МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
ВОЛГОГРАДСКАЯ АКАДЕМИЯ

В. В. Намнясев, Д. А. Чухнин, Д. В. Васильев

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ХИЩЕНИЕМ ДЕНЕЖНЫХ СРЕДСТВ С БАНКОВСКИХ СЧЕТОВ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ВРЕДОНОСНЫХ ПРОГРАММ

Учебное пособие

Волгоград
ВА МВД России
2018

УДК 343.985.7(075.8)
ББК 67.523.13я73
Н 24

Одобрено
редакционно-издательским советом
Волгоградской академии МВД России

Намнясев, В. В.

Н 24 Особенности расследования преступлений, связанных с хищением денежных средств с банковских счетов с использованием компьютерных вредоносных программ : учеб. пособие / В. В. Намнясев, Д. А. Чухнин, Д. В. Васильев. – Волгоград : ВА МВД России, 2018. – 68 с.

ISBN 978-5-7899-1145-7

В учебном пособии дана уголовно-правовая и криминалистическая характеристика хищений, совершенных с использованием вредоносных компьютерных программ, а также рассмотрены вопросы, связанные с особенностями возбуждения уголовных дел, тактики производства отдельных следственных действий и спецификой использования специальных знаний.

Издание ориентировано на курсантов и слушателей образовательных организаций системы МВД России, обучающихся по специальности «Правовое обеспечение национальной безопасности», сотрудников органов внутренних дел Российской Федерации.

УДК 343.985.7(075.8)
ББК 67.523.13я73

Рецензенты: *Е. В. Токарева, К. А. Титовский*.

ISBN 978-5-7899-1145-7

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Постоянное развитие и совершенствование компьютерной техники приводит к ее повсеместному распространению, повышению уровня ее доступности для различных слоев населения, а развитие технологий связи обеспечивает возможность подключения к сети Интернет практически в любом месте. Но, как и у большинства достижений научно-технического прогресса, у компьютерной техники есть оборотная сторона – она активно используется злоумышленниками для совершения преступлений.

Одним из наиболее распространенных видов криминального использования компьютерной техники является создание и распространение вредоносных программ. С момента написания первого вируса в ноябре 1983 г. появилось множество компьютерных вирусов и иных угроз.

В последние годы в нашей стране отмечается неуклонный рост количества преступлений, связанный с хищением денежных средств со счетов, платежных карт клиентов банков. Одним из способов хищения, набирающим популярность среди злоумышленников, является использование специальных вредоносных программ, созданных под различные операционные платформы, в частности OS «Android».

Из официального пресс-релиза МВД России от 11 апреля 2015 г. стало известно о задержании сотрудниками Управления «К» МВД России жителя Челябинской области, который, по данным следствия, разработал банковский вирус, предназначенный для хищения денег через программы мобильного банкинга, установленные на смартфонах под управлением «Android». Кроме него в состав преступной группы входили еще четыре человека. Предотвращенный ущерб от преступной деятельности составил более 50 млн рублей. В результате расследования установлено, что преступникам удалось «заразить» в общей сложности 340 тысяч мобильных устройств. Этот факт является наглядным примером масштаба данной преступной деятельности и указывает на необходимость разработки методики расследования преступлений, связанных с хищением денежных средств с банковских счетов с использованием компьютерных вредоносных программ.

Глава I
УГОЛОВНО-ПРАВОВАЯ И КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ХИЩЕНИЕМ ДЕНЕЖНЫХ СРЕДСТВ С БАНКОВСКИХ СЧЕТОВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ВРЕДОНОСНЫХ ПРОГРАММ

§ 1. Уголовно-правовая характеристика преступлений, связанных с хищением денежных средств с банковских счетов, совершаемых с использованием компьютерных вредоносных программ

Согласно Федеральному закону от 29 ноября 2012 г. № 207 Уголовный кодекс РФ дополнен шестью новыми составами, предусматривающими ответственность за различные виды мошенничества. Целесообразность введения в закон данных новелл до сих пор является предметом дискуссии в научных кругах. Тем не менее число хищений чужого имущества, совершаемых путем обмана или злоупотребления доверием (ст. 159–159.6 УК РФ) в целом продолжает расти. Так, в 2013 г. в России зарегистрировано 164 624 преступления; в 2014 г. несколько меньше – 147 821 преступление (–4,0 %). Затем с 2015 г. наблюдается резкий рост, зарегистрировано 200 598 преступлений (+24,6 %). В 2016 г. – 208 926 преступлений (+4,2 %), в 2017 г. – 211 056 преступлений (+1,0 %).

На фоне общего роста числа зарегистрированных мошенничеств наблюдается значительное увеличение количества хищений с использованием компьютерных технологий, которое составило 447 % (с 995 по итогам 2016 г. до 5 443 в 2017 г.). При этом их раскрываемость по итогам 2017 г. находилась на низком уровне и составляла лишь 7,4 % (в 2016 г. – 32,2 %). По итогам 6 месяцев 2018 г. ситуация не изменилась в лучшую сторону: в России зарегистрировано 1 789 компьютерных мошенничеств (+143,7%)[1].

Мошенничества, связанные с неправомерным доступом к компьютерной информации с последующим неправомерным списанием

[1] См.: Информация ФКУ «Главный информационно-аналитический центр МВД России». М., 2013. 2017.

денежных средств с банковских счетов граждан, являются одним из способов совершения преступлений, предусмотренных ст. 159.6 УК РФ. При этом нередко используются различные вредоносные программы.

Объектами преступлений, совершаемых в сфере расчетно-кассового обслуживания, выступают общественные отношения, обеспечивающие законный доступ к денежным средствам, находящимся на счетах физических (юридических) лиц. Основным объектом преступления, предусмотренного ст. 159.6 УК РФ, признаются отношения собственности, дополнительным – отношения в сфере охраны компьютерной информации.

Предметами преступных посягательств являются собственно денежные средства, находящиеся на счетах клиентов банка. В качестве предмета также следует выделить компьютерную информацию, которая умышленно подвергается негативному воздействию. Однако компьютерная информация, которую используют при совершении преступления, предусмотренного ст. 159.6 УК РФ, выступает не предметом, а средством совершения преступления. Так, в ч. 1 ст. 159.6 УК РФ говорится о хищении чужого имущества или приобретении права на чужое имущество «путем ввода, удаления, блокирования, модификации компьютерной информации…». Выполнение указанных действий возможно только с использованием компьютерной информации, заключенной в компьютерные программы, чаще всего вредоносные. Компьютерная информация в данном случае – это тот инструмент, с использованием которого похищается чужое имущество[1].

В примечании 1 к ст. 272 УК РФ указывается, что под компьютерной информацией понимают сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. У информации нет собственника, но имеется обладатель, поэтому информация, имея стоимость, не является имуществом, понимаемым как совокупность вещей[2].

---

[1] См.: Российское уголовное право. Особенная часть / под ред. В. П. Коняхина, М. Л. Прохоровой. М., 2015. С. 638.

[2] См.: Елин В. М. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. 2013. № 2. С. 74.

В соответствии с диспозицией ч. 1 рассматриваемой статьи данное преступление представляет собой хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Однако следует отметить, что рассматриваемый вид хищения является мошенничеством, который вне зависимости от разновидности (ст. 159–159.6 УК РФ) должен предусматривать два альтернативных способа, а именно:

1) обман, который определяется как ложное утверждение о том, что не соответствует действительности;

2) злоупотребление доверием, при котором виновный использует определенные отношения, основанные на доверии сторон, для получения от потерпевшего денег или иного имущества под условием выполнения заведомо не выполнимых или впоследствии не выполненных обязательств.

Злоупотребление доверием взаимосвязано с обманом. Виновный использует особые доверительные отношения, установившиеся между ним и собственником или иным законным владельцем, чтобы обман был более убедительным, либо прибегает к обману, чтобы заручиться доверием потерпевшего.

При совершении преступления, предусмотренного ст. 159.6 УК РФ, виновный, используя один (или несколько) из способов, указанных в диспозиции рассматриваемой статьи, фактически выдает себя за собственника денежных средств, находящихся на счету потерпевшего, и без его ведома и соответственно согласия обращает данные средства в свою пользу. Следует отметить, что при совершении данного мошенничества непосредственного контакта потерпевшего с обвиняемым не происходит.

Следовательно, при совершении преступления, предусмотренного ст. 159.6 УК РФ, фактически отсутствует обман, обязательным признаком которого является введение другого лица в заблуждение путем воздействия на сознание этого лица. Воздействие осуществляется не на психическую сферу человека, а на компьютерную информацию (субъект манипулирует такой информацией посредством технических средств). Потерпевший в это время ничего не знает о передаче имущества или права на имущество и не желает его передавать, а значит,

отсутствует такой признак мошенничества, как внешняя добровольность передачи имущества (права на имущество).

Совершение рассматриваемого преступления условно можно разделить на несколько этапов.

Первый этап совершения преступления, предусмотренного ст. 159.6 УК РФ, заключается в неправомерном доступе к компьютерной информации, что представляет собой незаконное либо не разрешенное собственником или иным законным владельцем информации несанкционированное обращение к данной компьютерной информации. При этом обязательным элементом, характеризующим данный этап, является то, что виновный стремится использовать эту компьютерную информацию с корыстной целью.

С точки зрения стадий совершения преступления (ст. 30 УК РФ) данный этап можно охарактеризовать как приготовление к совершению преступления по признаку «иного умышленного создания условий для совершения преступления». Следовательно, если действия виновного были пресечены в момент неправомерного доступа к компьютерной информации, то при наличии умысла на совершение мошенничества данное деяние следует квалифицировать по ч. 1 ст. 30 и ст. 159.6 УК РФ как не доведенные до конца по не зависящим от лица обстоятельствам.

Также к первому этапу могут относиться такие действия, как удаление, блокирование, модификация, копирование компьютерной информации.

Однако указанные действия, согласно содержанию ст. 159.6 УК РФ, фактически являются различными способами совершения преступления.

Удаление компьютерной информации по аналогии с уничтожением компьютерной информации – это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Следует отметить, что удаление и уничтожение (ст. 274 УК РФ) – это понятия, наполненные разным содержанием.

Удаление компьютерной информации по смыслу ст. 159.6 УК РФ – это прежде всего один из способов совершения преступления, из реализации которого образуются негативные для информации последствия. При этом, по нашему мнению, удаленная информация может быть восстановлена по инициативе ее законного владельца (потерпевшего) или лицом, которое собственно ее удалило.

Уничтожение информации, по смыслу ст. 274 УК РФ, – это последствия, которые явились результатом совершения данного преступления. Кроме того, по нашему мнению, уничтожение – это процесс необратимый. Восстановление информации в этом случае невозможно.

Блокирование компьютерной информации – это результат воздействия на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, т. е. совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением.

Модификация компьютерной информации – это внесение изменений в компьютерную информацию (или ее параметры).

Под иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей можно понимать любые другие способы воздействия на компьютерную информацию в целях совершения мошенничества.

Например, копирование компьютерной информации, а именно создание копии имеющейся информации на другом носителе, т. е. перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме – от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации[1].

В теории уголовного права выделяют и другие способы (приемы) мошенничества в сфере компьютерной информации: незаконное завладение регистрационными данными учетных записей; использование платежных сервисов интернет-ресурсов; взлом электронных кошельков; организация благотворительных акций через Интернет,

[1] См.: Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации» (утв. Генпрокуратурой России). Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 18.06.2018).

где на банковский счет предлагается перечислять денежные средства[1], внесение банкноты грубой подделки в банкомат[2].

Хищение может совершаться как со счетов граждан, привязанных к банковским картам, так и не привязанных к ним. Одним из наиболее распространенных видов криминального использования компьютерной техники является создание и распространение вредоносных программ, которые используются для хищения денежных средств со счетов клиентов банков.

Объективную сторону хищений с использованием вредоносных компьютерных программ условно можно разделить на несколько этапов:

1) использование вредоносной компьютерной программы (при необходимости – ее создание или модификация);

2) списание денежных средств со счетов потерпевших;

3) обналичивание похищенных денежных средств.

Для совершения хищений со счетов физических (юридических) лиц указанным способом, виновными лицами, как правило, выполняются подготовительные действия в виде создания (приобретения) и использования вредоносных программ для банковских ЭВМ в целях незаконного получения информации о ключах и паролях банковских систем управления счетами или доступа к системе дистанционного обслуживания счета.

Следует отметить, что, согласно содержанию диспозиции ст. 159.6 УК РФ, дополнительная квалификация по 272 или ст. 273 УК РФ не требуется, так как неправомерный доступ в любой форме к компьютерной информации является способом совершения данного вида мошенничества.

Представляется, что квалификации по совокупности не требуется только в том случае, если виновный использовал способы, указанные в диспозиции ст. 159-6 УК РФ, для совершения конкретного мошенничества, в отношении определенного потерпевшего (потерпевших).

---

[1] См.: Коломинов В. В. О способе совершения мошенничества в сфере компьютерной информации // Человек: преступление и наказание. 2015. № 3. С. 145–149.

[2] См.: Прозументов Л. М., Архипов А. В. Квалификация сбыта поддельных банкнот посредством банкоматов // Уголовное право. 2016. № 2. Доступ из справ.-правовой системы «КонсультантПлюс».

Если при совершении мошенничества создавались, использовались или распространялись вредоносные компьютерные программы, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, то, помимо квалификации по ст. 159.6 УК РФ, действия виновного лица могут быть квалифицированы по совокупности преступлений, предусмотренных ст. 272, 273 УК РФ.

Так, согласно разъяснениям постановления Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» (абзац 4 пункт 12) «в случаях, когда указанные деяния (мошенничество авт.) сопряжены с неправомерным внедрением в чужую информационную систему или с иным неправомерным доступом к охраняемой законом компьютерной информации кредитных учреждений либо с созданием заведомо вредоносных программ для электронно-вычислительных машин, внесением изменений в существующие программы, использованием или распространением вредоносных программ для ЭВМ, содеянное подлежит квалификации по ст. 159 УК РФ, а также, в зависимости от обстоятельств дела, по статьям 272 или 273 УК РФ, если в результате неправомерного доступа к компьютерной информации произошло уничтожение, блокирование, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети»[1].

