ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ УНИВЕРСИТЕТ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ ИМЕНИ В.Я. КИКОТЯ»

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, СОВЕРШАЕМЫХ ПРОТИВ СОБСТВЕННОСТИ

Сборник научных трудов

Московский университет МВД России
имени В.Я. Кикотя, 2019

ISBN 978-5-9694-0738-1

Москва
2019

ББК 67.52
Р24

Рецензенты:

старший преподаватель по ОВД 3 отдела управлению организованной преступной деятельности СД МВД России ***Н. Е. Клишкина****;*
начальник 3 ОРЧ УУР ГУ МВД России ***Э. Н. Богатырев***.

Р24 **Расследование преступлений в сфере компьютерной информации, совершаемых против собственности** : сборник научных трудов / А. В. Пузарин, М. А. Иванов, Д. Н. Захаров и др. – М. : Московский университет МВД России имени В.Я. Кикотя, 2019. – 120 с. − 1 электронный опт. диск (CD-R). − Системные требования: CUP 1,5 ГЦ; RAM 512 Мб; Windows XP SP3; 1 Гб свободного места на жестком диске.
ISBN 978-5-9694-0738-1

В сборнике статей содержатся материалы по вопросам кибербезопасности, информационной безопасности и расследования преступлений в сфере компьютерных технологий. Является базисом для разработки научно-исследовательских работ курсантов и слушателей для участия в конкурсах научно-исследовательских работ.

ББК 67.52

ISBN 978-5-9694-0738-1

Научное электронное издание

В авторской редакции
Корректор *Степанова А. А.*
Компьютерная верстка *Татариновой О. А.*
6,97 усл.-печ. л.

Московский университет МВД России имени В. Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12
http: //www.mosu.mvd.ru, e-mail: support_mosu@mvd.ru

СОДЕРЖАНИЕ

Лустин В. И.[1],

старший преподаватель кафедры информационной безопасности учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя

ПРАВОВЫЕ АСПЕКТЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Информация и информационные отношения как объект преступных посягательств. Понятие информационных преступлений. Уголовное законодательство об информационных правоотношениях. Предваряя рассмотрение содержания киберпреступлений, следует, прежде всего, уяснить сущность «информации» как нового криминалистического объекта с особым правовым регулированием, а также иных понятий, связанных с ним. Кроме того, необходимо подвергнуть анализу предпосылки и сопутствующие явления, способствующие совершению указанных преступных деяний, а также правовую основу борьбы с ними. Наряду с этим требуется уяснить наиболее важные понятия, касающиеся специального инструмента обработки информации – компьютера. Такая последовательность рассуждений позволит использовать специфическую научную терминологию для составления криминалистической характеристики преступлений в сфере компьютерной информации. При рассмотрении данных вопросов постараемся придерживаться стандартных международных подходов, сформулированных в рассмотренных выше правовых документах, в первую очередь, – Конвенции Совета Европы о киберпреступности.

В советский период считалось, что компьютерная преступность – это явление, присущее только зарубежным капиталистическим странам, и по причине слабой компьютеризации нашего общества у нас она отсутствует. Данное обстоятельство и привело к отставанию нашей страны в научных исследованиях по этой проблеме. Только к середине 1990-х гг. появились научные труды по проблемам борьбы с компьютерной преступностью, где рассматривались уголовно-правовые и криминологические аспекты этого криминального явления.

«Информационная революция» застигла нашу страну в сложный экономический и политический период и потребовала срочного нормативного регулирования проблем, возникающих в данной области. Вместе с тем, как известно, правовые механизмы включаются и становятся эффективными лишь после того, как общественные отношения, подлежащие регулированию, в достаточной мере стабилизируются. В последнее время в результате принятия ряда базовых нормативных актов в области регулирования информационных отношений наступил относительно благоприятный период для применения этих механизмов на практике.

Любые формы завладения сведениями ограниченного доступа без непосредственно выраженного согласия обладателя последних и их несанкционированного использования (за исключением случаев, прямо указанных в законе) являются неправомерными, поскольку уровень доступности информации определяется законом или непосредственно самим ее обладателем. Неправомерное использование информации, как уже подчеркивалось в ходе предыдущих лекций, наказуемо. Причем, наряду с гражданско-правовыми и административно-правовыми мерами, к нарушителям информационных отношений могут быть применены и уголовно-правовые санкции. Таким образом, информация и информационные отношения становятся соответственно предметом и объектом преступления. Преступные деяния данной категории охватываются общим понятием – *информационные преступления.*

Следует напомнить, что уголовно-правовые санкции предусмотрены для защиты целого ряда сведений ограниченного доступа и результатов интеллектуальной деятельности: государственной тайны (ст.ст. 275, 276, 283, 2831, 284 УК РФ), тайны частной жизни (ст. 137 УК РФ), тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), тайны усыновления (ст. 155 УК РФ), коммерческой, банковской, налоговой тайн (ст. 183 УК РФ), объектов авторского права и смежных прав, объектов патентного права, средств индивидуализации юридических лиц, товаров, работ, услуг и предприятий (ст.ст. 146, 147, 180 УК РФ), и др. Все составы преступлений, предусмотренные указанными статями Уголовного кодекса РФ, носят информационный характер.

К разновидностям информационных преступлений относятся компьютерные преступления, имеющие на этом общем фоне особую специфику. Следует отметить, что до настоящего времени в отечественной криминалистической науке все еще не сформировано четкого определения понятия компьютерного преступления, как нет его и в международной правовой практике.

В настоящее время среди российских ученых дискутируются различные точки зрения относительно классификации компьютерных преступлений. Сложности, связанные с однозначной формулировкой этих понятий, возникают, по-видимому, как по причине невозможности выделения единого объекта преступного посягательства, так и ввиду множественности предметов преступных посягательств с точки зрения их уголовно-правовой охраны.

Действующее российское законодательство в сфере противодействия компьютерной преступности под компьютерными преступлениями понимает предусмотренные уголовным законом общественно опасные деяния, при осуществлении которых предметом преступного посягательства оказывается машинная информация, используемая в различных сферах деятельности машинная информация одновременно рассматривается и в качестве орудия преступления. Наряду с ней в разряд орудий совершения подобных преступлений попадают сам компьютер, а также информационно-телекоммуникационная сеть (вычислительная среда, в которой эта информация циркулирует). Причем машинная информация, циркулирующая в вычислительной среде, должна быть зафиксирована на соответствующем носителе в форме, доступной для восприятия ЭВМ или передачи по телекоммуникационным каналам.

Как следует из вышесказанного, компьютер при совершении данных преступлений может выступать одновременно и в качестве предмета, и в качестве орудия совершения преступления. Данное свойство последнего определяется технологической спецификой его построения (архитектурой), под которой понимается концепция взаимодействия элементов сложной структуры, включающей в себя компоненты логической, физической и программной подсистем.

«Во многих случаях преступления, которые мы можем, согласно нашему общему определению, назвать «киберпреступлениями», –

в действительности уже существуют, за исключением того, что при их совершении так или иначе используется компьютерная сеть. Таким образом, человек мог использовать Интернет для построения финансовых пирамид, рассылки «писем счастья», привлечения клиентов в притоны, сбора ставок для нелегальных азартных игр, скачивания детской порнографии. Все эти деяния уже являются незаконными во многих юрисдикциях и могли бы быть совершены без использования компьютерной сети. «Кибераспект» не является необходимым элементом преступления, а служит лишь средством совершения преступления. Компьютерные сети предоставляют преступникам новые способы совершения «старых» преступлений. Существующие законы, запрещающие подобные действия, могут применяться к лицам, совершившим эти деяния с помощью компьютеров и сетей, точно так же, как и к тем, кто совершил их без использования новых технологий.

В других случаях преступление является уникальным и обязано своим существованием появлению сети Интернет. В качестве примера можно привести незаконный доступ. Он может быть уподоблен незаконному проникновению в помещение, но признаки незаконного компьютерного доступа отличаются от признаков физического взлома. В определении, данном в законах, взлом и проникновение обычно требуют физического входа на территорию помещения, признака, который не представлен в преступлении, произошедшем в киберпространстве. Таким образом, новые законы должны учитывать эту специфику»[1].

С учетом сказанного можно выделить следующие характерные особенности компьютерного преступления:

1) неоднородность предмета посягательства;

2) особенности машинной информации, рассматриваемой как в качестве предмета, так и в качестве средства (орудия) совершения преступления;

3) многообразие предметов и средств преступного посягательства;

4) особенности компьютера и компьютерной сети в целом, рассматриваемых и в качестве предметов, и в качестве средств совершения преступления.

---

[1] Scene of the Cybercrime: Computer Forensics Handbook by Debra Littlejohn Shinder, Ed Tittel (Editor), 2002 / пер. с англ. Т. Тропиной. Владивосток: ВЦИОП при Юридическом институте ДВГУ, 2003. С. 6–7.

С точки зрения криминалистических аспектов проблемы, под компьютерными преступлениями следует понимать предусмотренные уголовным законом общественно опасные деяния, совершенные с использованием средств электронно-вычислительной (компьютерной) техники.

В качестве основного классифицирующего признака принадлежности преступления к разряду компьютерных следует выделить словосочетание «использование средств компьютерной техники», независимо от того, на какой стадии преступления она использовалась: при его подготовке, в ходе совершения, или для сокрытия. Для обоснования этого утверждения более детально рассмотрим отдельные элементы вышеуказанного определения.

Первая его часть – общественно опасные деяния – не требует особых пояснений и зависит лишь от того, как они будут называться (квалифицироваться) согласно формулировкам уголовного закона[1]. Ранее уже отмечалось, что в «чистом» (обособленном) виде эти деяния встречаются крайне редко. Как правило, они совершаются в совокупности с иными преступлениями и имеют факультативный характер. Чаще всего на территории России и стран СНГ компьютерная информация используется для совершения таких общеуголовных преступлений, как нарушение интеллектуальных прав (ст.ст. 146, 147, 180 УК РФ); подделка, изготовление или сбыт поддельных документов, штампов, печатей и бланков (ст. 327 УК РФ); изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов (ст. 187 УК РФ); изготовление или сбыт поддельных денег или ценных бумаг (ст. 186 УК РФ); уклонение от уплаты налогов с организаций (ст. 199 УК РФ); нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ); незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну (ст. 183 УК РФ), и др.

Отдельно следует выделить такие виды преступлений, внесенных в Уголовный кодекс РФ на основании ФЗ РФ от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс РФ и отдель-

[1] Мелик Э. Компьютерные преступления: информационно-аналитический обзор // url: http://www.melik.narod.ru/glava_1.html (дата обращения: 06 февраля 2008 г.).

ные законодательные акты Российской Федерации»[1], как мошенничество с использованием платежных карт (ст. 1593 УК РФ) и мошенничество в сфере компьютерной информации (ст. 1596 УК РФ). По своему содержанию они весьма приближены к положениям ст. 8 Конвенции о киберпреступности.

Вторая часть анализируемого понятия компьютерного преступления требует более подробной детализации. Средства компьютерной техники по своему функциональному назначению можно подразделить на две основные группы: 1) аппаратные средства (HardWare); 2) программные средства (SoftWare). Известно, что под аппаратными средствами компьютерной техники понимаются механические, электрические и электронные технические устройства, используемые для систематизации и обработки данных. К ним относятся:

1) персональный компьютер (ПЭВМ или ПК) – комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач;

2) периферийное оборудование – аппаратные средства, имеющие подчиненный кибернетический статус в информационной системе (любое устройство, обеспечивающее передачу данных и команд между процессором и пользователем относительно определенного центрального процессора, комплекс внешних устройств ЭВМ, не находящихся под непосредственным управлением центрального процессора);

3) физические носители магнитной информации.

Следует напомнить, что под программными средствами компьютерной техники в соответствии с положениями ст. 1261 ГК РФ понимается представляемая в объективной форме совокупность данных и команд, предназначенная для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, получаемые в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения. К ним относятся:

1) программное обеспечение: совокупность управляющих и обрабатывающих программ, предназначенных для планирования и организации вычислительного процесса автоматизации программирования

[1] Российская газета. – 2012. – 3 дек.

и отладки программ решения прикладных задач, состоящее из следующих элементов:

– системных программ (операционные системы, программы технического обслуживания: драйверы, программы – оболочки, вспомогательные программы – утилиты);

– прикладных программ (комплекса специализированных программ), предназначенных для решения определенного класса задач, например, редакторы текстов, антивирусные программы и системы, программы защиты от несанкционированного доступа, табличные процессоры, СУБД, графические редакторы, системы автоматизированного проектирования (САПР), интегрированные системы, бухгалтерские программы, программы управления технологическими процессами, автоматизированные рабочие места (АРМ), библиотеки стандартных программ и т. п.;

– инструментальных программ (систем программирования), состоящих из языков программирования: Turbo C, Turbo C++, TurboPascal, Microsoft C, Microsoft Basic, Clipper и др., и трансляторов – комплекса программ, обеспечивающих автоматический перевод с алгоритмических и символических языков в машинные коды;

2) электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети, фигурирующая в п. 10 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации»[1].

Особое место среди прочих компьютерных преступлений занимают преступления в области компьютерной информации, которым посвящена отдельная 28-я глава уголовного кодекса РФ. На сегодняшний день к ним отнесены неправомерный доступ к компьютерной информации (ст. 272); создание, использование и распространение вредоносных компьютерных программ (ст. 273) и нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274).

[1] Мелик Э. Информация и информационные отношения как новый криминалистический объект // URL: http://melik.narod.ru/glava_1.html (дата обращения: 24 августа 2012 г.).

Русскевич Е. А.[1],

доцент кафедры уголовного права учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя, кандидат юридических наук

НОВОЕ ПОСТАНОВЛЕНИЕ ПЛЕНУМА ВЕРХОВНОГО СУДА РОССИЙСКОЙ ФЕДЕРАЦИИ О КВАЛИФИКАЦИИ МОШЕННИЧЕСТВ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

К числу наиболее значимых, на наш взгляд, следует отнести следующие разъяснения Пленума по поводу квалификации мошенничества в сфере компьютерной информации. Прежде всего, в п. 1 нового постановления Пленум Верховного Суда Российской Федерации по сути поставил точку в дискуссии относительно способа совершения преступления, предусмотренного ст. 159.6 УК РФ. Интерпретировав разъяснение высшей судебной инстанции, следует сделать вывод, что обман или злоупотребление доверием не являются способами мошенничества в сфере компьютерной информации. Таким образом, получил поддержку подход, согласно которому преступление, предусмотренное ст. 159.6 УК РФ, характеризуется своим специфическим способом, не вписывающимся ни в одну из традиционно выделяемых форм хищения. Нельзя не отметить, что в первоначальной редакции п. 1 постановления Пленума состоял из двух абзацев и содержал специальное указание на то, что мошенничество в сфере компьютерной информации совершается не путем обмана или злоупотребления доверия, а иным способом – путем вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации. Исключение данного разъяснения редакционной коллегией было мотивировано тем, что в теории уголовного права нет общепринятой позиции относительно того, является ли такое вмешательство разновидностью обмана или самостоятельным способом мошенничества[2].

Как представляется, проблема оценки манипуляций с компьютерной информацией как особого рода обмана имеет искусственный характер

---

[1] © Русскевич Е. А., 2019.

[2] Заседание Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. // Электронный ресурс: http://www.vsrf.ru/press_center/news/26093/ (дата обращения: 6 декабря 2017 г.).

и обусловлена изначально неудачной редакций ст. 159.6 УК РФ. Название данной нормы, к сожалению, представляет собой не адаптированный к российской правовой системе, почти автоматизированный перевод ст. 8 «Компьютерное мошенничество» (Computerfraud) Конвенции «О преступности в сфере компьютерной информации» (Будапешт, 23 ноября 2001 г.)[1]. Учитывая многовековую отечественную традицию толкования природы мошенничества и обмана как способа его совершения, изначально правильнее было бы предусмотреть ответственность за «хищение в сфере компьютерной информации», как это реализовано, например, в ст. 212 УК Республики Беларусь[2]. В сложившихся же условиях в ст. 159.6 УК РФ мы имеем новую форму хищения в сфере информационных технологий, которая мошенничеством не является, но называется таковым.

Пленум Верховного Суда Российской Федерации также сделал обоснованный вывод, что мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа или создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст.ст. 272, 273, 274.1 УК РФ. Соглашаясь с этим разъяснением, по существу, необходимо отметить следующее. Раскрывая в п. 20 содержание вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации, Пленум указывает, что оно «нарушает установленный процесс обработки, хранения, передачи компьютерной информации». Так или иначе, в данной части речь идет о причинении вреда отношениям по обеспечению безопасности компьютерных данных и систем, т. е. налицо двуобъектность мошенничества в сфере компьютерной информации, которая по правилам квалификации преступлений должна была бы исключать совокупность. Вместе с тем, она ее не исключает ввиду того, что нормы главы 28 УК РФ содержат более строгие санкции. Как справедливо отмечает П. С. Яни, даже если рассматривать преступление, предусмотренное ст. 272 УК РФ, в качестве способа совершения мошенничества в сфере

---

[1] Конвенция о преступности в сфере компьютерной информации (est № 185) от 23 ноября 2001 г. // Режим доступа: СПС «КонсультантПлюс».

[2] Уголовный Кодекс Республики Беларусь: с изм. и доп. на 5 января 2015 г. Минск : Нац. Центр правовой информ. Респ. Беларусь, 2015. С. 98.

компьютерной информации, содеянное должно квалифицироваться по совокупности ст. 159.6 УК РФ и названной нормы[1].

Выделяя ст. 159.6 УК РФ, законодатель, к сожалению, проигнорировал доктринальные пролегомены о повышенной опасности мошенничества в сфере компьютерной информации (ввиду его латентности, трансграничности, сверхтаргетированности и т. д.). Сравнительный анализ показывает, что данное преступление обладает меньшей степенью общественной опасности в сравнении как с общим мошенничеством (ст. 159 УК РФ), так и преступлениями в сфере компьютерной информации. Обладает, конечно же, формально, а не фактически. О необходимости устранения такого противоречия уже отмечалось в науке уголовного права[2].

Пожалуй, наиболее востребованным на правоприменительном уровне будет разъяснение Пленума, сформулированное в п. 21, согласно которому в тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и т. п.), такие действия подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. Таким образом, новые формы посягательства преимущественно на электронные денежные средства граждан Пленум предложил квалифицировать по старинке – как тайное хищение чужого имущества. Подобный подход вызывает ряд вопросов и требует некоторых замечаний. Прежде всего, объективно не всякое хищение, совершенное с использованием учетных данных, можно будет квалифицировать как кражу. Так, если соответствующая команда на списание денежных средств была отправлена открыто, в присутствии третьих лиц, не являющихся близкими виновному и осознававшими противоправный характер совершаемых действий, содеянное будет необхо-

---

[1] Яни П. С. Специальные виды мошенничества // Законность. – 2015. – № 8. – С. 40.

[2] Например: Лопашенко Н. А. Законодательная реформа мошенничества: вынужденные вопросы и вынужденные ответы // Криминологический журнал байкальского государственного университета экономики и права. – 2015. – Т. 9 – № 3. – С. 504 – 513; Русскевич Е. А. Наказание за мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) // Библиотека уголовного права и криминологии. – 2016. – № 5 (17). – С. 180–182 и др.

димо квалифицировать как грабеж. Более того, если возможность воспользоваться телефоном потерпевшего возникла в результате нападения, сопряженного с применением насилия, опасного для жизни или здоровья потерпевшего, либо с угрозой его применения, и манипуляции с «мобильным банком» были осуществлены непосредственно в процессе нападения, содеянное будет охватываться составом разбоя. Полагаем, что как кражу можно будет квалифицировать действия лица, которое отправило команду на перевод денежных средств позднее, после нападения и завладения телефоном потерпевшего,

В некотором смысле анализируемое разъяснение Пленума нивелирует смысл и значение самостоятельного определения ст. 159.6 УК РФ. Оно распространяет действие ст. 158 УК РФ на такие часто встречающиеся в сети Интернет посягательства на электронные денежные средства граждан, совершенные в результате завладения учетными данными потерпевшего путем обмана («социальная инженерия»), создания сайтов-двойников («фишинг»), незаконного перевыпуска сим-карт и использования вредоносного программного обеспечения.

С учетом последних разъяснений Пленума, как мошенничество в сфере компьютерной информации следует оценивать хищения денежных средств граждан и организаций в результате использования вредоносных компьютерных программ. Так, например, Бузин было сужден за совершение преступлений, предусмотренных ч. 2 ст. 273 УК РФ, ч. 2 ст. 272 УК РФ, ч. 2 ст. 159.6 УК РФ[1]. В соответствии с приговором суда, Бузин, обладая достаточными познаниями в области компьютерной техники и навыками работы в сети Интернет, приобрел путем копирования на накопитель своего персонального компьютера программы, заведомо приводящие к несанкционированному доступу, уничтожению, блокированию, модификации либо копированию информации. Функционально указанные программы были предназначены для управления удаленным компьютером по сети. После этого Бузин отправил на адрес электронной почты, ис-

[1] В п. 29 нового постановления Пленум лишь воспроизвел прежний подход, согласно которому под лицами, использующими свое служебное положение при совершении мошенничества, следует понимать должностных лиц, обладающих признаками, предусмотренными примечанием 1 к ст. 285 УК РФ, государственных или муниципальных служащих, не являющихся должностными лицами, а также иных лиц, отвечающих требованиям, предусмотренным примечанием 1 к ст. 201 УК РФ (например, лицо, которое использует для совершения хищения чужого имущества свои служебные полномочия, включающие организационно-распорядительные или административно-хозяйственные обязанности в коммерческой организации).

пользуемого индивидуальным предпринимателем в своей финансовой деятельности, письмо свободного содержания, в которое под видом документа вложил указанные вредоносные программы. Продавец-консультант индивидуального предпринимателя, не подозревая о вредоносном содержании письма, используя служебный компьютер, открыл данное письмо, тем самым автоматически установив на компьютер вредоносную программу. Далее Бузин, незаконно используя вредоносные программы, без согласия и без ведома легального обладателя информации (индивидуального предпринимателя), из корыстной заинтересованности осуществил неправомерный доступ к компьютеру последнего, что вызвало блокирование компьютерной информации и сделало невозможным использование информации законным владельцем. После этого, продолжая свои преступные действия, направленные на мошенничество в сфере компьютерной информации, используя вредоносные свойства программ, посредством которых получил возможность ознакомиться с информацией о банковским счете и находящимися на нем денежными средствами, принадлежащими индивидуальному предпринимателю, Бузин осуществил перевод денежных средств потерпевшего на счет своего абонентского номера телефона, причинив значительный материальный ущерб[1].

Теоретически обоснованным и практически значимым следует признать разъяснение Пленума об оценке мошеннических действий в сети Интернет с использованием так называемой «социальной инженерии». В соответствии со вторым абзацем п. 21 постановления, если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть Интернет (например, создание поддельных сайтов благотворительных организаций, интернет-магазинов, использование электронной почты), то такое мошенничество следует квалифицировать по ст. 159, а не ст. 159.6 УК РФ. Таким образом, принципиальным отличием общеуголовного мошенничества от компьютерного является наличие обмана или злоупотребления доверием потерпевшего, в результате чего он лично или через третьих лиц передает денежные средства или иное имущество злоумышленнику. Следует

[1] Приговор советского районного суда г. Улан-удэ, Республика Бурятия, от 22 сентября 2015 г. по делу № 1-715/2015.

отметить, что введение в заблуждение потерпевшего может быть следствием работы вредоносного программного обеспечения, что само по себе не исключает необходимость квалификации содеянного по ст. 159 УК РФ. Так, спорным представляется решение суда по следующему делу: братья Сдобновы были осуждены по ч. 2 ст. 159.6 УК РФ и ч. 2 ст. 273 УК РФ. Согласно материалам дела, виновные создали в сети Интернет-сайты, в стартовый файл которых заранее были интегрированы вредоносные программы, заведомо предназначенные для блокирования функций операционной системы персональных компьютеров. Одновременно с блокированием пользователям приходили сообщения якобы от правоохранительных органов (МВД России, Управления «К» МВД России и др.), содержащие сведения о необходимости перечисления денежных средств по соответствующим реквизитам в качестве оплаты наложенного на пользователя сети Интернет административного штрафа за просмотр и копирование материалов порнографического содержания. Полученные от потерпевших денежные средства Сдобновы в дальнейшем тратили на собственные нужды[1]. Учитывая, что денежные средства списывались вредоносной программой не автоматически, а перечислялись потерпевшими самостоятельно в качестве оплаты несуществующих административных штрафов за просмотр порнографических материалов, содеянное, на наш взгляд, подпадает под действие общей нормы о мошенничестве.

Пленум скорректировал традиционный подход к определению момента окончания хищения, если его предметом выступали безналичные денежные средства, в том числе электронные денежные средства. Согласно новой позиции, такое хищение следует считать оконченным не с момента зачисления денежных средств на счет виновного или третьих лиц, а с момента их изъятия у владельца (п. 5). Данное решение Пленума было продиктовано двумя обстоятельствами: 1) редакционная коллегия отметила, что высокий уровень развития товарно-денежных отношений, информационных технологий и банковских услуг позволяет за считанные минуты осуществлять перевод и зачисление денежных средств, оплату товаров и др. В связи с этим с момента списания денеж-

[1] Приговор первомайского районного суда оренбургской области от 8 июля 2016 г. по делу № 1-58/2016.

ных средств со счета потерпевшего у виновного появляется реальная возможность по их беспрепятственному распоряжению и 2) в отдельных случаях у правоохранительных органов не всегда имеется возможность достоверно установить, куда были перечислены похищенные денежные средства потерпевшего, что само по себе не должно влиять на квалификацию мошенничества как оконченного преступления[1].

Указанное разъяснение высшей судебной инстанции в целом следует оценить положительно. Как известно, случаи неверного толкования момента окончания компьютерного мошенничества на практике встречались. Например, как покушение на компьютерное мошенничество были квалифицированы действия лиц, задержанных в отделении банка уже при попытке получения похищенных денежных средств с расчетного счета фирмы-однодневки, куда были перечислены похищенные денежные средства юридического лица в результате заражения вредоносным программным обеспечением служебного компьютера организации с установленной системой «Банк-Клиент»[2]. Вместе с тем, ошибочно полагать, что данное разъяснение не может иметь исключений. На наш взгляд, несмотря на положения п. 5 нового постановления Пленума, как покушение на мошенничество в сфере компьютерной информации, следует оценивать ситуации, когда в рамках оперативно-разыскных мероприятий по запросу правоохранительных органов финансовая организация заранее приостановила любые расходные операции по счету, на который впоследствии были зачислены похищенные злоумышленниками денежные средства. Отметив положительные аспекты разъяснений нового постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», следует также указать и на отдельные проблемы, которые, к сожалению, не получили своего разрешения.

Прежде всего, Пленум специально не указал, что использование лицом возможностей, связанных с замещением должности и выполнением функций рядового работника, не может лечь в основание квалификации содеянного как мошенничества, совершенного лицом с использованием

---

[1] Заседание Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. // Электронный ресурс: http://www.vsrf.ru/press_center/news/26093/ (дата обращения: 6 декабря 2017 г.).

[2] Приговор пресненского районного суда г. Москвы от 23 января 2014 г. по делу № 1-43/2014.

своего служебного положения, в том числе по ч. 3 ст. 159.6 УК РФ. Вместе с тем, в правоприменительной практике является достаточно распространенным признание такими лицами продавцов-консультантов, специалистов обслуживания клиентов, системных администраторов и других работников, имеющих доступ к компьютерной информации в связи с осуществлением ими сугубо технических функций[1]. Ориентируясь на формирующиеся тенденции судебно-следственной практики, Н. А. Лопашенко совершенно справедливо подчеркивает, что нельзя расширять до бесконечности круг лиц, которые использующих свое служебное положение[2]. Понятно, что совершение подобного рода преступлений во многом становится возможным благодаря занимаемой лицом должности. Однако нельзя утверждать, что системный администратор, как и другие категории рядовых работников, отвечают обязательным критериям о наличии организационно-распорядительных или административно-хозяйственных функций. Полагаем, что отсутствие прямого указания по данному вопросу в новом постановлении Пленума не позволит окончательно устранить теоретические и, что более важно, правоприменительные противоречия.

