ученые в своих работах отождествляют понятия преступности в Интернете, киберпреступности, компьютерной преступности [16].

Еще один подход предполагает параллельное существование понятий интернет-преступности и компьютерной преступности как части и целого. По мнению, например, Р.И. Дремлюги, не каждое преступление в сфере компьютерной информации представляет собой интернет-преступление, в то же время такие традиционные преступления, как мошенничество, кража, вымогательство и др., совершенные посредством сети Интернет, — это интернет-преступления.

Причем их последствия не обязательно должны наступать в сети Интернет [17]. С учетом описанных выше подходов к пони- манию компьютерной преступности полагаем целесообразным рассматривать данное понятие в узком и широком смысле.

В узком смысле, по мнению авторов, компьютерная преступность представляет собой совокупность преступлений, при совершении которых в качестве основного объекта выступают охраняемые законом общественные отношения в сфере безопасного создания, хранения, обработки и передачи компьютерной информации, а предметом являются компьютерная информация, средства ее хранения, обработки, передачи и защиты, информационно-телекоммуникационные сети.

Компьютерная преступность в широком смысле — это совокупность преступлений, при совершении которых объектом выступают любые общественные отношения в сфере информационных технологий и безопасного функционирования компьютерной информации.

При этом компьютерная информация, средства ее создания, хранения, обработки и передачи (компьютеры, смартфоны, кассовые аппараты, банкоматы, платежные терминалы и иные компьютерные устройства), информационно-телекоммуникационные сети не только являются предметом преступного деяния, но и используются в качестве средства и орудия совершения преступления.

Таким образом, понятие компьютерной преступности в узком смысле охватывает преступления в сфере компьютерной информации, уголовная ответственность за которые предусмотрена в гл. 28 Уголовного кодекса Российской Федерации, а в широком смысле включает в себя понятия киберпреступности, интернет-преступности, преступности в сфере компьютерной информации, преступности в сфере информационных технологий.

Представляется, что такой подход к пониманию компьютерной преступности позволит оценить всю сложность, многообразие, разноуровневость рассматриваемого криминального явления и найти определенный баланс среди существующих научных позиций.

Анализ структуры компьютерной преступности, с точки зрения авторов, следует проводить исходя именно из широкого смысла данного понятия с учетом существующих нормативных, экспертных и доктринальных аспектов.

Например, исследуя «нормативный» под- ход к структуре компьютерной преступности, в Доктрине информационной безопасности Российской Федерации можно выделить следующие противоправные деяния, выступающие угрозами безопасности информационных и телекоммуникационных средств и систем: противоправные сбор и использование информации; нарушение технологии обработки информации; внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия; разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации; уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, теле- коммуникации и связи; уничтожение, повреждение, разрушение или хищение машинных и других носителей информации; несанкционированный доступ к информации, находящейся в банках и базах данных, а также иные деяния.

В свою очередь, заключенная в Будапеште 23 ноября 2001 г. и ратифицированная почти 50 государствами Конвенция Совета Европы о преступности в сфере компьютерной информации закрепляет пять групп компьютерных преступлений, образующих компьютерную преступность:

- преступления против конфиденциальности, целостности и доступности компьютерных данных и систем;

- правонарушения, связанные с использованием компьютерных средств;

- правонарушения, связанные с содержанием компьютерных данных;

- правонарушения, связанные с нарушением авторского права и смежных прав;

- акты расизма и ксенофобии, совершенные посредством компьютерных сетей.

Российская Федерация в силу различных политических, юридических, информационных и иных объективных причин не ратифицировала вышеуказанную конвенцию Совета Европы. Однако, несмотря на данный факт, МВД России, к чьей компетенции относится выявление, рас- следование и раскрытие компьютерных преступлений, придерживается практически аналогичной классификации преступных деяний.

В поддержку данной позиции говорит и то, что российский законодатель в ряде статей УК РФ (например, в ст. 171.2, 228.1, 242, 242.1, 242.2) предусмотрел

специальный квалифицирующий признак — совершение преступления с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть Интернет).