На наш взгляд, в связи с появлением в уголовном законе состава мошенничества в сфере компьютерной информации вопрос о квалификации содеянного по совокупности со ст. 272 или 273 УК РФ должен решаться с учетом правила квалификации при конкуренции части и целого[2]. При этом следует принимать во внимание соотношение санкций соответствующих частей ст. 159.6 и ст. 272 и 273 УК РФ[3].

---

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 (Текст постановления официально опубликован не был). Доступ из справ.-правовой системы «КонсультантПлюс».

[2] См.: Третьяк М. И. Правила квалификации компьютерного мошенничества и преступлений, предусмотренных гл. 28 УК РФ // Уголовное право. 2014. № 4. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] См.: В некоторых обобщениях судебной практики предлагается квалифицировать содеянное только по ст. 159.6 УК РФ «во избежание двойного вменения» (см., напр.: Справка Камчатского краевого суда). URL: http://oblsud.kam.sudrf.ru/modules.php?№ame=docum_sud&id=2487 (дата обращения: 15.06.2018).

Так, для правильной квалификации мошенничества в сфере компьютерной информации, совершенного лицом с использованием своего служебного положения, надлежит сравнить санкции ч. 3 ст. 159.6 и ч. 3 ст. 272 УК РФ. В соответствии с уголовным законодательством мошенничество в сфере компьютерной информации, совершенное лицом с использованием своего служебного положения (см. санкцию ч. 3 ст. 159.6 УК РФ)[1], относится к категории тяжких преступлений, где санкция предусматривает лишение свободы на срок до шести лет; неправомерный доступ к компьютерной информации, совершенный лицом с использованием своего служебного положения (ч. 3 ст. 272 УК РФ) – преступление средней тяжести (верхний предел санкции – пять лет лишения свободы). Следовательно, ч. 3 ст. 159.6 УК РФ полностью включает в себя содеянное и дополнительной квалификации по совокупности преступлений не требуется.

Квалификация по совокупности со ст. 273 УК РФ необходима всегда, если в целях совершения мошенничества лицом создана или распространена вредоносная компьютерная программа, так как действия, предусмотренные ч. 1 ст. 273 УК РФ, не предусмотрены объективной стороной рассматриваемого преступления[2].

Разграничение составов преступлений, предусмотренных ст. 159.6 и ст. 272 УК РФ, должно проводиться по следующим элементам и признакам: объекту, предмету, объективной стороне, субъективной стороне.

Основным объектом преступления, предусмотренного ст. 272 УК РФ, выступают общественные отношения в сфере обеспечения безопасности компьютерной информации. Основным объектом преступления, предусмотренного ст. 159.6 УК РФ, признаются отношения собственности, дополнительным – отношения в сфере охраны компьютерной информации.

---

[1] См.: О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 03.07.2016 № 325-ФЗ (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс».

[2] См., напр.: Справка Камчатского краевого суда. URL: http://oblsud.kam.sudrf.ru/modules.php?№ame=docum_sud&id=2487 (дата обращения: 15.06.2018).

Предметом мошенничества в сфере компьютерной информации выступает имущество или право на имущество. Предметом преступления, предусмотренного ст. 272 УК РФ, является компьютерная информация, которая умышленно подвергается негативному воздействию.

Объективная сторона преступления, предусмотренного ст. 159.6 УК РФ, состоит в хищении чужого имущества или приобретении права на чужое имущество, совершенном следующими способами: ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в информационную или информационно-телекоммуникационную сеть. Данные способы мошенничества направлены на обращение в пользу виновного чужого имущества, обращение его в свою пользу и влекут причинение имущественного ущерба. В составе неправомерного доступа к компьютерной информации (ч. 1 ст. 272 УК РФ) общественно опасные последствия ограничиваются уничтожением, блокированием, модификацией либо копированием компьютерной информации.

Умысел виновного при совершении преступления, предусмотренного ст. 159.6 УК РФ, в итоге направлен на хищение имущества либо приобретение прав на него; умысел при неправомерном доступе к компьютерной информации – на получение определенных сведений.

Хищение денежных средств посредством неправомерного доступа к компьютерной информации чаще всего совершается в сети Интернет путем удаленного доступа к счетам потерпевших. В ходе выполнения объективной стороны мошенничества виновный, как правило, использует компьютер и модем. Нередко это мобильное компьютерное устройство наиболее удобно для входа и работы в сети Интернет, применяется Wi-Fi роутер. В отличие от модема посредством роутера доступ в сеть Интернет можно осуществить более чем с одного компьютера.

Состав преступления, предусмотренного ст. 159.6 УК РФ, по конструкции относится к материальным, т. е. предусматривает в качестве обязательных признаков, помимо собственно деяния, также причинно-следственную связь и наличие общественно опасных последствий.

Общественно опасные последствия рассматриваемого мошенничества выражаются в виде прямого имущественного ущерба собственнику или иному владельцу имущества (обладателю права на чужое имущество).

Субъективная сторона преступления характеризуется прямым умыслом. Для квалификации содеянного по ст. 159.6 УК РФ должно быть доказано, что виновный имел целью использование компьютерной информации в корыстных целях.

Субъект преступления – общий (физическое лицо, вменяемое, достигшее 16-летнего возраста).

§ 2. Криминалистическая характеристика преступлений, связанных с хищением денежных средств с банковских счетов, совершаемых с использованием компьютерных вредоносных программ

При рассмотрении криминалистической характеристики хищений с банковских счетов, совершаемых с использованием компьютерных вредоносных программ, вначале необходимо определить особенности ее структуры.

Анализ уголовных дел по преступлениям указанной направленности позволил выделить следующие ее элементы:

– механизм совершения преступлений;
– способ совершения преступления;
– характеристику личности преступника (преступников);
– цель и мотив преступлений;
– обстоятельства совершения преступления (время, место);
– информацию о личности потерпевшего (потерпевших);
– источники и механизм следообразования.

Механизм совершения хищений с использованием вредоносных компьютерных программ условно можно разделить на несколько этапов: использование вредоносной компьютерной программы (при необходимости – ее создание или модификация) – списание денежных средств со счетов потерпевших – обналичивание похищенных денежных средств.

Способ совершения подобных хищений напрямую связан с созданием и использованием вредоносных компьютерных программ.

В настоящий период с развитием средств вычислительной техники и телекоммуникаций создано несколько операционных платформ, предназначенных для различных компьютерных устройств. Одной из самых распространенных в России, одновременно самой подверженной деятельности вредоносных программ для ЭВМ является OS

«Android», на ядре которой функционирует более половины всех мобильных устройств (смартфонов, планшетных компьютеров) в России.

Необходимо отметить, что критерии «вредоносности» компьютерных программ определены в самой диспозиции ст. 273 Уголовного кодекса РФ: «Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации».

Существуют различные типы вредоносных компьютерных программ, которые могут быть использованы в самых разнообразных целях. При хищении денежных средств с банковских и иных платежных счетов используются вредоносные программы «троянского типа». Данные программы распространяются людьми, в отличие от вирусов и червей, которые распространяются самопроизвольно. Задачами «троянцев» являются сбор информации и ее передача (копирование) злоумышленнику, уничтожение информации или злонамеренная модификация, нарушение работоспособности компьютерного устройства, использование ресурсов компьютерного устройства в противоправных целях.

Для хищения денежных средств с банковских и иных счетов граждан злоумышленники используют различные виды «троянских» вредоносных программ, созданных для разных операционных систем. При этом, согласно сведениям ЗАО «Лаборатория Касперского», 98 % подобных вредоносных программ создано именно для операционной платформы «Android». Среди них можно выделить программы семейств «Android.bankbot», «Trojan-SMS.AndroidOS.Svpeng», «Trojan-SMS.AndroidOS.FakeInst».

Несмотря на ряд особенностей функционирования задачи данных программ являются схожими – получить доступ и возможность удаленного управления мобильным устройством другого пользователя. В качестве наглядного примера рассмотрим алгоритм работы вредоносной программы троянского типа «Android.BankBot.34.origin».

После установки на мобильное устройство «Android.BankBot.34.origin» размещает на главном экране операционной системы ярлык, имеющий значок одного из популярных приложений. Данный ярлык в дальнейшем удаляется, если вредоносная программа запускается непосредственно владельцем зараженного мобильного устройства.

В случае если пользователь не запустит вредоносную программу самостоятельно, этот ярлык сохраняется. Вредоносная программа способна автоматически начать свою работу, загрузившись вместе с операционной системой. После запуска программа запрашивает у пользователя доступ к функциям администратора мобильного устройства, начинает отслеживать активность пользователя и ожидает запуска последним ряда популярных приложений («WhatsApp», «Viber», «Instagram», «Facebook», «Twitter» и др.).

Как только будет запущена одна из указанных программ, «Android.BankBot.34.origin» отобразит поверх ее интерфейса собственное окно, имитирующее запрос ввода конфиденциальной информации (логин и пароль, номер телефона или сведения о кредитной карте). Полученные таким образом данные передаются на управляющий сервер.

Для передачи похищенной информации злоумышленникам, а также для получения от них команд «Android.BankBot.34.origin» соединяется с управляющим сервером, расположенным в анонимной сети «Tor». Во время первого сеанса связи с удаленным центром вредоносная программа выполняет регистрацию зараженного мобильного устройства, передавая основные сведения о нем (IMEI-идентификатор, название модели).

Получив от сервера необходимую команду, «Android.BankBot.34.origin» может выполнить следующее действия:

– начать или остановить перехват входящих и исходящих SMS;

– выполнить USSD-запрос;

– внести в черный список определенный номер, сообщения с которого будут скрываться от пользователя (по умолчанию в списке содержатся сервисные номера ряда телефонных операторов, системы мобильного банкинга известного российского банка, а также популярной платежной платформы);

– очистить список блокируемых номеров;

– передать на сервер информацию об установленных на устройстве приложениях;

– выполнить отправку SMS -сообщения;

– передать на сервер идентификатор вредоносной программы;

– отобразить на экране диалоговое окно или сообщение в соответствии с полученными с управляющего сервера параметрами

(например, в команде может задаваться текст, предназначенный для демонстрации на экране, количество полей для ввода данных и т. п.)[1].

Таким образом, вредоносная троянская программа «Android.BankBot.34.origin», «прописавшись» на мобильном устройстве пользователя, позволяет злоумышленникам считывать полную информацию о данном устройстве и об установленном на него программном обеспечении, а самое главное – перехватывать, блокировать доступ законного пользователя и отправлять SMS-сообщения от его имени без его ведома. Приведенные возможности программы по несанкционированной блокировке, копированию и модификации информации наглядно характеризуют ее вредоносность.

Дальнейший механизм совершения хищения проявляется во взаимодействии подобной вредоносной компьютерной программы с программой дистанционного банковского обслуживания (далее – ДБО), установленной на компьютерном устройстве потерпевшего.

К примеру, в ПАО «Сбербанк России» существует два основных вида программного обеспечения ДБО: «Мобильный банк» и «Сбербанк-Онлайн».

«Мобильный банк» представляет собой программное приложение, функционирующее на терминалах сотовой связи (мобильных телефонах, планшетах), позволяющее путем отправки SMS-сообщения и USSD-команд на определенный номер, принадлежащий банку (по линии ПАО «Сбербанк России» по всей территории РФ данный номер определен как «900»), управлять своим банковским счетом, а именно: получать информацию о состоянии счета банковской карты, осуществлять различные платежи, перевод денежных средств со счета банковской карты на счета других банковских карт, принадлежащие клиенту. Провайдером при этом является организация, предоставляющая услуги сотовой связи (голосовые данные, SMS-сообщения, MMS-сообщения и др.). Таким образом, пользование услугой «Мобильный банк» возможно при наличии подключенного к оператору сотовой связи мобильного устройства. Сеть Интернет для работы данного приложения не требуется.

Схема проведения операции по банковской карте через услугу «Мобильный Банк» выглядит следующим образом: на своем мобильном устройстве гражданин (являющийся клиентом банка и абонентом

[1] См.: Android.BankBot.34.origin. URL: http://vms.drweb.ru/virus/?i=4249551&lng=ru (дата обращения: 08.02.2018).

оператора сотовой связи одновременно) формирует SMS-сообщение определенного содержания на номер «900» (который показывает все движения денежных средств по банковской карте клиента) или USSD-команду и передает на сервер оператора сотовой связи. Далее сервер оператора сотовой связи передает SMS-сообщение или USSD-команду в процессинговый центр банка ПАО «Сбербанк России», который расположен в г. Москве. Процессинговый центр, в свою очередь, обрабатывает команду/сообщение и проводит соответствующую операцию со счетом карты.

Схема проведения операции по банковской карте через услугу «Мобильный Банк» выглядит следующим образом: на своем мобильном телефоне клиент формирует SMS-сообщение определенного содержания на номер «900» (который показывает все движения денежных средств по банковской карте клиента) или USSD-команду и передает на сервер оператора сотовой связи. Далее сервер оператора сотовой связи передает SMS-сообщение или USSD-команду в процессинговый центр банка ПАО «Сбербанк России», который расположен в г. Москве, представляющий собой определенное количество серверов с определенным программным обеспечением. Процессинговый центр, в свою очередь, обрабатывает команду/сообщение и проводит соответствующую операцию со счетом карты.

Таким образом, используя возможности вредоносной программы по доступу ко всем SMS-сообщениям, поступающим на мобильный телефон потерпевшего, а также отправки с его номера SMS-сообщений и USSD-команд, используя сервисы приложения «Мобильный банк» путем несанкционированных денежных переводов и осуществляется хищение денежных средств с банковской карты потерпевшего.

В ПАО «Сбербанк России» также имеется компьютерная система дистанционного банковского обслуживания под названием «Сбербанк-Онлайн». Для доступа к ней необходима авторизация путем введения реквизитов – «логина» и «пароля». Получить данные реквизиты возможно у оператора в любом отделении ПАО «Сбербанк России», написав соответствующее заявление, а также в любом банкомате и терминале банка, предъявив банковскую карту (банкомату, терминалу) и воспользовавшись соответствующим пунктом меню, в результате чего банкомат/терминал выдаст кассовый чек, в котором будут отражены «логин» и «пароль». Подключившись

к системе ДБО «Сбербанк-Онлайн», клиент банка, находясь в любом месте и в любое время, имея доступ к сети Интернет, может совершать операции со всеми своими счетами (лицевые, расчетные, депозитными и т. д.), оплачивая коммунальные услуги, услуги связи, осуществлять денежные переводы.