Неразрешенным остался вопрос об отграничении мошенничества в сфере компьютерной информации от присвоения и растраты с использованием сервисов дистанционного банковского обслуживания (например, когда бухгалтер совершает хищение денежных средств путем отправки подложного платежного поручения в электронной форме). В теории уголовного права отмечается, что независимо от того, являлся ли преступник материально ответственным лицом, а похищаемое имущество было вверено ему, такие действия все равно следует квалифицировать по ст. 159.6 УК РФ, если имело место использование компьютерной информации или информационно-коммуникационных сетей[3]. Примеры из

---

[1] Например: Приговор мирового суда судебного участка № 2 Богдановского судебного района свердловской области от 3 марта 2014 г. По делу № 1-20/2014.

[2] Лопашенко Н. А. Посягательства на собственность. М., 2012. С. 502.

[3] Потапкин С. Н., Солдатов А. В., Утешева Т. Т., Данилов Д. А. Вопросы объективной стороны мошенничества в сфере компьютерной информации в судебно-следственной практике // Библиотека научных публикаций электронного юридического справочника система гарант. – №1 (5). – 2015. – С. 3.

судебно-следственной практики[1] также демонстрируют тенденцию оценки таких действий по ст. 159.6 УК РФ. На наш взгляд, с учетом разъяснений нового постановления Пленума содеянное необходимо квалифицировать по ст. 160 УК РФ по причине специфического содержания предмета хищения – на момент изъятия имущество является вверенным виновному.

Список литературы

1. Комментарий к уголовному кодексу Российской Федерации (постатейный). Т. 1. 2-е изд., перераб. и доп. / под ред. засл. юриста РФ, д.ю.н., проф. А. В. Бриллиантова // Режим доступа: СПС «КонсультантПлюс».

2. Лопатина Т. М. Проблемы уголовно-правовой защиты сфер компьютерной информации: современный взгляд на мошенничество // Право и безопасность. – 2013. – № 3–4 (45). – С. 89–95.

3. Лопашенко Н. А. Законодательная реформа мошенничества: вынужденные вопросы и вынужденные ответы // Криминологический журнал байкальского государственного университета экономики и права. – 2015. – Т. 9. – № 3. – С. 504–513.

4. Лопашенко Н. А. Посягательства на собственность : монография. – М., 2012. – 528 с.

5. Потапкин С. Н., Солдатов С. В., Утешева Т. Т., Данилов Д. А. Вопросы объективной стороны мошенничества в сфере компьютерной информации в судебно-следственной практике // Библиотека научных публикаций электронного юридического справочника системы гарант. – 2015. – №1 (5). – С. 3.

6. Русскевич Е. А. Наказание за мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) // Библиотека уголовного права и криминологии. – 2016. – № 5 (17). – С. 180–182.

7. Третьяк М. И. Проблемы квалификации новых способов мошенничества // Уголовное право. – 2015. – № 2. – С. 94–98.

8. Хилюта В. В. Хищение с использованием компьютерной техники или компьютерное мошенничество? // Библиотека криминалиста. – 2013. – № 5 (10). – С. 55–65.

9. Шумихин В. Г. Седьмая форма хищения чужого имущества // Вестник пермского университета. – 2014. – № 2 (24). – С. 229–233.

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

[1] Приговор хамовнического районного суда г. Москвы от 15 мая 2014 г. По делу № 1-49/2014; Приговор Салаватского городского суда Республики Башкортостан от 21 мая 2015 г. по делу № 1-113/2015.

Захаров Д. Н.[1],

доцент кафедры информационной безопасности учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя, кандидат технических наук;

Мельцева И. С.[2],

старший научный сотрудник учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя;

Тычкова А. О.[3],

научный сотрудник учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя;

Сребродольская С. А.[4],

старший преподаватель-методист кафедры информационной безопасности учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя

УГРОЗЫ СОВРЕМЕННОЙ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Угрозы условно можно разделить на следующие две разновидности: мошенничество в его «классическом» виде – использование поддельных документов при осуществлении операций со счетами и денежными средствами, размещенными в кредитно-финансовых организаций, а также «кибермошенничество». «Кибермошенничество» характеризуется трансграничностью. Общей характеристикой подобных правонарушений является отсутствие прямого взаимодействия жертвы и злоумышленника. На данный момент мошенничество является самой большой проблемой. Находясь в любой точке планеты, злоумышленник может работать с дистанционными каналами самообслуживания в любой точке страны. В настоящий момент актуальными угрозами современной преступности в сфере информационных технологий остаются угрозы, направленные на хищение денежных средств со счетов клиентов. Здесь проявляется и социальная инженерия, и атаки, направленные на мобильные устройства клиентов.

Не сбавляет позиций вредоносное программное обеспечение [1].

За прошедший 2017-й год основным трендом были трояны-шифровальщики. Они представлялись в многочисленных вариациях, некоторые безвозвратно шифровали данные, без возможности расшифровки, даже в случае уплаты выкупа.

Публикация исходного кода программного обеспечения Агентства Национальной Безопасности США, которое было модифицировано и использовано многими злоумышленниками (пример: EternalBlue).

Любой желающий, обладающий навыками программирования, может создать свою вариацию вредоносного программного обеспечения. Поиск уязвимых машин осуществляется по классической комбинации Shodan+masscan на нескольких VDS.

Новым трендом на 2018-й год является майнинг. Создатели вредоносного программного обеспечения стремятся заразить как можно большее количество компьютеров с целью использования их вычислительных ресурсов. Для этой цели используют даже код веб-приложений.

Продвигается новая услуга Ransomwareas Service: заплатив разработчику некоторую сумму, можно приобрести «билд» или подписку на использование вредоносного программного обеспечения, которое будет реализовывать требуемый функционал.

Отдельно развивается вредоносное программное обеспечение, нацеленное на компьютерную инфраструктуру промышленных предприятий. Злоумышленники исследуют протоколы взаимодействия и прошивки устройств, с целью поиска уязвимостей и разработки плана нападения.

Разработка вредоносного программного обеспечения под банкоматы и POS-терминалы была и остается актуальной находит все новые уязвимости в операционной системе и прикладном программном обеспечении, установленном на подобных устройствах.

Новым трендом конца 2017/2018 года является криптовалюта и ICO. В мире существует несколько платформ для разработки смарт-контрактов. Платформы постоянно совершенствуются, но еще содержат уязвимости и архитектурные просчеты, позволяющие злоумышленникам похищать средства из криптовалютных кошельков. Ряд злоумышленников, решив не размениваться на кошельки рядовых пользо-

вателей, осуществляют взлом бирж криптовалюты, с целью последующего перевода имеющихся на кошельках биржи средств на свои кошельки.

Оглядываясь на политическую сферу, многие громкие политические события связывают с деятельностью киберпреступников, осуществляющих атаки на государственные ресурсы. Подобные атаки являются действенным методом влияния на общественное мнение и становятся еще одним политическим инструментом. Примером являются пресловутые «русские хакеры», от действий которых многие пострадали.

В заключении необходимо отметить, что в России принят ряд законодательных инициатив, направленных на регулирование государственных интересов в различных сферах высоких технологий, таких как блокчейн технологии, криптовалюта. Данные законодательные инициативы являются попыткой догнать научно-технический прогресс в сфере высоких технологий. Эти попытки, к сожалению, не увенчаются успехом. Примером является деятельность Роскомнадзора, исполняющего решение суда с целью блокировки запрещенного на территории РФ мессенджера Telegram. В результате метода «веерных» блокировок пострадали сервисы многих компаний, в том числе и из государственного сектора. Мессенджер как работал, так и работает. Проблема заключается в том, что для хостинга используются крупнейшие мировые облачные сервисы западных компаний (Amazon, Google, Microsoft). Юрисдикция российских судебных решений на них не распространяется; заблокированные клиенты, которые арендовали вычислительные мощности, не приносят такого количества прибыли, как оставшаяся часть клиентов. Это неравенство, подкрепленное жесткими законами рынка и бизнеса, ведет к тому, что любые попытки со стороны государства и силовых структур, связанные с отрегулированием или запретом, игнорируются.

Список литературы

1. Актуальные киберугрозы, 2017. Тренды и прогнозы // www.ptsecurity.com URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf (дата обращения: 8 мая 2018 г.).

Долбилов А. В.[1],

заместитель кафедры экономической безопасности
МосУ МВД России имени В.Я. Кикотя, кандидат экономических наук

СОВРЕМЕННЫЕ КИБЕРУГРОЗЫ ОРГАНИЗАЦИЙ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ

Высокие темпы внедрения финансовых технологий в деятельность отечественных банков способствуют увеличению предоставления электронных банковских услуг и более масштабному использованию клиентами банков удаленного доступа к своим счетам для осуществления разнообразных платежей и переводов.

Однако процесс внедрения дистанционного банковского обслуживания российскими кредитными организациями сопровождается возникновением новых криминальных угроз для деятельности банков, представляющих собой, во-первых, хакерские атаки на системы дистанционного банковского обслуживания; во-вторых, активное использование методов социальной инженерии, в результате применения которых владелец банковского счета, будучи введенным в заблуждение, либо сам переводит средства со своего банковского счета на счет преступников, либо передает конфиденциальную информацию (свои персональные данные, данные банковской карты, пароли, коды), необходимую для получения доступа к банковскому счету.

При этом необходимо отметить, что деятельность преступников носит организованный характер и не имеет национальных границ.

Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России (ФинЦЕРТ Банка России) подготавливаются ежегодные обзоры несанкционированных переводов денежных средств с использованием платежных карт, несанкционированных операций со счетов юридических лиц, сведения об инцидентах, произошедших при эксплуатации операторами по переводу денежных средств и операторами услуг платежной инфраструктуры объектов информационной инфраструктуры.

Согласно обзору несанкционированных переводов денежных средств за 2017 год, отмечается снижение объема (рис. 1) и увеличение количества (рис. 2) несанкционированных операций с использованием платежных карт в 2017 году. Разнонаправленная тенденция снижения объема и увеличения количества несанкционированных операций с использованием платежных карт обусловлена снижением средней суммы одной несанкционированной операции в 2017 году до 3 тыс. руб.

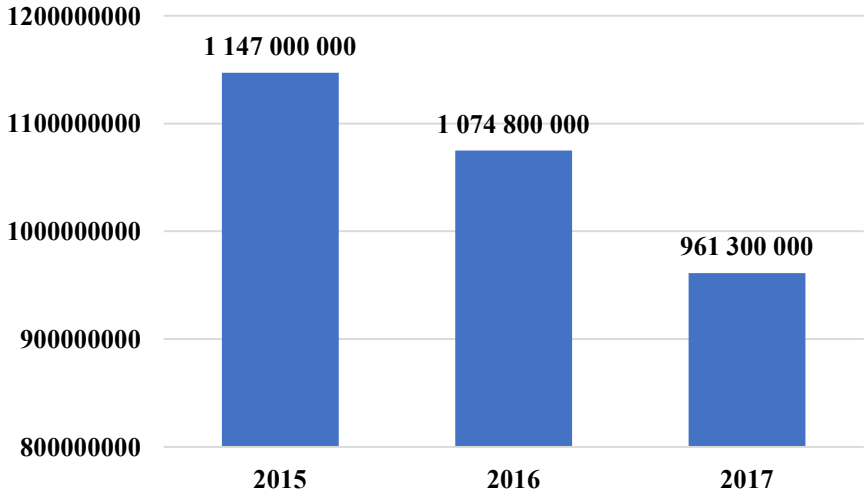

Рис. 1. Объем несанкционированных операций с использованием платежных карт в 2015–2017 гг., руб.

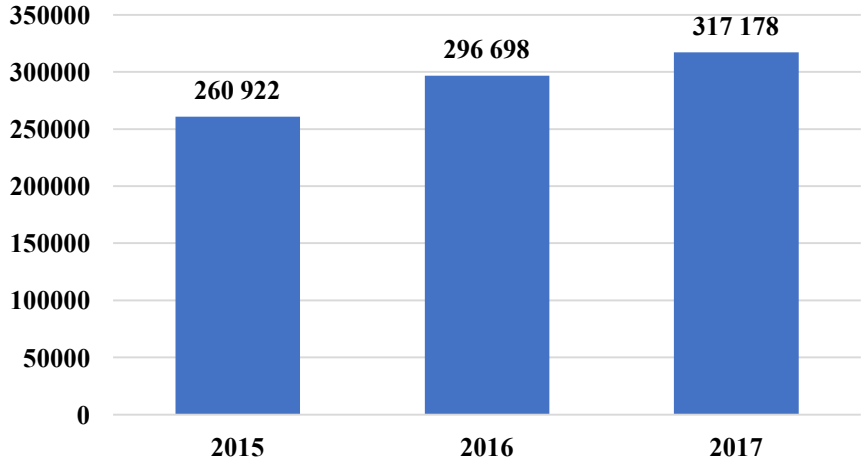

Рис. 2. Количество несанкционированных операций с использованием платежных карт в 2015–2017 гг., ед.

Также, согласно обзору несанкционированных переводов денежных средств за 2017 год, отмечается снижение объема (рис. 3) и увеличение количества (рис. 4) несанкционированных операций со счетов юридических лиц в 2017 году. Под несанкционированными операциями со счетов юридических лиц понимаются события, связанные с покушением на хищение денежных средств со счета юридического

лица с использованием систем дистанционного банковского обслуживания.

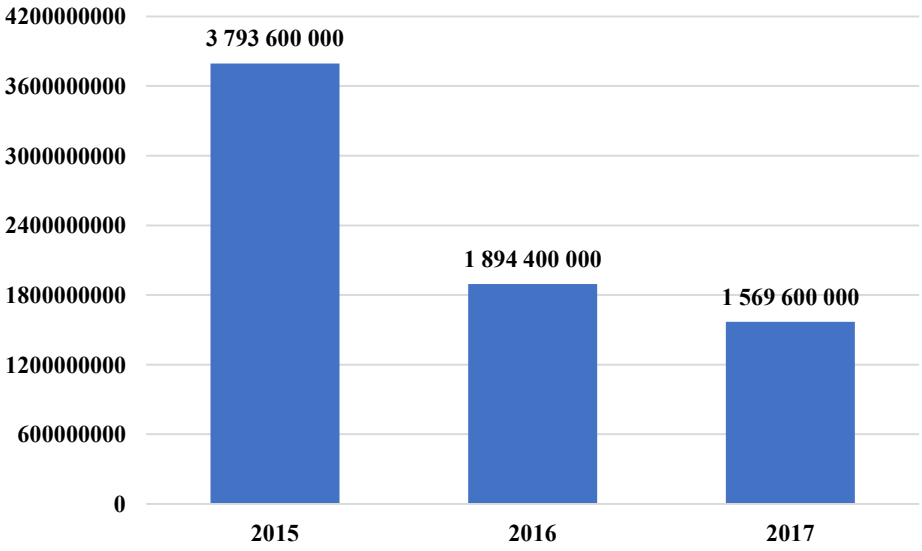

Рис. 3. Объем несанкционированных операций со счетов юридических лиц в 2015-2017 гг., руб.

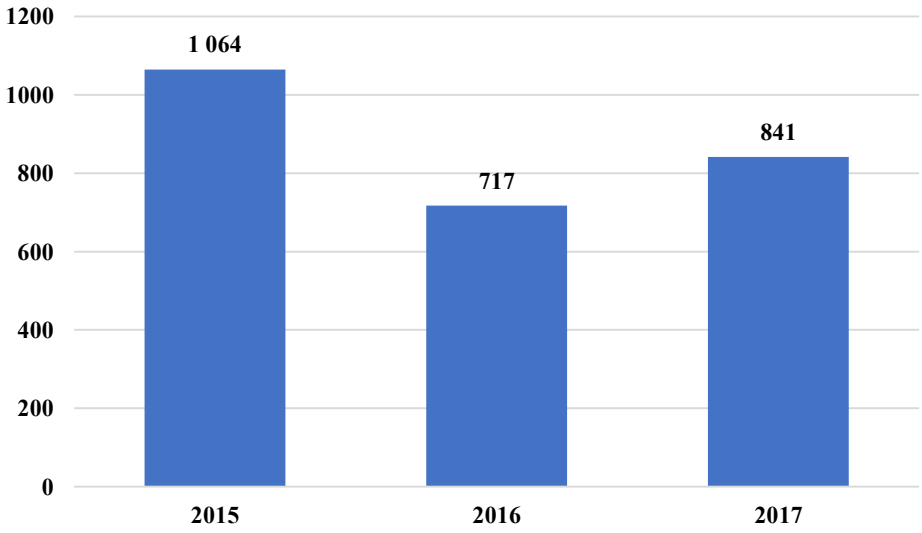

Рис. 4. Количество несанкционированных операций со счетов юридических лиц в 2015–2017 гг., ед.

При этом, как отмечается в обзоре, на долю остановленных несанкционированных операций со счетов юридических лиц в 2017 году приходится не менее половины от общего объема денежных средств (рис. 5). Однако динамика соотношения объема остановленных и неостановленных несанкционированных операций со счетов юридических лиц показывает ежегодное уменьшение доли остановленных несанкционированных операций с 62 % в 2015 году, до 51 % – в 2017 году. Под остановленными несанкционированными операциями понимаются операции, по которым перевод денежных средств не достиг окончательности либо

окончательность перевода денежных средств наступила, но денежные средства заблокированы на счета получателя в соответствии с законодательством Российской Федерации до получения обоснования перевода денежных средств.

Рис. 5. Соотношение объема остановленных и неостановленных несанкционированных операций со счетов юридических лиц в 2015–2017 гг., %

Согласно обзору несанкционированных переводов денежных средств за 2017 год, объем несанкционированных операций в результате инцидентов, произошедших у кредитных организаций, составил 1,35 млрд рублей.

В качестве основных причин несанкционированных операций с использованием платежных карт указываются: использование электронного средства платежа без согласия клиента вследствие противоправных действий, потери, нарушения конфиденциальности; нарушение клиентом порядка использования электронного средства платежа; побуждение владельца электронного средства платежа к совершению операции путем обмана и злоупотребления доверием; воздействие вредоносного кода и т. п.

В качестве основных причин несанкционированных операций со счетов юридических лиц указываются: нарушение порядка использования электронного средства платежа и использование электронного

средства платежа без согласия клиента. Учитывая, что юридические лица в основном осуществляют операции через системы дистанционного банковского обслуживания со стационарных компьютеров, причины в большинстве случаев могут быть сведены к воздействию вредоносного кода.

Как отмечают кредитные организации, на сегодняшний день значительный объем хищений средств со счетов клиентов банков обусловлен относительной простотой их совершения при помощи методов социальной инженерии, использование которых, как правило, не предполагает специальных технических знаний и технических средств у преступников.

Хищения и покушения на хищения средств со счетов клиентов банков, совершаемых методом социальной инженерии, непрерывно увеличиваются и в настоящее время составляют до 90 % от общего числа хищений и покушений на хищения, совершенных против физических лиц, являющихся клиентами банков.

Особенностью хищений, совершаемых с использованием метода социальной инженерии, является подтверждение правомерности совершения операции по счету клиента банка владельцем счета, который, находясь под влиянием злоумышленников, даже в случаях, когда служба банка по противодействию кибермошенничеству в системе дистанционного банковского обслуживания, при осуществлении фрод-мониторинга всей информации по клиенту, входящей и исходящей, на предмет обнаружения мошеннических действий, определяет операции как подозрительные.

Метод социальной инженерии активно используется хакерами и при атаках клиента банка с помощью вредоносного программного обеспечения, позволяя получить удаленный доступ к устройству клиента.

К основным видам ущерба от деятельности киберпреступников в банковской системе можно отнести:

- финансовый ущерб, связанный с несанкционированными переводами денежных средств с использованием платежных карт, несанкционированных операций со счетов юридических лиц;

- выведение похищенных у юридических и физических лиц средств из легального оборота и направление их на воспроизводство преступной деятельности;
- нарушение финансовой устойчивости деятельности кредитной организации;
- нанесение репутационного ущерба кредитным организациям и, как результат, формирование недоверия к их деятельности.

К основным причинам повышенных банковских рисков, связанных с использованием дистанционного банковского обслуживания, можно отнести:

- наличие уязвимостей в применяемых кредитными организациями информационных системах и платежных приложениях;
- недостатки в обеспечении информационной безопасности, отсутствие должного соблюдения кредитными организациями требований, установленных нормативными актами и отраслевыми стандартами;
- отсутствие эффективно функционирующей системы координации деятельности кредитных организаций по противодействию кибератакам.

Таким образом, с одной стороны, любая кибератака представляет угрозу финансовой устойчивости кредитной организации, а с другой стороны, киберугрозы становятся в настоящее время все более значимым риском в деятельности кредитных организаций и потенциально могут иметь последствия для стабильности отечественной банковской системы, если целью кибератак станут системно значимые банки, центральный банк или объекты финансовой инфраструктуры (включая платежные системы).

Хрусталева Т. А.[1],

заместитель начальника кафедры юридической психологии УНК ПСД МосУ МВД России имени В.Я. Кикотя, кандидат психологических наук;

Сударик А. Н.[2],

заместитель начальника кафедры психологии УНК ПСД МосУ МВД России имени В.Я. Кикотя, кандидат психологических наук;

Кравченко А. В.[3],

старший научный сотрудник УНК ПСД МосУ МВД России имени В.Я. Кикотя

ИСПОЛЬЗОВАНИЕ ЗНАНИЙ МЕХАНИЗМОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Время технических и физических преступлений, связанных с хищением физических ключей доступа в сфере интернет-технологий, неумолимо проходит. На первый план выходят преступления более тонкого и изощренного вида на основе социальной инженерии. Преступники быстро ориентируются и активно используют провалы в законодательстве (неоднозначное понятие банковской тайны и ее признаки, длительное время на бюрократические проволочки). Так же правоохранители упираются в дотошное прочтение и буквальное использование понятий «разглашение информации третьим лицам» участниками кредитно-банковской системой, что способствует мгновенному выводу средств на сторонние банки и потере следственной цепочки. Отсутствие оперативного взаимодействия (электронного документооборота) между платежными системами, банками и правоохранителями позволяет преступникам использовать это время на сокрытие следов преступлений.

Все вышесказанное подчеркивает актуальность изменения и уточнения законодательных актов, создания центров по оперативному обмену данных, но как бы ни была совершенна техническая и организационная система безопасности, она всегда будет спотыкаться о челове-

ческий фактор, который используют злоумышленники, обучаемые социальными инженерами.

Об этом свидетельствует рост на 45,8 % количества преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, по сравнению с аналогичным периодом прошлого года и на 16,9 % преступлений, совершенных по ст. 159–159.3, 159.5–159.6 УК РФ (мошенничество, рис. 1)[1].

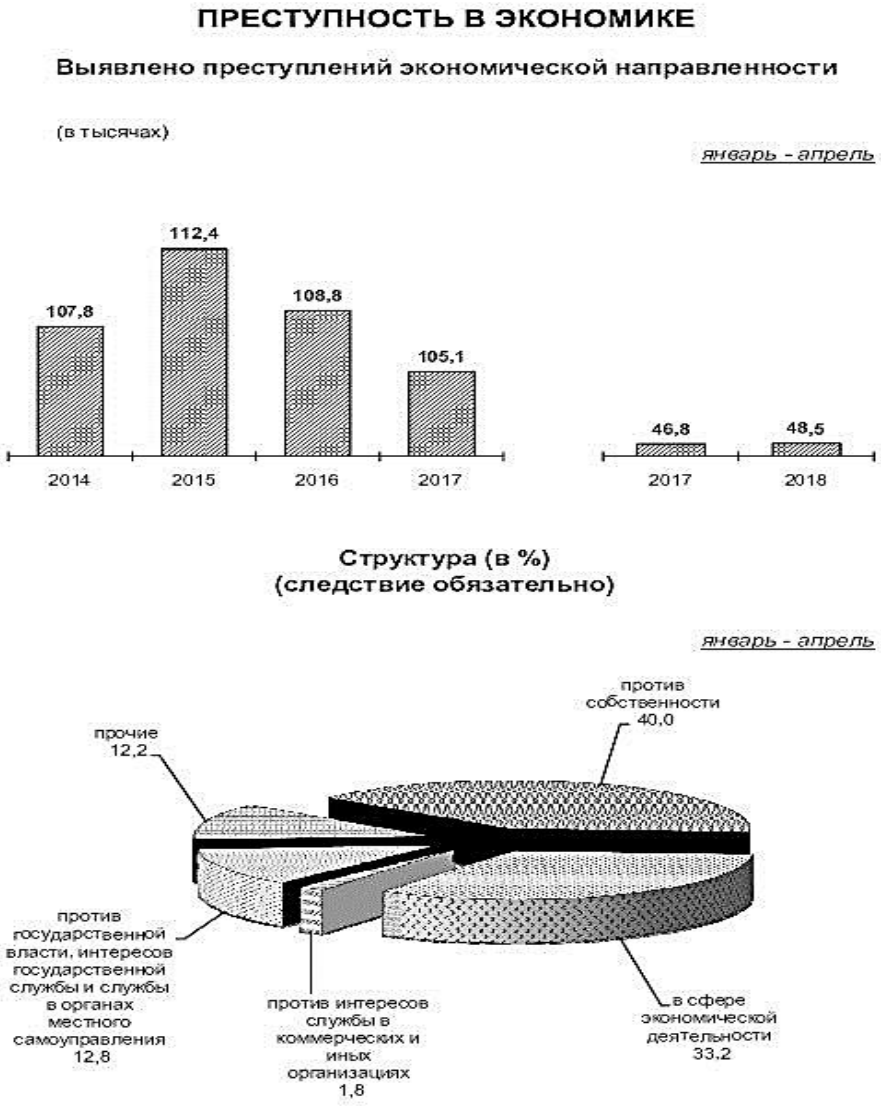

Рис. 1. Статистика преступлений за январь–апрель 2018 г.

Внимание Президента России в выступлении на расширенном заседании коллегии МВД России 28 февраля 2018 г., где он отметил низкий уровень раскрываемости преступлений против собственности, совер-

[1] https://xn--b1aew.xn--p1ai/reports/item/13357360 (Электронный ресурс Министерства внутренних дел России, обращение 8 мая 2018 г.)

шаемых с использованием компьютерных и телекоммуникационных технологий[1].

Обозначенные Президентом России вопросы не только актуальны, но и достаточно сложны, поскольку существующая ситуация свидетельствует о значительных изъянах в системе защиты населения и государственных институтов от киберугроз[2].

Современная статистика по угрозам информационной безопасности с каждым годом менее утешительная и заставляет в корне пересмотреть свое отношение ко многим вопросам и самой проблеме информационной безопасности.

Так, по материалам отчетов Dalott Global Security Survey, 2016, по мнению респондентов, в числе основных внешних угроз ИБ уверено лидируют вирусы и черви (63 % опрошенных), технологии фишинга и фарминга (51 %), шпионское ПО (48 %), приемы социальной инженерии (25 %).

Значительное изменение претерпела сама «хакерская иерархия». Ее верхний уровень возглавляют социальные инженеры, делающие свой бизнес на умелом управлении психологией легальных пользователей сети, которые, сами того не подозревая, самостоятельно осуществляют несанкционированную инсталляцию вредоносных программ и вирусов. Не безызвестное стремление человека получить желаемое «на халяву». Пиратский рынок наводнен различными средствами, инструментами, конструкторами и «игрушками», которые при желании способен освоить каждый. Это порождает немало хакеров-одиночек, в той или иной мере. Способны причинить значительный вред любой организации, что и происходит на самом деле. Но о подобных инцидентах компании предпочитают умалчивать, и статистика по ним в официальных источниках невелика.

---

[1] Информация о расширенном заседании коллегии МВД России // url:http://kremlin.ru/events/president/news/56949 (дата обращения: 28 февраля 2018 г.).

[2] Г ончар В. В. Актуальные вопросы подготовки кадров для противодействия преступлениям в сфере информационных технологий// профессиональное образование сотрудников органов внутренних дел. Педагогика и психология служебной деятельности: состояние и перспективы: сборник научных трудов II международной конференции имени В.Я. Кикотя (6–7 июня 2018 г.): научное электронное издание. М. : МосУ МВД России имени В.Я. Кикотя, 2018. – 607 с. С. 557–560.

Если рассматривать результаты общедоступной научной деятельности, то можно наблюдать, что социальная инженерия – это молодое направление. Как наука с принципами ее практической реализации возникла в СССР, в рамках «человеческой инженерии» (humanengineering), направленной в основном на повышение безопасности труда и повышение эффективности работы машин, снижение утомляемости работника и обеспечение комфортности в системах «человек – машина».

В 20–30-е годы XX века в СССР организовывается движение, направленное на управление производством и научную организацию труда. Научной основой движения становятся прикладные разработки социальной инженерии[1].

Далее, в 50–60-е годы прошлого столетия, социальная инженерия получила дальнейшее развитие в Европе и США[2].

