Это Методичка МВД по организации расследования хищения денежных средств, совершенных с использованием компьютерных технологий. С полным алгоритмом (логикой) действий опера и нормативно – правовой базой + реальная статистика по преступлениям.

Современное состояние мирового сообщества характеризуется интенсивным развитием телекоммуникаций, всеобъемлющим проникновением современных информационных технологий в различные области человеческой деятельности. Не является исключением платежная система.

Средства телекоммуникаций, вместе с новыми информационными технологиями, становятся инструментом при разработке новых банковских продуктов и механизмов их распространения, что расширяет сферу деятельности коммерческих банков и иных финансовых организаций. Электронные платежи и средства расчета в точке продажи - примеры использования новых технологий, коренным образом меняющих финансовую индустрию.

Между тем, средства телекоммуникаций и новые информационные технологии (компьютерные технологии) создают условия для подготовки, совершения и сокрытия хищений денежных средств с их использованием, к которым относятся: «виртуальный» характер дистанционных банковских операций; доступность «открытых» телекоммуникационных систем; высокая скорость выполнения транзакций; глобальный характер межсетевого операционного взаимодействия1; изменения в информационном контуре банковской деятельности и появление в нём новых участников (провайдеры, сотовые операторы, аутссрсинговые и иные организации); зависимость реализации банковских операций (банковской деятельности) от надежности не только различного рода провайдеров, сотовых операторов, аутсорсинговых и других организаций, но и от аппаратно-программного обеспечения банковских операций; уязвимость программного кода банковских информационных систем.

При этом преступники не только используют компьютерные технологии в своих целях, но и разрабатывают программные продукты (вредоносные и троянские программы) для облегчения подготовки, совершения и сокрытия таких хищений, новые методы (способы) компрометации банковских карт, персональных компьютеров, банковских автоматизированных систем, в том числе методы передачи скомпрометированной информации. Так, по данным компании «Лаборатории Касперского» только в 2015 г. ими отражено попыток атак вредоносного программного обеспечения для хищения денежных средств через Онлайн-доступ к банковским счетам на 1 966 324 компьютерах пользователей, что на 2,8 % больше, чем в 2014 г. В течение года веб-антивирусом компании было задетектировано 121 262 075 уникальных вредоносных объектов (скрипты, эксплойты, исполняемые файлы и т. д.), выявлено 6 563 145 уникальных хостов для проведения атак через сеть Интернет.

По данным ведомственной статистики в России в 2015 году в сфере телекоммуникаций и компьютерной информации было зарегистрировано 8446 краж и 13464 мошенничества, что составило 362,5 % и 615,6 % по сравнению с предыдущим годом соответственно. При этом большинство таких преступлений совершается в кредитно-финансовой системе (банковской и платежных системах).

Неслучайно 3 июня 2016 г. Председатель Правительства Российской Федерации Д. А. Медведев провел совещание с руководителями заинтересованных в обеспечении информационной безопасности в кредитно-финансовой сфере Российской Федерации ведомств и коммерческих банков, на котором, в частности, отметил: «Мошенники, которые занимаются киберпреступлениями, атакуют не только электронные кошельки конкретных владельцев, но и вообще элементы всей кредитно-финансовой системы, счета банков, финансовых компаний, государства. Они хорошо изучили уязвимость программного продукта, тем более что каждый программный продукт пишется людьми и всегда есть те или иные бреши, которые могут быть пробиты в этих продуктах, даже несмотря на то, что технологии меняются, усложняются, становятся более защищенными. Есть и просто использование доверчивости обычных людей. Активность таких преступников и количество таких преступлений растет повсеместно». В то же время, он обратил внимание на повышенную сложность борьбы с киберпреступностью, а также на большой ущерб, который она наносит России и мировой экономике в целом.

Экспертные оценки и результаты анализа статистических данных подтверждают слова Председателя Правительства Российской Федерации. Так, по данным Председателя Сберегательного банка России Г. Грефа, со временем «нападений» на всех участников финансового рынка станет только больше. Согласно его выступлению, «Только сейчас в мире действует примерно 40 млн киберпреступников. Если восемь лет назад примерно 97-98 % преступлений совершалось с помощью традиционных средств и только два-три процента - с помощью киберсредств, то сейчас ситуация перевернулась. Примерно полтора процента преступлений - это традиционные преступления - разбои, нападения, мошенничества и так далее, а примерно 98,5 % - это киберпреступность. Ущерб от деятельности хакеров в 2015 году в мире составил 500 миллиардов долларов, более 5 миллиардов долларов из которых, по оценке Сбербанка, приходится на Россию. Официальная оценка потерь рынка в России - 4 миллиарда долларов. Наша экспертная оценка - 5,5 миллиарда долларов за 2015 г., это по России в целом».

По данным ведомственной статистики в 2015 г. закончены расследованием либо разрешены в отчетном периоде уголовные дела о 1096 кражах, совершенных в сфере телекоммуникаций и компьютерной информации, из них только по 753 кражам уголовные дела направлены в суд. При этом количество таких преступлений, уголовные дела о которых приостановлены за нерозыском лиц либо в случае неустановления лиц, было 6283. Соответствующие данные по мошенничеству в сфере телекоммуникаций и компьютерной информации составили 1658, 1350 и 9473 преступлений.

Как представляется, положительные результаты в расследовании хищений денежных средств, совершаемых с использованием компьютерной информации, могут быть достигнуты только при условии совместных и согласованных действий законодателя, органов исполнительной власти, в том числе правоохранительных, организаций банковской и платежных систем, коммерческих компаний, осуществляющих деятельность в сфере информационной безопасности, а также компетентных органов зарубежных государств.

Между тем следователи органов внутренних дел осуществляют свою деятельность в текущих условиях несогласованного банковского, корпоративного и иного законодательства, отсутствия механизмов

взаимодействия с коммерческими структурами и, прежде всего, банками, провайдерами, операторами сотовой связи, отвечающих современным требованиям, нехватки специалистов в сфере компьютерных технологий, способных оказать помощь в расследовании хищений, отсутствия необходимой в достаточном количестве и качестве специальной криминалистической техники (напр., аппаратно-программных комплексов).

Перечисленные и иные объективные обстоятельства затрудняют деятельность следователей органов внутренних дел, осуществляющих досудебное производство по делам о хищениях денежных средств, совершаемых с использованием компьютерных технологий. В то же время, как показало исследование, следователи, специализирующиеся на расследовании обозначенных преступлений, не обладают достаточными профессиональными и специальными знаниями, умениями и навыками в области соответствующей уголовно-процессуальной деятельности.

В связи с этим неслучайно руководством Следственного департамента МВД России уделяется пристальное внимание совершенствованию профессиональной подготовки следователей органов внутренних дел, приобретению и закреплению ими навыков расследования хищений денежных средств с использованием компьютерных технологий, с учетом обозначенных условий. В частности, им было инициировано проведение совместного с Академией управления МВД России исследования проблем организации расследования хищений денежных средств, совершаемых с использованием компьютерных технологий, и подготовка на этой основе учебно-практического пособия.

В ходе работы представителями заказчика были уточнены цель и задачи настоящего пособия. Так, целью работы явилось представление системы научных положений организации расследования хищений денежных средств, совершаемых с использованием компьютерных технологий. Для достижения указанной цели решались следующие задачи: формирование уголовно-правовой и криминалистической характеристики хищений денежных средств, совершаемых с использованием компьютерных технологий; детализация орудий и способов хищений денежных средств, совершаемых с использованием компьютерных технологий; выявление особенностей механизма следообразования хищений денежных средств, совершаемых с использованием компьютерных технологий; разработка общих рекомендаций по отдельным направлениям организации расследования хищений денежных средств, совершаемых с использованием компьютерных технологий, а именно: рассмотрения сообщений о хищениях; предварительного расследования; взаимодействия при расследовании; производства отдельных следственных действий.

Представляется, что настоящее учебно-практическое пособие будет способствовать повышению профессиональной подготовки следователей органов внутренних дел, специализирующихся на расследовании хищений денежных средств, совершаемых с использованием компьютерных технологий, а также станет методическим обеспечением выявления и раскрытия обозначенного вида преступлений сотрудниками оперативных подразделений системы МВД России.

При подготовке пособия использованы данные, полученные в ходе первого этапа научного исследования и отраженные в аналитическом обзоре

результатов деятельности органов предварительного следствия в системе МВД России по организации и осуществлению расследования хищений денежных средств, совершаемых с использованием компьютерных технологий, а также статистические данные ГИАЦ МВД России, информация ОПС территориальных органов МВД России на окружном, региональном и межрегиональном уровнях о результатах их деятельности за 2013-2015 гг., результаты анализа материалов уголовных дел и анкетирования следователей органов внутренних дел, специализирующихся на расследовании преступлений, совершаемых с использованием компьютерных технологий.

В связи с поступившими предложениями от следователей органов внутренних дел авторами настоящей работы предпринята попытка проиллюстрировать наиболее сложный материал схемами, снимками и другими формами наглядного изображения.

Понятие и уголовно-правовая квалификация хищений денежных средств, совершаемых с использованием компьютерных технологий

Под хищением денежных средств, совершаем с использованием компьютерных технологий, для целей настоящей работы можно понимать совершенное с корыстной целью противоправное безвозмездное изъятие и (или) обращение чужих денежных средств, числящихся на банковских и иных счетах, в пользу виновного или других лиц путем применения средств хранения, обработки и (или) передачи компьютерной информации, причинившее ущерб их собственнику или иному владельцу.

Ранее отмечалось, что должностные лица ОПС при расследовании хищений денежных средств, совершаемых с использованием компьютерных технологий, испытывают трудности в вопросах квалификации данных преступных деяний, что предопределено отсутствием судебно-следственной практики и соответствующих официальных разъяснений Верховного Суда Российской Федерации6, Генеральной прокуратуры Российской Федерации. Данные обстоятельства актуализируют рассмотрение вопросов квалификации данных видов хищений, знание о которых позволят не допускать ошибок по уголовным делам, а в необходимых случаях аргументировано отстаивать позицию в общении с надзирающим прокурором.

Перечень хищений денежных средств, совершаемых с использованием компьютерных технологий, включает: кражу (ст. 158 УК), мошенничество с использованием платежных карт (ст. 159.3 УК), мошенничество в сфере компьютерной информации (ст. 159.6 УК), присвоение и растрату (ст. 160 УК).

Как кражу (ст. 158 УК) следует квалифицировать действия лица, совершившего незаконное изъятие денежных средств с банковского счета путем использования банковской карты, вредоносных программ (кодов) и других средств в тайне от потерпевшего или иных лиц (например, представителей кредитной организации).

Мошенничество с использованием платежных карт (ст. 159.3 УК) предполагает хищение денежных средств, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или

иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации.

Анализ материалов уголовных дел по вопросам привлечения лиц к ответственности за совершение мошенничества с использованием платежных карт (ст. 159.3 УК) позволяет сделать вывод об отсутствии в настоящее время единства судебной практики при квалификации соответствующих деяний.

Сравнительный анализ состоявшихся приговоров показывает, что в отсутствие сформированной судебной практики преступные действия лиц, совершенные в однотипных ситуациях, получают в судах различную оценку. Данное обстоятельство со всей очевидностью свидетельствует о необходимости скорейшей выработки Верховным Судом Российской Федерации единой правовой позиции и доведения ее до судей и следователей.

Обман, традиционно используемый при совершении любого мошенничества, понимается в двух аспектах - активный, когда лицу сообщаются заведомо ложные, несоответствующие действительности сведения, и пассивный обман - в умолчании об истине, в несообщении юридически значимых фактов. При совершении мошенничества с использованием платежных карт обман направлен в адрес уполномоченного работника кредитной торговой или иной организации, то есть лица, на которое в установленном порядке (в соответствие с законом или договором) официально возложены обязанности по осуществлению деятельности, связанной с консультированием, приемом платежей и передачей товаров, выдачей наличных денежных средств и т. п.

Рассматриваемый признак хищений - обман уполномоченного работника является разграничительным признаком данного состава преступления от кражи, совершенной с использованием платежной карты. Так, в случае снятия денег через банкомат без участия работника кредитной или торговой организации действия виновного лица квалифицируются по ст. 158 УК, а в случае приобретения товаров в магазинах с использованием чужой банковской карты, то есть при участии работника торговой организации - по ст. 159.3 УК (см.: п. 13 Постановления № 51).

Особым средством, используя которое виновное лицо совершает изъятие или обращение денежных средств в свою пользу или в пользу третьих лиц, выступают кредитные, расчетные или иные платежные карты.

Расчетная (дебетовая) карта как электронное средство платежа используется для совершения операций ее держателем в пределах расходного лимита - суммы денежных средств клиента, находящихся на его банковском счете, и (или) кредита, предоставляемого кредитной организацией-эмитентом клиенту при недостаточности или отсутствии на банковском счете денежных средств (овердрафт).

Кредитная карта как электронное средство платежа используется для совершения ее держателем операций за счет денежных средств, предоставленных кредитной организацией-эмитентом клиенту в пределах расходного лимита в соответствии с условиями кредитного договора.

К иным платежным картам относятся, например, предоплаченные карты, представляющие собой электронное средство платежа, используемое для осуществления перевода электронных денежных средств, возврата остатка электронных денежных средств в пределах суммы предварительно

предоставленных держателем денежных средств кредитной организацией-эмитентом в соответствии с требованиями Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе».

Данные средства (платежные карты) мошенничества должны быть либо поддельными, либо принадлежащими другому лицу. Поддельными признаются платежные карты, которые подделаны частично либо полностью. Характер, способ, качество, количество поддельных платежных карт влияния на квалификацию не оказывают.