Для функционирования данной услуги обязательно использование сети Интернет, чем она отличается от услуги «Мобильный банк», где использование сети Интернет не требуется. В услуге «Сбербанк-Онлайн», также в отличие от «Мобильного банка», видны все счета, принадлежащие клиенту, и операции по ним, т. е. они более широкие.

Таким образом, для совершения хищения с использованием системы ДБО «Сбербанк-Онлайн» злоумышленникам необходим доступ к сведениям о реквизитах доступа к ней – «логине» и «пароле». Информацию о них злоумышленники получают также в результате использования вредоносных компьютерных программ «троянского» типа, механизм функционирования которых аналогичен описанному выше.

Последующие этапы механизма совершения хищений – вывод денежных средств со счетов потерпевших и последующее обналичивание рассмотрены ниже в описании функций участников преступной группы.

Характеристика участников преступления

Сложность механизма совершения подобных преступлений такова, что осуществить в одиночку их практически невозможно, и они совершаются, как правило, в составе преступных групп. Данные преступные группы характеризуются:

– организованностью, устойчивостью, сплоченностью – имеют четко выработанное, неизменное внутреннее строение, наличие лидера, соподчинение между членами и взаимосвязь, рассчитываются на длительное существование с постоянными формами и методами преступной деятельности, направленными на совершение неопределенного количества преступлений;

– длительностью и масштабностью преступной деятельности – ее размах может охватывать в потенциале территорию различных субъектов Российской Федерации;

– четкой специализацией участников – совершением хищений денежных средств с банковских карт путем незаконного доступа к ним в результате незаконного использования специальных компью-

терных программ в сети Интернет и внедрения их в принадлежащие гражданам компьютерные устройства, последующего списания данных денежных средств посредством их снятия в платежных терминалах и банкоматах различных кредитных организаций;

– объединенностью – члены группы связаны между собой единой преступной целью, приобрели преступные навыки для выполнения общей преступной цели;

– отработанной системой конспирации и защиты от раскрытия;

– строгим иерархическим строением – распределением ролей между членами с выполнением каждым строго своих обязанностей, подчиненностью участника руководителю. Выделяют следующих виды участников группы, совокупная деятельность которых полностью характеризует механизм совершения хищений:

1. Организатор.

2. Распространители вредоносных программ.

3. «Заливщики» (люди, которые выводят деньги со взломанных счетов).

4. Участники «дроп-проекта», предназначенного для обналичивания похищенных денежных средств: руководитель дроп-проекта, «дроповоды», «дропы».

5. В зависимости от масштаба деятельности преступной группы в некоторых случаях для совершения хищений специально создаются новые вредоносные программы. Для этого в состав преступной группы также может входить их разработчик (разработчики).

Как видно из описания состава преступной группы, процесс обналичивания похищенных денежных средств является отдельным сложным этапом, имеющим своим особенности, на которых остановимся подробно.

Конечным звеном обналичивания являются так называемые «дропы» – держатели платежных средств, которые по команде «дроповода» обналичивают деньги, поступившие на счет, либо переводят их на другой счет, указанный «дроповодом». «Дропы», в свою очередь, делятся на два вида: «разводных» и «неразводных». «Разводные» «дропы» – это люди, которые, по крайней мере на первых порах своего сотрудничества с «дроповодом», не осознают, что они участвуют в преступлении. Как правило, задача получения и перевода денег преподносится «разводным» «дропам» под каким-нибудь благовидным предлогом. Например, «дроповод» может создать

юридическое лицо и нанять на исполнительную должность (генерального или финансового директора, например) человека, который будет выполнять функцию «разводного» «дропа»: подписывать корпоративные документы, которые на самом деле будут служить легальным прикрытием для вывода украденных денег. «Неразводные» «дропы» прекрасно осведомлены о том, для чего они выполняют задания «дроповодов».

Способов вывода денег, применяемых дроп-проектами, много. В зависимости от суммы похищаемых денег могут быть использованы либо частные владельцы платежных карт, готовые за небольшую плату обналичить поступления и передать их представителю «дроповода», либо специально созданные юридические лица, представители которых оформляют «зарплатные проекты» (множество платежных карт для сотрудников фирмы для перечисления зарплаты) в банке, обслуживающем это юридическое лицо;

– объединенностью – члены группы связаны между собой единой преступной целью, приобрели преступные навыки для выполнения общей преступной цели;

– отработанной системой конспирации и защиты от раскрытия.

Отличительной особенностью таких преступных групп, несмотря на их четкую организацию и сплоченность, является то, что члены группы, выполняя конкретные функции, могут быть не знакомы друг с другом, или знакомы только с кем-то из других участников. Например, «дропы», как правило, знакомы с «дроповодом», но не знакомы и ни разу не виделись с заливщиком и тем более другими, стоящими выше по рангу членами преступной группы.

Как было отмечено, каждый из видов участников преступной группы отвечает за конкретный этап совершения преступления (распространение вредоносных программ, вывод, обналичивание), при этом во время совершения преступных действий они могут находиться на территории различных субъектов РФ, что вызывает сложности в определении конкретного места совершения преступления. Таким образом, уместно вести речь о месте окончания преступления, которым выступает место расположения банкомата (терминала), через который обналичены похищенные денежные средства, либо место открытия банковского счета, на который они перечислены.

Время совершения хищения напрямую зависит от момента поступления крупной денежной суммы на счет потерпевшего (например, заработной платы). Имея доступ к состоянию счета, преступники дожидаются данного момента, после чего осуществляют вывод денег. В ряде случаев, применимо к особо крупным суммам, операции по выводу денежных средств преступники стараются проводить под конец банковского дня, лишая возможности потерпевшего и банк оперативно заблокировать транзакцию.

Целью данных преступлений является незаконное завладение денежными средствами, принадлежащими и хранящимися на банковских и иных платежных счетах клиентов, мотив является только корыстным.

Потерпевшими при совершении рассматриваемых хищений являются клиенты банков, использующих программное обеспечение дистанционного банковского обслуживания, компьютерные устройства которых подверглись заражению вредоносными программами «троянского типа».

Основными **источниками информации о следах** преступных действий являются компьютерное устройство потерпевшего (следы наличия и использования компьютерных вредоносных программ), детализация телефонных и иных соединений потерпевшего (сведения об отправленных и полученных SMS-сообщениях и USSD-команд, банковский процессинговый сервер (сведения о незаконных банковских транзакциях со счета потерпевшего), интернет-сервера, используемые преступниками. Особенности фиксации следов при совершении хищений подробно рассмотрены в гл. 2.

Глава II
ОСОБЕННОСТИ ПРОВЕРКИ СООБЩЕНИЯ О ПРЕСТУПЛЕНИИ И ПЕРВОНАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ С БАНКОВСКИХ СЧЕТОВ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ВРЕДОНОСНЫХ ПРОГРАММ

§ 1. Специфика проверки сообщения о преступлении, связанном с хищением денежных средств с банковских счетов с использованием компьютерных вредоносных программ. Особенности принятия решения о возбуждении уголовного дела

Объектами преступлений, совершаемых в сфере расчетно-кассового обслуживания, выступают общественные отношения, обеспечивающие законный доступ к денежным средствам, находящимся на счетах физических (юридических) лиц.

Предметами преступных посягательств являются собственно денежные средства, находящиеся на счетах клиентов банка. В силу того, что данная категория преступлений совершается посредством использования вредоносных программ, которые можно определить как средства совершения преступления, то в качестве предмета также следует выделить компьютерную информацию, которая умышленно подвергается негативному воздействию[1].

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

Хищение денежных средств, совершаемое с использованием вредоносных программ, возможно только с прямым умыслом. Виновный осознает, что внедряет вредоносную программу в программное обеспечение компьютера потерпевшего. Предвидит, что в результате таких действий неизбежно произойдет несанкционированное

[1] См.: Российское уголовное право. Особенная часть / под ред. В. П. Коняхина, М. Л. Прохоровой. М., 2015. 638.

выполнение команд, обеспечивающих незаконный доступ к денежным средствам, находящимся на счетах потерпевшего, и наступление последствий в виде причинения имущественного вреда собственнику. Желает наступления этих последствий.

Данная разновидность хищения предполагает обязательный признак, – корыстную заинтересованность, т. е. стремление получить материальную выгоду в виде наживы или избавления от затрат[1].

Исходя из конкретных обстоятельств, уголовное дело по фактам преступных посягательств в указанной сфере может быть возбуждено по признакам преступлений, предусмотренных ст. 158 УК РФ (кража, т. е. тайное хищение чужого имущества), 159 УК РФ (мошенничество, т. е. хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием), 159.6 УК РФ (мошенничество в сфере компьютерной информации, т. е. хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации, или информационно-телекоммуникационных сетей). Следует отметить, что злоупотребление с компьютерной информацией должно быть именно способом данного хищения. Если лицо использует смартфон, электронную почту или интернет-магазин для отправления сообщений, содержащих заведомо ложную информацию, тем самым вводя в заблуждение конкретных потерпевших, то способом хищения будет не злоупотребление с компьютерной информацией, а обман человека, такое мошенничество следует квалифицировать по ст. 159 УК РФ, а не по ст. 159.6 УК РФ[2].

Хищение денежных средств, совершаемое в сфере расчетно-кассового обслуживания способом неправомерного доступа к компьютерной информации (ст. 272 УК РФ) посредством создания, использования и распространения вредоносных компьютерных

---

[1] См.: Уголовное право Российской Федерации. Общая и Особенная части / под ред. А. И. Чучаева. М., 2013. С. 268.

[2] См.: Уголовное право России. Части Общая и Особенная: учебник. 2-е изд., перераб. и доп. / под ред. А. В. Бриллиантова. Доступ из справ.-правовой системы «КонсультантПлюс».

программ (ст. 273 УК РФ), следует квалифицировать по совокупности преступлений.

Для совершения хищений со счетов физических (юридических) лиц с использованием вредоносных компьютерных программ виновные лица, как правило, выполняют следующие подготовительные действия:

– создание и использование вредоносных программ для банковских ЭВМ в целях незаконного получения информации о ключах и паролях банковских систем управления счетами;

– создание и использование вредоносных программ для банковских ЭВМ в целях их внедрения в компьютеры клиентов для незаконного получения информации о ключах и паролях доступа к системе дистанционного обслуживания счета[1].

Преступные посягательства на сведения ограниченного доступа в подавляющем большинстве случаев совершаются в целях подготовки хищения денежных средств банков (и их клиентов). К таким сведениям относятся: во-первых, общедоступная информация и информация, доступ к которой ограничен федеральными законами (информация ограниченного доступа); во-вторых, информация, к которой относятся сведения, составляющие банковскую, коммерческую, налоговую и иную тайну, а также персональные данные физического лица[2] (конфиденциальная информация[3]).

Поводами и основаниями для возбуждения уголовных дел по фактам хищений денежных средств с использованием вредоносных компьютерных программ чаще всего являются:

– заявления и сообщения конкретных потерпевших (к ним относятся как частные лица, так и руководители предприятий, учреждений, организаций);

– информация, полученная в результате проведения оперативно-разыскных мероприятий;

---

[1] См.: Гамза В. А., Ткачук И. Б. Особенности преступных посягательств на банковскую безопасность в сфере обслуживания счетов клиентов // Управление в кредитной организации. 2011. № 2. С. 102.

[2] Там же. С. 98.

[3] Об утверждении Перечня сведений конфиденциального характера: указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015). Доступ из справ.-правовой системы «КонсультантПлюс».

– выявление признаков преступления следователем, прокурором или судом;

– сведения, полученные из иных источников (средства массовой информации, сеть Интернет и т. п.).

Поступившую в правоохранительные органы информацию необходимо подвергнуть процессуальной проверке, по окончании которой принять решение в порядке ст. 144–145 УПК РФ. В связи с этим следователь совместно с оперативным сотрудником должен ознакомиться с собранными по делу материалами и выбрать наиболее оптимальный момент для возбуждения уголовного дела, а также определить характер и последовательность первоначальных следственных действий, организационных и иных мероприятий. Успех расследования хищений денежных средств со счетов потерпевших посредством использования вредоносных программ во многом обеспечивают: быстрота и решительность действий следователя и оперативного сотрудника в самые первые часы производства по делу; организованное взаимодействие с различными подразделениями правоохранительных органов; наличие специалиста в области компьютерной обработки информации.

Поскольку процессуальная проверка согласно чч. 1 и 3 ст. 144 УПК РФ проводится в жестко регламентированные сроки, представляется целесообразным составить план ее реализации, куда включить:

1) получение письменного объяснения от заявителя;

2) осмотр места происшествия. Осмотру подлежит компьютерное устройство (телефон, смартфон, планшетный персональный компьютер, электронные носители и содержащаяся на них компьютерная информация);

3) получение письменных объяснений у лиц, на которых указывает заявитель или имеются достоверные сведения о них как о возможных очевидцах происшедшего события;

4) консультации со специалистами в области компьютерной информации;

5) истребование и анализ необходимых документов, отражающих незаконность проведения операций с банковскими счетами заявителя и подтверждающих факт хищения денежных средств с использованием компьютерных вредоносных программ;

6) истребование и проверка подлинности и действительности документов, подтверждающих материальный ущерб, причиненный

заявителю хищением денежных средств с банковских счетов с использованием компьютерных вредоносных программ;

7) осмотр полученных предметов и документов;

8) анализ имеющейся информации и решение вопроса о необходимости назначения экспертиз, например судебной компьютерной экспертизы. В порядке ч. 3 ст. 80 УПК РФ получение в письменном виде заключения эксперта и (или) специалиста. По необходимости допрос эксперта и (или) специалиста по обстоятельствам, изложенным в экспертизе и требующим специальных познаний для их уяснения.