В СССР дальнейшее развитие социальной инженерии наблюдается с 80-х гг. Наиболее яркий интерес к социальной инженерии в России стал проявляться с 90-х гг. Тогда научные сотрудники: О. А. Уржа, Ю. М. Резник, В. В. Щербина и их коллеги пытались воссоздать отечественное социоинженерное направление, но не получили никакой поддержки от государства. Однако позже эта область вновь стала набирать обороты в нашей стране, что продолжается и по сей день.

Суть же социальной инженерии – в гибкости, приспособляемости к окружающим динамичным обстоятельствам с тем, чтобы достичь поставленной цели. Она рассматривает институты как средства, обслуживающие определенные цели, и оценивает уровень их организованности с точки зрения их целесообразности, эффективности и простоты.

Интересен алгоритм социоинженерной деятельности применительно к объекту влияния:

1) оценка состояния объекта социоинженерной деятельности;

2) прогнозирование наиболее вероятных вариантов развития внутренней и внешней среды объекта прогноза;

---

[1] Гастев А. К. Как надо работать. Практическое введение в науку организации труда. – 2-е изд. М., 1972.

[2] Чернова Г. Р. Социальная психология : учеб. для вузов. СПб. : ЛГУ имени А. С. Пушкина, 2010. – 200 с.

3) моделирование будущего состояния объекта исследования с использованием математических, кибернетических, прогностических и других методов;

4) разработка социального проекта нового состояния исследуемого объекта;

5) социальное планирование в соответствии с социальным проектом;

6) осуществление проекта с помощью современных социальных технологий и коммуникаций (например, фейсбук, твиттер, в вконтакте и т. п.).

Основываясь на понятиях социальной инженерии с психологической стороны, мы говорим, что:

– социальная инженерия – это один из разделов социальной психологии, направленный на то, чтобы внедрять в их сознание некоторую модель поведения и тем самым манипулировать их поступками[1];

– социальная инженерия – это метод (атак) несанкционированного доступа к информации или системам хранения информации без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным[2];

– социальная инженерия – это набор прикладных психологических и аналитических приемов, которые злоумышленники применяют для скрытой мотивации пользователей публичной или корпоративной сети к нарушениям устоявшихся правил и политик в области информационной безопасности.

Основываясь на вышепривиденном понятийном аппарате, статистике и алгоритме действий совместно со специалистами отдела по борьбе с мошенниками одного из крупных банков мы провели полевой эксперимент с целью выявить более актуальные на сегодняшний день схемы мошенничества для составления необходимых знаний сотрудникам ОВД при подготовке их в учебных заведениях МВД России.

---

[1] Голованов О. Краткий словарь по социологии. М. : «Проспект», 2014.

[2] Бычек В., Ершова Е. Социальная инженерия в интеллектуальной битве «добра» и «зла» // Защита информации. Inside. – 2006. – №6. С. 20–27.

Участвуя в учебных оперативно-следственных группах, мы прослушали 174 ситуации, связанные с мошенничеством в отношении граждан.

После анализа и услышанного мы обобщили и выделили наиболее популярные схемы обмана посредством социальной инженерии (рис. 2):

– родственник в беде;
– обман в социальных сетях;
– покупка товаров/оплата услуг («самопереводы»);
– обман на сайтах бесплатных объявлений;
– помощь в получении кредита;
– помощь в оформлении визы ;
– «касса взаимопомощи»;
– «романтическое знакомство» или «невеста»;
– обман пенсионеров;
– подбор персональных данных публичных лиц в контактном центре банка;
– замена SIM-карты;
– фрод-рассылки.

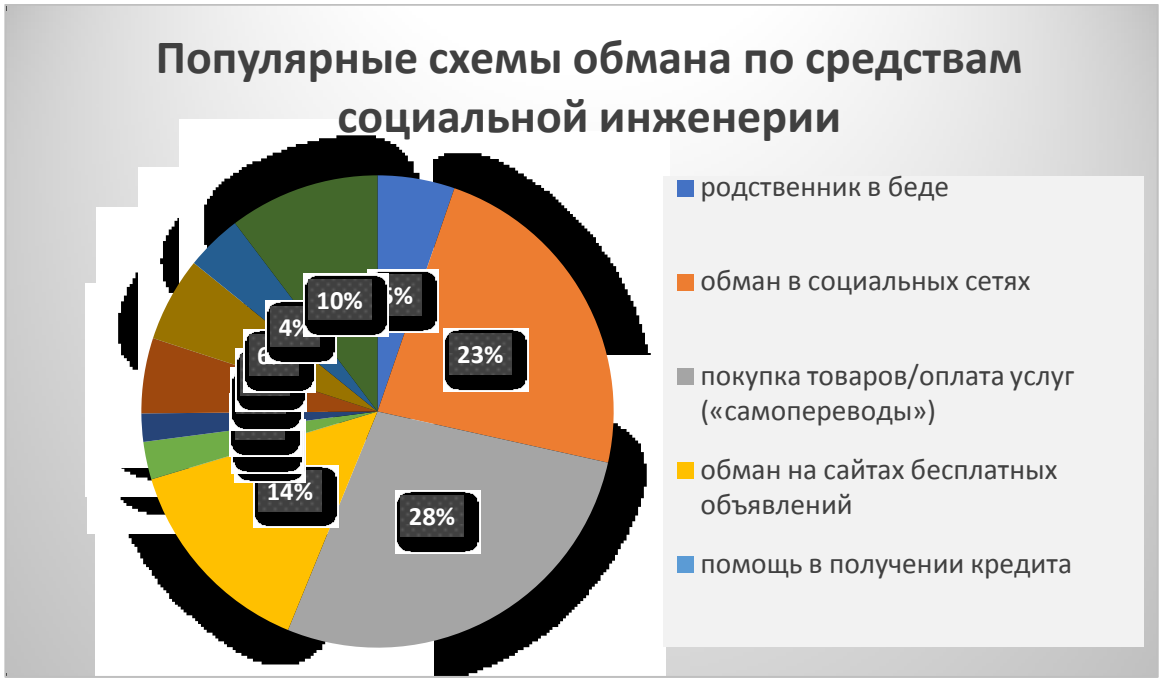

Рис. 2. Распределение популярных схем обмана посредством социальной инженерии

С учетом количества участников и статистических параметров можно сделать вывод, что выявленные виды мошенничества

распространяются на каждый третий случай в статистике МВД России (4583 преступления за период январь–апрель 2018 года).

Как было омечено выше, большинство из них остаются нераскрытыми. Существует много причин низкого уровня нераскрываемости этих преступлений, но мы считаем, одна из них – низкая обученность по тематике «социальной инженерии» сотрудников, обучающихся в учебных заведениях МВД России. В дальнейшем, приходя в территориальные органы и сталкиваясь с этим набирающим рост видом преступлений, они не в состоянии грамотно провести расследование.

И второе – это недифференцированный отбор курсантов по специальности «Информационная безопасность» и дальнейшая специализация[1].

Следовательно, основой государственной политики в области информационной безопасности является обучение и воспитание соответствующих кадров, которые обеспечили бы эффективную работу на результат в области информационной безопасности России.

Данный подход предусматривает необходимость существенных изменений как в структуре, так и в организации учебного процесса в образовательных учреждениях МВД России, организующих подготовку специалистов в области не только информационной безопасности, но и сотрудников оперативных подразделений, дознавателей, следователей, прокуроров и психологов.

По нашему мнению, достаточно быстрый и положительный результат может дать взаимодействие образовательных организаций с организациями, имеющими определенные достижения в области обеспечения собственной информационной безопасности (банками, лабораториями информационной безопасности).

По нашему мнению, для совершенствования подготовки сотрудников правоохранительных органов, специализирующихся на раскрытии и расследовании преступлений в сфере информационных технологий

[1] Кравченко А. В. Совершенствование отбора курсантов на специальность «Информационная безопасность» // Профессиональное образование сотрудников органов внутренних дел. Педагогика и психология служебной деятельности: состояние и перспективы: сборник научных трудов II международной конференции имени В.Я. Кикотя (6–7 июня 2018 г.): научное электронное издание. М. : МосУ МВД России имени В.Я. Кикотя, 2018. – 607 с. С. 580–585.

целесообразно ввести курс по изучению социальной инженерии, как на курсантов, так и для офицеров, проходящих повышение квалификации.

Список литературы

1. Бычек В., Ершова Е. Социальная инженерия в интеллектуальной битве «добра» и «зла» // Защита информации. INSIDE. – 2006. – №6. – С. 20–27.
2. Бэндлер Ричард, Гриндер Джон «Большая энциклопедия НЛП». – М. : «АСТ», 2017.
3. Гастев А. К. Как надо работать. Практическое введение в науку организации труда. – 2-е изд. – М., 1972.
4. Генне О. В. Заметки о социальной инженерии // Защита информации. INSIDE. – 2006. – №6. – С. 16–19.
5. Голованов О. Краткий словарь по социологии. – М. : Проспект, 2014.
6. Гончар В. В. Актуальные вопросы подготовки кадров для противодействия преступлениям в сфере информационных технологий // Профессиональное образование сотрудников органов внутренних дел. Педагогика и психология служебной деятельности: состояние и перспективы: сборник научных трудов II Международной конференции (6–7 июня 2018 г.) : научное электронное издание. М. : МосУ МВД России имени В.Я. Кикотя, 2018. – С. 557–560.
7. Данилов М. П. Самая опасная уязвимость // Защита информации. INSIDE. – 2006. – №6. – С. 32–35.
8. Карпман Стивен A GAME FREE LIFE. The new transactional analysis of intimacy, openness, and happiness. «Метанойя». 2016, С. 342.
9. Кевин Митник. Искусство вторжения. – М. : «ДМК-пресс, Компания АйТи», 2005.
10. Кузнецов Максим, Симдянов Игорь. Социальная инженерия и социальные хакеры. – СПб. : БХВ-Петербург, 2007.
11. Литвак М. Психологическое айкидо : учебное пособие. – Ростов-на-Дону : «Феникс», 2018. С. 219.
12. Никитин М. Ю. Противодействие терроризму и преступности в телекоммуникационной среде // Профессиональное образование сотрудников органов внутренних дел. Педагогика и психология

служебной деятельности: состояние и перспективы : сборник научных трудов II Международной конференции (6–7 июня 2018 г.) : научное электронное издание. – М. : МосУ МВД России имени В.Я. Кикотя 2018. – С. 596–604.

13. Чернова Г. Р. Социальная психология : учеб. для вузов. – СПб. : ЛГУ имени А. С. Пушкина, 2010. – 200 с.

14. Шейнов В. П. Скрытое управление человеком: психология манипулирования. – М. : АСТ Харвест, 2006.

15. Кравченко А. В. Совершенствование отбора курсантов на специальность «Информационная безопасность» // Профессиональное образование сотрудников органов внутренних дел. Педагогика и психология служебной деятельности: состояние и перспективы : сборник научных трудов II Международной конференции (6–7 июня 2018 г.) : научное электронное издание. – М. : МосУ МВД России имени В.Я. Кикотя, 2018. – С. 580–585.

16. https://xn--b1aew.xn--p1ai/reports/item/13357360 (Электронный ресурс Министерства внутренних дел России, обращение 08 мая 2018 г.).

17. Информация о расширенном заседании коллегии МВД России // URL:http://kremlin.ru/events/president/news/56949 (дата обращения: 28.02.2018).

Иванов В. Ю.[1],

доцент кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
МосУ МВД России имени В.Я. Кикотя, кандидат технических наук;

Полехин С. А.[2],

курсант факультета подготовки специалистов
в области информационной безопасности
МосУ МВД России имени В.Я. Кикотя

АНАЛИЗ МЕТОДОВ ИССЛЕДОВАНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОС ANDROID

Реверс-инженеринг – это не что иное, как процесс извлечения знаний или полезной информации из любого продукта, независимо от того, применяется ли он при восстановлении велосипеда или автомобиля, или любого продукта, изготовленного человеком. Вы пришли бы, чтобы узнать много новых и интересных вещей после того, как сломали фактический продукт в разных частях и снова собрали их.

Сегодня мы поговорим о Viper. Под таким коротким названием скрывается модульная структура для организации двоичных файлов и их анализа. Viper ориентирован на аналитиков вирусов и разработчиков эксплоитов, но он также пригодится для обычных реверсеров из-за интересных модулей, база данных которых постоянно пополняется. Кроме того, важным преимуществом является то, что он написан на Python и позволяет Вам изменять его для себя «на лету».

Viper – это открытая, BSD-лицензированная совместная разработка, которая в значительной степени зависит от вклада всего сообщества.

Также проанализируем исходный apk приложения для выявления признаков malware.

Сам по себе apk-файл представляет собой обычный архив, в котором хранится исходный код приложения, которое мы будем анализировать. Проблема заключается в том, чтобы получить исходный код приложения. Обычно приложения под android пишутся на языке программирования Java.

Java Virtual Machine (сокращенно Java VM, JVM) – виртуальная машина Java – основная часть исполняющей системы Java, так называе-

мой Java Runtime Environment (JRE). Виртуальная машина Java исполняет байт-код Java, предварительно созданный из исходного текста Java-программы компилятором Java (javac). JVM может также использоваться для выполнения программ, написанных на других языках программирования. Например, исходный код на языке Ada может быть откомпилирован в байт-код Java, который затем может выполниться с помощью JVM.

JVM является ключевым компонентом платформы Java. Так как виртуальные машины Java доступны для многих аппаратных и программных платформ, Java может рассматриваться и как связующее программное обеспечение, и как самостоятельная платформа. Использование одного байт-кода для многих платформ позволяет описать Java как «скомпилировано однажды, запускается везде» (compileonce, runanywhere).

Но стандартный исходный код имеет расширение class. В нашем же случае мы имеем файлы с расширением smali. Smali – это bytecode виртуальной машины dalvik, который выдается при декомпиляции apk через apktools.

Java + Android SDK = Dalvik.

Dalvik + baksmali = дизасемблирование байт-кода (smali).

Smali схож с Java-байт-кодом. Но, так как в процессорах ARM-архитектуры много регистров, Google решили сэкономить и заменить долгие прогулки в память (в стек, как в JVM) на быстрые походы в регистры. Поэтому основное отличие байт-кода Dalvik от байт-кода JVM – ориентированность на регистры.

Например,

System.out.println («Hello») в JVM-байт-коде выглядит приблизительно так:

getstaticSystem.out // PrintWriterнастеке

ldc «Hello» // PrintWriter, «Hello» – два объекта на стеке

invokevirtualPrintWriter.println (String): void // обаобъекта забирают ся состека, а Print Writer выполняется виртуальный метод с параметром «Hello».

В Dalvik-байт-коде:

sget-object v0, System.out // Print Writer в нулевом регистре

const-string v1, «Hello» // «Hello» впервомрегистре

invoke-virtual Print Writer.println (String): void, v0, v1 // вызвать виртуальный метод println на объекте v0 с параметром v1.

Собственно, move-object перекладывает объект из регистра в регистр, а все эти v0, v1 и т. д. – и есть регистры (valueregisters).

Кроменихестьещеparameterregisters – p0, p1 и т. д. В этих регистрах оказываются значения, переданные в метод как параметры. Если метод не статический, то в p0 будет находиться this;

invoke-direct напоминает invokespecial в JVM – он вызывает не виртуальный, не статический метод. Примером могут служить финальные (и/или приватные) instance-методы.

Кроме того, в smali (в отличие от .class) нет пула констант, они задаются прямо в коде. Это связано с тем, что на все классы, находящиеся в одном dex, есть только один общий пул констант – это уменьшает объем по сравнению с .class и экономит время, потраченное на интернирование строк при загрузке классов.

Для начала изучим AndroidManifest.xml. В корневой папке каждого приложения должен находиться файл AndroidManifest.xml (который именно так и называется). Файл манифеста содержит важную информацию о приложении, которая требуется системе Android. Только получив эту информацию, система может выполнить какой-либо код приложения. Среди прочего файл манифеста выполняет следующие действия:

Он задает имя пакета Java для приложения. Это имя пакета служит уникальным идентификатором приложения.

Он описывает компоненты приложения – операции, службы, приемники широковещательных сообщений и поставщиков контента, из которых состоит приложение. Он содержит имена классов, которые реализуют каждый компонент, и публикует их возможности (указывает, например, какие сообщения Intent они могут принимать). На основании этих деклараций система Android может определить, из каких компонентов состоит приложение и при каких условиях их можно запускать.

Он определяет, в каких процессах будут размещаться компоненты приложения.

Он объявляет, какие разрешения должны быть выданы приложению, чтобы оно могло получить доступ к защищенным частям API-интерфейса и взаимодействовать с другими приложениями.

Он также объявляет разрешения, требуемые для взаимодействия с компонентами данного приложения.

Он содержит список классов Instrumentation, которые при выполнении приложения предоставляют сведения о профиле и прочую информацию. Эти объявления присутствуют в файле манифеста только во время разработки и отладки приложения и удаляются перед его публикацией.

Он объявляет минимальный уровень API-интерфейса Android, который требуется приложению.

Он содержит список библиотек, с которыми должно быть связано приложение.

Информация, которую мы получаем после изучения Manifest’a:

android.permission.INTERNET – позволяет приложениям открывать сетевые сокеты;

android.permission.ACCESS_COARSE_LOCATION – приложение сможет получать доступ к приблизительному местоположению;

android.permission.ACCESS_FINE_LOCATION – приложение сможет получать доступ к точному местоположению;

android.permission.ACCESS_NETWORK_STATE – позволяет приложениям получать доступ к информации о сетях;

android.permission.CHANGE_NETWORK_STATE – позволяет приложениям изменять состояние сетевого подключения;

android.permission.CAMERA – требуется для доступа к устройству камеры;

android.permission.VIBRATE – позволяет получить доступ к вибратору;

android.permission. MODIFY_AUDIO_SETTINGS – позволяет программе изменять глобальные настройки звука;

android.permission. – Позволяет получить доступ к фонарю;

android.permission.WRITE_EXTERNAL_STORAGE – позволяет программе писать на внешнее хранилище;

android.permission.READ_PHONE_STATE – позволяет читать только доступ к состоянию телефона;

android. permission.ACCESS_WIFI_STATE – позволяет приложениям получать доступ к информации о сетях Wi-Fi;

android.permission.CHANGE_WIFI_STATE – позволяет приложениям изменять состояние подключения Wi-Fi;

android.permission.CHANGE_CONFIGURATION – позволяет приложению изменять текущую конфигурацию;

android.permission.BROADCAST_STICKY – позволяет программе транслировать липкие намерения;

android.permission.RECORD_AUDIO – позволяет программе записывать аудио;

android.permission.NFC – позволяет приложениям выполнять операции ввода-вывода по NFC;

android.permission.RECEIVE_BOOT_COMPLETED – позволяет приложению получать ACTION_BOOT_COMPLETED, который транслируется после завершения загрузки системы;

android.permission.WRITE_SETTINGS – позволяет программе читать или записывать системные настройки;

android.permission.DISABLE_KEYGUARD – позволяет приложениям отключать блокировку клавиатуры, если она не защищена;

com.android.launcher.permission.INSTALL_SHORTCUT – позволяет программе устанавливать ярлык в Launcher.

Вывод

Первоначально эта концепция применялась только для аппаратного обеспечения, но теперь она также очень широко используется в программном обеспечении, улучшает существующее программное обеспечение или дублирует его. Цель применения этого процесса в программном обеспечении – разработка программного обеспечения с использованием языка программирования (который может быть понятен любому программисту), который скомпилируется с использованием компиляторов и создает двоичный код (т. е. машинный язык, который может быть понят системным), поэтому обратный процесс разработки появляется, когда этот код машинного языка требует преобразования обратно в считываемый код с помощью декомпиляторов.

Пузарин А. В.[1],

начальник кафедры специальных информационных технологий учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя

ПОЛУЧЕНИЕ ТАЙМ-ЛАЙНА ИНЦИДЕНТА

Инцидент кибербезопасности представляет собой одно или серию нежелательных событий информационной безопасности (ИБ), связанных с атаками из внешних по отношению к объекту информационных сред глобального киберпространства, которые имеют значительную вероятность компрометации бизнес–операций и угрожают кибербезопасности. Каждый инцидент имеет свои особенности, так как может реализовываться посредством различных методик и средств. Рассмотрим на примере атаки вредоносного программного обеспечения «троян».

Сбор первоначальных сведений об инциденте

К этапам заражения троянцем можно отнести следующее:

Социальная инженерия, которая включает в себя, как правило, доверенный источник или телефонный звонок.

Далее идет отправка сообщения на электронную почту жертвы. В качестве примера, оно может содержать следующий текст:

Добрый день!
Прошу вас ознакомиться с изменениями в реквизитах.
--
Best regards,
Maria Petrova
Senior accountant
Tel.: +7 (495) 123 45 67, ext. 1001
petrova.m@hackedcompany.com
www.hackedcompany.com

Рис. 1. Пример текста сообщения, отправляемого жертве

Следующим этапом жертва открывает вложения, находящиеся в указанном выше письме (в нашем случае – в файле «Реквизиты ООО выгрузка из 1с.doc.exe», см. рис. 2):

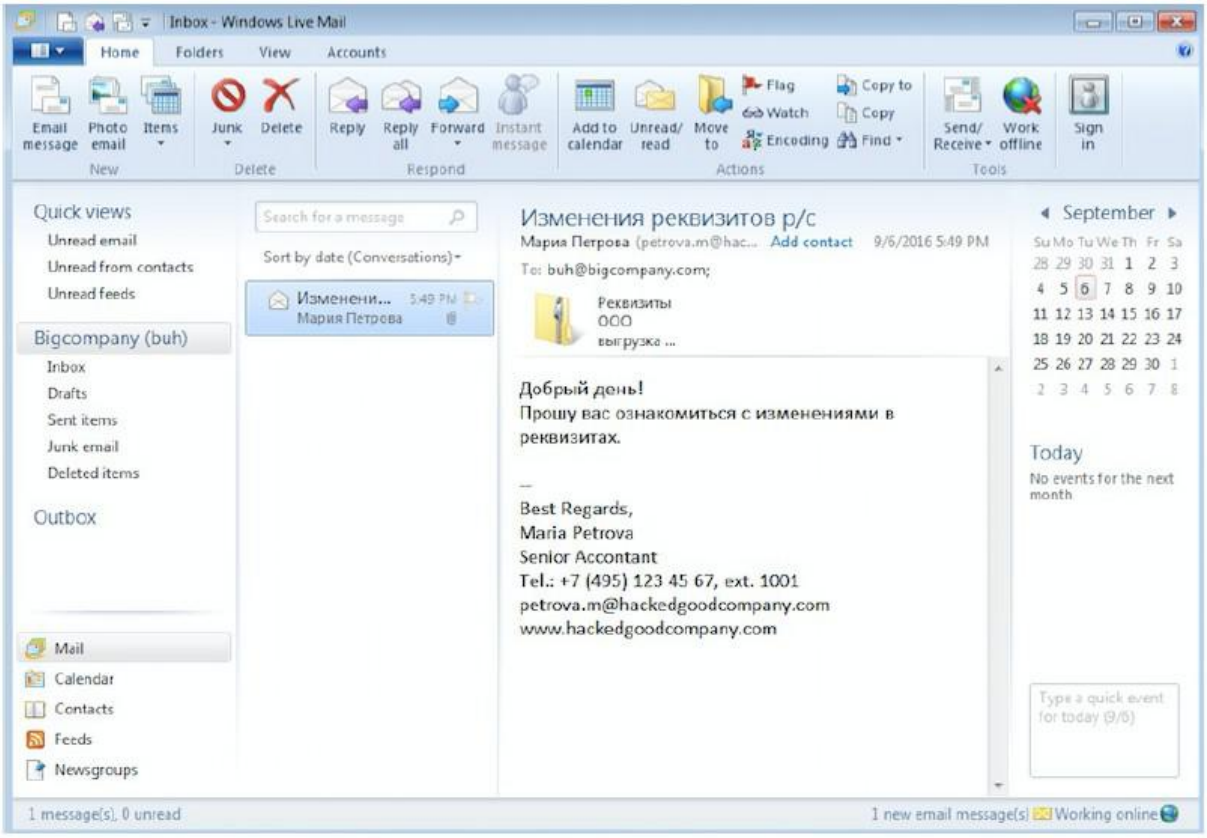

Рис. 2. Пример открытия жертвой письма

Посредством вышеперечисленных действий происходит выгрузка программы в оперативную память, после чего осуществляется выполнение всех ее процессов.

За этим следуют такие последствия, как:

– увеличение привилегий;

– backconnecttoCnCServer;

– загрузка полезных данных и т. д.

Извлечение сведений из предоставленных носителей информации

Запускаем VMwarePlayer и открываем в ней установленную операционную систему SiftWorkstation. Как только она загрузится, открываем HEX-редактор и открываем файл «image.raw». Должно отобразиться на рис. 3.

Как мы видим, в правой части имеется запись: «Invalidpartitiontable. Errorloadingoperatingsystem. Missingoperatingsystem». Таким образом, нетрудно понять, что на данном виртуальном носителе существуют проблемы в работе главной загрузочной записи (MBR) или загрузочного сектора.

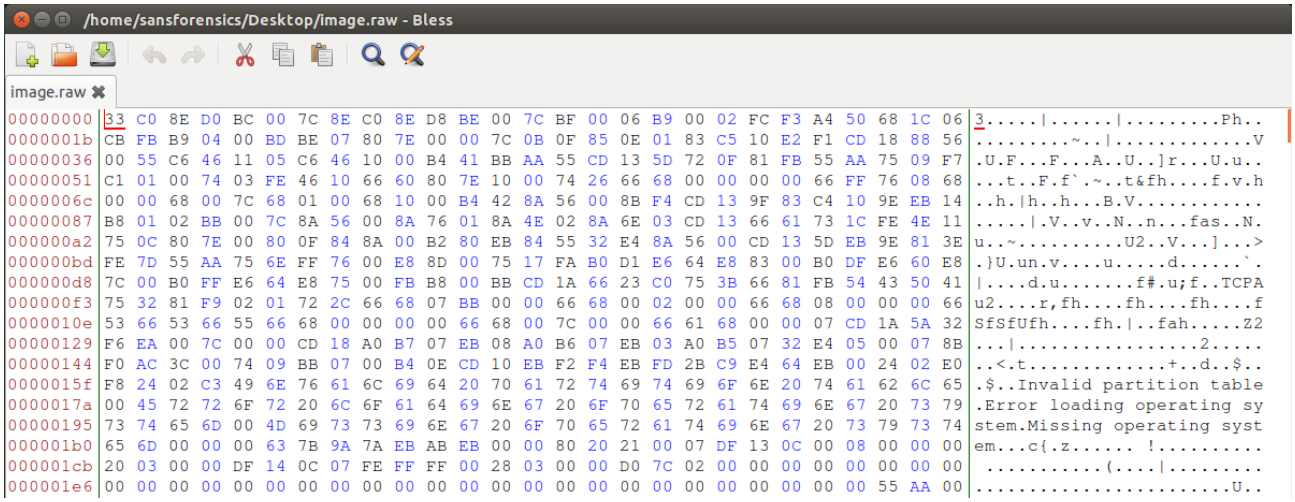

Рис. 3. Просмотр образа диска через HEX-редактор

Теперь следующим этапом попытаемся узнать, что же так негативно повлияло на главную загрузочную запись. Итак, открываем консоль и вводим команду «log2timeline.py timeline.dmpimage.raw»:

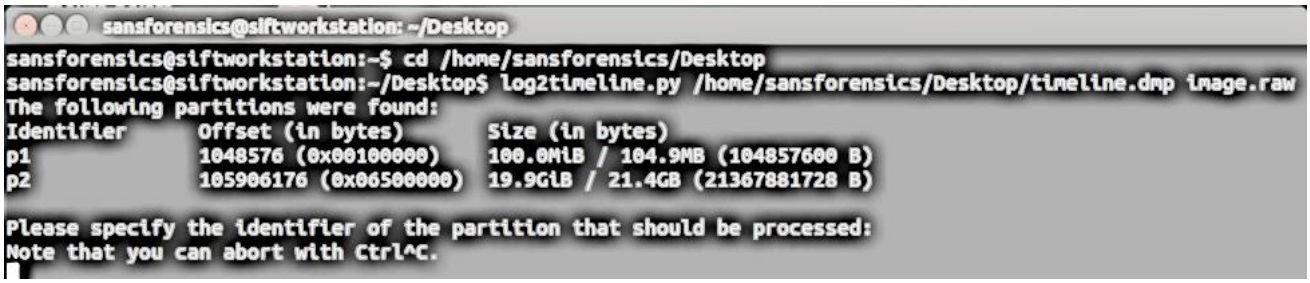

Рис. 4. Результат ввода команды «log2timeline.py timeline.dmpimage.raw»

Нас просят выбрать один из найденных разделов для извлечения из него всех найденных событий в файл timeline.dmp. Выбираем p2 (так как в нем содержится вся необходимая для анализа пользовательская информация). Перед нами может появиться следующее окно:

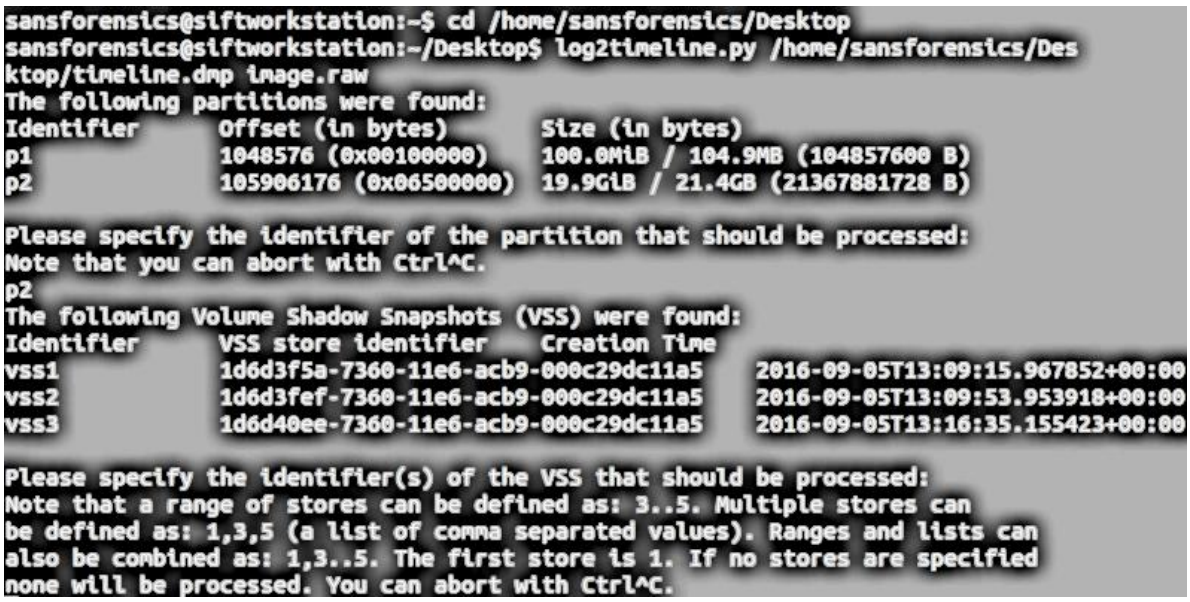

Рис. 5. Результат ввода команды «p2»

Как мы видим, найдены снимки службы теневого копирования тома. Ниже мы можем обнаружить следующие наименования столбцов: «VSSstoreidentifier» – уникальный идентификатор, «CreationTime» – время создания теневой копии. Далее говорится, что необходимо выбрать идентификаторы службы теневого копирования тома для их дальнейшей обработки. Выбираем vss1, vss2 и vss3, введя команду ls (см. рис. 6).