Изготовление поддельной платежной карты в целях дальнейшего хищения денежных средств, принадлежащих другому лицу, квалифицируется как приготовление к мошенничеству с использованием платежных карт по ч. 3 ст. 30 и ст. 159.3 УК и дополнительной квалификации по ст. 187 УК не требует. Вменение последней статьи необходимо лишь в том случае, если виновный изготовил поддельную кредитную либо расчетную карту с целью последующего ее сбыта.

Принадлежащей другому лицу является чужая платежная карта, на которую у лица, ею завладевшего, нет ни реального, ни предполагаемого права. При этом законный владелец карты не предоставлял виновному никаких полномочий по пользованию данным средством платежа. В руки мошенника карта могла попасть любым способом (в результате хищения, вследствие находки и т. д.).

При квалификации анализируемого преступного деяния необходимо иметь в виду, что платежные карты могут не выбывать из владения держателя. Имея доступ к конфиденциальным сведениям об электронных средствах платежа, преступники, используя удаленный доступ, могут осуществить перевод различных денежных сумм на собственные счета или счета соучастников. Но и в этом случае хищение должно сопровождаться обманом уполномоченного работника кредитной, торговой или иной организации. В противном случае действия виновных лиц следует квалифицировать как кражу (ст. 158 УК РФ). Например, в производстве СУ УТ МВД России по Приволжскому федеральному округу находилось уголовное дело № 351579, возбужденное по признакам преступления, предусмотренного ст. 159.3 УК РФ. Следствием установлено, что А.В. Ефименко совершил хищение со счетов граждан денежных средств путем оформления и оплаты без их ведома электронных железнодорожных билетов, которые впоследствии предъявлялись к возврату с получением наличных денежных средств. Ефименко привлечен к уголовной ответственности по 5 эпизодам преступлений, предусмотренных п. «в» ч. 2 ст. 158 УК РФ, осужден к исправительным работам на срок 1 год 6 мес.

Как мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) квалифицируется безвозмездное, с корыстной целью обращение лицом в свою пользу или в пользу других лиц денежных средств, совершенное с использованием компьютерных технологий, путем обмана или злоупотребления доверием (например, путем представления в кредитную организацию поддельных платежных распоряжений), сопряженного с вводом, удалением, блокированием, модификаций компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (напр., системы ДБО).

Анализ материалов уголовных дел позволяет сделать вывод об отсутствии в настоящее время единства следственной и судебной практики при квалификации деяний, сопряженных с мошенничеством в сфере компьютерной информации. Сходные по своему составу деяния квалифицируются, в одних случаях, как мошенничество в сфере компьютерной информации (ст. 159.6 УК), а в других - как кража (ст. 158 УК) и неправомерный доступ к компьютерной информации (ст. 272 УК) в совокупности. Такое толкование норм уголовного закона является недопустимым, препятствует выработке единой следственной и судебной практики по вопросу привлечения к уголовной ответственности за совершение хищений денежных средств с использованием компьютерных технологий и должно быть устранено, на что обращается внимание исследователями10.

Так, 4 января 2015 г. в период с 20 часов 47 минут до 21 часа 07 минут В.А. Эктов, заведомо зная, что к находящемуся в его пользовании абонентскому номеру XXX-XXX-XX-XX подключена услуга «Мобильный банк» и «Автоплатеж», с помощью которого он может осуществить доступ к лицевому счету, открытому в ОАО «Сбербанк России» на имя П.В. Цыкунова, путем вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации, формировал SMS-сообщения специального формата, представленные в форме электрических сигналов, для перевода денежных средств в сумме 10000 руб. Данные SMS-сообщения путем ввода отправлял на короткий номер «900» с командой о перечислении денежных средств со счета потерпевшего на счет своего абонентского номера ОАО «Мегафон», чем причинил ему значительный материальный ущерб.

В подобного рода случаях преступники используют случайно оказывавшийся в их распоряжении доступ к лицевому счету лица, на чье имя ранее был зарегистрирован абонентский номер телефона и который продолжительное время им не пользовался. После перерегистрации этого номера преступник получает информацию о движении денежных средств по лицевому счету первоначального пользователя абонентским номером по SMS-сообщениям «Мобильного банка», а также возможность распоряжаться этими средствами.

Как отмечают руководители ОПС, до первой половины 2014 г. вопрос квалификации таких преступных действий оставался до конца неурегулированным и зависел от позиции надзирающих прокуроров, а также судей, усматривавших в содеянном либо совокупность преступлений, предусмотренных ст. 158, 272 либо 159.6 УК РФ11. Например, по одному из уголовных дел следствием установлено, что в период с 7 по 16 мая 2013 г. Ковалева, воспользовавшись услугой «Мобильный банк», подключенной потерпевшим Поляковым, 28 ноября 2008 г. при оформлении последним банковской карты ОАО «Сбербанк России», похитила посредством направления SMS-сообщений на специальный номер «900» принадлежащие потерпевшему денежные средства в сумме 5400 руб., переведя их на принадлежащий своему мужу счёт банковской карты ЗАО «ВТБ24», а также на свой счёт, находящийся в пользовании.

После согласования с надзирающим прокурором по данному факту следователем СО МО МВД России «Железногорский» Курской области возбуждены уголовные дела по признакам преступлений, предусмотренных п. «в» ч. 2 ст. 158 и ч. 2 ст. 272 УК РФ соответственно, которые впоследствии соединены в одно производство и по итогам расследования направлены в суд.

Судебная инстанция в полном объёме согласилась с обвинительной позицией ОПС и назначила наказание Ковалевой по совокупности преступлений в виде одного года трёх месяцев исправительных работ по основному месту работы с удержанием 5 % заработной платы ежемесячно в доход государства.

В то же время по другому уголовном делу, когда следствием было установлено, что в период с 22 ч. 00 мин. 5 октября 2013 г. до 23 ч. 55 мин. 6 октября 2013 г. Смецкой посредством SIM-карты, ранее принадлежащей потерпевшему Кондрашову, посредством услуги «Мобильный банк», которая также ранее была подключена последним при оформлении им банковской карты ОАО «Сбербанк России», похитил с его лицевого счёта денежные средства в сумме 10 000 рублей, надзирающий прокурор Железнодорожного административного округа г. Курска занял позицию, что данное деяние содержит признаки состава преступления, предусмотренного ч. 2 ст. 159.6 УК РФ. Данное уголовное дело также успешно прошло судебную инстанцию.

В настоящее время после того, как данный проблемный вопрос освещён в обзоре «О мониторинге практики применения ст. ст. 159.1-159.6 УК РФ», подготовленном сотрудниками Следственного департамента МВД России, судебно-следственная практика по указанным преступно-наказуемым деяниям приобрела единообразный вид, а именно: действия по уничтожению, блокированию и модификации компьютерной информации, если они совершены с целью хищения чужого имущества, квалифицируются по ст. 159.6 УК РФ, что, по мнению авторов настоящей работы, является неправильным по вышеуказанным обстоятельствам.

В связи с этим следует поддержать руководство СУ УМВД России по Владимирской области, инициировавшее оперативное совещание, на котором обсудили практику возбуждения уголовных дел СО МВД России «Ковровский» в августе 2015 г. по фактам хищения денежных средств с банковских счетов граждан посредством незаконного использования услуги «Мобильный банк». Руководствуясь указаниями надзирающего прокурора, на территории Ковровского района Владимирской области данные уголовные дела были возбуждены по признакам преступлений, предусмотренных ст. 159.6 УК РФ. Участники совещания пришли к выводу, что такие хищения следует квалифицировать по признакам преступлений, предусмотренных ст. 158 УК РФ.

По нашему мнению, деяние не образует состава мошенничества в сфере компьютерной информации, если перечисление чужих денежных средств с использованием компьютерных технологий на другой банковский счет совершено без участия уполномоченного работника кредитной организации. В этом случае содеянное следует квалифицировать по соответствующей части ст. 158 УК РФ.

Хищение чужих денежных средств, находящихся на счетах в кредитной организации, путем использования компьютерных технологий, следует квалифицировать как мошенничество в сфере компьютерной информации только в тех случаях, когда лицо путем обмана или злоупотребления доверием ввело в заблуждение уполномоченного работника кредитной организации (напр., в случаях подтверждения уполномоченному работнику кредитной организации платежа по якобы подлинному платежному распоряжению).

В отличие от кражи, мошенничество в сфере компьютерной информации совершается путем обмана или злоупотребления доверием, под воздействием которых владелец денежных средств (клиент кредитной организации, потерпевший) или иное лицо (уполномоченный представитель кредитной организации) не препятствует их изъятию путем перечисления на счета других лиц с использованием компьютерных технологий. При этом обман как способ совершения хищения денежных средств с использованием компьютерных технологий, ответственность за которое предусмотрено ст. 159.6 УК РФ, может состоять в сознательном сообщении заведомо ложных, не соответствующих действительности сведений (например, подтверждает якобы совершенный владельцем счета платеж и т. п.) либо в умышленных действиях (например, электронное или телефонное подтверждение о якобы подписанном платежном распоряжении), направленных на введение клиента кредитной организации или представителя самой кредитной организации в заблуждение.

Справедливости ради отметим, что ранее Верховный Суд Российской Федерации в пояснительной записке разъяснил, что преступление, предусмотренное данной статьей, не совершается классическими для любого мошенничества способами - обман или злоупотребление доверием. Субъект лишь получает доступ к соответствующим сведениям, что в результате приводит к хищению чужого имущества или приобретению права на чужое имущество. Между тем специалисты полагают, что «поскольку в диспозиции ст. 159.6 УК РФ заимствуется термин «мошенничество», то это дает полное основание для вывода о необходимости установления факта обмана или злоупотребления доверием при совершении рассматриваемого преступления, поскольку оно, как и все предшествующие, закрепляет специальный состав, основывающийся на «материнском» составе мошенничества, и соответствует ему по набору характерных признаков. С другой стороны, указанные доводы можно признать надуманными, исходя из того, что законодатель не предусмотрел обман или злоупотребление доверием в качестве признака мошенничества в сфере компьютерной информации. В этом случае сомнителен сам факт отнесения рассматриваемого преступления к мошенничеству».

Способы мошенничества выражены в совершении различных операций с компьютерной информацией, а именно: ввод компьютерной информации; удаление компьютерной информации; блокирование компьютерной информации; модификация компьютерной информации;

иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

При совершении рассматриваемого преступления виновное лицо может совершить одно действие, образующее объективную сторону, либо выполнить несколько указанных действий.

Как присвоение или растрата (ст. 160 УК РФ) квалифицируется противоправное безвозмездное обращение денежных средств с использованием компьютерных технологий, вверенных лицу в силу должностного или иного служебного положения (напр., лицо, имеющее право подписи электронных платежных распоряжений), в свою пользу или пользу других лиц, причинившее ущерб потерпевшему или кредитной организации.

Хищение денежных средств с использованием компьютерных технологий путем присвоения состоит в безвозмездном, совершенном с корыстной целью, противоправном обращении преступником вверенных ему полномочий по управлению чужими денежными средствами посредством уполномочия его подписывать электронные платежные распоряжения в свою пользу против воли потерпевшего. Хищение путем растраты должно квалифицироваться как противоправные действия лица, которое в корыстных целях истратило вверенные ему денежные средства против воли собственника путем их расходования или передачи другим лицам с использованием компьютерных технологий.

Решая вопрос об отграничении составов присвоения или растраты от кражи, должностные лица ОПС должны установить наличие у преступника вышеуказанных полномочий. Совершение тайного хищения денежных средств с банковских счетов лицом, не обладающим такими полномочиями, но имеющим доступ к компьютеру, подключенному к системе ДБО, в силу выполняемой работы или иных обстоятельств, должно быть квалифицировано по ст. 158 УК РФ.

Отметим, что последующая реализация прав, удостоверенных похищенными денежными средствами, в том числе путем обналичивания, перечисления на другие банковские счета, осуществление расчета от своего имени или от имени третьих лиц, не снимая денежных средств со счета и т. п., представляет собой распоряжение данными средствами и не требует дополнительной квалификации как кража, мошенничество в сфере компьютерной информации, присвоение или растрата.

От хищения следует отличать случаи, когда лицо, изымая и (или) обращая в свою пользу или пользу других лиц чужие денежные средства с использованием компьютерных технологий, действовало в целях осуществления своего действительного или предполагаемого права на эти средства (например, если лицо, обладающее единственной (первой) подписью платежных распоряжений, в целях обеспечения возмещения задолженности по заработной плате перечислило денежные средства со счета нанимателя - юридического лица на свой собственный счет). При наличии оснований, предусмотренных ст. 330 УК РФ, виновное лицо в указанных случаях должно быть привлечено к уголовной ответственности за самоуправство.

Предметом рассматриваемого вида, хищения являются безналичные денежные средства, находящиеся на банковских и иных счетах. Справедливости ради отметим, что в литературе встречается иное толкование предмета преступления. Так, П.С. Яни свыше полутора десятилетий назад, рассматривая конкретное дело по неправомерному завладению безналичными деньгами, писал: «Когда гражданин Егунов положил 1000 рублей на свой счет в банке, он в соответствии с гражданским законодательством перестал быть их собственником. «Хозяином» этих денег стал банк, который вправе совершать с ними различные предусмотренные банковским законодательством операции. Однако обратим внимание на кавычки. Они означают, что ввиду отсутствия наличных средств (вместо них имеются лишь записи на счетах) в отношении денег у всех, кто оперирует ими, возникают лишь права требования, которые и переходят от банка к другой стороне в кредитном договоре, и т. д. И поскольку безналичные деньги - это не вещь, которую можно похитить, а право требования, то

похитить их нельзя». Другой автор полагает, что предметом хищений в данном случае выступают имущественные права.