В плане могут быть указаны и другие мероприятия, которые не являются следственными. В график очередности выполнения указанных процессуальных действий (оперативно-разыскных, проверочных и организационных мероприятий) могут быть внесены коррективы. Необходимо, чтобы в результате процессуальной проверки сообщения о преступлении сотрудник органа предварительного расследования:

1) получил четкое и полное представление о характере деятельности и структуре объекта, где было совершено хищение;

2) выяснил коммуникативные и иные тактико-технические характеристики используемой компьютерной техники и программного обеспечения;

3) уяснил организацию охраны объекта информатизации и вид конкретной компьютерной информации (каким законом или подзаконным нормативно-правовым актом она охраняется);

4) изучил служебные обязанности лиц, имеющих санкционированный доступ к охраняемой законом компьютерной информации, а также прямые или косвенные отношения к ценностям (имуществу), которые стали предметом правонарушения.

С учетом данных, полученных в результате предварительной проверки поступивших материалов, принимается решение о возбуждении уголовного дела, об отказе в его возбуждении или передаче сообщения о преступлении по подследственности в соответствии со ст. 151 УПК РФ[1].

Приемы обнаружения признаков преступления по заявлениям и сообщениям носят преимущественно проверочный и оценочный характер. Один из таких приемов заключается в детальной правовой

[1] См.: Вехов В. Б. Особенности проведения доследственной проверки по делам о преступлениях в сфере компьютерной информации // Эксперт-криминалист. 2013. № 4. С. 3.

оценке приведенных в заявлении либо сообщении сведений. Такую оценку следует осуществлять на стадии процессуальной проверки сообщения о преступлении. Поступившая в правоохранительные органы информация об общественно опасном деянии тщательно анализируется и оценивается с точки зрения противоправности. В настоящее время компьютерные технологии постоянно совершенствуются и стремительно сменяют друг друга[1]. В результате ошибок лиц, использующих ЭВМ, нередко случаются сбои в работе аппаратуры. Следовательно, принимая решение по поступившим материалам, необходимо учитывать и низкий уровень знаний многих пользователей, в результате чего нормальное функционирование программного обеспечения может быть расценено как проявление вредоносных программ.

Процессуальная проверка сообщения о преступлении включает в себя выполнение следующих процессуальных действий:

1. Получение объяснения от заявителя, в котором следует отразить следующую информацию:

– реквизиты счета заявителя, с которого произошло несанкционированное списание денежных средств;

– дату и время обнаружения заявителем списания денежных средств со счета (данная информация позволит определить время совершения хищения);

– сумму списанных со счета денежных средств (если списание денежных средств осуществлялось неоднократно, то следует выяснить, когда это произошло, какие суммы и в какой валюте списывались);

– подключен ли заявителем сервис СМС-информирования о произведенных операциях по счету (если такой сервис подключен, то поступали ли на его номер СМС-сообщения, уведомляющие о списании денежных средств со счета. В объяснении необходимо отразить точное время поступления и отправки этих сообщений. Данная информация может быть получена из истории сообщений в памяти телефона. Кроме того, в объяснении целесообразно указать марку телефона (смартфона, планшета), которым пользуется заявитель

[1] См.: Кравец Е. Г. Применение научно-технических средств в процессе доказывания // Проблемы реализации уголовного и уголовно-процессуального законодательства на современном этапе: материалы Всеросс. науч.-практ. конф., 8–9 декабря 2011 г. Волгоград, 2012. С. 353–360.

при осуществлении операций с денежными средствами, а также, какая операционная система установлена на данном гаджете);

– поступали ли на номер телефона потерпевшего СМС-сообщения с запросом на осуществление операции с денежными средствами (если такое сообщение поступало, то отправлялось ли сообщение с подтверждением согласия на проведение транзакции;

– производил ли сам заявитель указанные транзакции, отправлял ли СМС-сообщения с подтверждением на их проведение);

– местонахождение мобильного телефона заявителя в период списания денежных средств со счета (данная информация позволит установить круг подозреваемых лиц, которые могли бы воспользоваться телефоном заявителя для осуществления денежных операций и отправки СМС-сообщения с подтверждением их проведения);

– на основе анализа информации о движении денежных средств, полученной из выписки по счету потерпевшего, уточнить у последнего, знакомы ли ему адресаты (направления) списания денежных средств (номера банковских счетов, лицевые счета мобильных телефонов, ФИО адресатов).

Прежде чем получить объяснение, необходимо уточнить, получил ли заявитель в банке справку или расширенную выписку по своему счету, с которого производилось несанкционированное списание денежных средств. Опрашивать заявителя целесообразно при наличии у него как минимум одного из указанных документов.

2. Производство осмотра, выемки. Согласно ст. 176 УПК РФ до возбуждения уголовного дела целесообразно провести осмотр места происшествия, отметив в протоколе индивидуальные признаки мобильного телефона (смартфона). В описании данного предмета следует указать марку (SAMSUNG, LG, FLY и т. п.), цвет передней и задней панели, материал, из которого изготовлен корпус, размеры, номер IMEI и иные индивидуальные признаки. В рамках производства осмотра места происшествия необходимо изъять мобильный телефон (смартфон) заявителя в целях проведения экспертного исследования, а также детального осмотра и приобщения к материалам уголовного дела в качестве вещественного доказательства. Кроме того, в ходе осмотра необходимо задокументировать факт поступления и отправки сообщений разрешительного и уведомительного характера, а также, по возможности, зафиксировать наличие или отсутствие

вредоносных программ. Более подробно порядок проведения осмотра рассмотрен в разделе «Использование специальных познаний».

3. Запрос у оператора связи детализации телефонных соединений по абонентскому номеру заявителя за период, в который совершено хищение (в случае, если сам заявитель не предоставил указанную информацию). Помимо самой детализации телефонных соединений в запросе необходимо затребовать сведения о местоположении базовых станций, фиксирующих соединения абонента, и об IMEI терминала связи, в котором использовалась данная сим-карта. Анализ полученной информации, ее сопоставление с показаниями заявителя позволит сделать выводы о характере и способе совершения хищения. Более подробно данный вопрос рассмотрен в разделе «Использование специальных познаний».

4. Запрос сведений в банках (иных платежных системах, операторах связи) о счетах, на которые были незаконно переведены денежные средства со счета заявителя, а также о дальнейшем движении денежных средств по данным счетам.

Следует отметить, что получение подобных сведений на стадии процессуальной проверки вызывает определенные сложности, связанные с действием ст. 26 «Банковская тайна» Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности». Согласно ее положениям справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, а также справки по счетам и вкладам физических лиц выдаются (при наличии согласия руководителя следственного органа) органам предварительного следствия по делам, находящимся в их производстве, а также органам внутренних дел при осуществлении ими функций по выявлению, предупреждению и пресечению налоговых преступлений.

Справки по счетам и вкладам физических лиц выдаются кредитной организацией им самим, судам, органам принудительного исполнения судебных актов, актов других органов и должностных лиц, организации, осуществляющей функции по обязательному страхованию вкладов, при наступлении страховых случаев, предусмотренных федеральным законом о страховании вкладов физических лиц в банках Российской Федерации, а при наличии согласия руководителя следственного органа – органам предварительного следствия по делам, находящимся в их производстве.

Справки по операциям и счетам юридических лиц и индивидуальных предпринимателей, по операциям, счетам и вкладам физических лиц выдаются на основании судебного решения кредитной организацией должностным лицам органов, уполномоченных осуществлять оперативно-разыскную деятельность, при выполнении ими функций по выявлению, предупреждению и пресечению преступлений по их запросам, направляемым в суд в порядке, предусмотренном ст. 9 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», при наличии сведений о признаках подготавливаемых, совершаемых или совершенных преступлений, а также о лицах, их подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела. Перечни указанных должностных лиц устанавливаются нормативными правовыми актами соответствующих федеральных органов исполнительной власти.

Справки по операциям, счетам и вкладам физических лиц выдаются кредитной организацией руководителям (должностным лицам) федеральных государственных органов, перечень которых определяется Президентом Российской Федерации, Председателю Центрального банка Российской Федерации и высшим должностным лицам субъектов Российской Федерации (руководителям высших исполнительных органов государственной власти субъектов Российской Федерации) при наличии запроса, направленного в порядке, определяемом Президентом Российской Федерации, в случае проверки в соответствии с Федеральным законом «О противодействии коррупции» сведений о доходах, расходах, об имуществе и обязательствах имущественного характера, соблюдения запретов и ограничений[1].

Таким образом, для получения сведений по банковским счетам в рамках процессуальных проверок по всем иным категориям преступлений (в том числе интересующих нас преступлений против собственности, предусмотренных ст. 158, 159 УК РФ) на стадии процессуальной проверки возможно лишь в рамках оперативно-разыскной деятельности, на основании постановления суда, разрешающего получение данных сведений. Как правило, это подразумевает дополнительное заведение оперативного производства. Учитывая, что

[1] См.: О банках и банковской деятельности (с изм. и доп., вступ. в силу с 09.02.2016): федер. закон от 02.12.1990 № 395-1 (ред. от 29.12.2015). Доступ из справ.-правовой системы «КонсультантПлюс».

срок процессуальной проверки по материалам данной категории не превышает 10 суток, сведения по банковским счетам целесообразно запрашивать в рамках уже возбужденного уголовного дела на основании запроса следователя.

Полное и качественное проведение проверки сообщения о преступлении нередко является достаточным для правильной квалификации деяния, содержащего в себе признаки хищения денежных средств с банковских и электронных счетов пользователей с использованием компьютерных вредоносных программ. По окончании проверки, при наличии состава преступления, следователь принимает решение о возбуждении уголовного дела, после чего приступает к производству следственных действий, направленных на процессуальное закрепление добытых доказательств.

Однако следует учитывать, что на практике установить факт неправомерности списания денежных средств со счета заявителя в рамках процессуальной проверки не всегда представляется возможным в связи с ее ограниченным сроком. Уголовные дела в таких случаях часто возбуждаются непосредственно по заявлению потерпевшего, на основе справки по счету (о списании денежных средств).

Таким образом, необходимые мероприятия, например, получение детализации телефонных соединений, сведений о движении денежных средств по счетам, осмотр мобильного телефона (смартфона) заявителя проводятся уже на первоначальном этапе расследования уголовного дела.

§ 2. Особенности первоначального этапа расследования хищений денежных средств с банковских счетов с использованием компьютерных вредоносных программ

Деятельность сотрудника органа предварительного расследования на стадии возбуждения уголовного дела о совершении любого преступления, в т. ч. уголовных дел, связанных с хищением денежных средств с банковских счетов с использованием компьютерных вредоносных программ, включает в себя следующие основные элементы:

– изучение имеющихся фактических данных (оценка поступившей исходной информации о преступлении);

– проверка заявления и сообщения, если в исходной информации отсутствуют достаточные данные, указывающие на признаки преступления;

– выдвижение версий, определение вопросов, подлежащих выяснению;

– определение круга следственных действий и организационных мероприятий, подлежащих проведению по каждой версии, сроков и последовательности их проведения, а также исполнителей;

– корректировка плана в соответствии с получаемой информацией;

– принятие и процессуальное оформление решения о возбуждении уголовного дела[1].

Подробный допрос потерпевшего по аналогичным вопросам, отраженным в объяснении. В частности, в протоколе необходимо детально зафиксировать: реквизиты счета заявителя, с которого произошло списание денежных средств; информацию об обнаружении заявителем несанкционированной транзакции (дата и время операции); точную сумму причиненного ущерба; информацию о подключении заявителем сервиса СМС-информирования о произведенных операциях по счету; местонахождение мобильного телефона (смартфона) потерпевшего в период списания денежных средств со счета.

Одним из следственных действий, проводимых в процессе расследования преступлений, связанных с хищением денежных средств с банковских счетов с использованием компьютерных вредоносных программ, является допрос подозреваемого. В ходе данного допроса следователь может установить обстоятельства, имеющие значение для уголовного дела. При этом большое влияние на содержание действий следователя оказывает следственная ситуация, складывающаяся на момент начала допроса.

Перед началом допроса подозреваемого необходимо детально изучить и проанализировать материалы уголовного дела. Изучению подлежат процессуальные документы, содержащие сведения о совершенном преступлении. Это могут быть, например, протоколы допросов свидетелей, потерпевших, заключения судебных экспертиз. Кроме того, анализируются ответы на запросы в различные организации, например, справки или расширенные выписки по счетам, с которых производилось несанкционированное списание денежных средств. Необходимо изучение результатов оперативно-разыскной

[1] См.: Филиппов А. Г. Планирование расследования // Криминалистика: учебник для вузов МВД России / редкол.: Б. П. Смагоринский, А. Ф. Волынский, А. А. Закатов, А. Г. Филиппов. Волгоград, 1994. Т. 2: Техника, тактика, организация и методика расследования преступлений. С. 277.

деятельности. Целесообразно также проанализировать иные материалы, например, должностные инструкции, регламентирующие деятельность отдельных банковских служащих.

Особое внимание следует уделить сбору и анализу информации, характеризующей допрашиваемое лицо. Это будет способствовать выбору правильной линии поведения во время производства этого следственного действия.

Представляют интерес следующие сведения о подозреваемом:

1) сведения о наличии знаний и умений, а также опыта работы в сфере применения компьютерных технологий;

2) сведения о приобщении подозреваемого к профессиональному сообществу в сфере применения компьютерных технологий;

3) сведения, указывающие на возможность совершения преступления группой (по предварительному сговору или организованной группой);

4) сведения, позволяющие охарактеризовать физиологическое и социально-психологическое состояние подозреваемого.

Необходимые сведения о личности подозреваемого можно получить путем направления письменного поручения органу дознания о производстве оперативно-разыскных мероприятий (например, в целях установления факта обучения в учебном заведении, реализующем соответствующие образовательные программы; установления круга знакомых и т. д.). Одновременно можно допросить лиц из числа знакомых подозреваемого (например, в целях установления наличия у подозреваемого знаний и умений в сфере компьютерных технологий, а равно фактов их «сетевого» применения). Кроме того, целесообразно направить запрос в учебное заведение и (или) место работы (в целях установления факта получения подозреваемым образования, в том числе дополнительного, в сфере компьютерных технологий и (или) опыта работы в этой области). Эффективным является изучение архивных уголовных дел, фиксирующих ранее совершенные подозреваемым преступления (особенно, если речь идет о преступлениях в сфере компьютерной информации)[1].