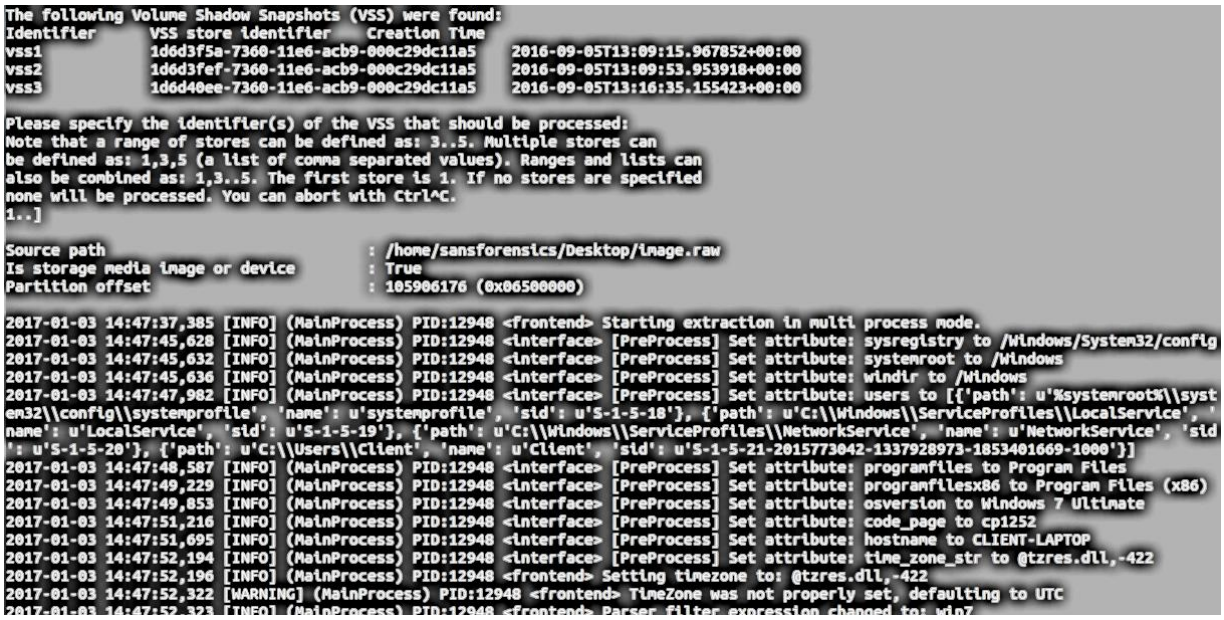

Рис. 6. Результат ввода команды «ls»

Теперь ждем, когда все события с файла image.raw запишутся в файл timeline.dmp. Это может занимать достаточно продолжительное время.

После того, как файл будет сформирован, мы можем из него вытащить много полезной информации, например, тот факт, что пользователь ранее пользовался ОС Windows 7 Ultimate и в ней использовал для входа в систему учетную запись под названием «Client» (см. рис. 7).

2016-09-07 18:16:40,881 [INFO] (MainProcess) PID:12214 <frontend> Starting extraction in multi process mode.
2016-09-07 18:16:43,710 [INFO] (MainProcess) PID:12214 <interface> [PreProcess] Set attribute: sysregistry to /Windows/System32/config
2016-09-07 18:16:43,714 [INFO] (MainProcess) PID:12214 <interface> [PreProcess] Set attribute: systemroot to /Windows
2016-09-07 18:16:43,717 [INFO] (MainProcess) PID:12214 <interface> [PreProcess] Set attribute: windir to /Windows
2016-09-07 18:16:45,590 [INFO] (MainProcess) PID:12214 <interface> [PreProcess] Set attribute: users to [{'path': u'%systemroot%\\system32\\config\\systemprofile', 'name': u'systemprofile', 'sid': u'S-1-5-18'}, {'path': u'C:\\Windows\\ServiceProfiles\\LocalService', 'name': u'LocalService', 'sid': u'S-1-5-19'}, {'path': u'C:\\Windows\\ServiceProfiles\\NetworkService', 'name': u'NetworkService', 'sid': u'S-1-5-20'}, {**'path': u'C:\\Users\\Client', 'name': u'Client'**, 'sid': u'S-1-5-21-2015773042-1337928973-1853401669-1000'}]
2016-09-07 18:16:46,084 [INFO] (MainProcess) PID:12214 <interface> [PreProcess] Set attribute: programfiles to Program Files
2016-09-07 18:16:46,502 [INFO] (MainProcess) PID:12214 <interface> [PreProcess] Set attribute: programfilesx86 to Program Files (x86)
2016-09-07 18:16:46,900 [INFO] (MainProcess) PID:12214 <interface> [PreProcess] Set attribute: osversion **to Windows 7 Ultimate**
2016-09-07 18:16:47,854 [INFO] (MainProcess) PID:12214 <interface> [PreProcess] Set attribute: code_page **to cp1252**
2016-09-07 18:16:48,325 [INFO] (MainProcess) PID:12214 <interface> [PreProcess] Set attribute: hostname **to CLIENT-LAPTOP**
2016-09-07 18:16:48,766 [INFO] (MainProcess) PID:12214 <interface> [PreProcess] Set attribute: time_zone_str **to @tzres.dll,-422**
2016-09-07 18:16:48,768 [INFO] (MainProcess) PID:12214 <frontend> Setting timezone to: @tzres.dll,-422
2016-09-07 18:16:48,832 [WARNING] (MainProcess) PID:12214 <frontend> TimeZone was not properly set, defaulting to UTC
2016-09-07 18:16:48,833 [INFO] (MainProcess) PID:12214 <frontend> Parser filter expression changed **to: win7**

Рис. 7. Просмотр сформированного журнала событий

Введем команду psort.py -w /home/sansforensics/Desktop/timeline.csv –oL2tcsv /home/sansforensics/Desktop/timeline.dmp “date> '2016-09-06'” для того, чтобы сформировать файл timeline.csv, который содержал бы все события на момент 06.09.2016 года. После успешного выполнения данной операции должно появиться следующее окно:

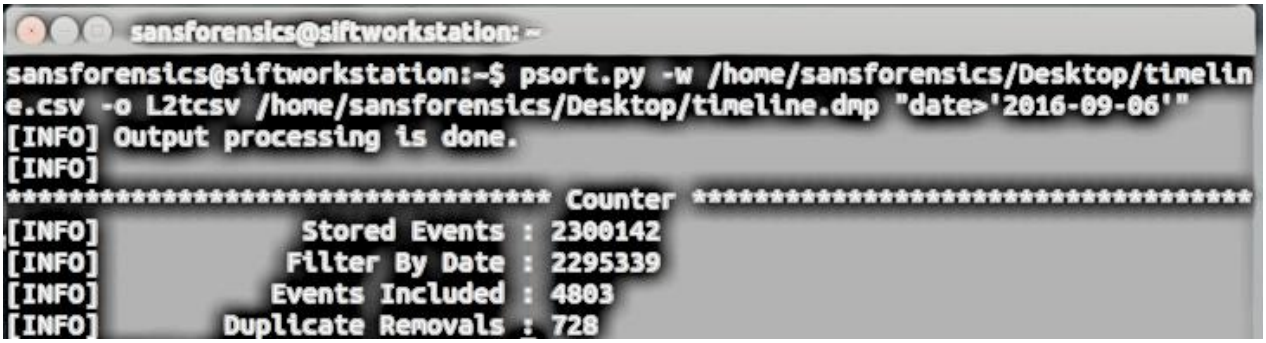

Рис. 8. Результат ввода команды «psort.py -w /home/sansforensics/Desktop/timeline.csv –oL2tcsv /home/sansforensics/Desktop/timeline.dmp “date> '2016-09-06'”»

Анализ обнаруженного вредоносного программного обеспечения, изучение следов работы вредоносного программного обеспечения.

После того, как мы сформировали журнал событий на период 6 сентября 2016 г., нам необходимо глубоко его проанализировать на наличие вирусов. Как мы видим, в 13:52:47 UTC был запущен файл mimi.exe (см. рис. 9).

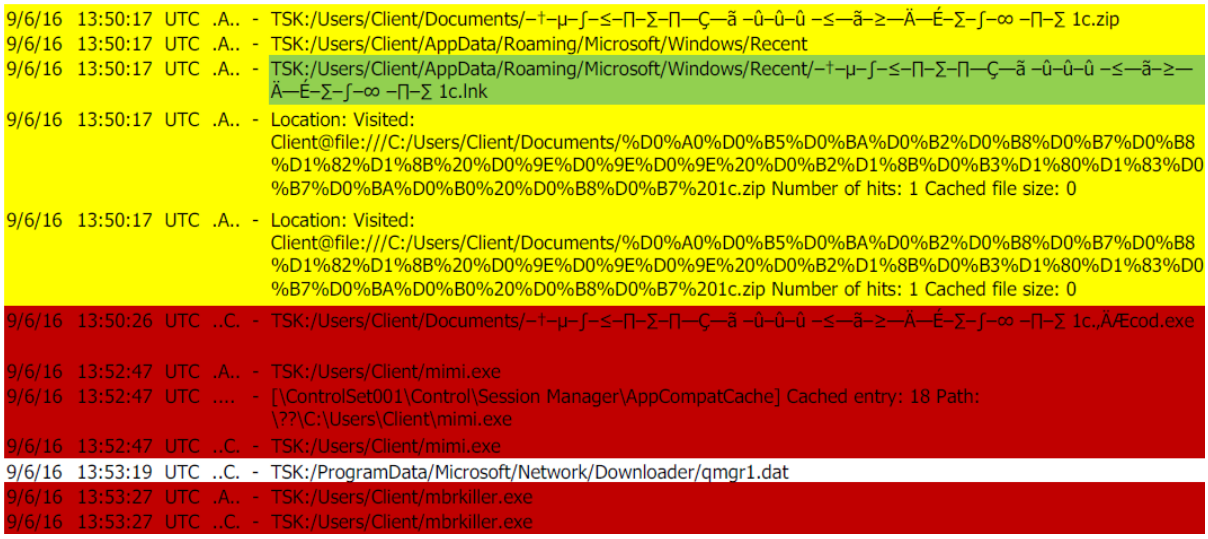

Рис. 9. Обнаружение в журнале событий вредоносного файла «mimi.exe»

Это троянец типа «BackDoor.Bladabindi.1856». Со всей технической информацией касательно него можно ознакомиться исходя из следующего рисунка:

Техническая информация

Вредоносные функции:

Для обхода брандмауэра удаляет или модифицирует следующие ключи реестра:

- [<HKLM>\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List] '%TEMP%\mimi.exe' = '%TEMP%\mimi.exe:*:Enabled:mimi.exe'

Создает и запускает на исполнение:

- '%TEMP%\mimi.exe'

Запускает на исполнение:

- '<SYSTEM32>\netsh.exe' firewall add allowedprogram "%TEMP%\mimi.exe" "mimi.exe" ENABLE

Изменения в файловой системе:

Создает следующие файлы:

- %TEMP%\mimi.exe

Сетевая активность:

Подключается к:

- 'th#####ocent.no-ip.biz':1983

UDP:

- DNS ASK th#####ocent.no-ip.biz

Рис. 10. Техническая информация троянца типа «BackDoor.Bladabindi.1856»

Если продолжать анализировать дальше, то мы увидим, что в 13 часов 53 минуты 27 секунд UTC был запущен mbrkiller.exe. Он же и привел к затиранию главной загрузочной записи.

Теперь проанализируем дамп оперативной памяти. Выполним команду vol.py -f /home/sansforensics/Desktop/ram.vmemimageinfo для определения профилей (см. рис. 11).

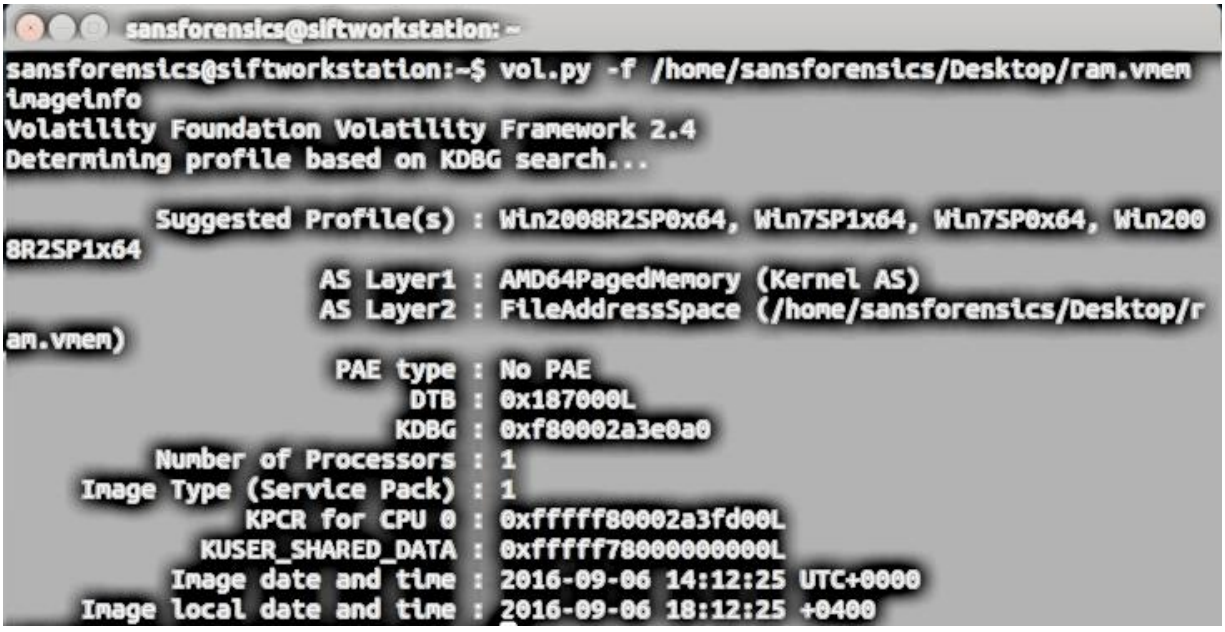

Рис. 11. Результат выполнения команды «vol.py -f /home/sansforensics/Desktop/ram.vmemimageinfo»

Теперь вводим команду vol.py -f /home/sansforensics/Desktop/ram.vmem --profile=Win7SP1x64 pstree для просмотра выполняющихся процессов в оперативной памяти и обнаружим троянский процесс mimi.exe и какой-то подозрительный процесс под названием 5:2878BK:

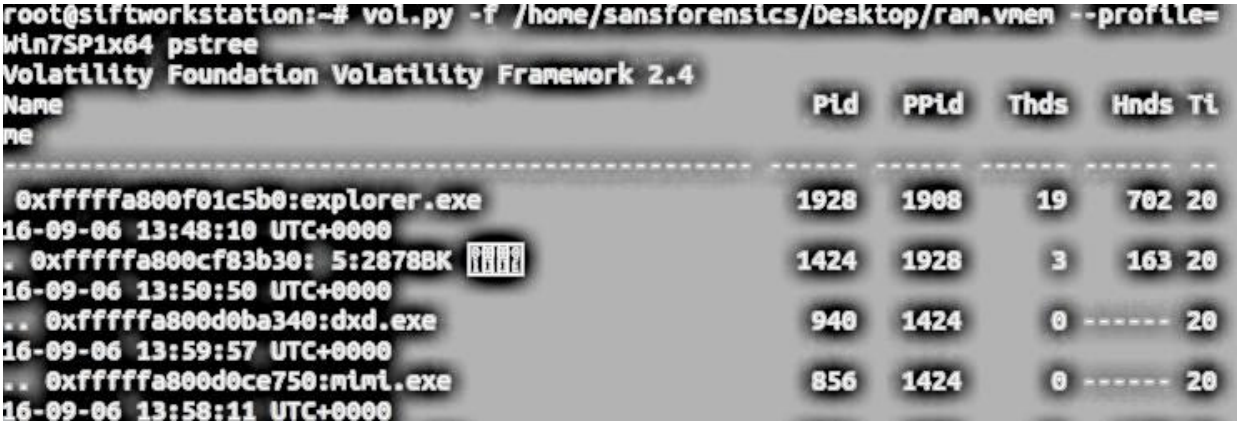

Рис. 12. Обнаружение выполняющихся троянских процессов

Теперь посмотрим на сетевую активность выполняющихся процессов в оперативной памяти, введя команду vol.py -f /home/sansforensics/Desktop/ram.vmem --profile=Win7SP1x64 netscan, и увидим подозрительную сетевую активность со стороны 0x3dbec910 TCPv4 192.168.180.131:49212 192.168.1.100:8080 ESTABLISHED 1424 5:2878BK. Она является подозрительной, потому что, во-первых, нет прямой сетевой активности со стороны mimi.exe, а значит, она может исходить от других процессов, которые могла сформировать троянская программа. Во-вторых, настораживает то, что данное смещение принимает значение «ESTABLISHED», и то, что в столбце «owner» стоит значение «5:2878BK» (см. рис. 13).

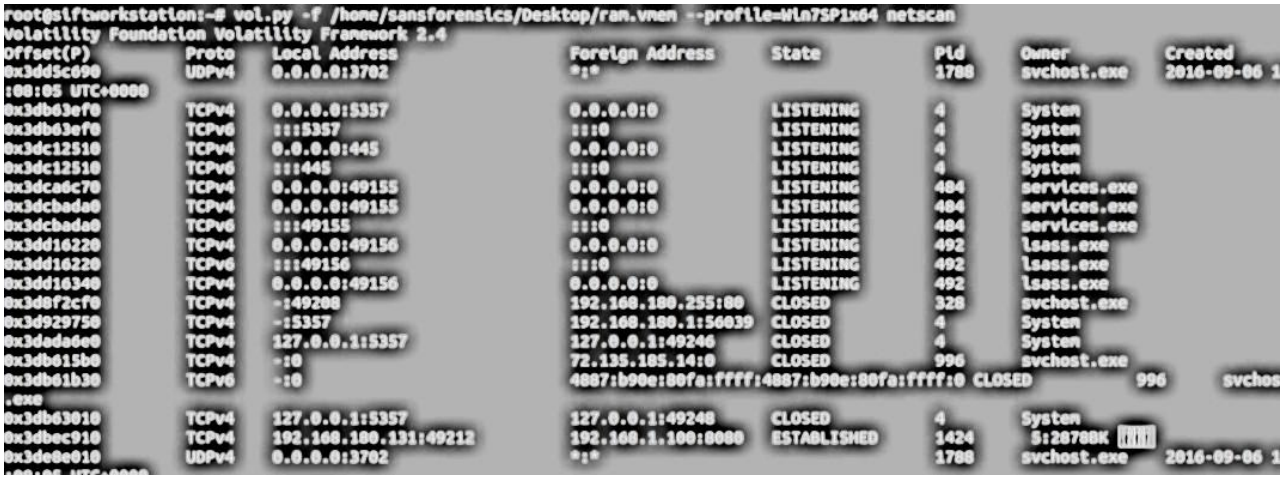

Рис. 13. Сетевая активность выполняющихся процессов в оперативной памяти

Теперь пришло время исследования реестра. Для этого необходимо ввести команду vol.py -f /home/sansforensics/Desktop/ram.vmem --profile=Win7SP1x64 hivelist.

Исходя из этих данных, нельзя однозначно сказать, что тут есть что-либо подозрительное. Поэтому следующим шагом введем команду vol.py -f /home/sansforensics/Desktop/ram.vmem --profile=Win7SP1x64

printkey -K «Software\Microsoft\WindowsNT\CurrentVersion» для просмотра содержимого, стоящего на автозапуске в «Software\Microsoft\WindowsNT\CurrentVersion».

Файл ntuser.dat, расположенный в C:\Users\Client\, был изменен 06 сентября 2016 г. в 13:58:16 (см. рис. 14).

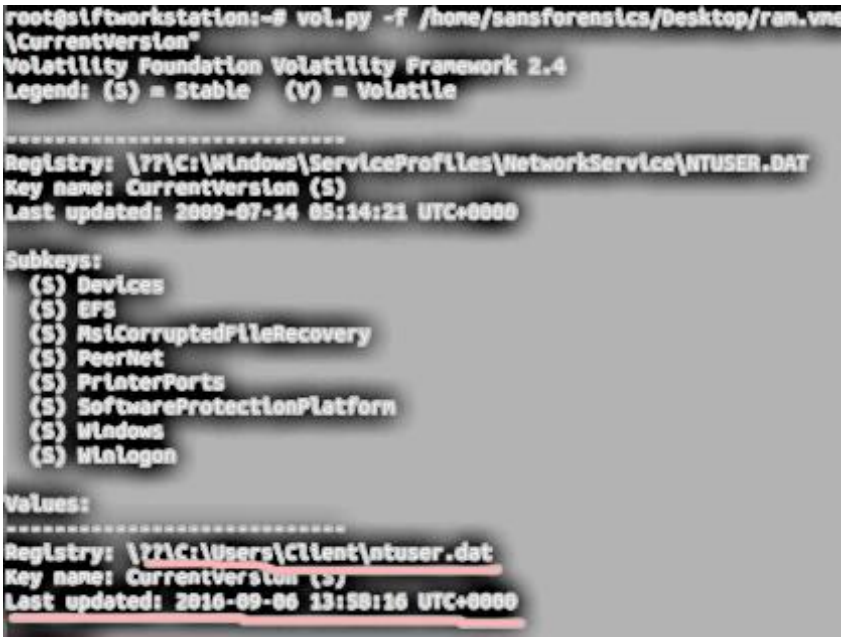

Рис. 14. Обнаружение изменений файла ntuser.dat

Анализируя журнал событий на период 6 сентября 2016 г., мы можем обнаружить, что в 13:58:11 злоумышленником удаленно было запущено программное обеспечение mimikatz.exe, которое позволяет выискивать в оперативной памяти учетные записи пользователей и относящиеся к ним пароли для входа в систему (см. рис. 15).

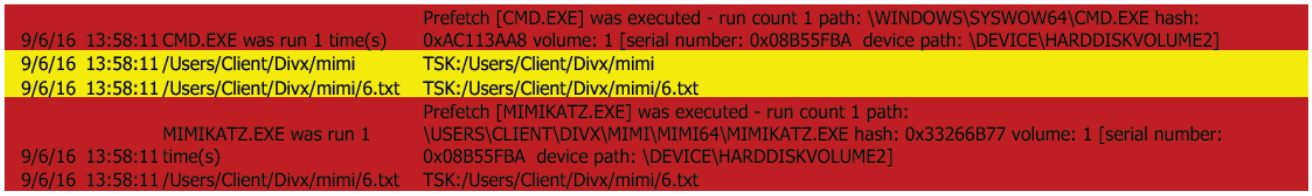

Рис. 15. Обнаружение запуска программы mimikatz.exe

Как правило, злоумышленник в этой программе сначала вводит команду privilege::debug (в случае успеха появится запись Privilege ‘20’ OK), после чего вводит securlsa::logonpasswordsfull для получения списка всех учетных записей и паролей к ним из оперативной памяти:

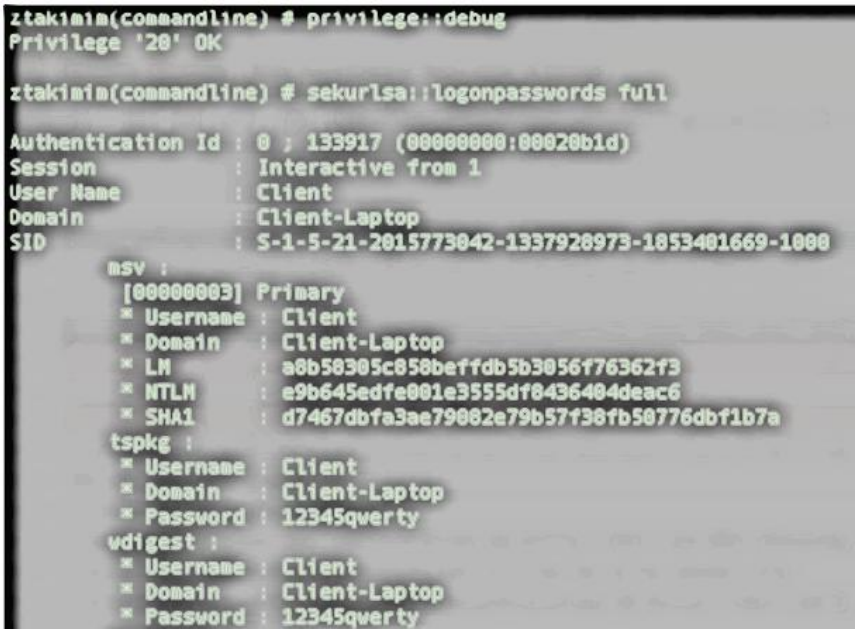

Рис. 16. Получение злоумышленником списка учетных записей с паролями

На последнем этапе необходимо ввести команду vol.py –f /home/sansforensics/Desktop/ram.vmem --profile=Win7SP1x64 malfind для просмотра скрытого или внедренного кода (библиотек dll) процесса 5:2878BK (см. рис. 17).