2.2. КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Несмотря на сложившийся «нормативный» подход правоохранительных органов к структуре компьютерной преступности, или, как принято говорить в экспертном сообществе, к «рынку киберпреступности», специалисты и эксперты в сфере информационной безопасности имеют собственную точку зрения на структуру компьютерной преступности в Российской Федерации.

В частности, эксперты международной компании Group-IB, специализирующейся на предупреждении и расследовании киберпреступлений, считают, что основными преступными деяниями, образующими «рынок киберпреступности» в России, являются:

- мошенничество в системах интернет-банкинга; фишинг;

– хищение электронных денег;

– услуги обналичивания иных нелегальных доходов;

- спам (противоправная реклама медикаментов и различной контрафактной продукции, поддельного программного обеспечения, незаконное распространение информации об услугах в сферах обслуживания, образования, туризма и др.); продажа трафика;

– продажа эксплойтов;

– продажа загрузок;

– анонимизация;

– DDoS-атаки.

В свою очередь, специалисты Центра глобальных исследований и анализа угроз «Лаборатории Касперского» (GReAT), анализирующие ежегодное состояние киберпреступности в России и других странах мира, к компьютерным преступлениям (на профессиональном сленге — к компьютерным угрозам), составляющим киберпреступность, относят:

- целевые кибератаки;

– кибершпионаж;

– хактивизм;

– кражу конфиденциальных данных;

– кибервымогательство;

– кибератаки, совершаемые по найму (кибернаемничество);

- использование вредоносного программного обеспечения для мобильных устройств;

- целевой фишинг;

– нарушение тайны частной жизни;

– использование эксплойтов для уязвимостей программного обеспечения;

- кибервымогательство;

– создание и использование ботнетов.

По мнению экспертов лаборатории PandaLabs, входящей в состав международной компании Panda, производящей антивирусное программное обеспечение, в 2015 г. основными преступными деяниями, формирующими компьютерную преступность в России, стали:

- кибершантаж (например, вредоносные – программы типа CryptoLocker, которые после проникновения в компьютер шифруют все типы документов, могущих представлять ценность для пользователя (электронные таблицы, документы, базы данных, фотографии и пр.), после чего киберпреступники начинают шантажировать свою жертву, требуя заплатить выкуп за возможность восстановления файлов);

- направленные кибератаки на информационные ресурсы компаний, организаций, учреждений и т.д.;

- кибератаки на платежные терминалы для – кражи данных банковских карт клиентов;

- APT-атаки (APT — Advanced Persistent – Threats) — так называемые постоянные угрозы повышенной сложности, представляющие собой вид направленных атак, которые нацелены на крупные компании или стратегически важные институты; взлом подключенных к Интернету – устройств («интернет-вещей»), от IP-камер и до принтеров, которые, являясь частью Интернета, обладают программным обеспечением, что делает их весьма уязвимыми для взлома киберпреступниками и причинения ущерба пользователю;

- атаки на смартфоны, а также иные мобильные устройства с целью кражи паролей и данных пользователей.

Таким образом, мнение экспертного сообщества о структуре компьютерной преступности и компьютерных преступлениях несколько отличается от «нормативного» подхода правоохранительных органов, так как основывается на программно-технических критериях, однако не противоречит ему, поскольку практически все так называемые киберугрозы подпадают под действие УК РФ.

Исследование научной литературы по рассматриваемой теме также показывает неоднозначность мнений ученых относительно структуры компьютерной преступности в России.

Например, Д.К. Чирков и А.Ж. Саркисян в структуре компьютерной преступности выделяют только те преступные деяния, которые учитываются ГИАЦ МВД России как преступления, совершенные в сфере телекоммуникаций и компьютерной информации [18].