[1] См.: Тактика допроса подозреваемого по преступлениям, совершаемым с использованием интернет-технологий (на примере статьи 272 УК РФ): метод. рекомендации. Омск: Омская академия МВД России, 2014.

Рабочий этап допроса подозреваемого по преступлениям, связанным с хищением денежных средств с банковских счетов с использованием компьютерных вредоносных программ, протекает в каждом конкретном случае по-разному. Вместе с тем следователь при допросе должен учитывать общие правила, адаптируя их к особенностям конкретного преступления.

В целях установления типа вредоносной программы, алгоритма ее действия, а также источника ее распространения назначается компьютерная экспертиза изъятого мобильного устройства заявителя. Более подробно данный вопрос рассмотрен в разделе «Использование специальных познаний».

Установление лиц, причастных к совершению преступлений, как правило, основывается на полученной информации о счетах и движении денежных средств по ним. В случаях, когда денежные средства были переведены с банковского счета потерпевшего также на иные банковские счета, методика расследования уголовных дел аналогична стандартной методике расследования банковских хищений и основана на установлении и отработке конечного адресата вывода денежных средств.

В настоящее время денежные средства, похищенные с банковского счета потерпевшего, злоумышленники изначально перечисляют на лицевые счета различных операторов сотовой связи и электронно-платежных систем («Qiwi», «Webmoney», «Яндекс.Деньги» и иные). В дальнейшем денежные средства посредством использования современных возможностей различных электронно-платежных сервисов обналичиваются или используются для электронной оплаты различных товаров и услуг.

Характерным примером является функционирование электронного платежного сервиса «RuRu» (www.ruru.ru, ЗАО «Национальная сервисная компания», г. Москва). Данный сервис, используя ресурсы Интернета, позволяет различными способами выводить денежные средства с лицевого счета сотового оператора ОАО «ВымпелКом» (бренд «Билайн»). В данном случае для получения информации о конечном (либо промежуточном) получателе похищенных денежных средств необходимо истребовать сведения технического характера как у оператора сотовой связи, так и у представителя платежного сервиса.

При этом необходимо учитывать, что денежные средства, поступившие на счет абонентского сотового номера, не обязательно будут обналичены. Как было замечено выше, они могут быть использованы в качестве электронной оплаты различных товаров и услуг (например, оплата всевозможных интернет-сервисов, сайтов знакомств, онлайн-игр, социальных сетей, товаров из интернет-магазинов). Также перечисление денежных средств со счета одного абонентского номера на другой может использоваться в качестве оплаты за различные товары и услуги между лицами, отбывающими наказания в виде лишения свободы.

В данных случаях для установления конечного адресата необходимо истребовать у соответствующего оператора технические сведения (IP-адреса создания, администрирования) о том или ином аккаунте – учетной записи (в социальной сети, интернет-магазине и т. д.). Это в итоге позволит «привязать», как правило, обезличенного пользователя Интернета к реальному человеку или месту.

§ 3. Использование специальных познаний при расследовании хищений денежных средств с банковских счетов, совершаемых с использованием компьютерных вредоносных программ

В расследовании преступлений, связанных с хищением денежных средств с использованием вредоносных компьютерных программ, для установления личностей преступников, их местонахождения, а также доказывания их вины особое значение приобретает использование специальных познаний.

Одним из направлений применения специальных познаний при расследовании хищений с платежной карты клиента банка с использованием компьютерных вредоносных программ является изучение технической документации о телефонных соединениях потерпевшего, совершенных в период хищения (детализации, биллинга).

Детализация телефонных соединений потерпевшего может являться важным источником информации о характере и способе хищений денежных средств в случаях их совершения с использованием средств сотовой связи. Таким образом, для качественного анализа и получения на его основе результирующей информации необходимо обладание специалистом знаниями в сфере функционирования сетей сотовой связи, мобильных устройств и программного обеспечения к ним.

В данном случае специальные познания могут применяться как в процессуальных формах – участие специалиста при осмотре документов, допрос специалиста, так и в непроцессуальной, например, в форме консультаций специалиста следователю при подготовке следственных действий.

Часто на первоначальном этапе расследования потерпевший при допросе поясняет, что он не получал входящих SMS-сообщений с запросом на проведение денежного перевода и SMS-сообщений с подтверждением платежа также не отправлял. Сведения о данных сообщениях на телефоне потерпевшего также отсутствуют. Из его показаний следует, что телефон «самостоятельно» совершил все необходимые действия для осуществления денежного перевода с помощью сервисов мобильного банкинга.

Основной задачей специалиста при этом является установление факта и технологии списания денежных средств в ходе изучения телефонных соединений.

Действие большинства компьютерных вредоносных программ, функционирующих на операционных системах мобильных устройств, предназначенных для хищения денежных средств с платежных карт, основано на возможностях удаленного перехвата и отправки SMS-сообщений с мобильного устройства потерпевшего. Если подобные сообщения поступали и отправлялись на абонентский номер потерпевшего, информация о них содержится в детализации телефонных соединений.

Процессуальный порядок истребования детализации телефонных соединений в рамках уголовного дела четко определен ст. 186.1 УПК РФ – «При наличии достаточных оснований полагать, что информация о соединениях между абонентами и (или) абонентскими устройствами имеет значение для уголовного дела, получение следователем указанной информации допускается на основании судебного решения, принимаемого в порядке, установленном ст. 165 УПК РФ». Получение и изучение детализации телефонных соединений потерпевшего является одним из первичных мероприятий, в связи с чем данную информацию целесообразно получить еще на стадии процессуальной проверки (например, в порядке осуществления оперативно-разыскной деятельности).

При проведении осмотра протокола телефонных соединений потерпевшего в качестве специалиста целесообразно привлечь сотрудника

технического отдела сотового оператора либо иных организаций, деятельность которых связана с разработкой и обслуживанием биллинговой информацией для сетей сотовой связи.

При этом задачами специалиста будут являться:

1. Изучить и пояснить следователю информацию обо всех телефонных соединениях потерпевшего за период, в который осуществлены незаконные списания денежных средств с платежной карты.

2. Зафиксировать все входящие и исходящие SMS-сообщения между абонентским номером потерпевшего и сервисным номером (номерами) банка. Отразить точную последовательность и время их поступления и отправки.

3. Зафиксировать информацию об IMEI (индивидуальный номер мобильного оборудования) мобильных устройств, в которых использовался абонентский номер потерпевшего в период совершения хищения, а также непосредственно до и после обозначенного периода (по ближайшим соединениям). В пояснении следователю сделать вывод об идентичности либо различии используемых номеров IMEI.

4. Зафиксировать информацию об адресах базовых станций, фиксировавших телефонные соединения потерпевшего в период хищения, а также непосредственно до и после обозначенного периода.

Таким образом, в результате изучения телефонных соединений и пояснений специалиста должны быть установлены следующие факты:

– отправлялись ли на сервисный банковский номер команды на проведение и подтверждение платежа с номера потерпевшего;

– если да, то отправлялись ли данные сообщения с мобильного устройства потерпевшего либо с какого-то иного;

– откуда территориально отправлялись данные SMS-сообщения.

Если сведения технического характера, содержащиеся в протоколе телефонных соединений, требуют дополнительных пояснений, следователь может прибегнуть к еще одной форме использования специальных познаний – допросу специалиста.

Важной формой использования специальных познаний при расследовании преступлений рассматриваемой категории является участие специалиста в осмотре ЭВМ (персонального компьютера, ноутбука, планшета, смартфона, иных устройств), принадлежащей потерпевшему.

Первоначальный осмотр ЭВМ может проводиться в рамках осмотра предметов. Однако проведение данного действия целесообразней еще на стадии процессуальной проверки сообщения о преступлении, а именно в ходе осмотра места происшествия.

Анализ следственной практики по рассматриваемым преступлениям выявил ряд проблем организационного и технического характера, с которыми сталкивается следователь при проведении данного вида осмотра. Основной причиной низкой результативности осмотров мест происшествий является недостаточная компетентность лиц, осуществляющих осмотр.

На первоначальном этапе расследования основной задачей является установление способа и механизма совершения хищения, в частности, документирование факта использования компьютерных вредоносных программ. Для ее решения крайне важно правильно с правовой и технической стороны осуществить осмотр компьютерного устройства, которым пользовался потерпевший. От этого зависит установление способа совершения хищения, последующая квалификация преступного деяния, а также планирование дальнейших следственных действий.

При этом следователь либо иное лицо, осуществляющее процессуальную проверку, как правило, не обладает необходимым уровнем знаний и навыков. В связи с этим для правильной и полной фиксации интересующей информации, содержащейся в мобильном устройстве, необходимо привлечение специалиста, обладающего специальными познаниями в сфере технического устройства мобильных терминалов.

Знание алгоритма функционирования компьютерных вредоносных программ, предназначенных для хищения денежных средств с платежных карт клиентов банка, также является необходимым критерием для выбора специалиста, участвующего в осмотре мобильного устройства.

При проведении осмотра компьютерного устройства приоритетным вариантом является привлечение в качестве специалиста сотрудника подразделения экспертно-криминалистического центра территориального ОВД, специализирующегося на компьютерных экспертизах. Подобная возможность предельно ограничена по причине чрезмерной загруженности и небольшой численности указанной категории сотрудников.

В случае невозможности привлечения к осмотру сотрудника ЭКЦ возможно прибегнуть к помощи работников иных государст-

венных органов (например, федеральной службы по надзору в сфере связи, информационных технологий и массовых телекоммуникаций), а также негосударственных организаций (например, технических специалистов интернет-провайдеров, операторов сотовой связи, различных IT-компаний).

Основной информацией, подлежащей обнаружению и фиксации на компьютерном устройстве потерпевшего в ходе осмотра, является наличие вредоносной компьютерной программы (программ), а также следов ее использования.

Принцип действия компьютерных вредоносных программ, предназначенных для хищения денежных средств с банковских счетов, для всех операционных платформ является схожим и заключается в сборе информации и удаленном управлении банковским счетом потерпевшего в целях дальнейшего списания с него денежных средств.

Так, в предыдущих разделах рассматривался пример, когда троянская программа семейства «Android.BankBot», «прописавшись» на мобильном терминале пользователя, позволяет злоумышленникам считывать полную информацию о данном устройстве и установленном на нем программном обеспечении, а самое главное – перехватывать и отправлять SMS-сообщения от имени пользователя без его ведома.

В следственной практике ярким проявлением «вредоносности» программ указанного типа явился массовый характер хищения денежных средств со счетов клиентов Сбербанка России, использующих на своих мобильных устройствах программное приложение «Мобильный банк».

Вредоносная троянская программа данного типа, установленная на зараженное мобильное устройство потерпевшего, под видом обновления популярного приложения (например, «Adobe Flash Player») собирала и отправляла на сервер сведения о наличии ПО «Мобильный банк», анализировала его активность, в результате чего злоумышленники получали информацию о платежной банковской карте пользователя, привязанной к данному приложению. Далее, используя удаленное администрирование мобильного устройства пользователя, а также возможности сервиса ПО «Мобильный банк», злоумышленники отправляли SMS-сообщения с командой на перевод денежных средств с платежной карты потерпевшего. При этом входящее SMS-сообщение, поступающее от сервера банка о необходимости

подтверждения платежа, перехватывалось вредоносной программой и было скрыто от пользователя. В ответ на данное сообщение троянской программой отправлялось SMS-сообщение с подтверждением проведения платежа, содержащее (при необходимости) одноразовый код подтверждения.

Таким образом, на стадии осмотра целью привлечения специалиста являются обнаружение, установление типа вредоносной программы, принципа ее функционирования, фиксации следов ее использования.

Действия специалиста при осмотре компьютерного устройства заключаются в следующем:

– определение внешних признаков устройства, его размеров, модели, а для терминалов сотовой связи (планшетов, смартфонов) – сведений об IMEI-номере, используемых на момент осмотра абонентском номере и сим-карте;

– определение системных параметров устройства – установленные операционная система, программные приложения, параметры быстродействия (процессор, оперативная память и т. д.). Особое внимание на данном этапе уделяется наличию/отсутствию установленных программных приложений ДБО (дистанционного банковского обслуживания), а также антивирусных программ. Необходимо отразить свойства данных приложений, даты и время установки и последнего использования;

– непосредственное обнаружение на компьютерном устройстве вредоносной программы либо следов ее применения, документирование факта осуществления несанкционированных платежей. Для этого проводится изучение журнала работы программ ДБО, а также антивирусного программного обеспечения. В первом случае фиксируются сведения обо всех проведенных платежах за интересуемый период (дата, время, адресат денежного перевода и другие). Во втором случае необходимо зафиксировать информацию обо всех обнаруженных угрозах и предупреждениях. В ходе осмотра также целесообразно провести дополнительное сканирование системы на предмет обнаружения вредоносных программ с последующей фиксацией его результатов. При этом крайне важно предварительно выставить правильные настройки сканирования (без опции удаления и других мер к обнаруженным угрозам), чтобы по неосторожности не удалить сами вредоносные программы, а также следы их функционирования;

– при осмотре сотовых терминалов (планшетов, смартфонов) необходимо изучение и фиксация журнала SMS-сообщений и телефонных соединений за период, в который осуществлено хищение денежных средств (проведены несанкционированные транзакции со счета потерпевшего). Подробно описывается и фиксируется каждое входящее и исходящее SMS-сообщение (время, дата, адресат отправки, полный текст сообщения, а также время, дата и адресаты входящих/исходящих телефонных звонков).

На протяжении всех описанных действий является обязательной фотофиксация полученных результатов осмотра. В процессе обнаружения вредоносных программ с использованием антивирусного программного обеспечения также необходимо использовать средства видеозаписи.

Стоит отметить, что на практике привлекаемые к осмотру специалисты не всегда обладают необходимым уровнем профессиональной компетенции. Решению данной задачи на высоком качественном уровне, а также возникающих при этом проблем может способствовать привлечение к осмотру мобильных устройств представителей специализированных экспертных учреждений, таких как ЗАО «Лаборатория Касперского», ООО «Доктор Веб», «Group-IB» и иных организаций, специализирующихся на экспертных исследованиях компьютерных вредоносных программ. Сотрудники данных организаций обладают всеми необходимыми знаниями и навыками, что позволяет в результате выстроить полную картину совершения преступления.