При решении вопроса о виновности лиц в совершении хищения денежных средств с использованием компьютерных технологий, следователь должен иметь в виду, что обязательным признаком любого хищения является наличие у лица корыстной цели, то есть стремление изъять и (или) обратить чужие денежные средства в свою пользу либо распорядиться ими как своими собственными, в том числе путем передачи их в обладание других лиц.

В соответствии с ч. 2 ст. 35 УК РФ кража, мошенничество в сфере компьютерной информации, присвоение или растрата считаются совершенными группой лиц по предварительному сговору (ч. 2 ст. 158, 159.6 и 160 УК) при условии, что в этих преступлениях участвовали два и более лица, заранее договорившиеся о совместном их совершении. Данный квалифицирующий признак имеет место и в тех случаях, когда согласно предварительной договоренности между соучастниками непосредственное изъятие денежных средств осуществляет один из них.

При квалификации действий виновных как хищения денежных средств с использованием компьютерных технологий группой лиц по предварительному сговору, должностным лицам ОПС необходимо установить: имел ли место такой сговор соучастников до начала действий, непосредственно направленных на хищение, состоялась ли договоренность о распределении ролей в целях осуществления преступного умысла, а также какие конкретно действия совершены каждым исполнителем и другими соучастниками преступления. В обвинительном заключении надлежит оценить доказательства, подтверждающие вину каждого из исполнителей и иных (организаторов, подстрекателей, пособников).

Действия лица, непосредственно не участвовавшего в хищении денежных средств с использованием компьютерных технологий, но содействовавшего совершению этого преступления советами, указаниями либо заранее обещавшего скрыть следы преступления, устранить препятствия, не связанные с оказанием помощи непосредственным исполнителям преступления, и т. п., надлежит квалифицировать как соучастие в содеянном в форме пособничества со ссылкой на ч. 5 ст. 33 УК РФ.

Кража (ч. 2 ст. 158 УК РФ), мошенничество с использованием платежных карт (ст. 159.3 УК РФ), мошенничество в сфере компьютерной информации (ч. 2 ст. 159.6 УК РФ), присвоение или растрата (ч. 2 ст. 160 УК РФ) по признаку причинения значительного ущерба гражданину, могут быть квалифицированы как оконченные преступления только в случае реального причинения значительного имущественного ущерба, который в соответствии с прим. 2 к ст. 158 УК РФ определяется с учетом его имущественного положения (наличие у него источника доходов, их размер и периодичность поступления, наличие у потерпевшего иждивенцев, совокупный доход членов семьи, с которыми он ведет совместное хозяйство и т.п.), но не может составлять менее двух тысяч пятисот рублей. Мнение потерпевшего о значительности или незначительности ущерба, причиненного ему в результате хищения, должно оцениваться следователем в совокупности с материалами дела, подтверждающими сумму похищенных денежных средств и имущественное положение потерпевшего.

Вопрос о наличии в действиях виновных квалифицирующего признака совершения мошенничества в сфере компьютерной информации в крупном или особо крупном размере (ч.ч. 3 ст. 159.3 и ст. 159.6 УК РФ) должен решаться в соответствии с прим. к ст. 159.1 УК РФ. Как мошенничество с использованием платежных карт или мошенничество в сфере компьютерной информации в крупном размере должно квалифицироваться совершение нескольких хищений денежных средств общим размером свыше одного миллиона пятисот тысяч рублей, а особо крупном - шесть миллионов рублей, если эти хищения совершены одним способом и при обстоятельствах, свидетельствующих об умысле совершить хищение в крупном или особо крупном размерах. Аналогичным образом должен решаться вопрос о наличии в действиях виновных квалифицирующего признака совершения кражи (ч. 3 ст. 158 УК РФ), присвоения или растраты (ч. 3 ст. 160 УК РФ) денежных средств с использованием компьютерных технологий с условием применения прим. 4 к ст. 158 УК РФ, из смысла которого крупным размером в ст. 158 и ст. 160 УК РФ признается ущерб в сумме, превышающий двести пятьдесят тысяч рублей, а особо крупным - один миллион рублей.

Квалифицировать кражу, мошенничество с использованием платежных карт, мошенничество в сфере компьютерной информации, присвоение или растрату как совершаемые организованной группой (ч.ч. 4 ст.ст. 158, 159.3, 159.6 и 160 УК РФ) возможно в случаях, когда такая группа лиц, в силу ч. 3 ст. 35 УК РФ, характеризуется признаком устойчивости, заранее объединилась для совершения одного или нескольких преступлений. Организованная группа отличается наличием в ее составе организатора (руководителя), стабильностью состава участников группы, заранее разработанного плана совместной преступной деятельности, распределением функций между членами группы при подготовке к совершению преступления и осуществлении преступного умысла.

Об устойчивости организованной группы может свидетельствовать не только большой временной промежуток ее существования, неоднократность совершения преступлений членами группы, но и их техническая оснащенность, длительность подготовки даже одного преступления, а также иные обстоятельства (например, специальные знания и навыки участников организованной группы в области создания вредоносных программ и т. п.).

При признании хищений денежных средств с использованием компьютерных технологий, совершенных организованной группой, действия всех соучастников независимо от их роли в содеянном подлежат квалификации как соисполнительство без ссылки на ст. 33 УК РФ.

В случае, если лицо подстрекало другое лицо или группу лиц к созданию организованной группы для совершения конкретных хищений денежных средств с использованием компьютерных технологий, но не принимало непосредственного участия в подборе ее участников, планировании и подготовке к совершению преступлений (преступления) либо в их осуществлении, то его действия следует квалифицировать как соучастие в совершении организованной группой преступлений со ссылкой нач. 4 ст. 33 УК РФ.

В организованную группу могут входить лица, не обладающие полномочиями по распоряжению, управлению или пользованию вверенными денежными средствами, которые заранее объединились для совершения одного или

нескольких преступлений. При наличии к тому оснований они несут ответственность согласно ч. 4 ст. 34 УК РФ как организаторы, подстрекатели либо пособники присвоения. Организаторы и руководители несут ответственность за все совершенные организованной группой преступления, если они охватывались их умыслом. Другие члены организованной группы привлекаются к ответственности за преступления, в подготовке или совершении которых они участвовали (ст. 35 УК РФ).

Под лицами, использующими свое служебное положение (ч. 3 ст. 159.3, 159.3 и 160 УК РФ), следует понимать должностных лиц, обладающих признаками, предусмотренными прим. 1 к ст. 285 УК РФ, а также иных лиц, отвечающих требованиям, предусмотренным прим. 1 к ст. 201 УК РФ (например, лиц, использующих для совершения хищения чужого имущества свои служебные полномочия, включающие организационно-распорядительные или административно-хозяйственные обязанности в коммерческой организации).

Обозначенный признак отсутствует в случае присвоения или растраты принадлежащих физическому лицу (в том числе индивидуальному предпринимателю без образования юридического лица) денежных средств, которые были вверены им другому физическому лицу на основании гражданско-правовых договоров или трудового договора. Указанные действия охватываются ч. 1 ст. 160 УК РФ, если в содеянном не содержатся иные квалифицирующие признаки, предусмотренные этой статьей.

Исполнителем присвоения денежных средств с использованием компьютерных технологий может являться только лицо, которому денежные средства были вверены потерпевшим на законном основании с определенной целью (например, осуществлять операции по счету и т. п.). Исходя из положений ч. 4 ст. 34 УК РФ, лица, не обладающие указанными признаками специального субъекта присвоения, но непосредственно участвовавшие в хищении денежных средств согласно предварительной договоренности с лицом, которому эти средства вверены, должны нести уголовную ответственность по ст. 33 и ст. 160 УК РФ в качестве организаторов, подстрекателей или пособников.

Хищение, совершенное с использованием компьютерных технологий путем подделки самим преступником платежного распоряжения, квалифицируется как совокупность преступлений, предусмотренных в зависимости от обстоятельств конкретного дела соответствующей частью ст. 187, а также соответствующими частями ст. 158 или 159.3, или 159.6, или 160 УК РФ, а если по не зависящим от него обстоятельствам преступник не смог изъять денежные средства, содеянное следует квалифицировать соответствующей частью ст. 187, а также ч. 3 ст. 30 УК РФ и соответствующей частью ст. 158 или 159.3, 159.6, 160 УК РФ.

В случаях, когда кража денежных средств с использованием компьютерных технологий повлекла уничтожение, блокирование, модификацию или копирование компьютерной информации, а также деяние было связанно с созданием, распространением и использованием компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (вредоносной программ), содеянное подлежит

квалификации по соответствующей части ст. 158 УК РФ, а также, в зависимости от обстоятельств дела, по ст. 272 или 273 УК РФ.

Хищения денежных средств путем мошенничества в сфере компьютерной информации, т. е. путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, сопряженные с созданием и распространение вредоносных программ для компьютера, следует квалифицировать по ст. 159.6 и 273 УК РФ. В данном случае дополнительной квалификации по ст. 272 УК РФ не требуется, так как неправомерный доступ к компьютерной информации, повлекший уничтожение, блокировку, модификацию или копирование компьютерной информации, полностью охватывается составом мошенничеством в сфере компьютерной информации.

Модификацию компьютерной информации - подделку (фальсификация) электронного платежного распоряжения для использования в целях совершения этим же лицом преступлений, предусмотренных ст. 158, 159.6 или 160 УК РФ, следует квалифицировать как приготовление к соответствующему виду хищения.

По общему правилу кража, мошенничество с использованием платежной карты и мошенничество в сфере компьютерной информации считаются оконченными, если имущество изъято и виновный имеет реальную возможность им пользоваться или распоряжаться по своему усмотрению (например, обратить похищенное имущество в свою пользу или в пользу других лиц, распорядиться им с корыстной целью иным образом). Данная позиция была подтверждена Пленумом Верховного Суда Российской Федерации, который в одном из своих постановлений разъяснил, что исходя из положений ст. 140 ГК РФ, мошенничество следует считать оконченным с момента зачисления денег на банковский счет виновного, либо на счета других лиц, т.е. когда получена реальная возможность распоряжаться поступившими денежными средствами по своему усмотрению16. Можно предположить, что данная рекомендация также обусловлена положениями действующего законодательства, согласно которому на наличные и безналичные денежные средства распространяется правовой режим вещей (ст. 128 ГК РФ).

Отметим, что указанная позиция Пленума Верховного Суда Российской Федерации находит поддержку в научной литературе.

Несмотря на данную позицию Пленума Верховного Суда Российской Федерации, при расследовании хищений денежных средств, совершенных с использованием компьютерных технологий, у следователей возникают проблемы (например, определение места возбуждения уголовного дела и т. п.). В связи с этим ранее одним из авторов настоящей работы рассматривался данный вопрос, по результатам которого были сделаны следующие выводы.

С одной стороны, момент окончания хищений (краж и мошенничеств), совершенных с использованием компьютерных технологий, не связан с переходом права собственности на похищенные денежные средства, а значит не может быть обусловлен зачислением денежных средств на банковский счет получателя средств. По отношению к похищенным и зачисленным по подложному платежному распоряжению на счета денежным средствам у преступника имеется право требовать их выдачи наличными или

перечисления на другие счета. С другой стороны, право распоряжения денежными средствами, находящимися на банковском счете, преступник реализует в момент выполнения кредитной организацией операции по поддельному платежному распоряжению (с момента наступления безотзывности перевода денежных средств). Именно в данный момент происходит фактическое изъятие и обращение чужих денежных средств в пользу преступника или другого лица. Преступник реализовал появившееся у него в результате хищения безналичных денежных средств право их требовать в момент наступления безотзывности перевода. Дальнейшее движение похищенных денежных средств происходит по воле преступника, использующего банковское законодательство и банковские правила, что свидетельствует о реализации им возможности распоряжаться похищенными денежными средствами.

Таким образом предлагалось рекомендации Пленума Верховного Суда Российской Федерации относительно момента окончания мошенничества изменить, отразив в них следующую позицию: кражу или мошенничество с использованием электронных средств платежа следует считать оконченными с момента принятия кредитной организацией подложного платежного распоряжения об осуществлении перевода чужих денежных средств при отсутствии или прекращении возможности его отзыва (момента списания денежных средств с банковского счета).

Анализ практики расследования хищений денежных средств, совершаемых с использованием компьютерных технологий, свидетельствует, что все чаще следователи сталкиваются с ситуацией необходимости квалификации таких деяний по ст. 210 УК РФ. При этом особенностью такой ситуации является то, что создание преступного сообщества (преступной организации) или участие в нем (ней) носит так называемый виртуальный характер, т. е. участники, в том числе руководители таких сообществ общались между собой только посредством электронных средств связи.

Для правильной квалификации совершенных хищений с использованием компьютерных технологий по ст. 210 УК РФ необходимо установить следующие признаки19:

1. Устойчивость, о которой могут свидетельствовать в частности такие признаки, как стабильность ее состава, тесная взаимосвязь между ее членами, согласованность их действий, постоянство форм и методов преступной деятельности, распределение функций между ее членами, длительность ее существования, количество совершенных преступлений, тщательная подготовка к их совершению, постоянный, плановый, конспиративный характер деятельности в виде преступного промысла.

Об устойчивости организованной группы может свидетельствовать не только большой временной промежуток ее существования, неоднократность совершения преступлений членами группы, но и их техническая оснащенность, длительность подготовки даже одного преступления, а также иные обстоятельства (например, специальная подготовка участников организованной группы к проникновению в хранилище для изъятия денег (валюты) или других материальных ценностей)20.

Обобщая теоретические представления и материалы судебной практики, можно прийти к выводу, что признак устойчивости означает внутреннюю

упорядоченность, согласованность и взаимодействие составных частей системы.