По мнению М.Б. Эмирова, А.Д. Саидова, Д.А. Рагимханова, к наиболее распространенным видам преступлений в глобальных компьютерных сетях можно отнести промышленный шпионаж, саботаж, вандализм, спуфинг (взлом паролей), мошенничество [19].

Другие авторы исходят из сложной структуры компьютерной преступности и рассматривают входящие в нее преступные деяния по нескольким критериям: объект, предмет посягательства, способ совершения и т.п. [11].

Например, по объекту посягательства выделяются следующие группы компьютерных преступлений: преступления против конфиденциальности, целостности, доступности компьютерных данных и компьютерных сетей; экономические компьютерные преступления; компьютерные преступления против личных прав и неприкосновенности частной сферы; компьютерные преступления

против общественных и государственных интересов [21].

По мнению авторов, для оценки структуры компьютерной преступности в России пред- почтительней использовать классификацию и статистику совершенных компьютерных преступлений, применяемые правоохранительными органами, т.е. «нормативный» подход.

Это обусловлено тем, что существующая методика учета зарегистрированных, расследованных, приостановленных и прекращенных уголовных дел по преступлениям данного вида уже апробирована временем, а уголовная статистика складывается из ежедневно поступающих данных от территориальных органов ФСБ, МВД,

Следственного комитета Российской Федерации. В силу этого правоохранительные органы обладают бóльшим объемом аналитической информации о структуре и масштабах компьютерной преступности в России, чем экспертное или научное сообщество, что не умаляет роли последних в исследовании данного криминального явления.

Так, на основании статистических данных ГИАЦ МВД России можно утверждать, что примерная структура российской компьютерной преступности выглядит следующим образом:

- нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан (ч. 1 ст. 138 УК РФ) — 0,40 %; незаконный оборот специальных технических средств, предназначенных для негласного получения информации (ст. 138.1 УК РФ), — 2,40 %;

- неправомерный доступ к компьютерной – информации (ст. 272 УК РФ) — 21,20 %;

- создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) — 9,80 %;

- нарушение правил эксплуатации средств – хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) — 0,02 %;

- нарушение авторских и смежных прав, – совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 146 УК РФ), — 11,10 %; кража, совершенная с использованием – компьютерных и телекоммуникационных технологий (ст. 158 УК РФ), — 9,78 %;

- мошенничество в сфере компьютерной – информации (ст. 159.6 УК РФ) и мошенничество, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 159 УК РФ), — 30,20 %;

- причинение имущественного ущерба путем обмана или злоупотребления доверием, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 165 УК РФ), — 0,20 %;

- незаконные организация и проведение – азартных игр, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 171.2 УК РФ), — 0,20 %;

- незаконные получение и разглашение – сведений, составляющих коммерческую, налоговую или банковскую тайну, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 183 УК РФ), — 2,80 %;

- незаконные изготовление и оборот порнографических материалов или предметов, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 242 УК РФ), — 6,10 %;

- изготовление и оборот материалов или – предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 242.1 УК РФ), — 5,30 %;

- использование несовершеннолетнего в – целях изготовления порнографических материалов или предметов, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 242.2 УК РФ), — 0,50 %7 .

Как видно, среди преступных деяний, образующих компьютерную преступность в Российской Федерации, преобладают:

- мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и мошенничество, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 159 УК РФ), — 30,20 %;

- неправомерный доступ к компьютерной информации (ст. 272 УК РФ) — 21,20 %; нарушение авторских и смежных прав, совершенное с ис- пользованием компьютерных и телекоммуникационных технологий (ст. 146 УК РФ), — 11,10 %;

- создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) — 9,80 %;

- кража, совершенная с использованием компьютерных и телекоммуникационных технологий (ст. 158 УК РФ), — 9,78 %.

Таким образом, наибольший удельный вес среди совершенных компьютерных преступлений приходится на мошенничество в сфере компьютерной информации и преступления в сфере компьютерной информации, которые в настоящее время составляют основу компьютерной преступности в России.