Таким образом, участие специалиста в осмотре компьютерного устройства потерпевшего является непременным условием на первоначальном этапе расследования хищений, совершаемых с использованием компьютерных вредоносных программ. Обязательным критерием выбора специалиста является его компетентность в сфере устройства мобильных терминалов и функционирования компьютерных вредоносных программ. Совокупность данных условий способствует правильной квалификации преступного деяния, планированию и проведению следственных действий на последующих этапах расследования.

Несмотря на важность участия специалиста при осмотре ЭВМ, принадлежащей потерпевшему, основной формой применения специальных познаний при расследовании уголовных дел, связанных

с хищением денежных средств с использованием компьютерных вредоносных программ, является проведение судебной экспертизы.

Стоит отметить, что после внесения Федеральным законом от 4 марта 2013 г. № 23-ФЗ изменений в ч. 4 ст. 195 УПК РФ, назначение и проведение судебных экспертиз стало возможным до возбуждения уголовного дела. В связи с этим отсутствует необходимость рассматривать иные формы экспертных исследований при расследовании обозначенной категории преступлений.

В случае необходимости экспертного исследования мобильного сотового устройства (планшетного компьютера, смарфона) проблемным вопросом, с которым может столкнуться следователь (дознаватель) при назначении судебной экспертизы, является правильное определение ее типа.

Приказ МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» четко определяет перечень родов (типов) судебных экспертиз, проводимых в экспертных подразделениях МВД России, а также виды проводимых в их рамках исследований.

Основным типом экспертиз, проводимых по уголовным делам рассматриваемой категории, является судебная компьютерная экспертиза, в рамках которой проводится исследование компьютерной информации. При расследовании преступлений, связанных с использованием компьютерных вредоносных программ, основным объектом исследования является как раз компьютерная информация, хранящаяся на мобильном устройстве. Таким образом, до октября 2015 г. проблем с определением типа судебной экспертизы не возникало.

Однако приказом МВД России от 27 октября 2015 г. № 1012 в Перечень был внесен новый тип судебной экспертизы – радиотехническая, в рамках которой проводится исследование радиоэлектронных устройств.

Учитывая, что объектом экспертного исследования при расследовании хищений, совершаемых с использованием компьютерных вредоносных программ, также являются мобильные устройства, назначение данного типа судебной экспертизы в определенных случаях является допустимым.

Выбор типа судебной экспертизы в каждом случае зависит от целей и задач конкретного исследования, а также от того, какой объект исследования является основным.

Принимая во внимание, что основной задачей судебной экспертизы при расследовании преступлений рассматриваемой категории является изучение структуры и алгоритма функционирования компьютерной вредоносной программы, рассмотрим особенности назначения и проведения компьютерной судебной экспертизы.

Учитывая особенности объекта исследования, необходимо верно обозначить цели и задачи назначаемой экспертизы, а также четко представлять для себя ее результат. Важное значение для этого имеет правильная формулировка вопросов, адресованных эксперту.

Поставленные перед экспертом вопросы должны отвечать следующим критериям:

– должны быть правильно сформулированы с технической и правовой точек зрения;

– соответствовать компетенции и фактическим возможностям эксперта (экспертного учреждения);

– в своей совокупности в полном объеме, четко и понятно отражать цель, задачи и необходимый результат исследования.

Для полного достижения целей исследования при назначении компьютерной экспертизы предлагается перечень следующих вопросов:

1. Имеются ли на представленном компьютерном устройстве файлы, которые антивирусная программа атрибутирует как компьютерные вредоносные программы?

2. Если да, то к какому типу компьютерных вредоносных программ они относятся?

3. Каков источник появления вредоносной программы на представленном устройстве?

4. Каков алгоритм функционирования данной вредоносной программы; какие цели и задачи она решает?

5. Обладает ли данная вредоносная программа возможностью удаленного администрирования компьютерным устройством? Если да, то каков источник удаленного администрирования?

6. Имеется ли связь работы вредоносной программы с работой других программных приложений, установленных на устройстве (в частности, приложений мобильного банкинга)? Если да, то в чем заключается воздействие вредоносной программы на работу данных приложений?

7. Каков адресат отправки вредоносной программой результатов своей работы (сетевой адрес ресурса)?

8. Имеются ли на представленном мобильном устройстве иные сведения об удаленном администрировании?

Данный перечень примерный и не является исчерпывающим. Однако, в случае получения ответов на указанные вопросы, следователь будет иметь полную картину о способе совершения хищения, источнике распространения вредоносной программы, адресате ее администрирования, а также способе и адресате несанкционированных денежных переводов со счета потерпевшего.

Следует отметить, что экспертно-криминалистические подразделения системы МВД России даже при наличии в них экспертов, специализирующихся на компьютерных экспертизах, проводят исследования на начальном уровне, в ходе которого не изучается программный код и заданный алгоритм функционирования вредоносной программы.

Проведение экспертизы на более качественном уровне возможно в ранее упомянутых организациях ООО «Доктор Веб», ЗАО «Лаборатория Касперского», «Group-IB».

Так, деятельность компании «Group-IB» воплощена в экосистеме «Bot-Trek» – линейке высокотехнологичных продуктов для мониторинга, обнаружения и предупреждения киберугроз, основанной на самых актуальных данных киберразведки и глубоком анализе реальных хакерских атак.

Согласно сведениям, размещенным на официальном интернет-портале компании, лаборатория компьютерной криминалистики и исследования вредоносного кода данной организации занимается сбором и оформлением цифровых доказательств более 10 лет. Для поиска и изъятия доказательств используется самое современное оборудование и программное обеспечение, признанные зарубежные и передовые отечественные продукты по компьютерной форензике.

При выезде на место инцидента и проведении оперативно-разыскных мероприятий используются мобильные криминалистические комплексы, которые позволяют изымать сведения без нарушения целостности (что сохраняет носитель информации в доказательной базе) и проводить их экспресс-исследования на месте.

Помимо самой информации для криминалиста важна хронология ее создания, доступа к ней и ее использования. Компания обладает собственными разработками, которые позволяют посекундно восста-

новить цепочку действий злоумышленника и обнаружить не детектируемые антивирусами вредоносные файлы.

Исследованием последних занимается специальное подразделение вирусной аналитики, задача которого – установить и зафиксировать следы, ведущие к разработчикам и операторам атаки[1].

Параллельная работа криминалистов и вирусных аналитиков обеспечивает быстрое, полное и, самое главное, качественное производство исследования. Высокое качество экспертиз лаборатории заслужило доверие не только корпоративных клиентов, но и госструктур.

Лаборатория Group-IB – единственная в России, в которой специалисты имеют сертификаты GIAC по Digital Forensics и Malware Analysis. Результаты экспертиз гарантированно принимаются в качестве доказательств не только в российских, но и в иностранных судах.

В заключение следует отметить, что только в результате проведения компьютерной экспертизы на необходимом качественном уровне возможно установление полного механизма совершения преступления, а также всех лиц, причастных к хищениям, в том числе распространивших и использовавших компьютерную вредоносную программу, а не только конечное звено цепи – обнальщиков.

[1] См.: Group-Ib.Расследования. URL: http://www.group-ib.ru/investigation.html#lab (дата обращения: 10.08.2018).

ЗАКЛЮЧЕНИЕ

Спецификой производства всех следственных действий при расследовании преступлений в сфере компьютерной информации является необходимость использования специальных познаний разных отраслей: электроники, программирования, телекоммуникаций и др., а также качественная подготовка к их проведению.

Использование специальных познаний необходимо осуществлять в виде:

– неофициальных консультаций у специалистов-профессионалов в различных отраслях науки и техники;

– участия специалистов при производстве следственных действий;

– производства экспертиз.

Постоянное совершенствование преступлений в сфере компьютерной информации, изобретение преступниками новых способов хищений денежных средств с использованием вредоносных компьютерных программ в сети Интернет затрудняют деятельность правоохранительных органов по их выявлению и доказыванию.

Хищения денежных средств, совершенные с использованием телекоммуникационных сетей общего пользования, за последние годы приобретают все более массовый характер. Раскрываемость этого вида преступлений остается на низком уровне. Деятельность преступников по созданию новых способов хищений с использованием вредоносных компьютерных программ становится более совершенной. Распространение преступлений в сфере высоких технологий неизбежно приводит сотрудников правоохранительных органов к необходимости детального изучения технических возможностей существующих компьютерных систем, их применения и использования в борьбе с правонарушениями в данной сфере деятельности. При этом следователи испытывают некоторые затруднения при расследовании преступлений данного вида.

Приложение

Образцы процессуальных документов, составляемых следователем при расследовании хищений денежных средств с банковских счетов с использованием компьютерных вредоносных программ

ПРОТОКОЛ
допроса потерпевшего

г. Энск «____» _____ 2019 г.

Допрос начат в: 08 час. 57 мин.
Допрос окончен в: 09 час. 34 мин.

Старший следователь СУ УМВД России по г. Энску, майор юстиции Иванов И. И., в помещении служебного кабинета № 7 УМВД России по г. Энску (д. 2 по ул. Плеханова г. Энска), в соответствии со ст. 189, 190 УПК РФ допросил по уголовному делу № 2018/21313/221 в качестве потерпевшего:

1.	Фамилия, имя и отчество	Круглова Марина Ивановна
2.	Дата рождения	10 сентября 1989 г. р.
3.	Место рождения	г. Энск
4.	Место жительства и (или) регистрации, телефон	г. Энск, ул. Сибирская, д. 4, кв. 18, сот. тел. 8-770-700-72-73
5.	Гражданство	РФ
6.	Образование	Среднее
7.	Семейное положение, состав семьи	замужем, детей на иждивении нет
8.	Место работы или учебы, телефон	работает мастером участка № 3 УК ООО «Чистый Энск»
9.	Отношение к воинской обязанности	невоеннообязанная
10.	Наличие судимости	нет

11. Паспорт или иной документ удостоверяющий личность свидетеля	паспорт РФ 3246 № 234734, выдан 12.11.2010 г. УФМС России по Энской области
12. Иные данные о личности свидетеля	не установлены

Иные участвующие лица: не участвовали

Лица, участвующие в допросе, были заранее предупреждены о применении при производстве следственного действия технических средств: не применялись.

Потерпевший (подпись потерпевшего)

Перед допросом следователем в соответствии с ч. 1 ст. 189 УПК РФ выполнены требования, предусмотренные ч. 5 ст. 164 УПК РФ, участвующим лицам разъяснены их права, обязанности и ответственность, порядок производства допроса.

Потерпевший (подпись потерпевшего)

Следователем разъяснены права потерпевшего, предусмотренные ч. 2 ст. 42 УПК РФ, а также положения чч. 3–10 ст. 42 УПК РФ. В соответствии с ч. 1 ст. 45 УПК РФ представителем потерпевшего может быть адвокат. В качестве представителя потерпевшего могут быть также допущены один из близких родственников потерпевшего либо иное лицо, о допуске которого ходатайствует потерпевший.

Кроме того, мне разъяснено, что в соответствии со ст. 51 Конституции Российской Федерации я не обязан(а) свидетельствовать против самого себя, своего супруга (своей супруги) и других близких родственников, круг которых определен п. 4 ст. 5 УПК РФ.

Об уголовной ответственности за дачу заведомо ложных показаний по ст. 307 УК РФ и по ст. 308 УК РФ за отказ от дачи показа-

ний, а также за уклонение от прохождения освидетельствования, от производства в отношении меня судебной экспертизы в случаях, когда не требуется мое согласие, или от предоставления образцов почерка и иных образцов для сравнительного исследования предупрежден(а).

Потерпевший (подпись потерпевшего)

По существу заданных мне вопросов могу показать следующее: работаю в Управляющей компании ООО «Чистый город». Для начисления заработанной платы работодателем я летом 2018 г. в «БинБонБанке», расположенном по адресу: 123123, г. Энск, ул. Смирнова, 23, открыла текущий счет № 40781021300000000023 и к данному счету получила банковскую карту платежной системы Виза № 1234-5678-1234-5678. Банковская карта была привязана к номеру моего мобильного телефона № 8 (999) 027-23-73. Кроме того, я попросила подключить мне услугу «Мобильный банк», позволяющую отслеживать движение средств по счету моей банковской карты путем получения смс-сообщений с короткого номера «777».

Я пользуюсь сотовым телефон Samsung Galaxy S7. С данного сотового телефона я имею возможность выхода в сеть Интернет, в том числе открывать и просматривать интернет-страницы в браузерах, а также перехода к ним по ссылкам.

ДД.ММ.ГГГГ мне на номер моего сотового телефона, подключенного к мобильному банку, поступило смс-сообщение от ранее неизвестного абонентского номера № 8 (941) 761-23-21 с текстом: «Диана Лазарева отправила Вам сообщение. Открыть «vk.cc/2VvrYz». Затем я со своего мобильного телефона, подключенного к сети Интернет, перешла по указанной ссылке, но открыть и прочитать сообщение не смогла. При этом я не заметила, что смартфон производил какие-либо еще операции, кроме открытия ссылки.

ДД.ММ.ГГГГ я проверила баланс счета своей банковской карты и выяснила, что ДД.ММ.ГГГГ у меня с банковской карты неизвестные лица похитили 15 500 рублей. Смс-сообщений о списании денежных средств со счета карты мне на мой сотовый телефон не поступало, как это должно было быть.

Четырехзначный пин код от банковской карты я никому не сообщала. Банковскую карту я никогда не теряла и никому не передавала как ее саму, так и ее данные.

Кто мог списать или снять с моего банковского счета денежные средства, я не знаю и никого не подозреваю.

Потерпевший (подпись потерпевшего)

В ходе допроса применялась видеозапись.

Перед началом, в ходе либо по окончании допроса от потерпевшего Кругловой М. И. заявления не поступили.

Потерпевший (подпись потерпевшего)

По окончании допроса протокол предъявлен для ознакомления потерпевшему Кругловой М. И. При этом разъяснено право делать подлежащие внесению в протокол оговоренные и удостоверенные его подписью замечания о его дополнении и уточнении.

Ознакомившись с протоколом путем личного прочтения замечания о его дополнении и уточнении не сделаны.