Он предполагает широкий комплекс признаков: определение целей совместной деятельности; планирование преступных акций; иерархическую структуру и распределение ролей между соучастниками; внутреннюю дисциплину с беспрекословным подчинением по вертикали; систему обеспечения орудиями и средствами совершения преступления; специализацию функций соучастников и самого сообщества; круговую поруку и конспирацию; отработанные схемы «отмывания» денег, полученных преступным путем, и их вложения в различные проекты; создание системы противодействия различным мерам социального контроля, включая обеспечение безопасности сообщества и установление связей с коррумпированными лицами государственного аппарата, и т. п.

2. Структурированность (данный признак заменил ранее характеризовавший преступное сообщество признак сплоченности) и единое руководство, т. е. наличие разветвленных управленческих, организационных, финансовых связей внутри самого сообщества, единой идеологии, многоуровневости в управлении, распределения функций среди структурных подразделений преступного сообщества (преступной организации); наличие кодекса поведения и ответственности за его нарушение; наличие механизма поддержания внутренней дисциплины, в том числе, с применением насилия, угроз и т .п.; наличие определенной суммы денежных средств, находящихся в общем распоряжении.

Без установления данных признаков нельзя квалифицировать хищения денежных средств, с использованием компьютерных технологий, как совершенные преступным сообществом. Количественный признак - наличие двух или более лиц - не может служить основанием для признания в действиях лиц преступного сообщества, даже при условии совершения ими тяжких или особо тяжких преступлений.

В п. 3 постановления Пленума Верховного Суда Российской Федерации от 10 июня 2010 г. № 12 «О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней)» отмечается, что преступное сообщество (преступная организация) может осуществлять свою преступную деятельность либо в форме структурированной организованной группы, либо в форме объединения организованных групп, действующих под единым руководством. При этом закон не устанавливает каких-либо правовых различий между понятиями «преступное сообщество» и «преступная организация».

Под структурированной организованной группой следует понимать группу лиц, заранее объединившихся для совершения одного или нескольких тяжких либо особо тяжких преступлений, состоящую из подразделений (подгрупп, звеньев и т. п.), характеризующихся стабильностью состава и согласованностью своих действий. Структурированной организованной группе, кроме единого руководства, присущи взаимодействие различных ее подразделений в целях реализации общих преступных намерений, распределение между ними функций, наличие возможной специализации в выполнении конкретных действий при совершении преступления и другие формы обеспечения деятельности преступного сообщества (преступной организации).

Под структурным подразделением преступного сообщества (преступной организации) следует понимать функционально и (или) территориально обособленную группу, состоящую из двух или более лиц (включая руководителя этой группы), которая в рамках и в соответствии с целями преступного сообщества (преступной организации) осуществляет преступную деятельность. Такие структурные подразделения, объединенные для решения общих задач преступного сообщества (преступной организации), могут не только совершать отдельные преступления (дачу взятки, подделку документов и т.п.), но и выполнять иные задачи, направленные на обеспечение функционирования преступного сообщества (преступной организации).

Следовательно, отсутствие в группе структурных подразделений дает основание сделать вывод об отсутствии преступного сообщества (преступной организации).

Объединение организованных групп предполагает наличие единого руководства и устойчивых связей между самостоятельно действующими организованными группами, совместное планирование и участие в совершении одного или нескольких тяжких или особо тяжких преступлений, совместное выполнение иных действий, связанных с функционированием такого объединения.

3. Цель преступного сообщества (преступной организации) -совершение одного или нескольких тяжких либо особо тяжких преступлений для получения прямо или косвенно финансовой или иной материальной выгоды.

Наличие специальной цели позволяет характеризовать деяние, предусмотренное ст. 210 УК РФ, как совершаемое с прямым умыслом.

При этом под прямым получением финансовой или иной материальной выгоды понимается совершение одного или нескольких тяжких либо особо тяжких преступлений (например, мошенничества в сфере компьютерной информации, совершенного организованной группой либо в особо крупном размере), в результате которых осуществляется непосредственное противоправное обращение в пользу членов преступного сообщества (преступной организации) денежных средств.

Под косвенным получением финансовой или иной материальной выгоды понимается совершение одного или нескольких тяжких либо особо тяжких преступлений, которые непосредственно не посягают на чужое имущество, однако обусловливают в дальнейшем получение денежных средств и прав на имущество или иной имущественной выгоды не только членами сообщества (организации), но и другими лицами.

4. Под созданием преступного сообщества понимаются действия, направленные на вербовку, вовлечение, приискание соучастников, четкое распределение ролей, то есть направлений деятельности и функциональных обязанностей, обеспечение иных условий совершения тяжких или особо тяжких преступлений.

5. Под руководством преступным сообществом (преступной организацией) или входящими в него (нее) структурными подразделениями следует понимать осуществление организационных и (или) управленческих функций в отношении преступного сообщества (преступной организации), его (ее) структурных подразделений, а также отдельных его (ее) участников как при

совершении конкретных преступлений, так и при обеспечении деятельности преступного сообщества (преступной организации).

Такое руководство может выражаться, в частности, в определении целей, в разработке общих планов деятельности преступного сообщества (преступной организации), в подготовке к совершению конкретных тяжких или особо тяжких преступлений, в совершении иных действий, направленных на достижение целей, поставленных преступным сообществом (преступной организацией) и входящими в его (ее) структуру подразделениями при их создании (например, в распределении ролей между членами сообщества, в организации материально-технического обеспечения, в разработке способов совершения и сокрытия совершенных преступлений, в принятии мер безопасности в отношении членов преступного сообщества, в конспирации и в распределении средств, полученных от преступной деятельности).

К функциям руководителя преступного сообщества (преступной организации) следует также относить принятие решений и дачу соответствующих указаний участникам преступного сообщества (преступной организации) по вопросам, связанным с распределением доходов, полученных от преступной деятельности, с легализацией (отмыванием) денежных средств, добытых преступным путем, с вербовкой новых участников, с внедрением членов преступного сообщества (преступной организации) в государственные (в том числе правоохранительные) органы.

Руководство преступным сообществом (преступной организацией) может осуществляться как единолично руководителем преступного сообщества (преступной организации), так и двумя и более лицами, объединившимися для совместного руководства (например, руководителем преступного сообщества (преступной организации), руководителем структурного подразделения, руководителем (лидером) организованной группы).

6. Под координацией преступных действий следует понимать их согласование между несколькими организованными группами, входящими в преступное сообщество (преступную организацию), в целях совместного совершения запланированных преступлений.

7. Под созданием устойчивых связей между различными самостоятельно действующими организованными группами следует понимать, например, действия лица по объединению таких групп в целях осуществления совместных действий по планированию, совершению одного или нескольких тяжких или особо тяжких преступлений.

Ответственность по ч. 1 ст. 210 УК РФ за координацию преступных действий, создание устойчивых связей между различными самостоятельно действующими организованными группами, разработку планов и создание условий для совершения преступлений такими группами или раздел сфер преступного влияния и преступных доходов между ними, совершенные лицом с использованием своего влияния на участников организованных групп, наступает с момента фактического установления контактов и взаимодействия в целях совершения указанных преступных действий.

8. Под участием в преступном сообществе (преступной организации) - ч. 2 ст. 210 УК РФ следует понимать вхождение в состав преступного сообщества (преступной организации), а также разработку планов по подготовке к совершению одного или нескольких тяжких или особо тяжких преступлений и

(или) непосредственное совершение указанных преступлений либо выполнение лицом функциональных обязанностей по обеспечению деятельности такого сообщества (финансирование, снабжение информацией, ведение документации, подыскание жертв преступлений, установление в целях совершения преступных действий контактов с должностными лицами государственных органов, лицами, выполняющими управленческие функции в коммерческой или иной организации, создание условий совершения преступлений и т. п.).

Преступление в форме участия лица в преступном сообществе (преступной организации) считается оконченным с момента совершения хотя бы одного из указанных преступлений или иных конкретных действий по обеспечению деятельности преступного сообщества (преступной организации).

В случаях, если лицо, не являющееся участником преступного сообщества, оказывает содействие преступному сообществу путем дачи советов, указаний, предоставления информации, средств или орудий совершения преступления и т. д., его действия должны квалифицироваться по ч. 5 ст. 33, ч. 2 ст. 210 УК РФ как пособничество в участии в преступном сообществе (преступной организации).

Уголовная ответственность участника преступного сообщества (преступной организации) за действия, предусмотренные ч. 2 ст. 210 УК РФ, наступает независимо от его осведомленности о действиях других участников сообщества (организации), а также о времени, месте, способе и иных обстоятельствах планируемых и совершаемых преступлений.

Действия участника преступного сообщества (преступной организации), не являющегося исполнителем конкретного преступления, но в соответствии с распределением ролей в составе этого сообщества выполняющего функции организатора, подстрекателя либо пособника, подлежат квалификации независимо от его фактической роли в совершенном хищении с использованием компьютерных технологий по соответствующей статье УК РФ без ссылки на ч. 3, 4 и 5 ст. 33 УК РФ, а также по ч. 2 ст. 210 УК РФ 23.

Кроме вышеперечисленных и закрепленных в УК РФ признаков преступное сообщество могут характеризовать и такие признаки, как: конспирация и коррумпированность; общая касса, связи с правоохранительными органами и др. При этом отсутствие данных признаков не влияет на квалификацию деяния по ст. 210 УК РФ.

Завершая рассмотрение вопросов квалификации хищений денежных средств, совершаемых с использованием компьютерных технологий, хотелось бы обратить внимание на проблему уголовно-правовых санкций, которая широко обсуждается в научной литературе.

Как известно, введение в УК РФ специальных составов мошенничеств явилось реакцией законодателя на удельный рост преступлений, совершаемых именно таким способом. Как результат, осуществляя особую у г о л о в н о - п р а в о в у ю регламентацию, законодатель отметил более высокую степень общественной опасности мошенничества, совершаемого с использованием компьютерных технологий, по сравнению с общей (ст. 159 УК РФ). Целью таких изменений явилось стремление привести уголовно-правовые запреты в соответствие с изменившимися условиями жизни общества, и тем самым повысить эффективность правового регулирования24. В связи с этим

вызывает, по меньшей мере, недоумение то обстоятельство, что законодатель, признав необходимость особого правового регулирования ответственности за мошенничество с использованием компьютерных технологий, и тем самым, как нам представляется, признав его повышенную опасность, установил за совершение преступления наказание менее строгое, чем предусмотренное базовой нормой об ответственности за мошенничество (ст. 159 УК РФ). Так, в санкции ч. 1 ст. 159.6 УК РФ отсутствует наказание в виде лишения свободы в отличие от ч. 1 ст. 159 УК РФ, в санкции которой сохранено данное наказание на срок до двух лет. В соответствии с санкцией ч. 2 ст. 159.6 УК РФ наказание в виде лишения свободы предусмотрено на срок до четырех лет, тогда как по ч. 2 ст. 159 УК РФ максимальный предел данного вида наказания составляет пять лет. Реализация ответственности за совершение преступления, предусмотренного ч. 3 ст. 159 УК РФ, предполагает возможность применения наказания в виде лишения свободы на срок до шести лет со штрафом в размере до десяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного месяца. В то же время максимальный срок лишения свободы, согласно ч. 3 ст. 159.6 УК РФ, понижен до пяти лет. Лишь санкции ч. 4 ст. 159 и 159.6 УК РФ полностью совпадают.

Также следует обратить внимание на сферу применения ч. 3 и 4 ст. 159.6 УК РФ, которая значительно уже сфер применения норм, содержащихся в ч. 3 и 4 ст. 159 УК РФ. Причина кроется в аутентическом толковании понятий «крупный» и «особо крупный» ущерб.

Как было отмечено, в соответствии с прим. 1 к ст. 158 УК РФ, крупным ущербом в ст. 159 УК РФ признается стоимость имущества, превышающая двести пятьдесят тысяч рублей, а особо крупным - один миллион рублей. При этом согласно прим. к ст. 159.1 УК РФ крупным размером в ст. 159.6 УК РФ признается стоимость имущества, превышающая один миллион пятьсот тысяч рублей, а особо крупным - шесть миллионов рублей.

Таким образом, размер ущерба для применения квалифицирующих признаков мошенничества в сфере компьютерной информации по сравнению с простым мошенничеством увеличен в шесть раз.

Ответственность за совершение мошенничества с использованием платежных карт, закрепленная в санкциях частей ст. 159.3 УК РФ, дословно соответствует формулировкам ст. 159.6 УК РФ, анализ которой произведен выше. При этом следует только отметить, что отнесение состава ст. 159.3 УК РФ к привилегированным, а не квалифицированным и, как следствие, установление более мягкой санкции по сравнению с общим составом мошенничества (ст. 159 УК РФ) является нелогичным законодательным решением, поскольку степень общественной опасности данного деяния в целом не ниже, а в отдельных случаях выше, чем деяния, ответственность за которое предусмотрена ст. 159 УК РФ

Структура криминалистической характеристики хищений денежных средств совершаемых с использованием компьютерных технологий

Под криминалистической характеристикой любой общности преступлений понимается абстрактное научное понятие о модели криминалистически значимых признаков рода и вида (групп) преступлений, проявляющихся в организационно-упорядоченной совокупности существенных обстоятельств их совершения, а также закономерных связях между ними, и служащих для решения задач расследования преступлений26.

Таким образом, при рассмотрении криминалистической характеристики хищений денежных средств, совершаемых с использованием компьютерных технологий, необходимо определить и описать как существенные обстоятельства (элементы) совершения данного вида преступных деяний, так и взаимосвязи между этими обстоятельствами, чтобы полученная теоретическая модель способствовала предварительному расследованию. Данную модель, по мнению авторов настоящей работы, образуют следующие обстоятельства (элементы): объект, предопределяемый предметом преступлений; средства преступлений (в широком смысле слова); субъект преступления (личность преступника).