Рассуждая о сущности компьютерной преступности в Российской Федерации, можно заключить, что компьютерная преступность:

- является разновидностью российской – преступности, существующей наравне с экономической, насильственной, коррупционной, экологической и иными видами преступности;

- тесно взаимосвязана с другими видами преступности в Российской Федерации, поскольку преступления в сфере компьютерной информации часто выступают способом совершения других уголовных деяний (кража, вымогательство, незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, государственная измена, шпионаж и др.).

- Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации носит высокотехнологичный характер, что вызвано использованием IT-технологий, информационно-телекоммуникационных сетей, компьютерных устройств, носителей компьютерной информации и т.п., которые выступают орудиями и средствами совершения компьютерных преступлений;

- обладает высокой степенью латентности, которая составляет от нескольких десятков до нескольких тысяч процентов по разным видам преступных деяний, что обусловлено различными объективными факторами (нежелание жертв компьютерных преступлений обращаться в правоохранительные органы, незаметность компьютерных преступлений для большинства населения в силу их совершения в виртуальной среде, сложность выявления компьютерных преступлений при отсутствии необходимого количества специалистов в правоохранительных структурах и т.д.);

- носит высокоорганизованный характер и тесно связана с организованной преступностью, так как значительное количество компьютерных преступлений (DDoS-атаки, банкинг, фишинг, создание ботнетов и др.) совершается организованными преступными группами;

- имеет «профессиональный» характер, – так как лица, совершающие компьютерные преступления, обладают преступной специализацией, не совершая иных видов преступных деяний; получают преступный доход (прибыль) в результате преступной деятельности;

- имеют необходимые знания, умения, навыки в сфере IT-технологий для совершения преступления; придерживаются определенных правил, законов, понятий и терминологии, позволяющих им общаться, обмениваться опытом и находить единомышленников; характеризуется трансграничностью, так – как киберпространство существует вне государственных границ и, будучи общедоступным, позволяет преступнику, находящемуся на территории одного государства, совершать преступления в отношении лиц, находящихся в другом государстве; носит транснациональный характер, так – как компьютерные преступники в силу своей принадлежности к компьютерному «андеграунду» для получения преступных доходов, облегчения совершения преступных деяний на территории двух и более государств вынуждены, независимо от национальности, объединяться в международные преступные группы;

- находится в состоянии динамического – развития, что обусловлено постоянным совершенствованием существующих и созданием новых IT-технологий, вовлечением в информационные отношения новых участников, расширением киберпространства за счет увеличения числа пользователей сети Интернет, мобильных компьютерных устройств, переходом к электронному документообороту все большего количества организаций, предприятий, учреждений;

- обрела черты экономической преступности, так как большинство компьютерных преступлений совершается в банковско-финансовом или корпоративном секторе (интернет-банкинг, банковский фишинг, кибервымогательство и т.д.), а деятельность преступников направлена на извлечение доходов (прибыли);

- трансформируется в преступность политического характера, что связано с активизацией противоправной деятельности в киберпространстве Российской Федерации представителей хактивистского движения, спецслужб и силовых структур зарубежных государств, международных экстремистских и террористических организаций (DDoS-атаки на правительственные сайты, кибершпионаж в отношении информационных ресурсов органов государственной власти, силовых ведомств, предприятий оборонно-промышленного комплекса, дипломатических представительств, распространение в сети Интернет экстремистских материалов, вербовка новых членов в террористические

организации и т.д.).

ЗАКЛЮЧЕНИЕ

Одна из социальных проблем современного технократического общества — появление компьютерной преступности, причиняющей колос- сальный вред общественным отношениям в информационной сфере.

Ее возникновение стало возможным из-за того, что граждане, используя компьютерные устройства в личных, производственных или служебных целях, имеют слабое представление о программировании и возможностях программного обеспечения, особенностях функционирования средств создания, хранения, обработки, передачи, защиты компьютерной информации, тем самым становясь потенциальными жертвами компьютерных преступников.