Потерпевший (подпись потерпевшего)

Настоящий протокол составлен в соответствии со ст. 166 (167) и 190 УПК РФ.

Старший следователь (подпись)

ПОСТАНОВЛЕНИЕ
о привлечении в качестве обвиняемого

г. Энск «____» _____ 20__ г.

Старший следователь СУ УМВД России по г. Энску, майор юстиции, Иванов И. И., рассмотрев материалы уголовного дела № 2018/21313/221.

УСТАНОВИЛ:

Немов Владимир Викторович, 01.01.2000 года рождения, уроженец г. Энска, в ДД.ММ.ГГГГ, находясь на территории г. Энска, действуя из корыстных побуждений, осознавая общественную опасность своих действий, предвидя неизбежность наступления общественно опасных последствий и желая их наступления, в целях совершения преступлений в сфере компьютерной информации и преступлений против собственности в октябре 2013 г. вступил в преступный сговор со своим знакомым Сомовым С. С. Для реализации своих преступных намерений Немовым В. В. и Сомовым С. С. была разработана схема совершения преступлений, основанная на познаниях последних в сфере компьютерной информации и техники, а также распределены преступные роли.

Так, Немов В. В., имея специальные познания в области компьютерной техники и программного обеспечения (далее по тексту – ПО), а также обладая опытом работы в информационно-телекоммуникационной сети Интернет (далее по тексту – ИТС Интернет), применил приобретенные им навыки для незаконного обогащения. При этом в период с ДД.ММ.ГГГГ, имея в личном пользовании персональный компьютер, подключенный к ИТС Интернет, находясь в неустановленных местах на территории г. Энска и Энской области, посещал форумы, в том числе www.haker.rt, www.vzlom.mu, на которых изучал содержащуюся на них информацию и совершенствовал свои навыки в области вредоносного ПО, его назначения, правил и порядка установки, а также порядка и способов его модификации, предназначенной для сокрытия вредоносных программ от средств защиты компьютерной информации (антивирусных средств), намереваясь использовать полученные навыки в дальнейшей преступной

деятельности по хищению денежных средств со счетов клиентов Публичного Акционерного Общества «БинБонБанк».

Реализуя свои преступные намерения, Немов В. В. в период с ДД.ММ.ГГГГ через ИТС Интернет у неустановленного следствием лица, находясь в неустановленном месте в г. Энска, приобрел вредоносную компьютерную программу «MoneyHack», способную несанкционированно уничтожать, блокировать, копировать компьютерную информацию владельцев телефонных аппаратов под управлением операционной системы «Android», являющихся держателями банковских карт Публичного Акционерного Общества «БинБонБанк» (далее по тексту – ПАО «БинБонБанк») с подключенной услугой «Мобильный банк». Приобретенная Немовым В. В. вредоносная компьютерная программа позволяла ему и Сомову С. С. без ведома владельцев мобильных телефонов отправлять от их имени SMS-сообщения с командами о запросе баланса денежных средств, находящихся на счетах банковских карт граждан, и о переводе денежных средств с данных счетов на счета третьих лиц без уведомления о произведенных операциях.

Далее Немов В. В. совместно с Сомовым С. С. в период с октября 2018 г. по ДД.ММ.ГГГГ включительно арендовал в ООО «ИнформЦентр» (ИНН 1212121212, г. Энск, ул. Моторная, 12), ЗАО «ТелекомКомКом» (ИНН 6363636363, г. Энск, ул. Строителей, д. 2) и ООО «Технологии Будущего» (ИНН 434343443 г. Энск, ул. Центральная, 14) веб-серверы, которым совместно с Сомовым С. С. присваивал доменные имена: www.777money.us и на которых затем совместно с Сомовым С.С. разместил приобретенную им ранее вредоносную компьютерную программу «MoneyHack». Кроме этого, Немов В. В. занимался тестированием приобретенной у неустановленного лица вышеуказанной вредоносной компьютерной программы, совершенствовал ее, устранял возникающие ошибки в веб-скриптах путем написания программного кода (PHP), который включал в себя добавление команд для проверки баланса на банковских картах ПАО «БинБонБанк» и перевода денежных средств со счетов банковских карт граждан на подконтрольные им номера мобильных телефонов или банковские счета, оформленные на лиц, не подозревающих о его и Сомова С. С. преступной деятельности.

Через ИТС Интернет Немов В. В. подыскивал номера сотовых телефонов граждан, являющихся держателями банковских карт ПАО

«БинБонБанка», и совместно с Сомовым С. С. занимался SMS-рассылкой сообщений, содержащих ложные сведения со ссылками на адреса веб-серверов, где была размещена вредоносная программа «MoneyHack». В целях конспирации своей преступной деятельности от правоохранительных органов использовал компьютерную программу «OpenVPN», предназначенную для сокрытия IP-адресов, с которых осуществлялись через ИТС Интернет соединения с веб-серверами, где находилась вредоносная компьютерная программа «MoneyHack», а также с электронными платежными системами, на счета которых ими перечислялись похищенные у граждан денежные средства.

Сомов С. С., согласно отведенной ему роли, финансировал приобретение вредоносной компьютерной программы «MoneyHack», совместно с Немовым В. В. в период с ДД.ММ.ГГГГ включительно от имени вымышленных лиц арендовал в ООО «ИнформЦентр» (ИНН 1212121212, г. Энск, ул. Моторная, 12), ЗАО «ТелекомКом-Ком» (ИНН 6363636363, г. Энск, ул. Строителей, д. 2) и ООО «Технологии Будущего» (ИНН 434343443 г. Энск, ул. Центральная, 14) веб-серверы, которым совместно с Немовым В.В. присваивал доменные имена. Используя свои связи с работниками ООО «Сотонист» Дьяковым А. А., Поповым П. П., осуществлявшими на территории г. Энска заключение с гражданами договоров на оказание услуг связи различных операторов сотовой связи и не подозревавшими о его истинных намерениях, в целях конспирации и сокрытия следов своей преступной деятельности оформлял через последних на вымышленные имена номера мобильных телефонов, а также приискивал лиц для оформления на их имена сим-карт операторов сотовой связи и банковских карт, необходимых для рассылки SMS-сообщений и вывода похищаемых у граждан денежных средств. Занимался приобретением компьютерной техники и мобильных телефонов, при помощи которых совместно с Немовым осуществлял рассылку SMS-сообщений, содержащих ложные сведения, со ссылками на адреса веб-серверов, где им и Немовым В. В. была размещена вредоносная компьютерная программа «MoneyHack».

После того, как обманутые граждане – держатели банковских карт ПАО «БинБонБанк» с подключенной услугой «Мобильный банк», переходили по ссылкам на адреса веб-серверов, где была размещена вредоносная программа «MoneyHack», что влекло за собой

ее установку на сотовые телефоны данных граждан, действуя помимо их воли и в тайне от них, Сомов С. С. совместно с Немовым В. В., используя свойства вредоносной программы, осуществлял неправомерный доступ к охраняемой законом компьютерной информации граждан, а именно получал информацию о моделях мобильных телефонов, их серийных номерах (IMEI), контактах пользователей телефонов, подключенных банковских картах к номерам мобильных телефонов граждан и о наличии денежных средств на счетах их банковских карт.

Пользуясь тем, что вредоносная компьютерная программа «MoneyHack» блокировала входящие SMS-сообщения гражданам о списании их денежных средств со счетов банковских карт, от имени владельцев абонентских номеров мобильных телефонов Сомов С. С. совместно с Немовым В. В. отправлял SMS-сообщения на номер «777» автоматизированной системы обработки и хранения компьютерной информации, принадлежащий ПАО «БинБонБанк», и осуществлял тем самым переводы денежных средств со счетов банковских карт граждан помимо их воли на подконтрольные ему и Немову В. В. банковские счета и номера мобильных телефонов.

Когда Банк на основании их команд осуществлял такие переводы денежных средств, Сомов С. С. совместно с Немовым В. В. распоряжался похищенными у потерпевших деньгами по своему усмотрению.

Так, Немов В. В., в период с ДД.ММ.ГГГГ, осуществив приобретение у неустановленного следствием лица вредоносной компьютерной программы «MoneyHack», которая согласно заключению эксперта № 666 от ДД.ММ.ГГГГ заведомо предназначена для несанкционированного уничтожения, блокирования, копирования компьютерной информации, находясь в неустановленном месте в г. Энске, совместно с Сомовым С. С., имея умысел на использование данной программы при совершении хищения денежных средств со счетов держателей банковских карт ПАО «БинБонБанка», действуя умышленно, из корыстной заинтересованности, посредством персональных компьютеров и доступа к ИТС Интернет арендовали в неустановленной организации неустановленный веб-сервер, на котором не позднее ДД.ММ.ГГГГ разместили вышеуказанную вредоносную компьютерную программу «MoneyHack».

Далее Немов В. В. и Фазилов А. Т., находясь в неустановленном месте в Октябрьском территориальном округе г. Энск, ДД.ММ.ГГГГ с имевшегося у них мобильного телефона с абонентским номером № 8 (000) 999-00-00 оператора сотовой связи ЗАО «Теле 6» осуществили SMS-рассылку текстового сообщения: «Дашенька отправила Вам сообщение. Открыть «www.777money.su/googl/dsa».

ДД.ММ.ГГГГ данное сообщение поступило на абонентский № 8 (000) 618-967-12 этого же оператора сотовой связи, принадлежащий незнакомой им Арбузовой С. А., проживающей по адресу: г. Энск, ул. Авиамоторная, 34, к телефону которой была подключена услуга «Мобильный банк» с привязкой к счету банковской карты № 1234-5678-1234-5678, открытому в Энском отделении № 5 ПАО «БинБонБанк» по адресу г. Энск, ул. Шоссейная, 1.

Арбузова С. А., получив данное сообщение и будучи обманутой относительно его содержания, перешла по указанной в сообщении ссылке «www.777money.su/googl/dsa», после чего с неустановленного следствием веб-сервера, арендованного Немовом В. В. и Сомовым С. С. в неустановленной организации, на ее мобильный телефон под управлением операционной системы «Android», помимо ее воли и в тайне от нее, установилась вредоносная компьютерная программа, отображаемая как «Игра Покер».

Установленная таким образом указанная вредоносная программа предоставила Немову В. В. и Сомову С. С. возможность несанкционированного доступа и копирования компьютерной информации, находящейся в мобильном телефоне Арбузовой С. А., содержащей сведения о состоянии счета ее банковской карты, а также возможность отправлять от имени последней SMS-сообщения в автоматизированную систему обработки и хранения запросов ПАО «БинБонБанк» (далее по тексту – Банк) через номер «777» с командами о перечислении денежных средств при помощи услуги «Мобильный банк» с ее абонентского номера.

В этот же день, ДД.ММ.ГГГГ, Немов В. В. и Сомов С. С., находясь в неустановленном месте в г. Энске, получив возможность распоряжаться денежными средствами Арбузовой С. А., используя вышеуказанную вредоносную компьютерную программу «MoneyHack», действуя умышленно, из корыстных побуждений, при помощи мобильных телефонов и персональных компьютеров, находившихся в их распоряжении, имея доступ к ИТС Интернет, в тайне от Арбу-

зовой С. А. осуществили ввод компьютерной информации на номер «777» автоматизированной системы обработки и хранения компьютерной информации, принадлежащий ПАО «БинБонБанк» и распоряжения от ее имени в Банк о перечислении 5 000 рублей со счета банковской карты последней на счет абонентского номера мобильного телефона Арбузвой С. А.

В тот же день ДД.ММ.ГГГГ Банк, получив от имени Арбузовой С. А. распоряжение о переводе денежных средств, осуществил автоматизированную проверку полученного запроса и, не выявив признаков нарушения безопасности при использовании системы, произвел операцию по переводу 5 000 рублей со счета банковской карты № 1234-5678-1234-5678 Арбузовой С. А. на счет абонентского номера мобильного телефона последней. При этом используемая Немовым В. В. и Сомовым С. С. вредоносная компьютерная программа «MoneyHack» заблокировала SMS-оповещение Арбузовой С. А. о перечислении денежных средств со счета ее банковской карты.

Далее Немов В. В. и Сомов С. С., в тот же день ДД.ММ.ГГГГ, находясь в неустановленном месте в г. Энске, продолжая свои преступные действия, убедившись, что денежные средства в сумме 5 000 рублей перечислены Банком со счета банковской карты Арбузовой С. А. на счет номера ее мобильного телефона, действуя умышленно, из корыстных побуждений, в целях использования вредоносной компьютерной программы «MoneyHack» при совершении хищения чужого имущества посредством мобильных телефонов, персональных компьютеров и доступа к ИТС Интернет, направив оператору сотовой связи ЗАО «Теле 6» команду, осуществили перевод 5 000 рублей с номера мобильного телефона Арбузовой С. А. 8 (000) 618-967-12 на счет № 987654321, принадлежащего WN-идентификатору AS234234AS электронной платежной системы «WebMoney», используемого ими.

Таким образом, Немов В. В. совершил умышленные преступления, а именно: предусмотренные ч. 2 ст. 273, ч. 3 ст. 272, п. в ч. 3 ст. 159.6 УК РФ, а именно использование компьютерной программы, заведомо предназначенной для несанкционированного уничтожения, блокирования, копирования компьютерной информации, группой лиц по предварительному сговору, из корыстной заинтересованности; неправомерный доступ к охраняемой законом компьютерной информации, повлекший блокирование, копирование компьютерной инфор-

мации из корыстной заинтересованности группой лиц по предварительному сговору; хищении чужого имущества путем ввода, блокирования, компьютерной информации с причинением значительного ущерба гражданину группой лиц по предварительному сговору с банковского счета.

(и т. д. если имеется несколько эпизодов преступной деятельности.)

На основании изложенного, руководствуясь ст. 171 и 172 (175) УПК РФ,

ПОСТАНОВИЛ:

Привлечь Немова Владимира Викторовича, 01.01.2000 года рождения, уроженца г. Энска, в качестве обвиняемого по данному уголовному делу, предъявив ему обвинение в совершении преступления, предусмотренного ч. 2 ст. 273, ч. 3 ст. 272, п. в ч. 3 ст. 159.6 УК РФ.