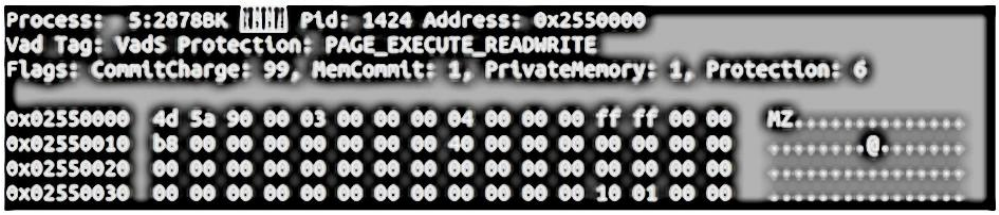

Рис. 17.

Рис. 18. Просмотр кода процесса 5:2878BK

Таким образом, был произведен сбор первоначальных сведений об инциденте, извлечены сведения из предоставленных носителей информации, произведен анализ обнаруженного вредоносного программного обеспечения и изучены следы работы вредоносного программного обеспечения.

Гончар В. В.[1],

доцент кафедры предварительного расследования
МосУ МВД России имени В.Я. Кикотя

ЕДИНООБРАЗНЫЙ ПОНЯТИЙНЫЙ АППАРАТ, КАК НЕОБХОДИМОЕ УСЛОВИЕ УСПЕШНОГО РАССЛЕДОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ПРЕСТУПЛЕНИЙ

В настоящее время проблемы информационной безопасности, защиты компьютерной информации, обеспечения защищенности сведений, образующих охраняемую законом тайну, расследования преступлений в сфере информационных технологий и иные подобные проблемы самым непосредственным образом связаны с обеспечением национальной безопасности государства, защитой конституционных прав и свобод человека и гражданина.

Нормативные правовые акты, активно принимаемые в последние месяцы, обозначили необходимость интенсивной информатизации многих сфер общественных отношений [1, 3]. В Указе Президента Российской Федерации от 7 мая 2018 г. № 204 среди основных национальных целей Российской Федерации в период до 2024 г. закреплены ускорение технологического развития страны, увеличение количества организаций, осуществляющих технологические инновации до 50 % от их общего числа, обеспечение ускоренного внедрения цифровых технологий в экономике и социальной сфере [2].

Одной из целей программы «Цифровая экономика Российской Федерации» является создание экосистемы цифровой экономики Российской Федерации, в которой данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности и в которой обеспечено эффективное взаимодействие, включая трансграничное, бизнеса, научно-образовательного сообщества, государства и граждан.

1 марта 2018 г. Президент Российской Федерации В. В. Путин в послании Федеральному Собранию отменил необходимость в кратчайшие сроки создать передовую законодательную базу, снять все барьеры

для разработки и широкого применения робототехники, искусственного интеллекта, беспилотного транспорта, электронной торговли, технологий обработки больших данных. Причем такая нормативная база должна постоянно обновляться, строиться на гибком подходе к каждой сфере и технологии [4].

Цифровая экономика, цифровая школа, беспилотные автомобили, цифровая медицина, «умные» дома и города – все это, до недавнего времени воспринимаемое как фантастическое будущее, становится настоящим.

Активное внедрение информационных технологий в различные сферы жизни общества и функционирования государства, недостаточное обеспечение информационной безопасности данных процессов, создает предпосылки увеличения компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее[1].

Статистика демонстрирует не простую ситуацию с выявлением, раскрытием и расследованием подобных преступлений. Так, в 2017 г. зарегистрировано 90587 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, из них раскрыто всего 20424 (менее 23 %) [5]. Этот статистический показатель в МВД России появился только в 2017 г., заменив показатель о количестве зарегистрированных и раскрытых преступлений в сфере компьютерной информации (используемый до 2016 г. включительно), в соответствии с которым за 2016 г. было зарегистрировано 1746 (раскрыто 903) преступления [6].

Сопоставив сведения официальной статистики с информацией из иных источников, можно осознать масштаб проблемы. Так, в ФСБ РФ сообщили, что за 2016 г. хакеры совершили 70 млн кибератак на объек-

[1] П. 14 Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

ты, находящиеся на территории России [7], а руководитель «Лаборатории Касперского» Евгений Касперский заявил, что в 2017 году специалистами лаборатории выявлено около 100 млн ранее не зарегистрированных вредоносных программ [8]. Без преувеличения, можно констатировать факт, что преступления в сфере компьютерной информации сегодня являются самыми латентными преступлениями, а проблема выявления, раскрытия и расследования подобных преступлений – одна из наиболее актуальных для научного сообщества и правоохранительных органов.

На сложность ситуации обратил внимание Президент Российской Федерации В. В. Путин, выступая на расширенном заседании коллегии МВД России 28 февраля 2018 г., отметив низкий уровень раскрываемости преступлений против собственности, совершаемых с использованием компьютерных и телекоммуникационных технологий [9].

Решение любой серьезной проблемы, а проблема низкой выявляемости и раскрываемости подобных преступлений, безусловно, является таковой, невозможно без понимания сути (смысла) этой проблемы. Понимание сути невозможно без уяснения определения основных понятий.

Перед началом рассмотрения отдельных категорий понятийного аппарата следует отметить, что автор при употреблении термина «преступления в сфере компьютерной информации» употребляет его в широком смысле и относит к ним все общественно опасные деяния, где компьютерная техника (компьютерная информация) выступает средством (способом) совершения преступления, т. е. не ограничивается анализом деяний, предусмотренных в гл. 28 УК РФ.

Если подходить формально юридически, под «преступлениями в сфере компьютерной информации» необходимо понимать только те, которые включены в одноименную Главу 28 УК РФ, а именно:

– ст. 272. Неправомерный доступ к компьютерной информации;

– ст. 273. Создание, использование и распространение вредоносных компьютерных программ;

– ст. 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;

– ст. 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Однако очевидно, что деяния, зафиксированные в ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации», являются: преступлениями; в сфере компьютерной информации, что следует из гипотезы этой статьи.

Проблема усугубляется тем, что дать однозначное определение этим преступлениям объективно затруднительно, так как есть сложности с выделением какого-либо одного объекта преступного посягательства [10, с. 84–85].

Различные ученые по-разному объясняют отсутствие в науке и практике однозначного определения «преступлений в сфере компьютерной информации»: одни – значительным практическим разнообразием подобных преступлений [11, с. 22–26], другие – отсутствием единообразной доктринальной позиции и отнесения конкретных общественно опасных деяний к таким преступлениям [12, с. 53–63].

В результате появились и активно используются в науке и практике значительное количество терминов, под которыми понимаются схожие общественно опасные деяния, например: «преступления в сфере компьютерной информации»[1], «компьютерные преступления» [13, с. 5], «киберпреступления» [14, с. 41–44], «преступления в сфере информационных технологий» [15, с. 130–135], «преступления в сфере информационно-коммуникационных технологий» [16, с. 73–80], «преступления против информационной безопасности» [17, с. 10], «преступления в сфере высоких технологий» [18, с. 41–46], «преступления, совершаемые с использованием информационно-телекоммуникационных технологий» [19, с. 42–44], «преступления в сфере высоких информационно-телекоммуникационных технологий» [20, с. 231], «преступления, совершаемые с использованием компьютерных технологий» [21, с. 1], «преступления в сфере электронной информации» [22, с. 22–26] и другие.

[1] Глава 28 УК РФ.

Не меньшее «разнообразие» определений однородных преступлений наблюдается и в нормативных правовых актах. Так:

– в п. 8 Окинавской хартии глобального информационного общества закреплено следующее: «Мы должны обеспечить осуществление эффективных мер – как это указано в Руководящих принципах по безопасности информационных систем ОЭСР – в борьбе *с преступностью в компьютерной сфере*» (выд. авт.) [23];

– в названии «Конвенции о преступности в сфере компьютерной информации» (ETS № 185) [24] зафиксирован термин *«преступность в сфере компьютерной информации»*, однако Россия приняла решение подписать данный документ в соответствии с Распоряжением Президента Российской Федерации «О подписании Конвенции о киберпреступности» от 15 ноября 2005 г. № 557-рп[1], в котором закреплен уже другой термин *«киберпреступность»*. Очевидно, что в данных документах *преступность в сфере компьютерной информации* и *киберпреступность* отождествлены;

– термин «*преступления в сфере компьютерной информации*» закреплен в гл. 28 УК РФ;

– термин «*преступления в сфере высоких технологий»* зафиксирован в Распоряжении Правительства Российской Федерации от 22 октября 1999 г. № 1701-р «О мерах по усилению борьбы с преступлениями в сфере высоких технологий»;

– в п. 96 Приказа МВД России № 786, Минюста России № 310, ФСБ России № 470, ФСО РФ № 454, ФСКН РФ № 333, ФТС РФ № 971 от 6 октября 2006 г. «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола» зафиксировано, что по соответствующим запросам может быть получена информация о физических и юридических лицах, имеющих отношение *к преступлениям в **сфере** высоких технологий*; а в п. 97 этого же Приказа рассматриваются требования к запросам *о преступлении* уже *в **области** высоких технологий* (выд. авт.);

---

[1] Россия приняла решение подписать «Конвенцию о преступности в сфере компьютерной информации» с заявлением в соответствии с распоряжением Президента РФ от 15 ноября 2005 г. № 557-рп, которое признано утратившим силу распоряжением Президента РФ от 22 марта 2008 г. № 144-рп.

– в п. 15 Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года[1] закреплена необходимость повышения эффективности …противодействия *преступности в сфере использования информационных и коммуникационных технологий* (выд. авт.);

– в п. 44 Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 31 декабря 2015 г. № 683, упоминается о предупреждении *преступности (в том числе в информационной сфере)* (выд. авт.);

– в п. 14 Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, в числе прочих рассматриваются *преступления с использованием информационных технологий* (выд. авт.); такой же термин закреплен в «Программе сотрудничества государств – участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий, на 2016–2020 годы» [25];

– в Проекте Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий, одобренного Постановлением Правительства Российской Федерации от 19 августа 2017 г. № 983, содержится еще один термин – *преступления в сфере информационных технологий*.

Этот перечень может быть продолжен.

Очевидно, что различие в терминологии указывает на отсутствие единого подхода к данной проблеме, как в научном сообществе, так и среди субъектов уполномоченных принимать нормативные правовые акты.

Попытки систематизировать и унифицировать понятийный аппарат в рассматриваемой сфере предпринимались достаточно давно. Так в марте 1993 г. на постоянно действующем межведомственном семинаре «Криминалистика и компьютерная преступность», организованном координационным бюро по криминалистике НИИ проблем укреп-

[1] Утверждены Президентом Российской Федерации 24 июля 2013 г. № пр-1753 // СПС КонсультантПлюс, 2018.

ления законности и правопорядка Генеральной прокуратуры и экспертно-криминалистическим центром МВД России, обсуждался вопрос состоятельности термина «компьютерные преступления» [13, с. 6], которые в то время отождествлялись большинством ученых с преступлениями в сфере компьютерной информации.

Одна группа ученых выступила против употребления данного термина, утверждая, что неверно дифференцировать преступления по виду технических средств, с помощью которых они совершаются [26, с. 167].

Другие ученые признавали справедливость формулировки термина «компьютерное преступление», так как данный термин уже воспринят как зарубежной, так и отечественной практикой [27, с. 37–37; 28, с. 9].

Прошедшие десятилетия не позволили сформировать единых подходов к определению термина «преступления в сфере компьютерной информации», так, как и сегодня в различных публикациях продолжают появляться авторские мнения по данному термину [29,с. 34–39; 30, с. 19–23].

Отсутствие законодательного определения «преступления в сфере компьютерной информации», различия в научном толковании этого термина приводят к ошибкам, допускаемым правоприменителями в процессе квалификации соответствующих деяний на стадии возбуждения уголовного дела и в процессе дальнейшего расследования.

Считаем, что одной из основных причин отсутствия единообразия в понимании, определении и правоприменении этого термина является отсутствие единообразного понимания его элементов. Так, понятие «преступление в сфере компьютерной информации» состоит из следующих элементов: «преступление»; «в сфере» и «компьютерная информация».

Определение понятий первых двух элементов не вызывает сложностей в восприятии и толковании, закреплено в ч. 1 ст. 14 УК РФ и в соответствующих словарях.

Сложнее с определением понятия «компьютерная информация». Считаем, что именно с неоднозначностью понимания и толкования данного термина связаны трудности с пониманием, толкованием

и правоприменением определения термина «преступления в сфере компьютерной информации».

В настоящее время нормативно закреплены несколько определений этого понятия.

В п. «б» ст. 1 Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (заключено в г. Минске 1 июня 2001 г.) компьютерная информация понимается как *информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи.*

В примечании 1 к ст. 272 УК РФ под компьютерной информацией понимаются *сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи*.

Данные определения не тождественны, порождают различные точки зрения в науке, создают значительные затруднения для правоприменителей при квалификации деяния на стадии возбуждения уголовного дела и дальнейшем расследовании.

Автор считает, что уяснение понятия «компьютерная информация» невозможно без осмысления понятия «информация», определение которого закреплено в ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» как сведения (сообщения, данные) независимо от формы их представления. Данное определение неоднозначно и неопределенно. Считаем, что понятие «информация», несмотря на широкую распространенность и наличие значительного количества исследований в этой области [31, с. 22–48; 32, с. 16–35; 33, с. 20–35], остается одним из самых дискуссионных в науке. Однако без уяснения единообразного юридического смысла данного понятия, невозможно уяснить смысл его правовых производных.

В заключение следует отметить, что пока не выработаны единообразные научные подходы и законодательно не закреплены определения понятия «преступление в сфере компьютерной информации», «компьютерная информация» и «информация», новые авторские определения

будут появляться и устаревать вместе с совершенствованием технологий обмена информацией. Создать единые представления о противодействии данным видам преступлений, сформировать единое учение о компьютерной информации и электронных документах, как самостоятельных видах доказательств, решить проблему выявления, раскрытия и расследования подобных преступлений будет практически невозможно. Стадия осмысления проблемы не закончится. Пути ее решения не будут найдены.

Список литературы

1. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «КонсультантПлюс», 2018.

2. Указ Президента Российской Федерации от 7 мая 2018 г. № 207 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // СПС «КонсультантПлюс», 2018.

3. Распоряжение Правительства Российской Федерации от 28 июля 2017 г. № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» // СПС «КонсультантПлюс», 2018.

4. http://kremlin.ru/events/president/news/56957.

5. https://мвд.рф/reports/item/12167987/.

6. https://мвд.рф/reports/item/9338947/.

7. https://www.rbc.ru/rbcfreenews/5887412f9a7947c9173d120b?from=newsfeed.

8. https://www.rbc.ru/technology_and_media/03/12/2017/5a2405079a7947213b28a893.

9. http://kremlin.ru/events/president/news/56949.

10. Гайдамакин А. А. Информационная безопасность в органах внутренних дел и применение информационных технологий в борьбе с преступностью / А. А. Гайдамакин и др. – Омск, 2010.

11. Чуищев, И. М. Может ли хакер защитить от компьютерных преступлений? / И. М. Чуищев. – М. : Юрист. – 1999. – №2.

12. Ястребов,Д. А. Институт уголовной ответственности в сфере компьютерной информации:Опыт международно-правового сравнительного анализа / Д. А. Ястребов // Государство и право. – 2005. – № 1.

13. Мазуров В. А. Компьютерные преступления: классификация и способы противодействия : учебно-практическое пособие. – М. : «Палеотип», «Логос», 2002.

14. Расулев А. К. Тенденции развития объекта киберпреступлений в англосаксонской правовой системе // Российский следователь. – 2016. – № 21.

15. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3.

16. Русскевич Е. А. Уголовное право и информатизация // Журнал российского права. – 2017. – № 8.

17. Лепехин А. Н. Расследование преступлений против информационной безопасности: теоретико-правовые и прикладные аспекты: монография. – Минск : Тессей, 2008.

18. Третьяк М. И. Проблема законодательной регламентации преступлений против собственности в сфере высоких технологий // Законность. – 2016. – № 7.

19. Колычева А. Н. К вопросу об использовании ресурсов сети Интернет в преступной деятельности // Российский следователь. – 2016. – № 24.

20. Кушниренко С. П. Преступления в сфере высоких информационно-телекоммуникационных технологий: анализ региональной судебно-следственной практики // Библиотека криминалиста. Научный журнал. – М. : Юрлитинформ. – 2013. – № 5 (10). – С. 231.

21. Шмонин А. В. и др. Организация расследования хищений денежных средств, совершаемых с использованием компьютерных технологий : аналитический обзор. – М. : Академия управления МВД России, 2015. – С. 1.

22. Соколов Ю. Н. Электронный носитель информации в уголовном процессе // Информационное право. – 2017. – № 3.

23. Окинавская хартии глобального информационного общества (принята на о. Окинава 22 июля 2000 г.) // СПС «КонсультантПлюс», 2018.

24. Конвенция о преступности в сфере компьютерной информации (ETS № 185) (Заключена в г. Будапеште 23 ноября 2001 г.) // СПС «КонсультантПлюс», 2018.

25. Решение Совета глав государств СНГ «О Программе сотрудничества государств–участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий, на 2016–2020 годы», принято в г. Бишкеке 16 сентября 2016 г. // СПС «КонсультантПлюс», 2018.

26. Курило А. П. О проблеме компьютерной безопасности // Научно-техническая информация. Сер. 1. Организация и методика информационной работы. – 1993. – № 8. – С. 7.

27. Батурин Ю. М. Проблемы компьютерного права. – М. : Юридическая литература, 1991.

28. Селиванов Н. Проблемы борьбы с компьютерной преступностью // Законность. – 1993. – №8.

29. Вехов В. В. Компьютерные преступления: способы совершения и раскрытия. – М. : Право и Закон, 1996. С. 20.

30. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. – 1997. – № 1.

31. Халиуллин А. И. Подходы к определению киберпреступления // Российский следователь. – 2015. – № 1.

32. Турышев А. А. Уголовно-правовые инструменты защиты информационного общества // Законы России: опыт, анализ, практика. – 2017. – № 10.

33. Манжуева О. М. Феномен информационной безопасности: сущность и особенности : дис. ... докт. философ. наук: 09.00.11. – Улан-Удэ, 2015.

34. Шутова А. А. Уголовно-правовое противодействие информационным преступлениям в сфере экономической деятельности: теоретический и прикладной аспекты : дис. … канд. юрид. наук: 12.00.08. – Нижний Новгород, 2017.

35. Бегишев И. Р. Понятие и виды преступлений в сфере обращения цифровой информации : дис. … канд. юрид. наук: 12.00.08. – Казань, 2017.

Любан В. Г.[1],

доцент кафедры оперативно-розыскной деятельности
МосУ МВД России имени В.Я. Кикотя,
кандидат технических наук;

Молянов А. Ю.[2],

доцент кафедры оперативно-розыскной деятельности
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук, доцент

ОПЕРАТИВНО-РАЗЫСКНАЯ ХАРАКТЕРИСТИКА РАСПРОСТРАНЕННЫХ МОШЕННИЧЕСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В последние годы борьба с мошенничествами в сфере информационно-телекоммуникационных технологий приобрела особую остроту и стала выделяться в качестве одного из приоритетных направлений. Нам представляется, что для успешного ее осуществления сотрудникам органов внутренних дел необходимо ознакомиться с классификацией современных способов их совершения. Ведь давно известно, что изучение способов совершения преступлений служит ценным источником сведений, необходимых для разработки средств, приемов и методов раскрытия, расследования и предупреждения преступлений [1, с. 4].

В теории оперативно-разыскной деятельности информация о способе совершения преступлений является важным элементом оперативно-разыскной характеристики преступлений, составляющим ее «ядерное» содержание.

Разберем способы совершения наиболее распространенных в практике мошенничеств в сфере информационно-телекоммуникационных технологий:

I. Мошенничества с использованием средств мобильной телефонной связи (так называемые, телефонные мошенничества):

1. Схема SMS-мошенничества – «Блокировка банковской платежной карты (далее по тексту «банковская платежная карта» – БПК) или несанкционированное списание с нее средств».

Человек получает SMS-сообщение, содержащее телефон для обратной связи (например, «Ваша карта VISA заблокирована. Справка по тел.: 8-960-848-88-85. ЦБ РФ»).

Перезвонившему на указанный в сообщении номер мошенники могут представиться сотрудниками службы безопасности банка; специалистами службы технической поддержки или контактного центра; сотрудниками платежной системы и др.

Преступники вводят человека в заблуждение и вытягивают из него информацию относительно реквизитов его банковской платежной карты. Нередко уже на этом этапе мошенники пытаются провести регистрацию (перерегистрацию) Интернет-банка потерпевшего, используя сервисы удаленной регистрации. Войдя в Интернет-банк потерпевшего, преступники получают доступ ко всем его счетам и вкладам. Причем хищение средств с вкладов или счетов становится для них приоритетной задачей, так как на них, как правило, имеется более внушительная сумма.

В случае, когда по какой-то причине преступники отказываются от схемы с регистрацией (перерегистрацией) Интернет-банка, они в убедительной форме предлагают потерпевшему срочно провести действия по разблокировке карты, по отмене перевода, по возврату зарезервированных средств и т. п. Следуя получаемым по телефону инструкциям, потерпевшие: подключают Мобильный банк на телефон мошенников; сообщают им реквизиты других своих банковских платежных карт; сообщают им логины и пароли от Интернет-банка; сами отправляют со своего телефона SMS-оферты для подтверждения операций.

В итоге сбережения потерпевших мошенники переводят на подконтрольные электронные платежные сервисы, БПК, банковские счета, лицевые счета телефонных номеров или используют для покупок в интернет-магазинах, интернет-казино, игровых интернет-платформах и др.

2. Схема мошенничества «Проблема с законом у родственника»:

Преступник звонит на мобильный или домашний стационарный телефон незнакомому человеку (стараясь выбирать граждан пожилого возраста) и представляется ему близким родственником (сыном, внуком), либо сотрудником правоохранительных органов (следователем,

оперуполномоченным, сотрудником ГИБДД и т. п.), задержавшим его близкого родственника.

Далее мошенник под видом запуганного родственника (изменив голос) или сотрудника правоохранительного органа сообщает потерпевшему, что у него самого или у его родственника возникли проблемы с законом (он сбил человека, задержан с наркотиками, находился за рулем в нетрезвом виде и др.), однако пока есть возможность эти проблемы уладить за определенную сумму.

Если потерпевший соглашается «дать взятку» за непривлечение «родственника» к уголовной или административной ответственности, то мошенник указывает способы передачи или перечисления денег.

Если мошенник настаивает на передаче денег нарочно, то за ними, как правило, приезжает таксист (курьер), который забирает деньги и в дальнейшем (все или их часть) передает (переводит) непосредственно инициатору преступления, его родственникам либо иным лицам, рекомендованным преступником при разговоре с таксистом (курьером) по телефону.

Если мошенник предлагает безналичный перевод, то деньги зачисляются на номера телефонов, БПК, электронные кошельки (Яндекс. Деньги, WebMoney, Qiwi и др.), или отправляются почтовым или банковским переводом (например, по системе Юнистрим, Western Union, Золотая корона и др.).

Подельник преступника, осуществивший снятие денежных средств с банковского счета или с БПК, используя банкомат, терминал самообслуживания, Интернет-банк, осуществляет перевод денежных средств преступнику или его родственникам [2].

3. *Схема телефонного мошенничества в отношении пожилых людей, пенсионеров, обманутых дольщиков, льготников и других незащищенных слоев населения под видом различных социальных выплат или компенсаций:*

Мошенники связываются с пожилым человеком, пенсионером, обманутым дольщиком, льготником или иным лицом из числа незащищенных слоев населения, позвонив ему на телефон (чаще домашний), и представляются сотрудниками: Пенсионного фонда России (ПФР);

банка; службы социальной защиты населения; ОВД, прокуратуры, или иных правоохранительных органов.

Человеку предлагают получить единовременную социальную выплату или компенсацию, например, по следующим причинам: он попадает под действие государственной программы «Дети войны» и ему положена путевка в санаторий и единовременная денежная выплата в размере от 200 до 500 тысяч рублей; он не пользуется социальными пособиями и ему полагается компенсация; он когда-то уже пострадал от мошенников, их поймали и теперь возвращают деньги и др.

Как правило, у мошенников уже имеется начальная информация об объекте мошеннической атаки (чаще всего, это: ФИО, дата рождения, адрес, телефон; сведения, что тот ранее уже становился жертвой мошенников, и др.). Данную информацию мошенники получают следующим образом: из открытого доступа в сети Интернет; используя утечку из правоохранительных органов; используя утечку из ПФР и других источников.

Для получения обещанной социальной выплаты или компенсации человек следует указаниям мошенников и сообщает номер своей БПК, а если карты нет, то оформляет ее; подключает услугу «Мобильный банк» и «привязывает» телефон мошенников к своей БПК; сообщает свои персональные данные; сообщает мошенникам логины и пароли входа в Интернет-банк, в том числе в его Мобильное приложение, SMS-коды для регистрации Интернет-банка и перевода средств, CVV2 (CVC2) коды и т. д.

В результате мошенники получают полный доступ к системе Интернет-банка и проводят несанкционированные операции с вкладов и карт клиента.

В случае, когда у потерпевших нет оформленных БПК, или нет средств на них, иногда мошенникам удается выманить от 30 до 70 тыс. руб., под видом оплаты 13 % налога на доходы.

II. Мошенничества с использованием сети Интернет (так названные интернет-мошенничества).

1. Схема мошенничества на российских торговых интернет-площадках бесплатных объявлений:

а) первый вариант, если «преступник–покупатель»:

Добропорядочный человек размещает объявление на подходящем сайте (Avito, Avto.ru, Из рук в руки и др.) о продаже какого-либо товара. Ему поступает звонок якобы от покупателя, готового приобрести данный товар по безналичному расчету, путем перевода средств на БПК, для чего запрашивает ее номер. Если продавец соглашается и сообщает номер БПК, то далее возможны следующие варианты развития событий:

– Мошенники делают попытку перерегистрации Интернет-банка потерпевшего. Необходимость сообщить пароли они объясняют, например, тем, что перевод осуществляется со счета коммерческого банка, а не с БПК, и поэтому перевод не проходит, пока не будет получено подтверждение паролем из SMS. Если человека удается таким образом обмануть, то денежные средства с его карт и вкладов похищаются посредством перевода на банковские счета, БПК или счета телефонных номеров.

– Мошенники внушают человеку, что для успешного перевода средств необходимо сделать номер их телефона доверенным перед Банком, для чего просят проделать эту процедуру с банкомата. Введенный таким образом в заблуждение человек сам подключает Мобильный Банк на телефон мошенников. Мошенники регистрируются в Интернет-банке и похищают средства потерпевшего с его БПК и вкладов.

– Мошенники совершают онлайн-покупку на крупную сумму, используя реквизиты карты потерпевшего (номер карты, CVV2 (CVC2) код, срок действия карты, имя владельца), которые он сам им сообщил;

б) второй вариант, если «преступник–продавец»:

Мошенники сами размещают объявление на подходящей торговой интернет-площадке (о сдаче жилья, продаже машины, квартиры, антиквариата и др.), указывают телефон и (или) адрес электронной почты для обратной связи и ждут потенциального покупателя. Характерной особенностью привлечения потенциальных клиентов является указание в объявлении самой низкой рыночной цены, создающее впечатление максимальной выгоды.

Когда поступает звонок от лица, готового приобрести товар, ему предлагается внести предоплату или полную сумму переводом на банковский счет, БПК, электронный кошелек или на счет телефонного номера. Показывать товар мошенники под разными предлогами отказываются и предлагают переслать фотографию товара на электронную почту или мессенджеры.

Преступник может некоторое время вести электронную переписку и даже демонстрировать потерпевшему фотографии товара. Стараясь убедить покупателя в своей надежности и качестве товара, мошенники могут долго оговаривать цену, способ оплаты, сроки и условия доставки.

В качестве распространенного предлога невозможности осмотра товара вживую сообщается, что собственник находится в другом городе, в командировке, переехал на постоянное место жительства за границу и др. Необходимость внесения предварительной оплаты объясняется большим спросом на предмет аренды или продажи, и скорейшая предоплата только подтвердит серьезность намерений именно этого клиента.

Получив деньги, мошенники удаляют объявление с интернет-площадки, не отвечают на звонки потерпевшего и отключают свои телефоны.

2. Схема мошенничества в интернет-магазинах:

Мошенники создают в Интернете сайт под видом интернет-магазина, в котором предлагают клиентам различный ассортимент популярных товаров. Залогом успешного привлечения потенциальных клиентов является указание самой низкой рыночной цены.

Потенциальный покупатель в поисках нужного товара обнаруживает в Интернете сайт мошенников и решает сделать в нем заказ, оставив свои контакты. Через какое-то время он получает от магазина электронное письмо (сообщение) с подтверждением заказа и счетом на предварительную оплату товара, в котором указаны реквизиты банка, БПК или универсального электронного платежного сервиса.