Видовым объектом хищений денежных средств, совершаемых с использованием компьютерных технологий, являются общественные отношения, складывающиеся в отношении собственности на денежные средства, находящиеся на банковских счетах, т. е. предмет преступления. Важное значение для расследования имеет форма данного предмета преступления - безналичные денежные средства, которая, с одной стороны, детерминирует субъекта и средства преступления, а с другой - тактику и методику расследования.

Рассмотрение и анализ субъекта хищений денежных средств, совершаемых с использованием компьютерных технологий (личности преступника), занимают особое место в соответствующей криминалистической характеристике, так как являются исключительно полезными с точки зрения выявления, раскрытия и расследования.

Анализ практики расследования хищений денежных средств, совершаемых с использованием компьютерных технологий, показал, что субъектами таких преступлений могут быть:

1) сотрудники организаций, в том числе руководители, бухгалтера, системные администраторы

2) бывшие сотрудники организации

3) иные лица.

Так, по полученным данным Т. М. Лопатиной, большинство злоупотреблений в финансовой сфере, связанных с нарушениями в области компьютерной информации, происходит при прямом или косвенном участии сотрудников: в связи с ошибками персонала - 55 %; в связи с защитой информации - 20 %; из-за действий обиженных сотрудников -9%; из-за внешнего нападения - 1-3 % и др.

Лица, причастные к хищениям денежных средств, совершаемых с использованием компьютерной информации, существенно различаются по уровню образования: от неоконченного среднего до наличия нескольких высших образований.

77 % из числа лиц, совершающих преступления с использованием компьютерных технологий, характеризуются высоким уровнем интеллектуального развития. Интеллектуальное развитие выше среднего характерно для 21 % преступников. Более низкий уровень установлен только у 2 % лиц.

Существуют несколько подходов к классификации личности компьютерных преступников по мотивам совершения преступлений. Приведем классификацию, предложенную В.Б. Веховым, дифференцирующую личность «компьютерного правонарушителя» на три группы:

1. Лица, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности. Характерной особенностью преступников этой группы является отсутствие у них четко выраженных противоправных намерений. Практически все действия совершаются ими с целью проявления своих интеллектуальных и профессиональных способностей.

2. Компьютерные преступления могут совершаться лицами, страдающими «компьютерными фобиями».

3. Профессиональные компьютерные преступники с ярко выраженными корыстными целями, так называемые «профи». В отличие от первой переходной группы «любителей» и второй специфической группы «больных», преступники третьей группы характеризуются многократностью совершения компьютерных преступлений с обязательным использованием действий, направленных на их сокрытие, и обладают в связи с этим устойчивыми преступными навыками.

В профессиональном плане преступники, особенно те, которые создают вредоносные (разрабатывают) программы и другие средства хищений, являются специалистами в области программирования, системного администрирования, автоматизированных систем, функционирующих в конкретных отраслях экономики (банковской, торговой и т. п.), а также владеют специальными навыками и умениями в сфере управления компьютерами и его составными компонентами.

Характеризуя таких лиц, исследователи обращают внимание на следующие их свойства и особенности поведения:

1) в подавляющем большинстве случаев они имеют склонности к точным наукам и представляют профессии технического или точного характера, при этом проявляют повышенный интерес к абстрактным видам искусства и нетрадиционным, религиозным учениям. Особое отношение у них к фантастике и фэнтези. Они, как правило, знают английский язык или, как минимум, хорошо читают на нем;

2) им характерен свободолюбий и эгоцентричный характер;

3) такие лица ведут «ночной» образ жизни, так как в это время достаточно свободны телефонные линии, действуют льготные тарифы на доступ к платным информационным сетям, и никто не мешает;

4) длительный период времени их сопровождает семейная неустроенность и холостяцкий образ жизни, обусловленные проведением основного своего времени возле компьютера;

5) внимание обустройству жилья и поддержанию в нем порядка они не уделяют.

Логическим центром жилища является компьютер, системный блок которого имеет внешние визуальные изъяны (зияющее отверстие от лазерного привода, высовывающийся шлейф для подключения жесткого диска и т. п.). Все это обусловлено огромным темпом изменения состава и конфигурации программного и аппаратного обеспечения. Постоянно подключаются какие-то устройства, устанавливаются, а затем уничтожаются компьютерные программы;

6) длительное общение с компьютерной техникой, которая сама, как правило, дает только точные ответы, приводит к тому, что эти лица, являясь профессионалами, часто почти автоматически начинают общаться с людьми в такой же строгой манере. Когда профессионалу задает вопрос профессионал, то он рассчитывает на формальный, строгий, точный ответ. То есть он старается сформулировать именно тот вопрос, точный ответ на который его на самом деле интересует. В разговорах задают уточняющие вопросы и часто переспрашивают отдельные детали, что зачастую вызывает раздражение собеседника. При этом обращает на себя внимание постоянное использование компьютерного жаргона, малопонятного непосвященным.

Специалисты отмечают следующую закономерность: чем изощрение и технически сложнее хищение денежных средств, тем меньшее количество людей способны его совершить. Зачастую складываются ситуации, когда лишь один способ совершения такого преступления или используемое орудие преступления может практически однозначно указать на человека, его совершившего.

Помимо профессиональных преступников выделяют также лиц:

- не обладающих серьезными познаниями в области компьютерных технологий, имеющих лишь некоторые пользовательские навыки работы с компьютером. Как правило, их действия направлены на уничтожение, блокирование, модификацию, копирование ничем не защищенной информации, после дополнительного обучения конкретным приемам,

- имеющих психические отклонения, к числу которых относят лиц, страдающих различными компьютерными фобиями.

Долгое взаимодействие с компьютерными технологиями, точными (в плане дисциплины мышления) знаниями приводит к существенному изменению психологии людей, их поступков и, как следствие, их характеров (образа мышления). В частности, психология, логика мышления и даже поведение профессиональных программистов во многих случаях отличаются от психологии, мышления и поведения «обычных» людей.

В соответствии со сложившимися к настоящему времени представлениями компьютерные преступники в целом делятся на три основные возрастные группы: 11 - 15, 17 - 25 и 30 - 45 лет. В основе данной классификации лежат результаты работы первой международной конференции Интерпола по компьютерной преступности (1995 г.). При этом считается, что первая возрастная группа в основном совершает кражи через кредитные карточки и телефонные номера, «взламывая» коды и пароли больше из-за любознательности и самоутверждения.

Вторая группа - это студенты, которые в целях повышения своего «познавательного» уровня похищают информацию из различных банков данных.

Третья группа включает в себя лиц, умышленно совершающих компьютерные преступления с целью получения материальной выгоды, а также ради уничтожения или повреждения компьютерных сетей.

На наш взгляд, такая классификация и характеристика возрастных групп компьютерных преступников не выдерживает критики, так как абсолютно не учитывает отечественной специфики. Очень трудно представить себе одиннадцатилетнего российского подростка, взламывающего коды и пароли в отечественных автоматизированных информационных системах или снимающего деньги с украденной кредитной карты. Учитывая отечественные учебные программы по информатике, уровень жизни населения, а следовательно распространенность современной вычислительной техники и возможности доступа в Интернет, необходимого уровня одаренный ребенок достигает только в более зрелом возрасте. Совершенно непонятным является верхнее ограничение возраста 45 годами. На наш взгляд, верхнего возрастного предела у компьютерных преступников не существует. Нам представляется более оправданным разбить отечественных правонарушителей в сфере компьютерной информации на две возрастные группы: с 14 до 20 лет и с 21 года и далее.

Совершаемые действия взрослыми преступниками, обладающими профессиональными навыками и жизненным опытом, носят осознанный корыстный характер, при этом, как правило, предпринимаются меры по противодействию раскрытию преступления и введению следствия в заблуждение. Практически все известные отечественные преступники в сфере компьютерной информации - представители мужского пола. Появляющиеся утверждения о том, что в последнее время увеличивается процент женщин-хакеров, ничего общего с отечественной реальностью не имеет.

Преступники-одиночки постепенно вытесняются с криминального рынка законспирированными, хорошо организованными и разветвленными группами, объединяющими людей из разных регионов России или стран мира. Данная тенденция предопределена тем, что большая часть хищений денежных средств, совершаемых с использованием компьютерных технологий, представляет собой достаточно сложное явление, в орбиту которого вовлекается достаточно большое количество людей с различными навыками, умениями, типовыми чертами характера и т. п. При этом каждый из этих людей может играть различную роль в совершении хищения и, следовательно, в разной мере может претендовать на место в организованной группе.

Некоторые разновидности хищений, совершаемых с использованием компьютерных технологий, объективно требуют более высокого уровня организованности, что предопределяет создание преступных сообществ, в которых отдельные группы выполняют строго определенные преступные действия, направленные на получение единого результата. Так, например, преступное сообщество, совершающее хищение денежных средств в системе ДБО, включает следующие подгруппы:

- лица, взаимодействующие с организатором и непосредственно вовлечённые в процесс хищений: заливщик, прозвонщик, руководитель обналичивания (дроповод);

- лица, взаимодействующие с руководителем обналичивания: поставщик юридических лиц, поставщик банковских карт, поставщик SIM-карт и дропов;

- лица, взаимодействующие с организатором, но не вовлеченные непосредственно в процесс хищений: программист, трафер, владелец/автор связки эксплойтов, криптор, поставщик доменов и серверов.

Кроме того, среди лиц, причастных к совершению хищений в системе ДБО, следует выделить так называемых «денежных мулов» или «финансовых агентов», которые предоставляют обналыцикам копии паспортов и иных документов, удостоверяющих личность, и (или) оформляют на себя документы (например, для регистрации или покупки фиктивных юридических лиц), в том числе банковские карты, с использованием которых осуществляются операции по обналичиванию похищенных денежных средств.

Необходимо еще раз отметить, что лица, участвующие в хищении денежных средств в системе ДБО, зачастую могут находиться не только в различных регионах Российской Федерации, но и за её пределами. Преступники получают необходимые данные и общаются с целью совершения хищений денежных средств в системе ДБО и иных компьютерных преступлений в глобальной сети Интернет.

Существует значительное количество закрытых общему доступу сайтов, форумов, блогов и т. п., где концентрируются лица, склонные к совершению рассматриваемых и иных компьютерных преступлений, происходит обмен информацией и опытом, в том числе участники объединяются в группы, сплачиваются и разрабатывают новейшие изощренные способы и методы совершения преступлений с использованием высоких технологий. Не видя друг друга, и часто не зная реальных имен сообщников, преступники могут на протяжении длительного времени совершать такие преступления.

Небезынтересно отметить, что выявлены случаи, когда преступным результатом, т. е. похищенными денежными средствами, пользуются третьи лица (не принимавших участие в подготовке, совершении и сокрытии преступления).

Таким лицами, как правило, становятся дропы, принимающие участие в обналичивании денежных средств, но не осведомленные об источниках их преступного происхождения. В то же время следственной практике известны случаи, когда такими лицами становятся работники коммерческих организаций.

Так, один из специалистов компании сотовой связи (г. Чебоксары) обнаружил в своем рабочем компьютере список SIM-карт, которыми обычно пользуются разного рода мошенники для аккумулирования похищенных денежных средств.

Убедившись, что счета преступников регулярно пополняются денежными переводами с разных регионов страны, он блокировал такие SIM-карты, создавал их дубликаты, с использованием которых переводил денежные средства на личные банковские счета. Таким образом, меньше чем за

полгода/не выходя из кабинета, данное лицо похитило более 500 тысяч рублей.

В качестве средств хищения денежных средств, совершаемых с использованием компьютерных технологий, необходимо рассматривать следующие структурные элементы: обстановку преступления; орудия совершения преступления; способы преступления.

Под обстановкой преступления понимается система различного рода взаимодействующих между собой объектов, явлений и процессов, характеризующих место и время преступного деяния, особенности поведения непрямых к такому деянию участников, психологические связи между ними и другие факторы объективной реальности, определяющие условия подготовки, совершения и сокрытия преступного деяния.

Обстановку хищений денежных средств, совершаемых с использованием компьютерных технологий, на наш взгляд, составляют организационные, технические, программные, пространственные, временные, социально-психологические факторы их подготовки, совершения и сокрытия. Особенностью данного рода преступлений является то, что на их совершение практически не оказывают влияние природно-климатические факторы.

Выявление особенностей сложившейся обстановки позволяет быстрее определить, на что следует обратить особое внимание при осмотре места происшествия, изучении компьютерного оборудования и документов, вызове и допросе свидетелей и решении вопросов о необходимости изъятия определенных документов и т. п.

Подготовка, совершение и сокрытие хищений денежных средств, совершаемых с использованием компьютерных технологий, разнесены в пространстве и во времени. Этим определяется особенность хищений денежных средств, совершаемых с использованием компьютерных технологий, в том числе связанных с созданием, использованием и распространением вредоносных программ: место непосредственного совершения противоправного деяния (место, где выполнялись действия объективной стороны состава преступления) и место наступления вредных последствий (место, где наступил результат противоправного деяния) не совпадают. Данная закономерность проявляется независимо от разновидности рассматриваемого преступного деяния. Исключением являются хищения денежных средств, совершаемые с использованием компьютерных технологий работниками коммерческих банков.

Местом, где в результате совершения рассматриваемого преступления наступил преступный результат, являются коммерческий банк или платежная система, где открыты счета, с которых незаконно списываются (похищаются) денежные средства, а также точки размещения банкоматов (при хищении находящихся в них денежных средств с использованием компьютерных технологий).