Старший следователь _____ **И. И. Иванов**

Настоящее постановление мне объявлено «____» _____ 2018 г. его текст прочитан лично.

Сущность предъявленного обвинения разъяснена. Одновременно мне разъяснены права, предусмотренные чч. 3–4 ст. 47 и ч. 2 ст. 3171 УПК РФ, а именно:

1) защищать свои права и законные интересы и иметь достаточное время и возможность для подготовки к защите;

2) знать, в чем я обвиняюсь;

3) получить копию постановления о привлечении меня в качестве обвиняемого, копию постановления о применении ко мне меры пресечения, копию обвинительного заключения, обвинительного акта или обвинительного постановления;

4) возражать против обвинения, давать показания по предъявленному мне обвинению либо отказаться от дачи показаний. При согласии дать показания я предупрежден о том, что мои показания могут быть использованы в качестве доказательств по уголовному делу, в том числе и в случае моего последующего отказа от этих

показаний, за исключением случая, предусмотренного п. 1 ч. 2 ст. 75 УПК РФ;

5) представлять доказательства;

6) заявлять ходатайства и отводы;

7) давать показания и объясняться на родном языке или языке, которым я владею;

8) пользоваться помощью переводчика бесплатно;

9) пользоваться помощью защитника, в том числе бесплатно в случаях, предусмотренных УПК РФ;

10) иметь свидания с защитником наедине и конфиденциально, в том числе до первого допроса, без ограничения их числа и продолжительности;

11) участвовать с разрешения следователя (руководителя следственного органа, дознавателя) в следственных действиях, производимых по моему ходатайству или ходатайству моего защитника либо законного представителя, знакомиться с протоколами этих действий и подавать на них замечания;

12) знакомиться с постановлением о назначении судебной экспертизы, ставить вопросы эксперту и знакомиться с заключением эксперта;

13) знакомиться по окончании предварительного расследования со всеми материалами уголовного дела и выписывать из уголовного дела любые сведения и в любом объеме;

14) снимать за свой счет копии с материалов уголовного дела, в том числе с помощью технических средств;

15) приносить жалобы на действия (бездействие) и решения органа дознания, начальника подразделения дознания, дознавателя, следователя, руководителя следственного органа, прокурора и суда в порядке, предусмотренном главой 16 УПК РФ, и принимать участие в их рассмотрении судом;

16) возражать против прекращения уголовного дела по основаниям, предусмотренным ч. 2 ст. 27 УПК РФ;

17) участвовать в судебном разбирательстве уголовного дела в судах первой, второй, кассационной и надзорной инстанций, а также в рассмотрении судом вопроса об избрании в отношении меня меры пресечения и в иных случаях, предусмотренных пп. 1–3 и 10 ч. 2 ст. 29 УПК РФ;

18) знакомиться с протоколом судебного заседания и подавать на него замечания;

19) обжаловать приговор, определение, постановление суда и получать копии обжалуемых решений;

20) получать копии принесенных по уголовному делу жалоб и представлений и подавать возражения на эти жалобы и представления;

21) участвовать в рассмотрении вопросов, связанных с исполнением приговора;

22) защищаться иными средствами и способами, не запрещенными УПК РФ;

23) заявлять ходатайство о заключении досудебного соглашения о сотрудничестве с момента начала уголовного преследования до объявления об окончании предварительного следствия в порядке, установленном ст. 317.1 УПК РФ.

Также мне разъяснено, что в соответствии с ч. 5 ст. 47 УПК РФ участие в уголовном деле защитника или законного представителя обвиняемого не служит основанием для ограничения какого-либо права обвиняемого.

Обвиняемый

Защитник

Постановление объявил, права разъяснил, копию настоящего постановления обвиняемому и его защитнику вручил

Старший следователь _____ **И. И. Иванов**

Копия настоящего постановления направлена прокурору г. Энска «_____» _____ 20___г.

Старший следователь _____ **И. И. Иванов**

Библиографический список

Законы, нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации. Принята на всенародном голосовании 12 декабря 1993 г. (с поправками от 30 декабря 2008 г.) // Рос. газ. – 2009. – 21 янв.
2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 №174-ФЗ // Собрание законодательства РФ. – 2001. – № 52 (ч. I). – Ст. 4921 (в ред. от 30.03.2018).
3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954 (в ред. от 13.07.2018).
4. О полиции: федер. закон от 07.02.2011 № 3-ФЗ // Рос. газ. – 2011. – 8 февр.
5. Об оперативно-розыскной деятельности: федер. закон от 25.08.1995 № 144-ФЗ // Собрание законодательства РФ. – 1995. – № 33. – Ст. 3349.
6. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ. – Доступ из справ.-правовой системы «КонсультантПлюс».
7. О связи: федер. закон от 7 июля 2003 г. № 126-ФЗ. – Доступ из справ.-правовой системы «КонсультантПлюс».
8. О банках и банковской деятельности: федер. закон от 02.12.1990 № 395-1 (ред. от 29.12.2015) (с изм. и доп., вступ. в силу с 09.02.2016). – Доступ из справ.-правовой системы «КонсультантПлюс».
9. Об утверждении Перечня сведений конфиденциального характера: указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015). – Доступ из справ.-правовой системы «КонсультантПлюс».

2. Монографии, учебники, учебные пособия

1. Баев, О. Я. Комментарий к Уголовно-процессуальному кодексу Российской Федерации: науч.-практ. издание / под общ. ред. В. В. Мозякова, Г. В. Мальцева, И. Н. Барцица. – Москва: Книга-Сервис, 2015. – 564 с.

2. Белик, С. П. Особенности производства следственных действий, требующих судебного решения: науч.-практ. пособие / С. П. Белик, В. Г. Войт, Ю. А. Саламаха. – Екатеринбург, 2014. – 115 с.

3. Белкин, Р. С. Криминалистика: учебный словарь-справочник. – Москва: Юрист, 1999. – 268 с.

4. Белкин, Р. С. Криминалистика: проблемы, тенденции, перспективы. От теории к практике / Р. С. Белкин – Москва: Юрид. лит., 1988. – 304 с.

5. Белкин, Р. С. Собирание, исследование и оценка доказательств. Сущность и методы. / Р. С. Белкин – Москва, 1966. 295 с.

6. Бобров, В. К., Божьев, В. П., Бородин, С. В. Научно-практический комментарий к Уголовно-процессуальному кодексу Российской Федерации / под общ. ред. В. М. Лебедева. – Москва: Спарк, 2004. – 560 с.

7. Болтенко, С. И. Тактические особенности следственных действий, проводимых с участием подозреваемых (обвиняемых) – рецидивистов / С. И. Болтенко. – Саратов: Изд. Сарат. юрид. ин-та, 2014. – 232 с.

8. Буцкова, О. И. К вопросу о свойствах доказательств по уголовным делам о хищениях денежных средств с банковских счетов граждан с использованием средств связи, сети «Интернет» / О. И. Буцкова // Юридическая наука и практика: вестник Нижегородской академии МВД России. – 2017. – № 4 (40). – С. 247–250.

9. Буцкова, О. И. Конфиденциальность персональных данных заявителя как препятствие принятию законного решения на стадии возбуждения уголовного дела о хищениях денежных средств с банковских счетов граждан, совершаемых с применением средств связи, сети Интернет / О. И. Буцкова // Теория и практика общественного развития. – 2017. – № 6. – С. 117–119.

10. Буцкова, О. И. Относимость, допустимость, достоверность и достаточность доказательств по уголовным делам о хищениях денежных средств с банковских счетов граждан с использованием

средств связи, сети Интернет // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2017. – № 2 (38). – С. 192–193.

11. Буцкова, О. И. Особенности проведения доследственной проверки и возбуждения уголовных дел о хищениях денежных средств с банковских счетов граждан, совершаемых с применением средств связи // Право: история, теория, практика : материалы IV Международной науч. конф. – Санкт-Петербург: Свое издательство, 2016. – С. 75–80.

12. Васильев, В. Л. Психология следственных действий / В. Л. Васильев. – Санкт-Петербург: Ин-т повышен, квалиф. следств. работников, 2015. – 554 с.

13. Васильченко, А. А. Вопросы обеспечения экономической безопасности в сфере противодействия хищениям денежных средств с лицевых счетов банковских карт граждан / А. А. Васильченко // Обеспечение безопасности в международном и национальном пространстве : материалы междунар. науч.-практ. конф. – Тамбов: ФГБОУ ВО «Тамбовский государственный технический университет», 2017. – С. 62–74.

14. Гавло, В. Г. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений / В. Г. Гавло. – Томск: Изд-во Томского ун-та, 2012. – 332 с.

15. Крашенинников, С. В. Вопросы квалификации преступлений, связанных с хищением денежных средств со счетов банковских карт посредством использования электронных платежных систем / С. В. Крашенинников, Е. И. Куприянов // Вестник Московского государственного областного университета. – Серия: Юриспруденция. – 2016. – № 4. – С. 72–78.

16. Крашенинников, С. В. Особенности рассмотрения сообщения о преступлении по факту хищения денежных средств со счетов банковских карт посредством использования электронных платежных систем / С. В. Крашенинников, Е. И. Куприянов // Рос. следователь. – 2017. – № 18. – С. 33–35.

17. Криворотов, А. И. Теоретические аспекты и практика применения компьютерных технологий в криминалистических учетах: автореф. дис. … канд. юрид. наук / А. И. Криворотов. – Волгоград: ВА МВД России, 2003.– 543 с.

18. Кругликов, В. Д. Способы совершения хищений денежных средств с банковских счетов физических лиц посредством сети Интернет как элемент криминалистической характеристики преступления / В. Д. Кругликов // Проблемы правовой и технической защиты информации: сб. науч. ст. V Всероссийской междисциплинарной молодежной научной конференции. – Барнаул: Алтайский государственный университет, 2017. – С. 81–84.

19. Куприянов, Е. И. С. В. Особенности производства отдельных следственных действий при расследовании преступлений, связанных с хищением денежных средств со счетов банковских карт посредством использования электронных платежных систем / Е. И. Куприянов, С. В. Крашенинников // Рос. следователь. – 2018. – № 6. – С. 11–14.

20. Лихолетов, А. А. Ответственность за хищения денежных средств, находящихся на банковских счетах граждан, в условиях реформирования уголовного законодательства / А. А. Лихолетов // Вестник Волгоградской академии МВД России. – 2016. – № 1 (36). – С. 59–63.

21. Мещеряков, В. А. Основы методики расследования преступлений в сфере компьютерной информации: дис. … д-ра юрид. наук / В. А. Мещеряков. – Воронеж: ВГУ, 2014. – 387 с.

22. Намнясев, В. В. Особенности проверки сообщений о хищениях денежных средств, совершенных с использованием вредоносных компьютерных программ / В. В. Намнясев, А. А. Нурушев, М. А. Семикин // Евразийский юридический журнал. – 2017. – № 12 (115). – С. 225–227.

23. Народенко, В. В. К вопросу о материальном признаке предмета хищения / В. В. Народенко // Известия Юго-Западного государственного университета. – 2017. – № 6 (75). – С. 212–218.

24. Пекарь, Е. В. Развитие документационного обеспечения информационной безопасности при работе по системе клиент-банк / Е. В. Пекарь // Ресурсам области – эффективное использование: сб. мат. XVII Ежегодной науч. конф. студентов Технологического университета. – 2017. – С. 168–175.

25. Попова, Т. В. Способы и преступные схемы хищений денежных средств с лицевых счетов банковских карт граждан / Т. В. Попова, А. В. Котяжов // Академическая мысль. – 2018. – № 2 (3). – С. 110–117.

26. Соловьев, Л. Н. Исследование преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ: автореф. … дис канд. юрид. наук. – Москва: МГУ, 2003. – 44 с.

27. Сухаренко, А. Н. Противодействие киберугрозам в России: состояние, динамика и тенденции / А. Н. Сухаренко // Диалог: политика, право, экономика. – 2018. – № 2 (9). – С. 26–35.

28. Тлиш, А. Д. Проблемы методики расследования преступлений в сфере экономической деятельности, совершаемых с использованием компьютерных технологий и пластиковых карт: дис. … канд. юрид. наук / А. Д. Тлиш. – Краснодар: Куб. гос. аграр. университет, 2012. – 253 с.

29. Усов, А. И. Концептуальные основы судебной компьютерно-технической экспертизы: дис. ... д-ра юрид. наук / А. И. Усов. – Москва: МИ МВД России, 2012. – 372 с.

30. Шакурова, Д. Ф. Риски в платежных системах: мошеннические схемы в мире банковских карт / Д. Ф. Шакурова // Экономика. Бизнес. Банки. – 2017. – № 2. – С. 204–210.

31. Шустова, Э. А. Мошенничество с банковскими картами / Э. А. Шустова // Общество и преступность: уголовно-правовые, пенитенциарные и криминологические аспекты: сб. науч. ст. участников II Всероссийской науч.-практ. конф. – Вятка: Вятский государственный университет, 2017. – С. 129–132.

32. Яковлев, А. Н. Теоретические и методические основы экспертного исследования документов на машинных магнитных носителях информации: дис. … канд. юрид. наук / А. Н. Яковлев. – Саратов: СЮИ МВД России, 2013. – 247 с.

Для заметок

Учебное издание

Намнясев *Виталий Владимирович*
Чухнин *Дмитрий Александрович*
Васильев *Дмитрий Владимирович*

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ХИЩЕНИЕМ ДЕНЕЖНЫХ СРЕДСТВ С БАНКОВСКИХ СЧЕТОВ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ВРЕДОНОСНЫХ ПРОГРАММ

Учебное пособие

Редактор *С. Н. Ненькина*
Технический редактор *С. А. Пан*
Компьютерная верстка *Н. А. Доненко*
Дизайн обложки *О. А. Напольских*

Волгоградская академия МВД России.
400089, Волгоград, ул. Историческая, 130.

Редакционно-издательский отдел.
400131, Волгоград, ул. Коммунистическая, 36.

Подписано в печать 20.12.2018. Формат 60х84/16. Бумага офсетная.
Гарнитура Times New Roman. Физ. печ. л. 4,25. Усл. печ. л. 4,0.
Тираж 50. Заказ 57.

ОПиОП РИО ВА МВД России. 400131, Волгоград, ул. Коммунистическая, 36.