В некоторых случаях покупатель перезванивает на телефонные номера, указанные на сайте, либо в электронных письмах (сообщениях). Мошенники убеждают его в том, что заказ принят, оговаривают сроки и условия доставки, а также прочие вопросы, создавая у потенциально-

го клиента впечатление надежности интернет-магазина, дорожащего своими клиентами.

Приняв решение о внесении предварительной оплаты, покупатель перечисляет денежные средства на присланный ему банковский счет, БПК или электронный кошелек.

С целью сокрытия следов преступления, еще некоторое время после получения денег мошенники отвечают потерпевшему, убеждают клиента в выполнении своих обязательств, объясняя задержку доставки товара различными непредвиденными обстоятельствами (задержками на таможне, проблемами у поставщика, большим количеством заказов, блокировкой банковских счетов, ожиданием поставки, указанной покупателем комплектации, и т. п.).

Обманув достаточное количество клиентов, мошенники перечисляют денежные средства с промежуточных банковских счетов и платежных сервисов на другие банковские счета, БПК, после чего обналичивают их и прекращают всякие контакты с потерпевшими.

3. Схема мошенничества *в социальных сетях и* Skype*:*

а) первый вариант – «от имени друга»:

Мошенники взламывают личный кабинет пользователя в социальных сетях или Skype и от его имени рассылают его друзьям (контактам) сообщения с различными просьбами, например, такими, как:

– с просьбой к «другу» одолжить денег, перечислить деньги на Интернет, оплатить телефон своего «родственника» и т. д., под предлогом, что он заболел, его уволили, он попал в аварию, ему срочно нужно оплатить Интернет, ему нужно пополнить счет БПК, а сделать это негде и т. п.

Если человек соглашается, ему приходит сообщение с номером БПК или номером телефона мошенников, на которые он должен перевести указанную сумму. Спустя некоторое время потерпевший узнает от друга, что его аккаунт был взломан и он не просил ни о какой материальной помощи;

– с просьбой помочь вывести деньги с Яндекс-кошелька или с БПК на другую карту, которой у них якобы нет, под предлогом, что деньги могут сгореть, так как истекает срок действия Яндекс-кошелька (БПК). Если человек соглашается, мошенники запрашивают у него номер

БПК, ее реквизиты, приходящие на телефон SMS-коды или логин и пароль для входа в Интернет-банк, после чего похищают средства со счетов и вкладов потерпевшего;

– сообщают «другу», что потеряли свой телефон или он сломался, и просят «друга» срочно прислать свой номер телефона в ответном сообщении. Срочность объясняют тем, что должны получить от третьего лица важное SMS-сообщение, а так как их телефон утерян (сломан), то просят у «друга» разрешение прислать сообщение на его номер. Мошенники также просят «друга» сразу после получения сообщения от третьего лица переслать его им через социальную сеть (Skype). В результате активации мошенниками кода подтверждения, полученного в сообщении от потерпевшего, у последнего с телефона автоматически списываются разные денежные суммы;

б) второй вариант – «от имени сотрудника банка»:

Мошенники создают аккаунт в социальных сетях, который по стилистике и содержанию выглядит как страница сотрудника банка. Они находят клиентов этого банка (например, просматривая ленты официальной группы банка) и предлагают им помощь или консультационные услуги от имени банка. Под предлогом соблюдения формального требования перед консультацией клиента псевдоконсультанты запрашивают у него все необходимые данные для регистрации в Интернет-банке и проведения операций в сети Интернет.

Данный способ рассчитан на клиентов банка в возрасте, зарегистрированных в социальных сетях, имеющих счета в банках, пенсионные БПК. В результате человека обманывают под предлогом ликбеза в вопросах использования всех возможностей и удобств Интернет-банкинга, получают доступ к его Интернет-банку и похищают средства с его счетов и вкладов.

Нужно заметить, что в практике органов внутренних дел встречаются и другие виды мошенничеств в сфере информационно-телекоммуникационных технологий, однако в данной статье мы ограничились описанием лишь наиболее распространенных из них, составляющих «львиную» долю от общего числа.

Список литературы

1. Зуйков Г. Г. Поиск преступников по признакам способов совершения преступлений : учебное пособие. – М. : ВШ МВД СССР, 1970.

2. В результате проведенного в ГУУР МВД России анализа было выявлено, что в 60 % случаев преступники совершают данные преступления, находясь в местах лишения свободы. Большинство преступлений данной направленности совершались осужденными, отбывающими наказание в исправительных учреждениях ФСИН России по Курганской (ИК-6), Самарской (ИК-28), Новосибирской (ИК-21) областям и в Ханты-Мансийском автономном округе (ИК-11) (См. подробнее: Памятка следователю о проведении проверки и расследовании уголовных дел по фактам мошенничеств с использованием мобильных средств связи / Подготовлена контрольно-методическим управлением Следственного департамента МВД России с использованием материалов ГСУ ГУ МВД России по Кемеровской области, СУ УМВД России по Белгородской области и ГУУР МВД России в 2015 году).

Иванов М. А.[1],

начальник учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя, кандидат технических наук

К ВОПРОСУ О КОНЦЕПТУАЛЬНЫХ ОСНОВАХ ПРАКТИКО-ОРИЕНТИРОВАННОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КРИТЕРИАЛЬНОЙ ОЦЕНКИ ЭФФЕКТИВНОСТИ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ В РАМКАХ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

В настоящее время практическим аспектам реализации практико-ориентированного обучения, в том числе специалистов в области информационной безопасности, уделяется все большее внимание. Так, в Московском университете МВД России имени В.Я. Кикотя реализована концепция подготовки квалифицированных специалистов в области расследования и раскрытия преступлений в сфере высоких технологий на основе практико-ориентированного подхода. Основной целью реализации практико-ориентированного подхода к подготовке специалистов в области расследования и раскрытия преступлений в сфере компьютерной информации является формирование практически значимых профессиональных умений и навыков специалиста.

К основным направлениям реализации практико-ориентированного подхода относится как развертывание современной полигонно-лабораторной базы, так и качественное методическое обеспечение учебных занятий на основе анализа и отработки актуальных прикладных задач обеспечения информационной безопасности, а также безопасности информационных технологий в правоохранительной сфере.

Помимо создания и совершенствования современной учебно-материальной базы, качественная реализация практико-ориентированного подхода к подготовке квалифицированных специалистов в области информационной безопасности, вероятно, невозможна без активного взаимодействия с ведущими высшими учебными заведениями,

осуществляющими подготовку специалистов по соответствующим программам подготовки.

В рамках первого направления, связанного с созданием и постоянным совершенствованием элементов комплекса учебно-материальной базы, в университете создан большой блок полигонов и лабораторий, где обучающиеся имеют возможность не только пополнять багаж знаний, но и отрабатывать практические умения и навыки в области решения задач информационной безопасности.

Весь комплекс полигонно-лабораторной базы структурирован в рамках трех уровней, а именно: базовый уровень, профессиональный уровень и уровень специализаций.

К учебным объектам базового уровня относятся такие полигоны и лаборатории, как: лаборатория математического моделирования, лаборатория статистического анализа, лаборатория методов математического моделирования, лаборатория физики, лаборатория дискретной математики, лаборатория теоретической физики, лаборатория средств вычислительной техники, лаборатория программирования, лаборатория обратного проектирования (реверс-инжиниринга). К учебным объектам профессионального уровня относятся: лаборатория систем связи, лаборатория программно-аппаратных средств обеспечения информационной безопасности, лаборатория электро-, радиоизмерений, лаборатория электротехники, полигон IT-технологий. К учебным объектам уровня специализации относятся: полигон информационно-аналитического обеспечения правоохранительной деятельности, лаборатория компьютерных экспертиз, лаборатория расследования инцидентов, лаборатория информационной безопасности в экономической сфере (банковских продуктов).

К перспективам реализации данного направления работы по реализации практико-ориентированного подхода относится развертывание лаборатории беспилотных летательных аппаратов и робототехники, лаборатории исследования проблем информационной безопасности блокчейн-технологий, лаборатории исследований прикладных аспектов применения больших данных (BigData) для решения задач правоохранительной деятельности, а также лаборатории исследования прикладных аспектов применения искусственного интеллекта и нейронных се-

тей. Функционирование данных лабораторий предполагается на основе работы вычислительного центра, также планирующегося к развертыванию в составе комплекса.

Другим реализуемым направлением реализации практико-ориентированного подхода к подготовке квалифицированных специалистов в области информационной безопасности является тесное взаимодействие с ведущими высшими учебными заведениями, осуществляющими подготовку специалистов по соответствующим направлениям подготовки, а также ведущими IT-компаниями по вопросам подготовки кадров для органов внутренних дел. В этой связи представляется необходимым организация проведения комплексных киберучений не только с привлечением обучающихся по направлению информационной безопасности, но и с участием обучающихся по другим направлениям подготовки, реализуемым в университете, с обязательным приглашением к участию практических сотрудников органов внутренних дел. Так, например, представляется целесообразным участие обучающихся из состава института подготовки сотрудников для органов предварительного расследования, института психологии служебной деятельности органов внутренних дел, факультета подготовки сотрудников для оперативных подразделений полиции, факультета подготовки сотрудников полиции для подразделений по охране общественного порядка и факультета подготовки специалистов в области информационной безопасности в составе учебных комплексных групп.

Этапами таких учений могут быть:

1-й этап – изучение практических аспектов противодействия дистанционным мошенничествам в финансово-кредитной сфере, получение вводного задания, в результате отработки которого необходимо составить ряд процессуальных документов;

2-й этап – получение и изучение учебных фабул уголовных дел, после чего участниками проведения учений осуществляется комплекс процессуальных действий с отработкой соответствующих документов. Проведение данного этапа предполагает задействование полигонно-лабораторной базы, в том числе лаборатории компьютерных экспертиз, а также лаборатории информационной безопасности в финансово-экономической сфере.

Итоговые результаты выполнения всего комплекса учебных задач, поставленных в рамках учений, определяются с обязательным привлечением практических сотрудников, имеющих опыт в раскрытии и расследовании преступлений в области компьютерной информации.

Таким образом, к перспективным направлениям повышения эффективности образовательного процесса квалифицированных кадров в области информационной безопасности и в области расследования и раскрытия преступлений в сфере высоких технологий можно отнести следующие:

– всесторонний анализ современной проблематики преступлений в сфере высоких технологий;

– разработка рекомендаций по противодействию формам проявления преступности в сфере высоких технологий;

– разработка предложений по совершенствованию сферы правового регулирования вопросов, связанных с противодействием противоправным деяниям с применением компьютерных технологий;

– научное и методическое обеспечение образовательного процесса подготовки специалистов как в области информационной безопасности, так и специалистов в области расследования и раскрытия преступлений в сфере высоких технологий.

Трущенков И. В.[1],

преподаватель кафедры технико-криминалистического обеспечения МосУ МВД России имени В.Я. Кикотя, кандидат юридических наук

ПРЕДУПРЕЖДЕНИЕ И РАСКРЫТИЕ ХИЩЕНИЙ ИЗ ИНТЕРНЕТ-МАГАЗИНОВ

Внедрение электронных платежей во многие сферы современного общества, с одной стороны, повышает качество жизни, а с другой – открывает возможности появления новых способов хищения денежных средств. В настоящее время одним из направлений деятельности современных преступников являются хищения, осуществляемые из магазинов, ведущих торговлю в сети Интернет, так называемых «интернет-магазинов». Специфика работы магазина такого типа заключается в том, что он представляет собой интернет-сайт, на «виртуальной витрине» которого демонстрируются товары, которые моно приобрести путем совершения электронного платежа. После оплаты товар доставляется по адресу, указанному клиентом.

Для осуществления электронных покупок в интернет-магазинах используется, как правило, платежная карта, представляющая собой средство оплаты со счета клиента, заключившего с банком-эмитентом договор на предоставление банковских услуг. В. Б. Вехов справедливо указывает, что платежная карта – это универсальный платежно-расчетный документ, имеющий хотя бы один реквизит, доступный восприятию средствами электронно-вычислительной техники и электросвязи в форме компьютерной информации.

Преступники с целью хищения из интернет-магазинов, используют чужие идентификационные данные платежных документов при проведении операции покупки товара. Тип кражи идентификационных данных банковских платежных систем получил название «кардинг». После приобретения товар, как правило, направляется на адрес перекупщика.

Следует отметить, что в данном случае речь идет о нескольких преступлениях – хищении идентификационных данных доступа к банков-

скому счету клиента и их незаконном использовании при осуществлении покупки.

Для обеспечения качественной работы и борьбы с кражами в службах информационной безопасности современных интернет-магазинов используются антифрод-системы. Эти программные продукты предназначены для определения и пресечения попытки приобретения товара с использованием чужих идентификационных данных. Система детектирования основана на определении нескольких ключевых параметров: соответствии адреса совершения покупки (на основании ip-адреса компьютера пользователя) и фактического адреса проживания владельца платежной карты, настроек интернет-браузера, характеристик аппаратной части персонального компьютера, и др.

Розыск преступников, занимающихся кардингом, представляет собой сложную задачу, решение которой видится только в комплексном подходе и обмене информацией между службами безопасности интернет-магазинов и подразделениями органов внутренних дел, занимающимися расследованием киберпреступлений. После получения сигнала от антифрод-системы о попытке хищения службой безопасности интернет-магазина не следует пресекать сделку, а должны проводиться мероприятия по передаче информации об ip-адресе, используемом оборудовании и местоположении возможного преступника в органы внутренних дел. При задержании получателя (как правило, такие люди в цепочке преступной группы не являются организаторами, а лишь забирают и передают или перепродают товар), следует обращать внимание на мобильные устройства и компьютеры, через которые осуществлялось общение с руководителем группы.

Для осуществления хищений злоумышленники используют, как правило, ноутбуки с внешними устройствами хранения данных – флешкартами или USB-жесткими дисками. Скрываемая информация нередко подвергается двойному шифрованию: сам жесткий диск шифруется с помощью программы VeraCrypt, TrueCrypt, BestCrypt или подобных. В дальнейшем на нем с помощью такой же программы создается шифрованный файл-контейнер, содержащий в себе образ виртуального жесткого диска с установленной операционной системой. Этот контейнер,

как правило, дополнительно маскируется под файл с кинофильмом. Для этого его расширение меняется на .avi, .mov, или подобные.

Современные технические средства не позволяют оперативно расшифровать сокрытую таким образом информацию, в связи с чем следует заранее узнать пароль, используемый злоумышленником, с помощью оперативно-разыскных мероприятий, либо от самого злоумышленника в процессе допроса. При этом следует учитывать, что программы, используемые для шифрования, позволяют использовать два пароля: один – настоящий, второй – поддельный, при вводе которого все данные удаляются, либо сотрудники полиции получают доступ к заранее заготовленному пустому образу жесткого диска, не содержащему доказательственную информацию. В связи с этим перед вводом пароля следует сделать побайтовую копию исследуемого жесткого диска или флеш-карты и работать только с этой копией.

Важным объектом, содержащим доказательственную информацию, является мобильный телефон. Как правило, преступники используют современные смартфоны для общения через программы-мессенджеры. Практически эти устройства всегда защищены паролем. Рассмотрим некоторые способы его преодоления.

Для получения доступа к некоторым смартфонам на Android можно воспользоваться сервисным режимом (EDL, режимы 9006/9008 для Qualcomm, LG UP для смартфонов LG и т. д.) для доступа к информации: всего около 15% устройств на Android используют шифрование раздела данных.

Также в Android доступны многочисленные способы разблокировки, объединенные общим названием SmartLock, если, к примеру, используется фитнес-трекер или часы и настроили разблокировку при наличии соединения Bluetooth с этим устройством.

Один из простых способов обойти SmartLock – сфотографировать лицо подозреваемого. Также можно разблокировать смартфон с помощью сканера отпечатков пальцев, просто приложив палец подозреваемого.

В отличие от iOS, где в резервную копию попадает практически все, но сам бэкап можно раз и навсегда защитить паролем, в Android бэкапы создаются или в облаке, или через ADB. В резервные копии попада-

ет довольно ограниченное количество данных, при этом зашифровать их нельзя. Впрочем, маркеры аутентификации (токены) от многих популярных мессенджеров и социальных сетей в бэкапы прекрасно попадают, так что этот момент необходимо иметь в виду. Сам бэкап в Android создается предельно просто: достаточно разблокировать телефон, включить режим разработчика, подключить телефон к компьютеру и выдать соответствующую команду.

Если с телефона снята резервная копия через ADB, в нее могут попасть:

– пароли от Wi-Fi-сетей, системные настройки;
– фотографии, видео и содержимое внутренней памяти;
– установленные приложения (APK-файлы);
– данные приложений, которые поддерживают резервное копирование (включая маркеры аутентификации).

Если на этом этапе получить данные не удалось, можно потребовать предоставить пароль от учетной записи Google – таким образом будет получена информация о контактах, фотографиях и видеозаписях, сохраненные местоположения телефона, заметки, календари и т. д.

Зачастую злоумышленники пользуются кастомным рекавери (TWRP), где доступен вариант создания зашифрованной резервной копии раздела данных, который также можно сохранить во вложенном контейнере на компьютере.

Суть метода: на смартфон устанавливается кастомный рекавери TWRP, устройство запускается в нем, делается nandroid-бэкап разделов system и data (они содержат саму ОС и данные/приложения соответственно), бэкап со смартфона (он хранится в каталоге TWRP на карте памяти) сохраняется, например, в Dropbox. Затем преступник сбрасывает смартфон до заводских настроек, привязывает его к левому аккаунту, устанавливает несколько приложений, вводит несколько неважных паролей в браузер – в общем, создает видимость активно используемого устройства. А затем вновь перезагружается в TWRP, и опять делает бэкап, и вновь сохраняет его в «облако».

В результате у преступника получаются два образа внутренней памяти телефона: в одном – основная система, во втором – «чистая», для

сотрудников полиции. В случае опасности преступник восстанавливает второй, «чистый» образ, получая таким образом смартфон без следов. При этом все настройки, программы и все остальное, вплоть до расположения иконок на рабочем столе, сохраняется в секретном рекавери.

Если iPhone оборудован датчиком отпечатков пальцев, достаточно приказать приложить палец к сканеру, чтобы разблокировать устройство. Такой способ разблокирования устройств не требует каких-то особых ордеров или разрешений со стороны правоохранительных органов.

Если телефон выключен или заблокирован паролем, необходимо приказать включить устройство и ввести пароль.

Также необходимо быстро конфисковать телефон, чтобы злоумышленник не успел сбросить устройство и стереть все данные. Зачастую преступники не отключают сохранение бэкап-версий внутренней памяти телефона в облаке – можно восстановить устройство из таких файлов, используя интернет. Для этого потребуется узнать у подозреваемого пароль Apple ID.

Если у подозреваемого с собой ноутбук, то бэкап-файл, возможно, был создан локально в скрытом контейнере в формате TrueCrypt или с помощью другой подобной программы. Сам контейнер может быть предъявлен для анализа и даже сообщен особый подставной пароль – определить наличие скрытого диска невозможно.

Если преступник установил пароль на резервные копии (в iTunes активирована опция EncryptiPhonebackup), необходимо узнать этот пароль.

Иногда пароли хранятся в связке ключей на телефоне AppleKeychain и облачном iCloudKeychain.

Для анализа смартфона может быть использовано специальное программное обеспечение, например, ElcomsoftForensicToolkit, Microsystemation XRY, CellebriteUfed, Wondersharedr.PhoneforiOS и Wondersharedr.Phonefor Android, и др. С их помощью можно посмотреть, например, историю браузера – посещенные сайты, список контактов, отправленные и полученные сообщения, сохраненные геометки, содержимое заметок, фотоснимки (в том числе, восстановить удаленные).

Кустарева Ж. В.[1],

кафедра эстетического воспитания детей дошкольного возраста Московского педагогического государственного университета

ВЗАИМОДЕЙСТВИЕ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ И ОБЩЕСТВЕННОСТИ ПО ПРЕДУПРЕЖДЕНИЮ КИБЕРПРЕСТУПЛЕНИЙ В ОТНОШЕНИИ ДЕТЕЙ И ПОДРОСТКОВ

Киберпространство – сравнительно новое, но уже плотно связанное со всеми остальными сферами жизни современного человека, глобальное информационное пространство, служащее для плодотворной деятельности, получения информации, а также досуга и общения.

Определение «киберпреступление» подразумевает преступление, совершенное в электронной сфере с использованием компьютерной системы или сети, а также против компьютерных систем и сетей.

Киберпреступления имеют ряд отличий от преступлений, совершаемых без использования компьютерных сетей и систем. Две главные проблемы расследования и предупреждения киберпреступлений [1]:

– электронная сфера позволяет преступникам оставаться анонимными;

– трансграничный характер преступлений: расстояние и законы других государств мешают борьбе с киберпреступниками.

Согласно Конвенции Совета Европы, киберпреступления делятся на пять групп: преступления против компьютерных данных и систем; с целью получения экономической выгоды в результате неправомерного использования технологий; связанные с содержанием данных или контентом; связанные с нарушением авторских и смежных прав; кибертерроризм, покушения на общественную безопасность, организация и совершение актов насилия.

При прогрессирующем уровне развития современных электронных систем и сетей неудивительно, что постоянно растет как уровень киберпреступлений, так и размер причиняемого ущерба.

В России с 1992 г. существует Бюро специальных технических мероприятий МВД России. Однако для борьбы с киберпреступлениями, в особенности направленными против физических лиц, требуется также активное участие и помощь населения в предупреждении и рассле-

довании таких преступлений. В частности, родителям и педагогам следует быть осведомленными о видах преступлений против детей в киберпространстве и вносить посильный вклад в защиту детей от преступников. Дети и подростки, в силу как недостатка знаний и опыта, так и причин, обусловленных возрастной психологией, наиболее беззащитны перед киберпреступниками [2, с. 75, 84]. Среди последних встречаются знатоки детской и подростковой психологии, использующие все новые методы вовлечения детей в преступления как в качестве жертвы, так и в качестве исполнителей.

Некоторые виды преступлений против детей и подростков в киберпространстве [3]:

Груминг – приставание к ребенку в сети, вхождение к нему в доверие с целью его использования для сексуального удовлетворения.

Моббинг – преследование, издевательство, запугивание и другие негативные воздействия на ребенка, часто с использованием фото- и видеоматериалов, запечатлевших жертв; травля; доведение до суицида.

Демонстрация и распространение материалов, наносящих вред физическому и/или психологическому здоровью ребенка, в частности, порнография, насилие, шок-контент, пропаганда неуважения к семье и стране, антисоциального поведения, употребления алкоголя, табака и наркотических веществ, сексуальной распущенности, правонарушений, преступлений и т. д.

Производство, распространение и использование детской порнографии и/или материалов, изображающих сексуальное насилие над детьми.

Следует помнить, что часто дети и подростки, становясь жертвами киберпреступниками, становятся также и соучастниками преступлений, в том числе выходящих за пределы электронной сферы: кибермошенники, похитители электронных денег, шантажисты, распространители наркотических веществ. Экстремисты ищут исполнителей среди представителей этих возрастных групп.

Для вовлечения в преступление и использование ребенка или подростка в качестве жертвы преступники используют множество методов; некоторые из них специфические, характерные только для интернет-среды. Пространство, в котором можно прикинуться кем угодно, предоставляет широкие возможности для пропаганды противоправных

действий, антипатриотических настроений, социальных девиаций, подогрева недоверия и ненависти к родителям, а также создания, вызывающего доверие и увлечение образа, к которому потянется потенциальная жертва. Используется тяга подростков к моде, стремлению стать популярным, бунтарству; чувство одиночества, характерное для этого возраста; нестабильность психики в периоды возрастных кризисов.

Для защиты детей и подростков в киберпространстве родителям и педагогам необходимо объединиться с правоохранительными органами в принятии мер по обеспечению информационной безопасности и укреплению информационной грамотности населения. В Указе Президента Российской Федерации № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» от 5 декабря 2016 г. обращается внимание на низкую осведомленность граждан в вопросах обеспечения личной информационной безопасности и подчеркивается необходимость мероприятий, обеспечивающих безопасность информационной инфраструктуры. В реализации программы «Цифровая экономика», призванной глобализировать национальное цифровое пространство, важная роль отводится укреплению защиты от киберугроз и правонарушений в информационно-коммуникационной среде [3, с. 132].

Для предотвращения киберпреступлений в отношении детей и подростков от населения требуется своевременная передача информации компетентным лицам; содействие лиц, обеспечивающих доступ несовершеннолетних в сеть «Интернет», в контроле за использованием программного обеспечения и контента; а также просветительская работа, обеспечивающая информационную грамотность взрослых и детей, в том числе для лучшей осведомленности о возможных угрозах [4, с. 28].

Со стороны правоохранительных органов необходимо регулярно информировать родителей и педагогов о возможных деструктивных воздействиях киберсреды, как для анализа и контроля времяпрепровождения детей и подростков в интернет-пространстве, так и для предупреждения родителями и педагогами несовершеннолетних детей и воспитанников. Важно доносить до детей разнообразие форм и степень вреда сетевых угроз на классных часах и уроках обществознания. Важным элементом предотвращения покушения на детскую безопасность в киберсреде является доверие ребенка к его близким, к которым он обращается за помощью в непонятных или опасных ситуациях.

Как со стороны родителей, так и со стороны детских учреждений и учебных заведений, следует наладить контролируемое использование детьми сети «Интернет» и связанных с киберсредой устройств. Параллельно следует насыщать информационно-коммуникационную среду профилактическими и просветительскими материалами, относящимися к обеспечению безопасности киберпространства.

На сегодняшний день, в рамках реализации Федерального закона от 21 марта 2015 г. № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию», работа по соблюдению интересов детей в киберпространстве ведется сразу в нескольких направлениях:

– создается онлайн-пространство, состоящее из крупных порталов и платформ легального детского и подросткового контента, интересующего школьников и полезного им, и в то же время безопасное;

– ежегодно проводится единый урок безопасности в сети Интернет для учащихся 5–11 классов;

– крупные информационные ресурсы и организации, обеспечивающие безопасность граждан, проводят слаженную работу по внедрению продуктов и мер для укрепления кибербезопасности пользователей [5].

Киберсреда все плотнее охватывает нашу жизнь, проникает во все области, развивается в геометрической прогрессии. Одновременно с ее ростом увеличивается и количество преступлений внутри нее и с ее использованием. Задача общества и правоохранительных органов – в целях безопасности детей и подростков вести активную совместную работу по просвещению, предупреждению и защите от киберугроз, обеспечивая безопасность информационного пространства.

Список литературы

1. Киберпреступление. Статья // https://urist.one/dolzhnostnye-prestupleniya/kiberprestupnost /kiberprestuplenie.html.

2. Столяренко Л. Д. Психология : учебник для вузов. – СПб. : Питер, 2016.

3. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3.

4. Гончар В. В. Совершенствование расследования преступлений в сфере информационных технологий // Эпоха науки.– 2017. – № 11.

5. Гребенкина Ю. В., Книжникова С. В. Риск вовлечения детей и молодежи в преступления через медиасреду // https://e-koncept.ru/2016/56419.htm.

Савенкова Д. Д.[1],

менеджер Департамента безопасности Сбербанка,
Управление противодействия кибермошенничеству,
ПАО «Сбербанк»

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ КАК МЕРА ЗАЩИТЫ ФИНАНСОВО-КРЕДИТНЫХ ОРГАНИЗАЦИЙ ОТ КИБЕРПРЕСТУПЛЕНИЙ

Проблема информационной безопасности в условиях развития глобального информационного общества приобрела особую актуальность. В связи с этим обращает внимание указание Президента Российской Федерации В. В. Путина Федеральному Собранию в Послании от 1 декабря 2016 г. на то, что в цифровых технологиях кроются риски и необходимо укреплять защиту от киберугроз, должна быть значительно повышена устойчивость всех элементов инфраструктуры, финансовой системы, государственного управления. Это вопрос национальной безопасности и технологической независимости России, в полном смысле этого слова – нашего будущего [9].

В Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, не только перечень угроз, а также совокупность средств, способных обеспечить надежную защиту информационной безопасности государства. Кроме того, также прямо указано, что общественные отношения в области обеспечения информационной безопасности как никогда нуждаются в правовом регулировании в связи с динамикой развития информационного общества, институализацией правовых институтов в области обеспечения информационной безопасности, являющейся важной составляющей национальной безопасности Российской Федерации.