Поэтому все большую актуальность приобретает вопрос информационной безопасности физических и юридических лиц, т.е. их защиты от несанкционированного доступа к компьютерной информации, вредоносных компьютерных программ и иных компьютерных угроз.

На простой, казалось бы, вопрос, что следует понимать под компьютерной преступностью, в научном сообществе нет однозначного ответа, и до сих пор ведутся многочисленные дискуссии о содержании и значении данного юридического понятия.

Одни авторы полагают, что компьютерная преступность — это совокупность преступлений, при совершении которых предметом преступных посягательств выступает компьютерная информация, и отождествляют при этом понятия компьютерного преступления и преступления в сфере компьютерной информации.

ЛИТЕРАТУРА

1. Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации: (по материалам Республики Дагестан) : дис. ... канд. юрид. наук : 12.00.08 / М.С. Гаджиев. — Махачкала, 2004. — 168 с.
2. Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью : дис. … канд. юрид. наук : 12.00.08 / Д.В. Добровольский. — М., 2005. — 218 с.

3. Дремлюга Р.И. Интернет-преступность / Р.И. Дремлюга. — Владивосток : Изд-во Дальневост. ун-та, 2008. — 240 с.
4. Евдокимов К.Н. Политические факторы компьютерной преступности в России / К.Н. Евдокимов // Информационное право. — 2015. — № 1. — С. 41–47.
5. Ефремова М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно- телекоммуникационных технологий / М.А. Ефремова. — М. : Юрлитинформ, 2015. — 200 с.
6. Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение : дис. … канд. юрид. наук : 12.00.08 / А.А. Жмыхов. — М., 2003. — 178 с.
7. Згадзай О. Э., Казанцев С. Я., Казанцева Л. А. Информатика для юристов: монография / под общ. ред. С. Я. Казанцева. М.: Мастерство, 2001. С. 235. 4
8. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ / И.Г. Смирнова, К.Н. Евдокимов, О.А. Егерева [и др.] ; под науч. ред. И.Г. Смирновой. — М. : Юрлитинформ, 2016. — 312 с.
9. Кривенцов П. А. Латентная преступность России: криминалистическое исследование: автореф. дисс. … канд. юрид. наук, 2014.
10. Криминология : учебник / под общ. ред. А.И. Долговой. — 4-е изд., перераб. и доп. — М. : Норма : Инфра-М, 2013. — 1008 с.
11. Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности : дис. ... д-ра юрид. наук : 12.00.08 / Т.М. Лопатина. — М., 2007. — 418 с.
12. Номоконов В.А. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. — 2012. — № 24. — С. 45–55.
13. Номоконов В.А. Киберпреступность: прогнозы и проблемы борьбы / В.А. Номоконов, Т.Л. Тропина // Библиотека криминалиста. — 2013. — № 5 (10). — С. 148–160.
14. Рассолов И.М. Право и Интернет. Теоретические проблемы / И.М. Рассолов. — М. : Норма, 2003. — 332 с.
15. Степанов-Егиянц В.Г. Проблемы разграничения неправомерного доступа к компьютерной информации со смежными составами / В.Г. Степанов-Егиянц // Право и кибербезопасность. — 2014. — № 2. — С. 27–32.
16. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : дис. … канд. юрид. наук : 12.00.08 / Т.Л. Тропина. — Владивосток, 2005. — 235 с.
17. Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности : авто- реф. дис. … канд. юрид. наук :

12.00.08 / И.Г. Чекунов. — М., 2013. — 22 с.
18. Чирков Д.К. Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны / Д.К. Чирков, А.Ж. Саркисян // Актуальные проблемы экономики и права. — 2013. — № 3. — С. 219–226.
19. Эмиров М.Б. Борьба с преступлениями в глобальных компьютерных сетях / М.Б. Эмиров, А.Д. Саидов, Д.А. Рагимханов // Юридический вестник Дагестанского государственного университета. — 2011. — № 2. — С. 63–66.