Следует отметить, что местом подготовки хищений денежных средств, совершаемых с использованием компьютерных технологий, могут являться жилые и служебные помещения, которые оборудуются компьютерной и иной техникой или аппаратурой, в том числе для приобретения, разработки, модификации и распространения вредоносных программ, сбора скомпрометированной информации, создания и направления в коммерческие

банки подложных электронных расчетных документов, создания скиммингового и иного оборудования для совершения хищения, а также других подготовительных действий. При этом перечисленные подготовительные действия даже по одному факту хищения, как правило, разнесены по разным местам (помещениям), в том числе значительно удаленным друг от друга и расположенным как в разных регионах страны, так и за рубежом.

Также местами подготовительных действий могут быть точки размещения банкоматов или POS-терминалов, в случае предварительного их оборудования скимминговым и иными устройствами.

Кроме того, к местам подготовки хищений денежных средств, совершаемых с использованием компьютерных технологий, можно отнести помещения, в которых располагаются сервера, в том числе в зарубежных странах. Данное обстоятельство подтверждается выявлением фактов совершения хищений с использованием PROXY-серверов с IP-адресами других государств.

Время рассматриваемого вида хищений также разнесено и зависит от их разновидностей. Согласно ч. 2 ст. 9 УК РФ временем совершения преступления признается время окончания общественно опасного деяния независимо от момента наступления последствий.

Как правило, юридические факты - хищение денежных средств, совершаемых с использованием компьютерных технологий, во многих случаях измеряются долями секунды. При этом время подготовки к такому хищению и его сокрытию чаще всего имеет продолжительный период (до нескольких месяцев).

Перечень условий совершения хищения достаточно многообразен и включает отдельные элементы и в целом автоматизированную информационную систему кредитной организации и ее возможности, в том числе способ подтверждения платежа (по SMS или электронной подписи), средства защиты компьютерной информации, правовые основы реализации компьютерных технологий и т.п.

Условия хищений денежных средств, совершаемых с использованием компьютерных технологий, неразрывно связаны с жертвой таких преступлений.

Характеристика жертвы до, во время и после совершения хищений помогает точнее определиться во многих обстоятельствах противоправного деяния.

Поведение жертвы всегда зависит от сложной совокупности внешних и внутренних факторов. Поведение (в широком смысле), которое предпринимает жертва, может существенно облегчить преступнику совершение хищения. Между преступником и жертвой в большинстве случаев можно выявить определенную взаимосвязь и определить причины, по которым денежные средства именно данного лица (как физического, так и юридического) стали целью преступного посягательства.

Необходимо также обратить внимание, что жертвы (пострадавшие) -коммерческие банки в большинстве своем стремятся не сообщать в правоохранительные органы о фактах совершения в отношении них хищений с использованием компьютерных технологий, тем самым создают препятствия для деятельности следователей.

Способы данного вида хищений детерминированы предметом преступного посягательства, а точнее его формой (безналичные денежные средства), доступ к которой обеспечивается автоматизированной информационной системой кредитной организации.

Практически невозможно привести исчерпывающий перечень способов хищений денежных средств, совершаемых с использованием компьютерных технологий, так как их содержание может составлять самые разнообразные действия, в зависимости от изобретательности, преступной квалификации и интеллектуальности преступника. Однако, несмотря на многообразие способов преступления рассматриваемого вида, можно выделить следующие: рассылка SMS-сообщений о выигрыше автомобиля или блокировке банковской карты; создание Интернет-сайтов по продаже авиабилетов или Интернет-магазинов, предлагающих товары по заниженным ценам и требующих перечисления предоплаты; размещение объявлений о продаже товаров в социальных сетях и на специализированных торговых площадках с требованием перечисления денег за покупку авансом; изготовление, распространение и использование вредоносных программ, позволяющих дистанционно подменять платежные распоряжения с компьютерных устройств жертв или управлять операциями выдачи денежных средств из банкоматов; дистанционное проникновение в компьютерные системы коммерческих банков и иных организаций, используя сбои или недостатки в их работе, позволяющие незаконно списывать денежные средства с банковских счетов и т. п.

Наиболее опасными и сложными в расследовании способами преступлений являются те, которые применяются для хищения денежных средств в системе ДБО как физических, так и юридических лиц, в том числе путем несанкционированного входа в компьютерную систему кредитных организаций либо использования сбоев в ее работе, а также для хищений денежных средств из банкоматов и с их использованием.

Хищения денежных средств в системе ДБО или путем несанкционированного входа в компьютерную систему кредитных организаций либо использования сбоев в ее работе связаны с операциями с компьютеров жертв и основаны на функциональных возможностях автоматической подмены платежных распоряжений в момент их отправки пользователями, а также автоматизированных процессах формирования и отправки платежного поручения.

Как правило, несанкционированный доступ на компьютерное устройство жертвы осуществляется путем его заражения вредоносными программами через уязвимости системного и прикладного программного обеспечения (операционные системы, WEB-браузеры, почтовые клиенты, социальные сети и т. д.) с последующим дистанционным похищением паролей и использованием ключей электронной подписи. Так, 27 февраля 2015 г. с 12.30 ч. до 13.00 ч. путем неправомерного доступа к компьютерной информации, хранящейся на жестком диске персонального компьютера директора (начальника) казначейства АКБ «Энергобанк» (ОАО), в котором установлено второе рабочее место участника торгов на Московской Межбанковской Валютной Бирже «Национальный клиринговый центр» (ММВБ), совершена модификация компьютерной информации, позволившая осуществить сделки с валютными денежными средствами в сумме более 4 000 000 000 рублей путем покупки 158 737 000 долларов США по среднему курсу 62, 6284 рублей за 1

доллар США и продажи 93 925 000 долларов США по среднему курсу 59, 6703 рублей за 1 доллар США через Московскую Межбанковскую Валютную Биржу «Национальный клиринговый центр», причинившие ущерб АКБ «Энергобанк» (ОАО) на общую сумму 469 861 520 рублей.

25 июня 2015 г. произошли несанкционированные списания с расчетного счета РОО РТ ГТО денежных средств в общей сумме 32 973 357 руб. по платежным поручениям, направленным в АО «ИК БАНК» для исполнения по системе удаленного доступа «Банк Клиент», адресованные получателям - физическим лицам на расчетные счета, открытые в ОАО «Сбербанк России» в городах Санкт-Петербург, Ижевск, Краснодар, Казань. При этом поступившие в АО «ИК БАНК» платежные поручения клиента в электронном виде были снабжены аналогом собственноручной подписи клиента (электронный ключ), проверка которой на сервере «Банк Клиент» дала положительный результат, что явилось основанием для исполнения распоряжения и последующей отправки переводов денежных средств.

Орудиями хищения денежных средств, совершаемых с использованием компьютерных технологий, являются компоненты (элементы) таких технологий, в том числе сеть Internet, электронные носители информации, специальные технические средства, компьютерные программы, бот-сети и т. п.

Как и способы хищений денежных средств, совершаемых с использованием компьютерных технологий, орудия преступлений будут подробно рассмотрены в следующих частях настоящей работы. Между тем отметим некоторые особенности способов обналичивания денежных средств, так как они могут являться как окончанием данного вида хищений, так и самостоятельным правонарушением, выходящим за рамки способа хищения.

Анализ технологий обналичивания похищенных денежных средств позволяет выделить некоторые их особенности, которые предопределяются типом жертвы (коммерческий банк или иная платежная система), способом хищения, общей суммой хищения. Так, если жертвой становится коммерческая организация, имеющая ограниченный круг контрагентов, то преступники вынуждены учитывать данное обстоятельство, так как все платежи будут обязаны пройти через определенный пул посредников. Дополнительно, «нештатный» пул контрагентов вызывает риски для преступников, т. е. подозрение и ненужные проверки (ручная обработка платежных поручений) со стороны коммерческого банка.

При хищении денежных средств путем получения контроля над АРМ коммерческого банка в сумме до 100 мил. руб., технология обналичивания представляет собой классическое дерево, когда денежные средства со счета коммерческого банка направляются на счета нескольких юридических лиц, далее от каждого такого лица на счета более мелких юридических лиц (таких транзакций может быть несколько), далее на карты физических лиц (от 600 до 7000 транзакций).

При хищении денежных средств путем получения контроля над АРМ коммерческого банка свыше 100 мил. руб., технология обналичивания заключается в осуществлении преступных переводов на счета юридических лиц, заблаговременно подготовленных в других коммерческих банках (как правило, путем приобретения фирм-однодневок). Получение денежных средств осуществляется через кассу коммерческого банка или в результате

«распыления» похищенных средств на заранее подготовленные карточные счета через банкоматы или покупки дорогостоящих товаров (например, ювелирных изделий и т.п.) либо путем перечисления на заранее подготовленные счета мобильных операторов связи, привязанные к SIM-картам.

При хищении денежных средств путем получения контроля над сервисом управления банкоматами (который в силу объективных обстоятельств - ограниченный объем кассет - не может превышать 100 млн. руб.), технология обналичивания является завершающим этапом такого хищения (получение денежных средств из банкомата по команде преступника).

Кроме того, технология обналичивания может включать каналы отправки денежных средств через системы расчетов, электронные кошельки и платежные системы, типа WebMoney, Яндекс деньги, QIWI (1500-2000 транзакций).

Способы вывода денежных средств из платежной системы WebMoney: банковская карта; карта, заказанная через сервис WebMoney; виртуальная карта; Интернет-банкинг; почтовый перевод; денежный перевод; банковский перевод; обменные пункты и дилеры WebMoney; электронные деньги; офис банка или партнера; биржа exchanger.ru.

Для целей обналичивания похищенных денежных средств преступники применяют технологию «рассеивания», включающую операции перечисления этих средств с одного банковского счета (например, карточного счета, расчетного счета юридического лица) на несколько банковских счетов, счетов иных платежных систем, счетов операторов сотовой связи и т. п.

Подводя итог вопросам, рассмотренным в настоящем параграфе, следует подчеркнуть, что знание должностным лицом ОПС криминалистической характеристики хищений денежных средств, совершаемых с использованием компьютерных технологий, позволяет предметно разрабатывать следственные версии и осуществлять целенаправленные следственные действия по их проверке, так как обстоятельства (элементы), образующие такую характеристику, находятся в закономерных связях друг с другом (системно-структурных, функциональных и т. п.). Основными (базовыми) элементами хищений данного вида являются: объект, предопределяемый предметом преступлений; средства преступлений (в широком смысле слова); субъект преступления (личность преступника).

Наличие закономерных связей между обстоятельствами (элементами) криминалистической характеристики хищений денежных средств, совершаемых с использованием компьютерных технологий, не исключает особенностей каждого конкретного деяния. Но подобного рода особенности, вместе с выявленными закономерностями, образуют систему («если да, то...»), закономерно влияющую на производство предварительного следствия.

Орудия хищений денежных средств, совершаемых с использованием компьютерных технологий

Орудия хищений денежных средств, совершаемых с использованием компьютерных технологий, как было ранее отмечено, являются компоненты

(элементы) таких технологий, в том числе сеть Internet, компьютерные программы, бот-сети, электронные носители информации, в том числе платежные карточки, специальные технические средства и т. п.

Рассматривая сеть Internet как орудие совершения хищений денежных средств с использованием компьютерных технологий, следует обратить внимание на следующие обстоятельства.

Как справедливо отмечается исследователями, информационное пространство (киберпространство) выступает в качестве средства, т. е. предмета материального мира или процесса, используемого в процессе совершения преступления как для непосредственного воздействия на объект посягательства, так и для действий вспомогательного характера. Следовательно, киберпространство при хищениях является орудием преступления, а его использование при хищениях - способом преступления. Также киберпространство можно рассматривать в качестве места преступления (в широком смысле), что само по себе осложняет расследование хищений денежных средств, совершаемых с использованием компьютерных технологии.

Уникальность компьютерной сети Internet состоит в том, что она не находится в собственности конкретного юридического или физического лица либо государства.

В результате почти во всех сегментах этой сети отсутствует государственное регулирование, цензура и другие формы контроля за информацией, циркулирующей в сети Internet. Такое положение дел открывает широкие возможности для доступа к любой информации, которые все шире используются в преступной деятельности. При использовании сети Internet в качестве виртуального места (среды) преступления, в первую очередь, привлекает внимание преступников возможность неограниченного обмена информацией криминального характера (например, об орудиях хищения, о вредоносных программах, скимменговом оборудовании, похищенной конфиденциальной информации с платежных карт и т. п.).

Другая привлекательная для преступников особенность сети Internet связана с возможностью осуществлять в глобальных масштабах информационно-психологическое воздействие на людей, в том числе с целью вовлечения их в деятельность преступных групп либо выполнения в «темную» определенной работы (например, разработка отдельных программных алгоритмов).

Криминалистически значимыми признаками сети Internet (Интернет) являются разнообразные протоколы или сетевые протоколы (напр., IP -Internet Protocol (Протокол Интернета), TCP - Transmission Control Protocol (Протокол управления передачей) или протокол TCP/IP), связывающие всевозможные типы компьютеров, физически передающих данные по телефонным кабелям и волоконной оптике через спутники и радиомодемы, сетевые адреса, а также сервисы или Итернет-сервисы (электронная почта, юриспруденции и криминалистики изучить достаточно сложно. Если при традиционном осмотре места происшествия следователь может запротоколировать, сфотографировать место преступления, то известные сложности возникают при осмотре процессов и явлений, происходящих в киберпространстве.

Криминалистическое значение имеет и другое обстоятельство. Пользователи Интернета подключаются к сети через компьютеры специальных

организаций, называемые поставщиками услуг Интернета или провайдерами. Подключение к Интернету с помощью поставщика услуг означает, что с помощью модема пользователя устанавливается соединение с компьютером поставщика, который и связывает пользователя с Интернетом.