26 октября 2017 г. на расширенном заседании Совета Безопасности Президентом Российской Федерации В. В. Путиным отмечено: «Мы должны четко представлять тенденции развития глобальной информационной сферы, прогнозировать потенциальные угрозы и риски.

---

[1] © Савенкова Д. Д., 2019.

И главное, наметить дополнительные меры, которые позволят нам не просто своевременно выявлять угрозы, а активно реагировать на них[1]» [5].

Жизнь множества людей незаметно для них самих во многом переходит в виртуальное пространство. И это явление, безусловно, ежедневно несет в себе все более новые угрозы. С увеличивающимся количеством пользователей сети Интернет растут и возможности у киберпреступников для совершения различного рода кибератак.

На сегодняшний день противодействие киберпреступности является проблемой мирового масштаба. Более того, киберпреступность превратилась в организованный бизнес, и достаточно прибыльный, в основе которого лежит, как правило, использование вредоносного программного обеспечения. Вредоносные компьютерные программы все чаще пишутся с целью незаконного обогащения за счет их дальнейшей перепродажи, а также в целях незаконного получения конфиденциальной информации пользователей и последующего хищения принадлежащих им денежных средств.

В России ежемесячная аудитория Интернета по состоянию на октябрь 2016 – март 2017 гг. достигла 87 млн человек, что составляет 71 % от всего населения страны [2]. По итогам 2017 г. число интернет-пользователей во всем мире впервые превысило 4 млрд человек, а современными мобильными устройствами (смартфонами) владеют около 2/3 населения планеты. На начало 2018 г. количество ежемесячных пользователей различных социальных сетей составило 3 млрд человек. При этом около 90 % пользователей заходили на эти интернет-площадки через смартфоны [18].

Если говорить о финансово-кредитных учреждениях, можно сказать, что здесь наиболее распространено использование современных информационных технологий и сети Интернет, причем, как для удобства предоставления своим клиентам новых банковских продуктов и услуг, так и для быстроты осуществления денежных переводов, что не может не привлекать внимания злоумышленников.

---

[1] Вместе с тем, рост угроз в информационном пространстве повышается, число рисков увеличивается, а негативные последствия разного рода компьютерных атак носят уже не локальный, а действительно глобальный характер и масштаб.

За 2017 г. бизнес потерял примерно 116 млрд рублей из-за кибератак – убытки из-за киберпреступников признала почти каждая пятая российская компания [6]. Злоумышленники взламывали банкоматы, электронные кошельки и даже целые платежные системы. За последний год около 15 хакерских группировок атаковали государственные структуры, военные ведомства и частные компании[1] [14].

Для злоумышленников киберпреступления во многом привлекательны за счет того, что сегодня совершенно из любой точки земного шара злоумышленники могут осуществлять подготовку и совершение киберпреступлений, поскольку теряет в стоимости компьютерная техника, а объекты таких преступных посягательств не обязательно должны находиться в непосредственной близости от преступников. Характерно и то, что для совершения компьютерных преступлений не требуется прикладывать особые усилия и затраты, ведь достаточно иметь компьютер, программное обеспечение и подключение к информационной сети. Глубокие технические познания также не обязательны – в сети Интернет можно найти большое количество специальных форумов, закрытых чатов в мессенджерах, в которых желающий может овладеть соответствующими познаниями и навыками, приобрести вредоносное программное обеспечение для последующего совершения правонарушений, похищенные номера кредитных карт, похищенные персональные и идентификационные данные пользователей, а также объединить усилия по проведению целенаправленных компьютерных атак на компьютерные системы различных объектов.

Открытость доступа к сети Интернет и, как следствие, затруднительность в отслеживании злоумышленников позволяет им совершать большинство компьютерных преступлений с использованием именно данной сети. Анонимность всемирной сети Интернет, уязвимость беспроводного доступа и использование прокси-серверов дают возможность существенно затруднить обнаружение злоумышленников – для совершения преступления может использоваться так называемая «цепочка серверов», о чем есть масса информации в открытом доступе в сети Интернет, и этому навыку также можно научиться [10].

---

[1] По прогнозам аналитиков, количество киберпреступлений в России к 2018 году грозит вырасти в четыре раза, а общие потери могут превысить два триллиона рублей.

Как уже ранее было отмечено, компьютерные преступления (или киберпреступления) могут быть совершены абсолютно из любого местоположения, в частности, при помощи выхода в сеть Интернет через точки общего доступа (рестораны, кафе, общественный транспорт), ведь при помощи современных технологий возможно получить несанкционированный доступ к чужой беспроводной сети Wi-Fi. Более того, злоумышленнику не нужно выбирать место преступления исходя из местоположения потенциальной жертвы, что больше присуще классическим видам преступлениям – для использования своих технических средств при совершении компьютерных преступлений он может выбрать любое удобное для себя место. Это еще одна отличительная черта, присущая компьютерным преступлениям, трансграничный характер.

Вышеперечисленные обстоятельства крайне затрудняют расследование компьютерных преступлений, которое требует максимально оперативного анализа и сохранения данных, которые ввиду своей уязвимости могут быть легко уничтожены злоумышленниками за считанные минуты.

По итогам 2017 г. наиболее распространенными преступлениями в сфере информационных и компьютерных технологий, с которыми пришлось столкнуться финансово-кредитным учреждениям, стали следующие:

– заражение вирусами рабочих компьютеров, в том числе с последующим вымогательством денежных средств;

– взлом почтовых ящиков сотрудников;

– атаки на сайты предприятий (взлом, вирусное заражение, DDoS-атаки);

– интернет-мошенничество или социальная инженерия (введение в заблуждение с целью получения денежных средств или конфиденциальной информации);

– несанкционированный доступ к информации предприятия;

– кража персональных данных клиентов;

– вмешательство в работу Интернет-банкинга [6].

Вместе с тем, за аналогичный период времени Сбербанк называет основной угрозой кибербезопасности в банковской сфере не вирусы,

а другой вид мошенничества – социальную инженерию (манипулирование поведением человека с использованием социальных и психологических навыков), на которую приходится 80 % всех атак на клиентов. Сбербанк ежедневно фиксирует около 2 тыс. обращений клиентов, связанных с мошенничеством, а за год в черные списки банка попадают около 50 тыс. мошенников, пытавшихся обмануть частных клиентов, и еще несколько тысяч, атаковавших юридических лиц [15].

Актуальным остается вопрос и о территориальной юрисдикции, в случае совершения правонарушения на территории другого государства. Это определяет необходимость правовой оценки действий компьютерного злоумышленника как со стороны государства, на территории которого он использовал технические устройства при совершении противоправных действий, так и государства, которому (или гражданам которого) причинен ущерб.

Необходимо признать, что сегодня в области международного сотрудничества по противодействию компьютерной преступности имеется целый ряд проблем.

11 января 2013 г. в Гааге (Нидерланды) в штаб-квартире Европола был открыт Европейский центр по борьбе с киберпреступностью (EC3), который должен стать единым европейским центром по борьбе с киберпреступностью с самым современным оборудованием и использующим современные технологии, а также имеющим сильную команду высококвалифицированных кадров [3][1].

Евросоюз ранее предлагал России подписать Конвенцию о преступности в сфере компьютерной информации 2001 г. (так называемая Будапештская конвенция о киберпреступности), которая вступила в силу 1 июля 2004 г.

В качестве альтернативы Будапештской конвенции Совета Европы о компьютерных преступлениях, Российской Федерацией подготовлен проект конвенции ООН «О сотрудничестве в сфере противодействия информационной преступности». Впервые документ был представлен

[1] Об этом заявила еврокомиссар по вопросам внутренних дел на церемонии открытия центра. Ec3 создан для обеспечения защиты граждан и компаний европейского союза от преступлений, совершаемых во всемирной сети интернет, а также в целях содействия проведению исследований, оценки угроз, осуществления анализа тенденций, прогноза и предупреждения заинтересованных структур государств–членов европейского союза.

иностранным партнерам на совещании руководителей спецслужб секретарем Совета безопасности Российской Федерации. Российский проект исключает возможность вмешательства спецслужб третьих стран в чужие компьютерные системы и отдельной статьей прописывает механизм защиты суверенитета [11]. Очевидно, что перспективы данного проекта во многом будут зависеть от мнения США [8][1].

Это подтверждает необходимость активного содействия по созданию системы международной информационной безопасности, развитию сотрудничества с партнерами на глобальных и региональных площадках, таких как ООН, БРИКС, Шанхайская организация сотрудничества, АТЭС, ОДКБ, СНГ и других, проведению межведомственных консультаций и переговоров, что позволит более эффективно бороться с современными угрозами.

Как уже ранее было сказано, принятие ряда новых нормативных правовых актов информационного законодательства Российской Федерации обозначило заложение правового фундамента для дальнейших практических шагов в направлении обеспечения информационной безопасности, предупреждения и пресечения правонарушений в информационной сфере, в том числе и путем установления юридической ответственности за их совершение.

В этой связи справедливо утверждение известного правоведа В. Ф. Яковлева о том, что право постоянно развивается и становится все более сложным и дифференцированным. Совершенствуется правовая ответственность, появляются новые ее варианты. Но для того, чтобы вопросы ответственности решались правильно и законодателем, и правоприменителем, следует исходить из того, что есть общее понятие ответственности как общеправовой категории. Однако ответственность в разных отраслях права отличается большим своеобразием [19, с. 5]. Представляется, что данное утверждение применимо и к вопросам, связанным с юридической ответственностью за правонарушения в информационной сфере.

---

[1] Министр иностранных дел России заявил, что Москва рассматривает киберпространство как сферу, где российско-американское сотрудничество необходимо. При этом, как пояснил сам госсекретарь США Рекс Тиллерсон: «Конечно же, обсуждение будет продолжаться в будущем».

Следует подчеркнуть, что чем стремительнее развивается сфера информационных технологий, тем больше новых видов правонарушений изобретают злоумышленники, которые не перестают совершенствовать свои навыки и придумывать новые способы незаконного обогащения в данной сфере. При этом, государству необходимо наращивать темп проведения мероприятий, направленных на профилактику, предупреждение и борьбу с киберпреступностью, поскольку, как показывает правоприменительная практика, относительная длительность и бюрократический подход к развитию нормативной правовой базы приводят к значительному отставанию таких мероприятий.

Как правило, успешные масштабные киберпреступления возможно совершать в рамках действия организованного преступного сообщества, члены которого не обязательно должны быть знакомы лично – они могут знать друг друга лишь по никнеймам, используемым в сети Интернет при подготовке и совершении киберпреступлений. Одновременно с этим злоумышленники используют и традиционные методы совершения преступления, но, как правило, уже на его финальной стадии, а именно при обналичивании похищенных денежных средств.

Таким образом, рост компьютерных преступлений именно в финансово-кредитной сфере требует от сотрудников правоохранительной системы помимо не только неукоснительного соблюдения и выполнения своих непосредственных служебных обязанностей по расследованию преступлений, но также понимания банковских процессов и финансовых отношений.

Обращает внимание проблема, связанная с нарушениями, допускаемыми сотрудниками правоохранительных органов при расследовании компьютерных преступлений[1] [17]. Это во многом обусловлено тем, что подавляющее большинство специалистов органов предварительного расследования занимается расследованием традиционных видов преступлений, либо они пытаются расследовать уголовные дела о киберпреступлениях традиционными методами, что абсолютно неэффективно. Необходимо помнить, что преступники всегда вооруже-

[1] Органы прокуратуры отменяют каждое второе постановление об отказе в возбуждении уголовного дела по сообщениям о киберпреступлениях и о приостановлении расследования соответствующих уголовных дел.

ны, быстро находят все более новые способы хищения денежных средств в сфере компьютерной информации, в то время как правоохранительным органам удается раскрыть незначительный процент от общего числа совершаемых киберпреступлений, учитывая суммы затрачиваемых государством бюджетных средств на содержание правоохранительных органов, что также неэффективно.

Существует и другая проблема в данном направлении, связанная с программой обучения следственных и оперативных работников правоохранительной системы. К примеру, курс криминалистики нуждается в кардинальном обновлении, поскольку он уже устарел. Радикально должны быть переработаны и созданы новые курсы, изменены научные подходы к исследованию данных вопросов. Сбербанк осознает всю глобальность данной проблемы и первым в стране начал вести такую деятельность по направлению переподготовки специалистов, их обучение киберграмотности, информационной безопасности и основам банковской системы. Представляется, что тесное сотрудничество финансово-кредитных учреждений с правоохранительными органами, а также ведущими вузами страны в рамках вышеуказанных направлений позволит эффективнее вести борьбу с киберпреступностью [4, с. 134].

Необходимо активное вовлечение и органов государственной власти в части, касающейся внедрения и разработки новых учебных программ на всех уровнях образовательной системы, что будет способствовать формированию правового фундамента для дальнейших практических шагов в направлении обеспечения информационной безопасности.

До недавнего времени судьи, прокуроры и следователи руководствовались в своей профессиональной деятельности нормативными правовыми документами, которые уже устарели и не дают ответов на все актуальные вопросы, что мешает представителям названных ветвей власти не только иметь правильное представление о киберпреступлениях и механизмах их совершения, но и общий подход к толкованию и правоприменению.

Так, в одном из своих решений Московский городской суд оставил без удовлетворения апелляционное представление государственного обвинителя, которая просила отменить приговор суда первой инстан-

ции, переквалифицировавшего действия виновного лица с ч. 2 и ч. 3 ст. 159 УК РФ на ст. 159.6 УК РФ.

Государственный обвинитель, мотивируя свою позицию, отметила, что «находит необоснованной и неправильной переквалификацию судом действий Д. со ст. 159 ч. 3 УК РФ по восьми преступлениям и ст. 159 ч. 2 УК РФ на ст. 159.6 ч. 2 УК РФ, указав, что для осуществления переводов денежных средств со счетов потерпевших Д. незаконно добился перевыпуска сим-карт потерпевших, используя которые, путем введения достоверных логина и пароля осуществлял перечисление денежных средств потерпевших через систему «*** Онлайн». Данная судом квалификация этих действий как мошенничество в сфере компьютерной информации – несостоятельна, поскольку указанные действия образуют простое мошенничество» [1]. В ответ на это судебная коллегия апелляционной инстанции справедливо отметила, что, несмотря на то обстоятельство, что виновный Д. для входа в систему «*** Онлайн» использовал подлинные логин и пароль при совершении преступления, оно не может служить основанием для совершения Д. простого мошенничества, не связанного с хранением компьютерной информации.

Таким образом, суд апелляционной инстанции квалифицировал действия виновного именно как вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Возражения прокурора судом были обоснованно отклонены.

На протяжении последних лет правоохранительные органы, принимая решения о квалификации действий виновного лица, также руководствовались некоторыми устаревшими положениями постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате». В частности, с появлением в 2012 г. шести новых специальных составов мошенничества некоторые положения вышеуказанного постановления Пленума фактически утратили актуальность.

В связи с этим, постановлением Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» признано утратившим

силу Постановление № 51. Новое Постановление достаточно актуально как для сотрудников правоохранительных органов, так и для специалистов финансово-кредитных учреждений, поскольку даны разъяснения по многим актуальным вопросам. Во-первых, Верховный суд Российской Федерации обратил внимание на нормы закона, содержащиеся в Гражданском кодексе Российской Федерации, по смыслу которых хищение чужого имущества охватывает собой понятие «электронные денежные средства». Таким образом, разъяснено, в каких случаях наступает уголовная ответственность за совершение хищения безналичных денежных средств, в том числе электронных денежных средств. Во-вторых, «социальная инженерия» должна квалифицироваться как кража (по ст. 158 УК РФ) [12, с. 33]. Таким образом, в случае хищения безналичных денежных средств, когда злоумышленник получает к ним доступ, воспользовавшись той конфиденциальной информацией держателя платежной карты, которую он сам сообщил злоумышленнику под воздействием обмана, содеянное квалифицируется как кража. В-третьих, «фишинг» должен квалифицироваться как мошенничество (по ст. 159 УК РФ). Таким образом, в случае хищения чужого имущества или приобретения права на него, когда злоумышленник распространяет заведомо ложные сведения в сети «Интернет» (поддельные сайты, интернет-магазины и т. д.), мошенничество квалифицируется по ст. 159, а не 159.6 УК РФ.

Кроме того, изменения, в которых, безусловно, нуждается российское законодательство в части противодействия киберпреступности, должно приниматься в соответствии с действующими международными нормативными правовыми актами (Будапештская Конвенция по киберпреступлениям от 23 ноября 2001 г., и др.), поскольку эффективное ведение борьбы с киберпреступностью, которая, как правило, носит международный характер, немыслимо на территории одного государства без международного сотрудничества.

Одним из ключевых направлений обеспечения информационной безопасности является усиление государственно-частного партнерства и развитие соответствующих регионально-ориентированных программ с учетом экономической заинтересованности кредитных организаций в повышении уровня защищенности их информационных ресурсов.

Представляется необходимым применение подходов, аналогичных тем, которые избраны в целях противодействия иным угрозам системного характера, например таким, как коррупция [13, с. 18].

Отдельного внимания заслуживает проблема недостаточного уровня киберграмотности населения. Большинство киберпреступлений совершается, в том числе, благодаря неосведомленности населения и клиентов кредитно-финансовых организаций, а также несоблюдения ими основных правил безопасности. В связи с этим значительную пользу в предупреждении киберпреступности имеют информационно-просветительские мероприятия в отношении новых рисков и угроз в информационных и компьютерных системах. Сбербанк регулярно предоставляет своим клиентам рекомендации по соблюдению кибергигиены, такие, например, как скачивание приложения «Сбербанк Онлайн» только с официальных ресурсов [16]. Важно соблюдать элементарные правила информационной безопасности, а именно: не пренебрегать антивирусом, создавать и использовать сложные пароли, не повторять их на всех используемых ресурсах, применять двухфакторную аутентификацию везде, где это возможно, использовать функции шифрования информации на жестких дисках, USB-носителях и применять шифрование для сохранения конфиденциальности переписки в интернете [7].

С 1 января 2018 г. вступил в силу Федеральный Закон от 26 июля 2017 г. № 187 «О безопасности критической информационной инфраструктуры Российской Федерации»[1]. Принятие нового закона направлено, в первую очередь, на создание государственной системы обнаружения, предупреждения и ликвидации последствий атак на информационные ресурсы государства.

Таким образом, можно сформулировать отдельные направления взаимодействия государственных органов и финансово-кредитных учреждений по противодействию киберпреступности в части обеспечения информационной безопасности:

[1] Ожидается, что будет реализован обмен информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры, а также между субъектами и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

1) содействие по созданию системы международной информационной безопасности, развитию сотрудничества с партнерами на глобальных и региональных площадках, таких как ООН, БРИКС, Шанхайская организация сотрудничества, АТЭС, ОДКБ, СНГ и других, проведению межведомственных консультаций и переговоров, что позволит более эффективно бороться с современными угрозами;

2) обоюдное сотрудничество в совокупности с усовершенствованием нормативной правовой базы в области информационного законодательства Российской Федерации как основа правового фундамента для дальнейших практических шагов в направлении обеспечения информационной безопасности, предупреждения и пресечения компьютерных преступлений;

3) образовательные курсы для граждан, в первую очередь, для социально незащищенных категорий граждан и пожилых людей в целях повышения осведомленности старшего поколения о финансовом рынке, банках, их продуктах, современных технологиях и возможностях их применения, а также о том, как научиться распознавать мошенников, финансовые пирамиды, правила кибергигиены;

4) обучение слушателей учебных заведений и переподготовка следователей в целях обучения и формирования квалифицированных специалистов для органов внутренних дел, противостоящих преступлениям в сфере высоких технологий;

5) продолжение научных исследований, направленных на изучение общих вопросов ответственности в области информационной безопасности, субъектов и объектов исследования. Необходимо также активное вовлечение органов государственной власти в части, касающейся внедрения и разработки новых учебных программ на всех уровнях образовательной системы, что будет способствовать формированию правового фундамента для дальнейших практических шагов в направлении обеспечения информационной безопасности.

Список литературы

1. Апелляционное определение от 6 мая 2013 г. № 10-2076/2013 URL: http://sudact.ru/regular/doc/gGEvq4TbVEWC/.

2. Аудитория пользователей интернета в России в 2017 г. составила 87 млн человек. URL:http://2017.russianinternetforum.ru/news/1298/.

3. В Гааге открылся Европейский центр по борьбе с киберпреступностью. URL: http://www.inform.kz/ru/v-gaage-otkrylsya-evropeyskiy-centr-po-bor-be-s-kiberprestupnost-yu_a2525445.

4. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 134.

5. Заседание Совета Безопасности. URL: http://www.kremlin.ru/ events/president/news/55924.

6. Киберущерб превысил 100 млрд. URL: https://www.rbc.ru/ newspaper/2017/12/20/5a38f3749a794710aa15581b.

7. Кузнецов С. К. Кибергигиена – личное дело? URL: https://iz.ru/ news/670025.

8. Лавров и Тиллерсон кратко обсудили в Москве вопросы кибербезопасности. URL: https://ria.ru/politics/ 20170412/1492126490.html.

9. Послание Президента Российской Федерации Федеральному Собранию от 01 декабря 2016 г. URL: http://www.consultant.ru/ document /cons_doc_LAW_207978/.

10. Прокси в цепочке. URL: https://xakep.ru/2001/08/24/13400/.

11. Противоботство сверхдержав: Россия предлагает изменить правила борьбы с киберпреступностью в мировом масштабе. URL: https://www.kommersant.ru/doc/3270121.

12. Русскевич Е. А. Разъяснения Пленума ВС РФ о квалификации мошенничества в сфере компьютерной информации // Уголовный процесс. – 2018. – № 2. – С. 33.

13. Савенков А. Н. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. – 2017. – № 10. – С. 18.

14. Сбербанк объявил войну киберпреступности. URL: http://vb.kg/economics/sberbank-obiavil-voiny-kiberprestypnosti.html

15. Сбербанк назвал главную киберугрозу в банковской сфере. URL:https://sberbank-online1.ru/sberbank-nazval-glavnuyu-kiberugrozu-v-bankovskoj-sfere/.

16. Сбербанк посоветовал соблюдать «кибергигиену» из-за фальшивых приложений. URL: https://www.rbc.ru/business/29/11/2017/ 5a1ed0c99a7947e8e144267b

17. Состоялось Координационное совещание руководителей правоохранительных органов по вопросам выявления и расследования преступлений в области информационно-коммуникационных технологий. URL: https://genproc.gov.ru/smi/news/news-1122742/.

18. Яковлев В. Ф. О понятии правовой ответственности // Журнал российского права. – 2014. – № 1. – С. 5–7.

Ткаченко Л. Б.[1],

старший преподаватель-методист
кафедры предварительного расследования
МосУ МВД России им. В.Я. Кикотя

ПРОБЛЕМНЫЕ ВОПРОСЫ ВОСПИТАНИЯ ПОДРОСТКА В СОВРЕМЕННОМ ОБЩЕСТВЕ В СВЕТЕ РАЗВИТИЯ ВЫСОКИХ ТЕХНОЛОГИЙ

В настоящее время применяемые технологии существенно упростили существование человека. Вычислительная техника является инструментом высокотехнологического прогресса и стоит здесь на особом месте. Высокие технологии в виде персонального компьютера стоят на особом счету во всех сферах человеческой жизни. Из глобальной электронной сети получают необходимые сведения; электронная почта связывает людей по всему миру; с помощью компьютера можно отдохнуть и поработать, не выходя из дома. Это и забава, и насыщение освободившегося времени в развитии ребенка. Свободного времени у ребенка, вернувшегося из школы, предостаточно. Приходя домой, ребенок, пользующийся социальными сетями и играющий в игры онлайн, неконтролируемый родителями, погружается в мир Интернета и игр, интересных ему.

Продолжительное пребывание в Интернете может негативным образом сказаться как на биологическом здоровье, так и на духовном благополучии души человека. Детей это касается в первую очередь. Игры в сети Интернет, разработанные и постоянно обновляющиеся, в том числе сформированные по принципу «охоты» или «борьбы», всецело поглощают подростка, и ребенок «уходит от реальности».

Производство и продажа компьютерных игр является более выигрышным предприятием, чем производство других программ, а «сетевые игры оказываются до того сильнодействующим и чарующим орудием влияния на потребителя, в частности, детей, что компьютерные технологии выступают оружием массового поражения». Значительная часть игр является чрезвычайно неблагоприятной составляющей для умственного и физического развития молодого организма. Быстроме-

няющиеся картинки, громкие звуки, тяжелая музыка чаще всего отрицательно влияют на психическое состояние ребенка. Достаточно взглянуть на играющего в практически любую игру младшего школьника или подростка: «напряженная поза, красное лицо, подергивание конечностей, крики, порой слезы».

Как отмечает Абраменкова В. : «Перед глазами ребенка разыгрывается сюжет, в котором его персонаж является главным героем. Ребенок им управляет и переживает с ним его виртуальную жизнь. Но эмоции у ребенка возникают настоящие. Он радуется, расстраивается, путается, гордится собой, испытывает чувство досады, проигрывает и побеждает» [1].

Чрезмерное увлечение компьютерными, так называемыми экшн-видеоиграми приводит и к плачевным результатам. Так, например, 28 января 2018 г. подросток напал с топором и коктейлем Молотова на школу в Бурятии. В его дневнике подробно изложены идеи этого нападения:

«Игры Doom и Painkiller постоянно крутятся у меня в голове, я представляю будущую бойню, как в этих играх. Как будто я главный герой и должен уничтожить нечисть. Это будет круто. Это будет как в Doom вместе с Painkiller», написал подросток в своем дневнике.

Школьник говорил о желании, «чтобы землю разорвало». «Я уже ничего не осознаю, не чувствую страха и жалости к врагам (нашей) моей планеты», – писал другой девятиклассник.

На листах бумаги дневника зафиксирована символика нацистской Германии.

Пятнадцатилетний ученик также писал, что «обожает» музыкальные группы KMFDM, Rammstein, Orbital и theProdidgy. Стоит отметить, что поклонником этих коллективов был Эрик Харрис – один из двух одноклассников, которые устроили массовое убийство в американской школе «Колумбайн» в 1999 году, где погибли 13 человек. Компьютерная игра Doom также связана с этой трагедией.

Дневник подростка косвенно указывает на давнюю гипотезу психологов о том, что экшн-видеоигры могут воздействовать на рост враждебности человека и его влечение к насилию.

Брюс Бартолоу и его коллеги из Университета Миссури в США в 2005 году провели исследование, и оно показало, что у игроков в жестокие видеоигры снижена так называемая реакция P300.

«P300» – характерный всплеск на графиках во время снятия у пациента электроэнцефалограммы, когда человек слышит необычные или пугающие звуки, или видит изображения со сценами насилия.

Огромное воздействие, которое виртуальные игры оказывают на развитие детей и подростков, бесспорно. До повсеместного распространения Интернета и компьютерных игр дети общались на открытом воздухе (на детской площадке, в скверах и т. д.). В настоящее время, когда технологии развиваются быстрыми темпами, дети развлекаются в «душных квартирах» и в мнимом мире с придуманными людьми. Такие понятия, как компьютерные игры и/или видеоигры, употребляются чаще всего вместе. Монитор, клавиатура и компьютерная мышь не могут использоваться при работе на компьютере по отдельности, необходима их планомерная совместная работа, поэтому представляется логичным совместное использование терминов видео и компьютерные игры. Следовательно, такие понятия, как Интернет, видео, устройства, используемые для работы на компьютере и для компьютерных игр, рассматриваются в данной статье как части единого целого.

За прошедшие тридцать лет индустрия по производству компьютерных игр дает многомиллионный прирост ежегодно. Большое количество спроса и предложений в этой сфере промышленности не может не заинтересовать. Интерес к этому вопросу можно выразить в нескольких словах: что является в компьютерных играх для детей и даже взрослого населения настолько захватывающим? Данная работа посвящена ответу именно на этот вопрос. После глубокого изучения данного вопроса сформирован ряд причин, указывающих на необходимость длительного и систематического проведения времени детьми за компьютерными играми: удовольствие, отсутствие иной задачи (задач); конкуренция, адаптация к обществу, право выбора, приобретение хобби, написание собственного сценария мира; интересный досуг, психотерапия; повторение игры заново (от исходной точки), при отсутствии задач – формирование условий, при которых есть возможность про-

должительное время иметь определенные цели; уход от реальной жизни, поиск независимости.

Компьютерные игры, в особенности для детей и подростков, наряду с пользой, могут иметь и отрицательное влияние. Когда ребенок тратит свое время на компьютерные игры, у него могут возникнуть проблемы в общении с семьей и со сверстниками, возможно изменение поведения в школе, а также велика вероятность попасть в зависимость от игр. Как и в других видах зависимости, где у человека появляется желание ощущать все больше и большее удовольствие, игроки начинают как можно больше времени проводить за компьютером.

В ходе исследования, касающегося исследования последствий чрезмерной игры на компьютере и зависимости от этого, были выявлены многие физиологические и психологические проблемы, постигающие подростков, а именно: постепенно формируется агрессивное поведение, появляются признаки жестокости, человек меняется в целом. Также наблюдалось ослабление чувств у игроков, гиперактивность, слишком раннее развитие ребенка, снижение психомоторных функций, неприятности со здоровьем, возникающие в связи с малоподвижностью и отсутствием интеллектуальной деятельности, неподобающее поведение в обществе, утрата индивидуализма, агрессивность в отношениях с друзьями и педагогами в школе, высокая степень враждебности по отношению к близким людям, неутешительные результаты успеваемости, необоснованная тревожность, асоциальное поведение, нежелание адекватно принимать действительность, отрицание дружбы и любых отношений, утрата граней между реальностью и придуманным миром, постоянное недовольство происходящими событиями.

Наиболее негативная составляющая компьютерных игр для детей была выявлена в процессе изучения форм различных зависимостей. Считаю, что игрозависимость – направление, которое необходимо исследовать более широко. В первую очередь, в исследовании подвластности ребенка от компьютерных игр нужно установить термин зависимости и выявить компонент избыточного увлечения играми. Патологическая увлеченность детей отмечается чаще всего от компьютерных игр, Интернета и даже азартных игр.

Состояние азарта способствует формированию у ребенка максимально комфортного состояния для души, однако игрок (или тот, кто наблюдает за игроком беспристрастно) ошибочно полагает, что он предельно контролирует свой ум, силу и эмоции.

Так, В. Абраменкова, делая обзор современных игр, свидетельствует «Об очевидных трансформациях детской картины мира. В ней появились сдвиги в сторону, во-первых, меркантилизации детского сознания, выражающегося в преувеличенном внимании к деньгам, желании заниматься бизнесом, в будущем приобрести финансовую самостоятельность как можно раньше; во-вторых, в вестернизации, за которой стоит культ силы, экспансии, агрессии в сочетании с романтизацией криминальной жизни. В-третьих, в детской картине мира нарастает тенденция к танатизации – мотивам смерти, гибели всего живого на земле, уничтожения природы, экологической катастрофы и т. п., тенденция к сексологизации, циничному отношению к интимной стороне взрослых и пр.» [1].

В 2006 г. Ван и Чиоу в своих исследованиях использовали тесты, состоящие из незаконченных предложений и неструктурированное интервью для выявления причин зависимости от игр в зрелом возрасте. В этой работе использованы качественные методики выявления игровой зависимости. Изучая исследования, касающиеся игровой зависимости, чаще можно увидеть анализ зависимости в зрелом возрасте, а также анализ увеличения жестокости [2].

Родительский контроль в среде использования ребенком компьютера, как и в других сферах его жизнедеятельности, очень важен. Правильным было бы установить для ребенка некоторые важные правила в использовании компьютера, иначе он не сможет сам определить, какое количество времени ему можно играть. Необходимо вести тетрадь компьютерных игр. Например, можно составить график игр, и родители будут контролировать его соблюдение. Во время слишком долгого провождения времени за компьютером можно давать некоторые задания и обязанности. Ребенку нужно предоставить больше времени для социального общения с друзьями, товарищами и сделать так, чтобы это происходило вне Интернета. Необходимо стараться, чтобы ребенок больше жил реальной жизнью: посещал кинотеатры, театры, музеи,

спортивные и другие мероприятия [3, с. 133]. Прекрасная альтернатива игровому компьютеру для ребенка, подростка – спортивная секция или художественная школа. Первая из перечисленных укрепляет тело, а вторая развивает дух.

Если у ребенка стали заметны психологические проблемы, нужно оказать ему соответствующую поддержку и помощь. Семья больше и качественнее должна проводить время с ребенком, вникать в его проблемы, к примеру, разговаривать с ребенком о жизни в школе и об отношениях со сверстниками. Нужно создать атмосферу доброжелательности, где можно поделиться своими тревогами и проблемами [4, с. 77].

Список литературы

1. Абраменкова В. Игры и игрушки наших детей: забава или пагуба? Современный ребенок в игровой цивилизации // https://elibrary.ru /author_items.asp?authorid=72739&show_option=1&show_refs/

2. Шокрю О. Анализ зависимости школьников от компьютерной игры // https://elibrary.ru/item.asp?id=25625136/

3. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3.

4. Гончар В. В. Влияние средств массовой информации на обучающихся // Материалы международной научно-практической конференции» Формирование социокультурных компетенций в непрерывном образовательном процессе». – М., 2009.

Торичко Р. С.[1],

следователь следственной группы 3-го отдела управления по расследованию организованной преступной деятельности Следственного департамента МВД России – следователь отдела № 1 следственной части ГСУ ГУ МВД России по Свердловской области;

Клишина Н. Е.[2],

старший следователь по особо важным делам 3-го отдела управления по расследованию организованной преступной деятельности СД МВД России

АКТУАЛЬНЫЕ ВОПРОСЫ, СВЯЗАННЫЕ С РАССЛЕДОВАНИЕМ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Следственным департаментом МВД России на протяжении нескольких последних лет активно расследуется преступная деятельность организованных групп в сфере компьютерных технологий. В связи с межрегиональным характером расследуемых преступлений и большим объемом планируемых следственных действий создавались следственные группы, в состав которых включались следователи из различных субъектов страны. Кроме того, в связи с необходимостью объединения нескольких эпизодов совершенных преступлений в одно производство Следственным департаментом МВД России изучены уголовные дела данной категории в ряде территориальных следственных подразделений.

Изучение запрошенных в территориальных подразделениях уголовных дел показало, что уровень подготовки следователей, оперативных сотрудников и экспертов органов внутренних дел в рассматриваемой сфере не всегда позволяет правильно и квалифицированно расследовать преступления данной категории, своевременно изымать и закреплять следы преступления, организовывать проведение следственных действий и координировать действия со смежными подразделениями [1, с. 131–134].

Так, на сегодняшний день законодатель предлагает квалифицировать преступления данной направленности по ст.ст. 159.6, 272–274 УК РФ или мошенничество в сфере компьютерной информации, неправомер-

ный доступ, создание, распространение и использование вредоносного программного обеспечения, а также нарушении правил эксплуатации средств хранения, обработки или передачи соответственно.

Следует отметить, что, руководствуясь указанными статьями, большинство преступлений в сфере информационных технологий возбуждаются по ст. 159.6 УК Российской Федерации. В некоторых регионах правоохранители склонны относить к числу преступлений, совершенных в сфере компьютерной информации, и незаконное использование объектов авторского права различного программного софта, а также незаконные изготовление и оборот порнографических материалов, квалифицируемых по ч. 2 ст. 146 и ст.ст. 242–242.1 УК Российской Федерации (соответственно).

Сложность в расследовании уголовных дел данной категории заключается в том, что доступ к компьютерной информации может быть осуществлен не только физически, но и логически, дистанционно через Глобальную сеть, чем активно пользуются лица, совершающие указанные преступления.

Вместе с тем, одной из основных проблем в расследовании киберпреступлений следует считать их трансграничный характер, использование при их совершении различных сетевых ресурсов, а также их изменчивость (волатильность) и скорость уничтожения цифровой информации.

Таким образом, сложность в расследовании киберпреступлений заключается в установлении фактического места нахождения точки подключения к сети и ее привязки к причастным лицам. При этом технические возможности позволяют скрывать и запутывать их обнаружение. Для разрешения данных обстоятельств требуется своевременное, оперативное установление следов совершенного преступления и их надлежащее закрепление, что зачастую связано с необходимостью анализа значительных массивов информации.

Для наиболее эффективного расследования данного вида преступлений следователям необходимо приобрести и совершенствовать базовые умения и навыки, среди которых наиболее важными являются следующие:

– «слепой печати» – обусловлен повседневной необходимостью составления процессуальных документов;

– скорочтения – обусловлен повседневной необходимостью изучения информации, содержащейся на различных носителях;

– планирования своей деятельности, в том числе в долгосрочной перспективе (день, неделя, месяц, год), – обусловлен необходимостью соблюдения запланированных мероприятий, а в случае изменения обстановки обеспечения минимальной потери личного времени и средств;

– поставленной речи и логического (по возможности грамотного) изложения своих мыслей в тексте – вызван необходимостью общения и составления мотивированных, емких и содержательных документов;

– нестандартного мышления – эффективно обеспечивает противовес активному увеличению способов совершения преступлений, а также обеспечивает эффективное решение задач в непредвиденных ситуациях.

Отдельного внимания заслуживает навык умения эффективной работы с первоисточником. В частности, необходимо приобрести общие знания норм материального и процессуального права Российской Федерации, как гражданского, так и уголовного, чтобы в последующем ориентироваться в нормативных актах.

При системном подходе к решению задачи успешного расследования киберпреступлений целесообразно научиться использовать вспомогательные источники, например, судебную практику, иные нормативные акты и комментарии к ним. Целесообразно совершенствовать навык поиска информации в открытых источниках (OSINT – разведка на основе открытых источников), в том числе в сети Интернет, посредством поисковых систем, социальных сетей и других публичных баз данных (сервисы whois (например: сайт https://2ip.ru), ИФНС России и т. д.). По возможности, при формировании своей позиции, исходить из совокупности информации, содержащейся в нескольких источниках.

Говоря о расследовании преступлений в сфере компьютерных технологий, необходимо отметить, что на сегодняшний только формируется практика их расследования, а действующее законодательство ввиду быстрого темпа развития технологий требует совершенствования в указанной части. Поэтому определить конкретный перечень нормативных актов и методических пособий, которые в последующем пона-

добятся в ходе расследования, не представляется возможным. Однако следует изучить актуальную часть судебной практики разрешения уголовных дел по ст.ст. 159.6, 272–274 УК Российской Федерации и действующее законодательство в сфере компьютерных технологий для понимания основ правоотношений в указанной сфере.

В качестве особенности в расследовании данных преступлений следует указать на необходимость участия квалифицированного специалиста при проведении ключевых следственных действий, таких как допрос, осмотр предметов (документов) или проверка показаний на месте. Данное требование в работе с электронными носителями информации обеспечивает полную и надлежащую обработку интересующих данных, а также их последующую сохранность. При работе с лицами, обладающими специальными познаниями в сфере компьютерных технологий, специалист обеспечивает объективность полученных сведений, а также позволяет доступно для следователя изложить технические процессы, с учетом терминологии и сленга, используемых в области вычислительной техники и программирования.

Отдельно следует рассмотреть участие квалифицированного специалиста при проведении осмотра места происшествия, обыска, а при необходимости, и выемки. В указанных случаях обеспечение участия специалиста не только является соблюдением требований уголовно-процессуального законодательства, но и позволяет еще «на адресе» производить предварительный осмотр и оценку обнаруженных электронных носителей информации, после чего принимать решение об их изъятии. Это необходимо еще и потому, что на месте проведения перечисленных следственных действий нередко обнаруживается большое количество электронных носителей информации, которые в последующем подлежат исследованию, что, в свою очередь, приводит к загруженности экспертных подразделений и затягиванию сроков проведения программно-технических судебных экспертиз. Кроме того, предварительный осмотр изъятых электронных носителей с участием специалиста позволяет детально изучить оперативно значимую информацию, после чего принять обоснованное решение о проведении экспертизы либо о проведении дополнительного осмотра (для фиксации интересующих сведений) или возврата носителей их владельцам в соответствии с требованиями уголовно-процессуального законодательства.

Это также освобождает экспертов от дачи заключений по не интересующим следствие сведениям.

Участие специалиста на этапе обнаружения электронных носителей информации позволяет надлежащим образом производить их изъятие и упаковку, расчет «контрольной суммы» с указанием временных меток. Соблюдение последнего условия так же обоснованно, так как «контрольная сумма» является идентификатором конкретного содержания информации, малейшее изменение которого приведет к изменению суммы. Тем самым обеспечивается целостность данных при их передаче и хранении. Поэтому приведенное условие подлежит выполнению в каждом случае первичной работы с носителем, так же, как и в случаях повторного обращения к нему, поскольку позволяет сличать показатели. Также следует отметить, что участие квалифицированного специалиста при обнаружении работающего ЭВМ (компьютера) позволит получить образ оперативной памяти, что необходимо для закрепления следов совершенного преступления, в частности, при использовании шифрования данных на исследуемых объектах.

Вместе с тем, следователям необходимо выработать привычку соблюдать и применять в работе с ЭВМ (компьютерами) правила информационной «гигиены» (т. е. такие правила, нарушение которых может повлечь ограничение конфиденциальности, изменение целостности или доступности информации), среди которых следует выделить использование современных технологий шифрования, таких как ПО Vera Crypt, Gnu PG, необходимых для защиты используемых, хранимых и передаваемых данных. Особое внимание следует уделить освоению следователями программных возможностей при работе с текстовыми документами Microsoft Word и электронными таблицами Microsoft Excel [2, с. 5–18].

Список литературы

1. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3.

2. Савенков А. Н. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. – 2017. – № 10.

Торичко Р. С.[1],

следователь следственной группы 3-го отдела управления по расследованию организованной преступной деятельности Следственного департамента МВД России – следователь отдела № 1 следственной части ГСУ ГУ МВД России по Свердловской области;

Клишина Н. Е.[2],

старший следователь по особо важным делам 3-го отдела управления по расследованию организованной преступной деятельности СД МВД России

АКТУАЛЬНЫЕ ВОПРОСЫ СОВЕРШЕНСТВОВАНИЯ ДЕЙСТВУЮЩЕГО ЗАКОНОДАТЕЛЬСТВА, РЕГЛАМЕНТИРУЮЩЕГО РАССЛЕДОВАНИЕ КИБЕРПРЕСТУЛЕНИЙ

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

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

Наиболее эффективным решением в данном вопросе представляется создание межгосударственного ведомства по борьбе с киберпреступлениями, включающего в свой штат наиболее подготовленных и компе-

тентных специалистов в рассматриваемой сфере из числа государственных служащих стран–участников данного ведомства, наделенных полномочиями, позволяющими осуществлять правоохранительную деятельность на их территориях, уровень обеспечения которого будет соответствовать уровню технического развития в сфере компьютерных технологий.

Следующая задача, требующая своего разрешения при расследовании киберпреступлений, обусловлена непрерывным развитием компьютерных технологий, высоким уровнем подготовки IT-специалистов, востребованных в основном в высокооплачиваемом частном секторе экономики. По этой причине бюджетные должности в государственных учреждениях Российской Федерации на сегодняшний день не во всех случаях могут предоставить данным специалистам надлежащий уровень материального и социального обеспечения, соответствующий приобретенным ими познаниям, в связи с этим в экспертных подразделениях органов внутренних дел имеется «кадровый голод» на IT-специалистов. Считаем, что эффективным способом решения данной проблемы может стать активная реализация на федеральном и региональном уровнях Российской Федерации положений о государственно-частном партнерстве (закрепленном в Федеральном законе от 13 июля 2015 г. № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации»).

Продолжая рассматривать данную тему, необходимо осветить отдельные актуальные вопросы, связанные с расследованием киберпреступлений на примере конкретного уголовного дела.

Так, Следственным департаментом МВД России окончено рассмотрение уголовного дела по обвинению участников организованной преступной группы в совершении создания, распространения и использования вредоносного программного обеспечения классификации «Lurk», осуществления с его помощью неправомерного доступа к компьютерной информации и хищения денежных средств со счетов хозяйствующих субъектов Российской Федерации (в том числе кредитных организаций) на общую сумму свыше 1,2 млрд рублей.

Всего за период следствия с февраля 2016 г. по апрель 2017 г. в разные периоды времени в состав следственно-оперативной группы во-

шли более 400 сотрудников правоохранительных органов. В течение указанного периода времени в качестве свидетелей допрошено порядка 7 тыс. лиц, проведено более 300 обысков и выемок в различных регионах Российской Федерации, изъято свыше 120 единиц компьютерной техники, по которым назначено и проведено не менее 30 целевых программно-технических судебных экспертиз, а общее количество назначенных и проведенных экспертиз и исследований свыше 100, рассмотрено более 200 ходатайств и жалоб. Приняты меры к возмещению причиненного ущерба путем наложения ареста на счета и имущество фигурантов на сумму не менее 600 млн рублей. Предъявлено обвинение 25 участникам организованного преступного сообщества (преступной организации) в совершении преступлений, предусмотренных ч.ч. 1 и 2 ст. 210, ч. 2 ст. 273 (7 эпизодов), ч. 3 ст. 272 (7 эпизодов) и ч. 4 ст. 159.6 (6 эпизодов) УК Российской Федерации. В настоящий момент по делу выполняются требования, предусмотренные ст. 217 УПК Российской Федерации.

Созданное преступное сообщество (преступная организация) отличалось высокой степенью организованности и управления, что позволяло взаимодействовать между собой различным преступным структурным подразделениям, основные из которых возможно условно разделить на два вида. Первое – финансовое, подразделение «обнальщиков», в состав которого вошли лица, ответственные за вывод и обналичивание похищенных денежных средств с подконтрольных счетов, действовавших на территории различных субъектов Российской Федерации. Второе – техническое, в состав которого вошли лица, обладавшие специальными познаниями в сфере компьютерных технологий, программирования, осуществлявшие разработку и на постоянной основе совершенствование вредоносного программного обеспечения «Lurk».

Наибольшую сложность в расследовании совершенных преступлений представляло второе подразделение. Так, технические возможности и познания в рассматриваемой сфере, которыми обладали участники организованного преступного сообщества (преступной организации), позволяли им производить предварительный отбор наиболее подходящих для последующего инфицирования компьютеров среди посетителей легитим-

ных сайтов в информационно-телекоммуникационной сети на основании общедоступных данных (IP (страна), версия интернет-браузера и плагинов, локаль (язык систем), время посещения). Тем самым обеспечивался постоянный трафик целевых пользователей, в частности, бухгалтеров. Впоследствии, путем эксплуатации уязвимостей в программном софте целевого пользователя, выполнялся «преступный» код под видом интернет-браузера, приводящий к загрузке компонентов вредоносного программного обеспечения и последующего инфицирования компьютера пользователя. При этом на первоначальной стадии технические возможности разработки позволяли, находясь в памяти процессов инфицированного компьютера, производить поиск представляющих интерес систем дистанционного банковского обслуживания, попутно собирая интересующую информацию (в частности, парольно-кодовую), при отсутствии указанных систем удалять следы своего присутствия с компьютера. В случае обнаружения интересующего программного обеспечения производить загрузку так называемого «трояна», позволявшего получить удаленное управление инфицированным компьютером и собирать информацию о его пользователе.

Кроме того, необходимо отметить, что для осуществления своей преступной деятельности участниками преступного сообщества (преступной организации) обеспечивалась коммуникация между ее участниками посредством использования сервиса мгновенного обмена сообщениями XMPP («Jabber»), электронной почты «e-mail», системы отслеживания ошибок «Trac» и других, расположенных в закрытой инфраструктуре (доступной по «VPN»), что позволяло им на протяжении долгого времени оставаться незамеченными для правоохранительных органов. Кроме того, подобный способ общения позволял их участникам не вступать в личные контакты и оставаться анонимными друг для друга.

Безусловно, на определенных этапах расследования возникали вопросы, требующие своего разрешения, среди которых необходимо выделить следующие.

Так, в ходе проведения следственных действий с участием членов преступного сообщества (преступной организации), обладающих специальными познаниями в сфере компьютерных технологий, возник так на-

зываемый «языковой барьер». Первоначальные протоколы их допросов были перегружены терминологией, сленгом и описанием технических процессов, которые, с точки зрения процессуалистов, трудночитаемые и труднопонимаемые. Часть обвиняемых выстраивали свою линию защиты, в том числе при даче показаний, описывая выполняемые ими технические процессы как легитимные и не нарушающие требований действующего законодательства Российской Федерации. В рамках расследованного уголовного дела данный вопрос разрешен путем привлечения к указанным следственным действиям в качестве специалистов сотрудников экспертных подразделений Лаборатории Касперского и компании «Бизон», что позволило внести ясность и объективность в содержание данных показаний, а также по возможности доступно для остальных участников уголовного судопроизводства изложить технические процессы в соответствующих протоколах следственных действий.

При проведении осмотров электронных носителей информации также возникла сложность, связанная с прочтением изложенных в протоколе данных и пониманием технических процессов. Для разрешения данной задачи принято решение о проведении с участием специалиста Лаборатории Касперского дополнительного единого осмотра предметов и документов, связывающего основные технические процессы с их разъяснениями и остальными материалами уголовного дела с проведением необходимого анализа. Кроме того, в рамках данного осмотра сформировано приложение с перечнем определенных следователем терминов и пояснений специалиста к ним.

Стоит отметить, что по ряду спорных вопросов было необходимо обратиться к сотрудникам прокуратуры и судьям, выяснить их позицию по затруднительным вопросам. Например, при составлении постановления о привлечении в качестве обвиняемого, а в последующем и обвинительного заключения, следователи столкнулись со следующим вопросом. Поскольку потерпевшими по данному уголовному делу признан ряд кредитных организаций, возникла сложность, связанная с тем, что счета так называемых дропов распространены по счетам сторонних банков. Данное обстоятельство указывало на необходимость приведения данных счетов в обвинении. Так как их достаточно много (свыше 10 тыс.), то в целях устранения технических сложностей, в том числе

связанных с человеческим фактором, с учетом позиции прокуратуры и суда, принято решение о том, чтобы в тексте обвинения указывать адрес банка, перечисляя ФИО дропа и сумму, а в обвинительном заключении исключить их из перечня лиц, подлежащих вызову в суд для допроса в качестве свидетелей.

При этом необходимо отметить, что обналичивание денежных средств в указанном объеме стало возможным благодаря использованию счетов тех же дропов, т. е. лиц, не входящих в состав преступной группы и неохваченных, необъединенных с ней единым преступным умыслом. Однако часть из них добровольно передавали третьим лицам свои персональные данные и доступ к счетам. Данные обстоятельства позволяют выделить еще одну проблему, связанную с тем, что отдельные группы населения склонны к передаче третьим лицам своих персональных данных за денежное вознаграждение, а в некоторых случаях данные могут быть получены в результате небрежности или легкомыслия их обладателей. Получив такие данные, злоумышленники от имени указанных лиц открывают счета в кредитных организациях, учреждают фирмы-«однодневки», назначают их номинальными руководителями, что, в свою очередь, способствует совершению преступлений. Одним из способов разрешения данной проблемы может стать формирование практики привлечения к ответственности лиц, добровольно передающих свои персональные данные, в том числе за денежное вознаграждение, третьим лицам.

Далее следует рассмотреть вопросы, указывающие на необходимость совершенствования законодательства в сфере расследования преступлений данной категории, которая обусловлена тенденцией, направленной на увеличение темпов распространения и расширения зоны влияния компьютерных технологий (как отдельной личности, в частности, так и общества в целом). Данные обстоятельства неуклонно приводят к необходимости совершенствования ряда положений как материального, так и процессуального права Российской Федерации.

На примере проблемы, связанной с «шифрованием», т. е. блокированием (полным или в части) компьютерной информации, при отсутствии признаков хищения чужого имущества или приобретения права на чужое имущество, рассмотрим положения УК Российской Федерации.

Так, санкции за указанные преступные действия могут в значительной степени превышать степень общественной опасности и размер наступивших в результате совершения преступлений последствий, связанных с причинением имущественного вреда (как в случае с вредоносным программным обеспечением «NePetya»). Рассматриваемые противоправные действия, как правило, квалифицируются по ч. 1 ст. 273 УК Российской Федерации, с максимальной санкцией в виде лишения свободы на 4 года со штрафом в размере до 200 тыс. рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

Следует отметить, что данное преступление может быть совершено с использованием легитимного программного обеспечения, что исключает его квалификацию по ст. 273 УК Российской Федерации. Отнесение указанных действий к ч. 1 ст. 272 УК Российской Федерации допустимо только в случае неправомерного доступа к «охраняемой законом» компьютерной информации, к тому же санкция за эти деяния не превышает двух лет лишения свободы.

Очевиден дисбаланс общественной опасности рассматриваемых преступлений и ответственности за них. Считаем целесообразным ужесточить санкции к ст.ст. 272–273 УК Российской Федерации. Также требуется расширить трактовку положения ч. 1 ст. 272 УК Российской Федерации при употреблении определения «охраняемой законом компьютерной информации», включив компьютерную информацию, затрагивающую права и законные интересы человека и гражданина.

Отдельного внимания заслуживает распространение в последнее время так называемых «вирусов–шифровальщиков» компьютерной информации, что нередко сопряжено с последующим вымогательством денежных средств в обмен на восстановление доступа к зашифрованной информации [1, с. 130–133]. Расширив трактовку положения ст. 163 УК Российской Федерации, возможно введение уголовной ответственности за требование передачи чужого имущества или права на имущество или совершения других действий имущественного характера в результате неправомерного доступа к компьютерной информации, а равно под угрозой распространения компьютерной информации, содержащей сведения, которые могут причинить существенный вред

правам или законным интересам потерпевшего или его близких. Аналогичным способом необходимо расширить трактовку положений и иных статей УК Российской Федерации (например: ст.ст. 138, 146, 174–175, 183 и т. д.).

Рассматривая положения УПК Российской Федерации, следует отметить, что на сегодняшний день нет возможности производить снятие информации с технических каналов связи с серверов подконтрольных лицам, совершившим правонарушения, в ходе следственного действия.

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

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

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

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

– о выявленных вредоносных объектах (указание сигнатуры или вердикта, по которому детектируется вредоносное программное обеспечение), с учетом предыдущего пункта (по образцу АДИС «Папи-

лон»), в том числе с указанием специалиста/эксперта, их установившего, и его контактного телефона;

– о последствиях, возникших в результате атаки;

– о способе вывода денежных средств (обналичивания);

– о счетах, банковских картах, фирм-«однодневок» и дропов (возможно номера операторов мобильной связи), на счета которых переведены денежные средства, данные о номинальных и фактических руководителях юридических лиц, а также данные оперативных сотрудников правоохранительных органов, их установивших, с указанием контактных телефонов;

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

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

Кроме того, необходимо отметить, что действующее уголовно-процессуальное законодательство Российской Федерации в объеме массива информации, который требуется получать, учитывать, хранить и обрабатывать при расследовании киберпреступлений в рамках расследуемых уголовных дел позволяет производить его закрепление преимущественно на бумажных носителях информации. Данное обстоятельство, в свою очередь, требует повышенного использования ресурсов, имеющихся в распоряжении правоохранительных органов, а именно:

– постоянное снабжение бумагой, необходимость которого в рамках одного уголовного дела может превышать годовой бюджет на данные нужды в районных подразделениях;

– обеспечение сохранности сформированных материалов уголовных дел на бумажных носителях, для чего требуются специализированные хранилища для объемных уголовных дел и/или специально обустроенные помещения для хранения;

– привлечение дополнительных кадровых ресурсов и/или выделение дополнительного времени для осуществления поиска среди хранящейся на бумажных носителях информации.

Однако наиболее эффективно в работе правоохранительных и судебных органов на всех этапах доказывания и работы с доказательствами разработать, внедрить и применить электронный документооборот.

С учетом приведенных обстоятельств, а также формирующейся на сегодняшний день практики расследования киберпреступлений, необходимо провести комплекс организационных мероприятий, направленных на:

– повышение уровня обеспечения и подготовки действующих следователей, оперативных сотрудников, специалистов экспертных подразделений органов внутренних дел, участвующих в расследовании подобных преступлений;

– повышение уровня координации и взаимодействия, в частности, между подразделениями органов внутренних дел, прокуратурой и судом;

– введение единого для всех ветвей власти электронного документооборота [2, с. 5–18].

Список литературы

1. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3.

2. Савенков А. Н. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. – 2017. – № 10.

Сборник научных трудов

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, СОВЕРШЕННЫХ ПРОТИВ СОБСТВЕННОСТИ

Научное электронное издание

В авторской редакции
Корректор *Степанова А. А.*
Компьютерная верстка *Татариновой О. А.*
6,97 усл.-печ. л.

Систем. требования: CPU 1,5 Гц; RAM 90,4 МБ; Windows XP SP3;
1 Гб свободного места на жестком диске.
Подписано к изданию 00.00.2019.

ISBN 978-5-9694-0738-1

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12