Компьютерная сеть провайдерской компании создается для обеспечения работ по предоставлению доступа в Интернет в соответствии с действующим законодательством, учредительными документами и лицензией на право предоставления услуги передачи данных и услуги телематических служб. Кроме того, работа сети организована таким образом, чтобы производить в автоматизированном режиме расчеты с клиентами за предоставляемые им услуги в зависимости от времени их использования и в соответствии с установленным прейскурантом цен. Для этих целей в сети провайдера имеется информация о присвоенном пользователю «имени» и «пароле», которая является коммерческой тайной и сообщается пользователю при заключении договора с ним для обеспечения его работы в сети Интернет.

Прежде чем приступить к рассмотрению компьютерных программ, как орудию совершения хищений денежных средств с использованием компьютерных технологий, отметим, что в современной научной литературе, наряду с соответствующим понятием, термины «программное обеспечение», «программный продукт» употребляются как синонимы, а в законодательстве закреплен термин «программа для ЭВМ».

При применении термина «программный продукт» подчеркивается статический признак, завершение какого-либо действия, тогда как в термине «обеспечение» больше выражается функциональный признак, направленность на достижение какого-либо результата. В связи с этим авторы настоящей работы полагают возможным использовать указанные термины как синонимы.

Компьютерная программа может существовать в двух материальных формах: в виде обычного рукописного или машинописного документа на бумаге (пленке), который называется «исходный текст» («исходник») и представляет собой алгоритм обработки данных и подачи управляющих команд, описанный с помощью языков программирования; в виде документированной компьютерной информации - электронного документа, который называется «объектный код» - исходный текст, преобразованный в электронно-цифровую форму с помощью инструментальных программ (систем программирования).

В литературе можно обнаружить разные классификации компьютерных программ. Так, Ю.А. Шафрин выделяет два класса программ: системное и прикладное программное обеспечение. Подробная классификация прикладных программ приведена О. Э. Згадзаем, С. JI. Казанцевым и А. В. Филипповым, однако авторы, наряду с программами широкого применения, внесли в перечень специализированные бухгалтерские программы и системы автоматического проектирования, которые следует выделить в класс специальных программ. В классификации, предложенной авторским коллективом под руководством Н. Г. Шурухнова, выделяются два основных класса программного обеспечения с последующим делением на подклассы: системное программное обеспечение (операционные и сервисные системы) и прикладное программное обеспечение (инструментальные системы и системы технического обслуживания).

А. П. Пятибратов дифференцирует программное обеспечение на три класса: системное, прикладное и специальное.

В. В. Крылов на основе назначения выделяет следующие группы программ49: операционная система (ОС); сервисные программы - нередко являются прямым продолжением программ ОС, делают удобной работу пользователя и (или) расширяют возможности системы; различные средства и языки программирования; текстовые и графические редакторы и процессоры; средства для обработки цифровых данных (табличные процессоры); системы управления базами данных (СУБД) и системы управления знаниями (экспертные системы); интегрированные пакеты, включающие в себя возможности обработки текстов, электронных таблиц, манипулирования данными, коммуникации и т. п.; специализированные программы для конкретной предметной области (обеспечивают обмен данными между компьютерами и периферийными устройствами, компьютеров между собой и т. п.); игровые программы от детских до деловых игр.

Как представляется, для компьютерных программ характерно свойство комплексности (многозадачности) применения, что делает любую классификацию весьма условной. В связи с этим для целей настоящей работы компьютерные программы как средство хищений денежных средств с использованием компьютерных технологий, будут дифференцироваться на две группы: вредоносные компьютерные программы и компьютерные программы, не являющиеся вредоносными, но обеспечивающие функционирование первых.

Электронный носитель информации - материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники. К основным видам современных электронных носителей информации относятся: USB флэш накопители; пластиковая карта;

внутренний накопитель на жестком магнитном диске; внутренний накопитель на магнито - оптическом диске (НМОД -винчестер);

гибкие магнитные диски (ГМД - дискеты); интегральная микросхема памяти (ИМСП)

карты памяти различных форматов (Compact Flash, Secure Digital, Multimedia Card и Memory Stick и др.); компьютер;

листинг - распечатка компьютерной информации на твердом физическом носителе (бумаге или пленке);

накопитель на магнитной ленте или специальной металлической нити (в кассетах или бобинах);

оперативное запоминающее устройство периферийных устройств; оперативное запоминающее устройство электронно-вычислительных машин (далее - ЭВМ или компьютеры);

оптические или магнитооптические диски различных видов (CD-R, CD-RW, DVD-R, DVD-RW, BLU-RAY и т. д.);

постоянное программируемое запоминающее устройство компьютера; физическое поле - материальный носитель физических взаимодействий искусственного или естественного происхождения;

электромагнитный сигнал средство переноса информации в пространстве и во времени с помощью электромагнитных колебаний (волн);

иные носители (например, ЗИП-драйверы - внешние накопители на жестких магнитных дисках; стимеры - внешнее устройство накопления информации).

Отметим, что электронный носитель информации с соответствующим программным обеспечением и периферийным оборудованием, является универсальным орудием хищений денежных средств, совершаемых с использованием компьютерной информации,

Компьютер включает следующие компоненты:

различные виды компьютеров (персональный компьютер, сервер компьютерной сети и электросвязи (пейджинговой, сотовой и др.), аппарат сотовой электросвязи с функцией работы в сети Интернет, банкомат, контрольно - кассовая машина с блоком фискальной памяти, электронная записная книжка, электронный переводчик, графическая станция, электронный издательский комплекс (типа «Ризограф»), супер смарт-карта и др);

периферийные устройства (видеоконтрольное устройство (дисплей, монитор), устройство управления компьютера (клавиатура, манипуляторы («мышь», джойстик, «шар» - трэк-болл, «световое перо», «сенсорный экран», Isopoint Control), печатающее устройство (принтер - матричный, струйный, термографический («лазерный»), графопостроитель, плоттер), устройство видеоввода информации (сканер, цифровая фото- или видеокамера), устройство графического ввода информации (графический электронный планшет, диджитайзер), устройство работы с пластиковыми картами (импринтер, считыватель (ридер) - оптический, магнитный или электромагнитный, перкодер или программатор) и др.;

аппаратные средства (соединительные провода, кабели, шины, шлейфы, разъемы, COM - порты, «шнурки», устройства электропитания, аппаратные средства защиты компьютерной информации от несанкционированного доступа и т.д.);

устройства приема и передачи компьютерной информации (модем -внутренний или внешний, другие средства телекоммуникации).

Платежные карты, как орудие совершения хищений и (или) обналичивания похищенных денежных средств, характеризуются следующими криминалистически значимыми признаками и свойствами.

Как известно, платежные (банковские) карты могут быть дебетовые, кредитные и смешанные.

Под банковской (платежной) картой понимается средство для составления расчетных и иных документов, подлежащих оплате за счет клиента, т. е. физического или юридического лица, заключившего с кредитной организацией-эмитентом банковской карты договор, предусматривающий осуществление операций с ее использованием. Она представляет собой пластиковый прямоугольник со специальной магнитной полосой, в памяти которой хранится информация, необходимая для расчетов за товары (работы, услуги) либо для снятия наличных денег за счет имеющихся на карточном счете сумм

Магнитная банковская карточка - это только отражение банковского счета владельца: ее магнитный индикатор содержит лишь информацию об имени владельца и номере его счета в банке. Поэтому при расчетах с использованием этой карты каждый раз необходимо обращаться к центральному компьютеру для получения информации о наличии на счете необходимой для оплаты товаров (работ, услуг) суммы денег. При использовании магнитной карты следует пройти процедуру персонификации - уточнения того факта, что картой владеет именно ее предъявитель Связь с системным кассовым терминалом нужна для дачи команды на списание определенной суммы денег, подлежащей оплате.

Чиповая карточка содержит микропроцессор (чип) - маленький квадратик или овал на лицевой стороне, в памяти которого содержится вся информация о банковском счете ее владельца: о количестве денег на счете, максимальном размере суммы, которую можно снять со счета единовременно, об операциях, совершенных в течение дня. Чиповая карточка - это одновременно и кошелек, и средство расчета, и банковский счет. И это все благодаря микропроцессору, главным достоинством которого является его высокая способность при постоянстве памяти надежно сохранять и использовать большие объемы информации. При этом чиповая карточка не нуждается в процедуре идентификации и персонификации, а значит, способна работать в режиме off-line, что не требует обращения при каждом необходимом случае к банку или компании, где открыт счет владельца карты.

С точки зрения технических возможностей, пластиковые карточки можно классифицировать на магнитные, микропроцессорные (или чиповые) и виртуальные. Последние созданы специально для оплаты покупок и услуг онлайн.

Виртуальные карты существует только в сети Интернет пространства и могут содержать ровно ту сумму, которая нужна для онлайн-покупок.

Владельцем платежной карты может быть как физическое лицо, имеющее в банке-эмитенте личный счет, так и юридическое лицо, которому открывается счет корпоративный.

Корпоративная карточка открывается юридическим лицам и предназначена для управления счетом юридического лица. Выдается она банком-эмитентом или организацией-распространителем отдельным сотрудникам организации, правомочным пользоваться ее средствами, а потому на корпоративной платежной карточке кроме названия организации выбивается имя пользователя, так что применять ее может только один человек, которому при оплате товаров, работ или услуг придется подтвердить свою личность.

Юридическое лицо может открывать карточки для нескольких своих сотрудников, причем каждой карточке будет соответствовать свой спецкартсчет.

Ограничений на количество открываемых карточек внутри одной организации не существует.

В настоящее время получили достаточно широкое распространение так называемые «зарплатные» карточки. Сотрудник организации или учрзждения, оформивший такой тип карты, получает заработную плату не наличными деньгами, а путем ее перечисления на спецкарточный счет.

Важно отметить, что эмитирование банковских карт и оказание услуг, называемых эквайрингом, осуществляют уполномоченные коммерческие банки.

Эквайринг - обслуживание банками торговых и сервисных точек (магазинов, гостиниц, ресторанов, мотелей, туристических фирм, пунктов проката автомобилей), где в качестве платежного средства принимаются пластиковые карточки различных систем Банк устанавливает в пунктах платежа специальную аппаратуру для контроля пластиковых карт, адаптирует к этой технологии кассовые аппараты, обеспечивает различные способы авторизации карт. Суть эквайринга заключается в том, что коммерческий банк оказывает торговым и сервисным предприятиям услугу, позволяющую им принимать к оплате пластиковые карты. Банк, осуществляющий эквайринг, берет на себя инкассацию платежных документов (чеков) и перечисляет денежные поступления на счет магазина, ресторана, гостиницы, то есть того предприятия, за чьи товары или услуги клиенты расплачивались пластиковыми деньгами.

В преступных целях используются как подлинные, так и поддельные банковские карты.

Подлинные банковские карты преступники приобретают разными способами:

- похищают карточку и PIN-код путем обмана и (или) злоупотребления доверием. Например, использование карты путём свободного доступа и разглашения ПИН-кода членами семьи, близкими друзьями, коллегами по работе. Также преступники могут использовать пластиковые карты, оформленные в коммерческом банке, но по каким-либо причинам не полученные клиентом этого банка;

- используют в преступных целях случайно найденную карточку;

- используют в преступных целях полученную в установленном порядке карточку.

Как правило, в целях хищения денежных средств с банковских счетов используются подлинные платежные (банковские) карты, приобретенные легально третьим способом.

В то же время, как свидетельствует практика, для данного вида преступления и (или) обналичивания похищенных средств наиболее часто используются поддельные банковские карточки.

Подделка банковской карты может быть полной или частичной.

При полной подделке на заготовки поддельных карточек наносятся логотип эмитента, поле для проставления подписи, точно воспроизводятся все степени защиты (используются подлинные реквизиты реально существующих карточек).

Частичная подделка карточки, как правило, сопряжена с изготовлением так называемого «белого пластика». Такая карточка не имеет внешних реквизитов, по которым возможна их идентификация (логотипа банка-эмитента и иной платежной системы, голограммы и других степеней защиты). На чистый лист пластмассы переносятся данные уже существующих карточек.

Также частичная подделка может быть осуществлена путем удаления с подлинной карты отмеченных там данных и внесение новых. Перед этим преступник получит настоящую карту путем внесения на вновь открытый счет минимально необходимой суммы и добывает информацию о владельце «солидного» счета. После чего замазывает образец подписи или наклеивает новое подписное поле, используя обычную клеящую бумагу, «сбривает» проэмбоссированные на плоскости карты данные или «выглаживает» полихлорвинил, из которого изготовлена карта с помощью обычного утюга или микроволновой печки, а после выравнивает поверхность нанесением добытой информации с помощью настольного пресса.

Как правило, банковские карточки подделывают преступные группы, члены которой получают реквизиты существующих платежных карт (номер, срок действия, CVC или CVV - три последних цифры на обороте карты), следующим образом:

1) непосредственно из кредитных и ретейровских организаций (магазинов, гостиниц, ресторанов, мотелей, туристических фирм, пунктов проката автомобилей и т. п.) куда соучастники поступают на работу или подыскивают среди сотрудников данных организаций лиц, кто продаст конфиденциальную информацию о реквизитах банковских карт клиентов. Например, осуществляя поиск инсайдеров в ритейле, которые готовы оказать содействие в подготовке и совершении хищения реквизитов платежных карт, как персонально (персонифицировано), так и опосредовано через объявления в сети Интернет. При этом анализ хакерских форумов показал, что одни преступники продают уже перепрошитые POS-терминалы, другие - прошивки цля POS-терминалов, третьи перепрошивают POS-терминалы за деньги или процент скомпрометированных дампов.

Преступники обеспечивают POS-терминалы ритейлеров прошивками, что превращает данные терминалы в скиммеры, которые покупаются через сеть Интернет. Прошивка позволяет преступникам собирать информацию о банковской карте потенциальной жертвы (Трек 1; Трек 2; дамп магнитной полосы и PIN-код от банковской карты).

Используя прошитые POS-терминалы, работники ритейлерских организаций собирают данные (реквизиты) о платежных картах и передают ее преступникам путем отправки SMS-сообщения или снятия данных напрямую через персональный компьютер.

Следует отметить, что преступники стремятся автоматизировать процесс заражения POS-терминалов и добиться как можно большего числа зараженных устройств посредством использования специальных вредоносных программ (троянских программ) для POS-терминалов. При этом используются как версии широко известных троянских программ (например, Anunak и др.), так и специально разработанные программы. Как правило, последние являются более простыми, но надежнее. Первые версии специально разработанных программ использовали простой черный список, выдирали каждый процесс и делали дампы данных банковских карт открытым текстом. Более поздние версии сканировали только определённые настройками процессы и использовали алгоритм RC4 для шифрования извлечённых данных карт на диске.

Так, троянская программа Memory Scraper позволяет преступникам скомпрометировать данные с платежных карт, обрабатываемых на

зараженном POS-терминале (трек 1 + трек 2). Данной программой заражается электронная кассовая система под управлением операционной системы Windows.

Кроме того троянская программа Memory Scraper имеет множество дополнительных функций:

пишет свою виртуальную файловую систему (VFS) и изменяет таблицу разделов в главной загрузочной записи (MBR)), что позволяет троянской программе работать на системном уровне с повышенной скоростью при заражении машины жертвы;

использует специальные постановочные знаки (фильтры) для определенных URL) путем перехвата нажатия клавиш на машине жертвы (функция кейлогера);

сканирует память системы на предмет данных, похожих по структуре на трек 1 или трек 2 (функция Memory /RAM Scraping);

использует инъекцию типа «CodeCave» для запуска вредоносной программы из памяти, что позволяет не нагружать CPU во время сканирования памяти;

устанавливает ключи реестра внутри Active Startup, руткиты Ring с целью гарантий того, что ключи реестра при попытке их просмотра будут скрыты;

использует уязвимости O-day для обхода системы контроля учетных записей и получения привилегий администратора.

Другая троянская программа для POS-терминалов под названием PoSeidon позволяет получать из их оперативной памяти данные банковских карт, а также имеет встроенный клавиатурный шпион.

Троянская программа для POS-терминалов - PwnPOS позволяет регистрировать все активные процессы, осуществлять поиск данных банковских карт и сохранять их в отдельном файле, который затем сжимает и зашифровывает. Впоследствии файл в виде электронного письма отправляется на определенный почтовый адрес преступника.

Троянская программа для POS-терминалов - Punkey распространяется посредством программ для удаленного доступа, при посещении вредоносных сайтов, а также через спам-рассылки.

Троянская программа для POS-терминалов - NitlovePOS, распространяемая, очевидно, посредством спам-кампаний с документом Word во вложении, который содержит вредоносный макрос, осуществляет сканирование запущенных процессов на скомпрометированной машине и перехватывает трек 1 и трек 2 с магнитной полосы банковской карты, затем посылает полученные данные на сервер управления преступника с использованием протокола SSL.

Для начала автоматизации процесса заражения POS-терминалов преступнику достаточно иметь: Metasploit Framework; сканер открытых портов Zmap; рабочую версию известного трояна для POS-терминалов;

2) с использованием аппаратно-программных средств (например, скиммеров) при оплатах в торговых и сервисных учреждениях (предприятия розничной торговли, общественного питания) посредством недобросовестного персонала, который незаметно для держателя платежной карты копирует

содержимое магнитной дорожки карты с использованием скиммингового устройства, которое при малых размерах может хранить данные сотен магнитных полос; Вместе с тем данный способ получения данных о владельцах пластиковых карт исключает возможность получения PIN-кода, что существенно снижает возможности неправомерного использования полученных данных. Кроме того, анализ и сопоставление последних платежных операций, совершенных владельцами пластиковых карт, позволит определить организацию, в которой произошла утечка информации о владельцах пластиковых карт.

3) с использованием аппаратно-программных средств (считывающих устройств), с целью дальнейшего изготовления и несанкционированного использования к опии/ дубликата платежной карты. Так, одно из самых распространенных таких устройств известно под наименованием скиммер.

Скиммеры появились примерно в 2002 году в Европе (первое упоминание о них поступило из Англии). Наверняка они существовали и раньше, ибо не имеют какой-то слишком уж сложной конструкции, а банкоматы на улицах европейских городов установлены уже достаточно давно.

Современный скиммер состоит из двух частей. Первая часть - это накладной симулятор приемника платежной карты в банкомате, содержащий считыватель, микросхему преобразователя информации, контроллер и накопитель.

Современные считыватели маленького размера, ширина его головки равна ширине магнитной ленты карты, толщина 2-2,5 мм (скиммер по сути находится внутри разъема). Скиммеры накапливают информацию о картах внутри или с помощью передатчика по беспроводным каналам (чаще всего это Bluetooth или SMS-сообщение), сразу передают ее на мобильный телефон или устройство, спрятанное в нескольких метрах от банкомата. Преступник находится поблизости или время от времени появляется возле банкомата, чтобы заменить наполненный информацией скиммер.

Вторая часть скиммера - накладная клавиатура, предназначенная для «съема» информации о PIN-коде карты, содержащая микросхему, спрятанную в клавиатуре, и разобранный мобильный телефон, настроенный на постоянную отправку SMS-сообщений. Поскольку клавиатура банкомата металлическая, то и накладную изготавливают из такого же материала, но она, как правило, на 0,5-1 см выделяется на общей плоскости банкомата и потому может быть обнаружена.

SMS-сообщение отсылается после нажатия клавиши Enter на клавиатуре или четвертой цифры PIN-кода либо любой клавиши.

Кроме того, существует усовершенствованный вариант, так называемый встраиваемый скиммер-передатчик, который способен отправлять считанную информацию на принимающее устройство, расположенное неподалеку от банкомата. В этом случае скиммер помещается внутрь ридера. В комплекте такого скиммера имеется камера, с помощью которой отслеживаются вводимые PIN-коды.

Также преступники используют скиммеры с тонким профилем и гибкие, способные работать от MP3-плеера или мобильного телефона. Последние позволяют преступникам похищать данные платежных карт при помощи

отправки SMS-сообщений. В этом случае после установки такого скиммера им больше не требуется взаимодействие с банкоматом.

В комплекте со скиммером вместо накладной клавиатуры используется мини-камера с памятью для считывания ПИН-кода, укрепленная в верхней части банкомата, над клавиатурой и т. п., с функцией передачи видеотрафика на сервер при помощи wi-fi и 3g в режиме онлайн.

Как было отмечено, в настоящее время преступники используют практически невидимый скиммер (миниатюрный прибор для перехвата информации, который вставляется в банкомат через небольшое отверстие, сделанное на его передней панели), а также размещают скиммер внутри банкомата через отверстие, сделанное над картоприемником, и монтируют перехватчик информации внутри устройства. Обычно скиммеры устанавливают поверх картоприемника банкомата либо внутри кардридера. Эксперты полагают, что скиммер нового образца считывает данные не с магнитной ленты платежной карты, а с кардридера банкомата.

Если классический скимминг характерен тем, что считывающее устройство номера карты имеет свою «надводную часть», ее можно увидеть невооруженным взглядом на месте картридера, то шимминг - это использование считывающего устройства, полностью погружаемого в щель картоприемника. Само приспособление, дабы поместиться в проеме и не мешать при этом погружению туда же карты, очень миниатюрно (менее 0,1 мм), оттого высокотехнологично, дорогостояще и соответственно менее распространено, чем классические скиммеры. Но если уж мошенники им воспользовались, то противопоставить ему что-либо на пользовательском уровне крайне сложно.

Информацию о PIN-коде можно получить с высокочувствительной инфракрасной камеры. Технология получения PIN-кода в данном случае выглядит следующим образом. Преступник, стоящий в очереди, делает снимок клавиатуры, на которой предыдущий пользователь набирал PIN -код. Клавиши, к которым прикасались, несколько теплее, причём последняя нажатая клавиша теплее предпоследней и так далее; Эффективность данного метода зависит от типа клавиатуры (металлические клавиатуры обладают большей теплопроводностью и температура их клавиш быстро выравнивается) и от того, не набирал ли клиент что-нибудь ещё на клавиатуре (например, сумму).

4) с использованием поддельного банкомата, оснащенного специальным считывающим устройством (муляж аппарата, оборудованного скимминговыми устройствами). Такой банкомат подключатся к сети 220 вольт, а изображение на экране создает впечатление его работоспособности. На стикере банкомата имеется указание о том, что принимаются карты VISA, MasterCard, AmEX и т.п. Такой банкомат принимает карту, требует ввода PIN-кода, после чего выдаёт сообщение о невозможности выдачи денег (под предлогом отсутствия денег в банкомате или технической ошибки) и возвращает карту. В банкомате происходит копирование данных с карты и PIN-кода, что позволяет преступникам впоследствии изготовить дубликат и снять с его помощью деньги со счёта клиента. Данный способ хищения денежных средств получил наззание «фантом».

5) с помощью специализированной (вредоносной) программы, которая в программное обеспечение банкомата вносит вредоносный вирус,

позволяющий выполнить две команды: на скимминг (считывание магнитной полосы и PIN-кода) и снятие денежных средств (так называемый прямой диспенс). Запуск вируса осуществляется с помощью специальных карт активации;

6) путем незаконного проникновения в базы данных о владельцах пластиковых карт крупных торговых сетей, коммерческие банки и (или) иные платежные системы через недокументированные сетевые подключения, открытые беспроводные сети, не обновленное программное обеспечение, незаблокированное подключение внешних устройств и т. п.;

7) путем рассылки по электронной почте держателям платежных карт запросов якобы от коммерческих банков с просьбой подтвердить или обновить персональную информацию клиентов, связанную с картами, установить антивирусное программное обеспечение и т.п. (фишинг);

8) с использованием телефонного автонабора, который круглосуточно набирает номера в определенном регионе. Когда потенциальная жертва снимает трубку, автоответчик предупреждает, что его пластиковая карточка находится в руках мошенников и просит срочно перезвонить по указанному номеру. При перезвоне компьютерный голос вежливо просит пройти сверку данных и ввести с клавиатуры телефона PIN-код пластика. Параллельно преступниками выясняется номер счета, полное имя и адрес держателя, срок действия его пластиковой карты;

9) организация фиктивных пунктов выдачи наличных (ПВН);

10) приобретение реквизитов пластиковых карт (дампы - записи содержимого магнитных лент карт и данные с поверхности карт - номера, сроки действия, имена держателей, CVV) на торговых (электронных) площадках или в кардерских магазинах. По мнению специалистов, средняя стоимость карты в кардерском магазине составляет 20 долларов, покупателям удается украсть деньги лишь с одной из трех карт, средняя сумма хищения - 2 тыс. долларов. Поставщики, собирающие данные карт, в том числе вышеуказанными способами, размещают миллионы записей на таких площадках.

Так, кардерский магазин - Swiped работал с 2008 года и считался одной из крупнейших торговых площадок. По состоянию на май 2014 года на Swiped продавались данные 6,78 млн карт из 148 стран мира. При этом за 2015 г. в магазин были выгружены данные 5,5 млн карт. Исследователи считают, что большую часть их составляют карты, скомпрометированные при взломе крупных американских ретейлеров Target и The Home Depot.

Необходимо отметить, что растущая техническая оснащенность преступников приводит к тому, что их действия приобретают комбинированный характер (использование подлинных платежных карт для изготовления подложных).

Например, после расходования всех доступных по утерянной или украденной карте средств она может быть перепродана «специалистам» по подделке платежных карт для повторного эмбоссирования и/или перезаписи информации на магнитной полосе.

Спегщалъные технические средства (СТС) - средства, предназначенные (разработанные, приспособленные, запрограммированные) для негласного получения (изменения, уничтожения, блокирования) информации, нарушения

работы отдельных компьютеров, компьютерных систем или их сети, к которым относятся:

магнитные материалы и технические устройства, генерирующие направленное электромагнитное излучение;

электромонтажный инструмент и материалы; контрольно-измерительные приборы и устройства; средства систем электросвязи и их компоненты.

Отметим, что анализ следственной практики не позволил выявить факты совершения хищений денежных средств с использованием компьютерных технологий, сопряженных с указанными СТС. Но, данное обстоятельство не свидетельствует о том, что такие средства не могут быть использованы преступниками в целях хищения.

Между тем преступники используют специальные технические устройства, типа Blackbox (хакеры назвали свое устройство ATM Pump), которые позволяют получать деньги из диспенсера банкомата. Данное устройство обладает следующими функциональными возможностями: работа через Wi-Fi; запуск устройства удаленно со специального брелока; работа батареи внутри банкомата до 1 месяца; автоматический запуск с полным удаленным управлением диспенсером.

Само устройство подключается к банкомату следующим способом. После вскрытия корпуса банкомата «родной» шлейф отключался и вместо него подключался один из шлейфов из устройства ATM Pump. «Родной» шлейф, который был отключен, подключался ко второму шлейфу устройства ATM Pump. После того, как устройство успешно устанавливалось, банкомат закрывался.

Таким образом, устройство ATM Pump выступало в качестве промежуточного звена, позволяя преступникам манипулировать диспенсером.

Используя брелок, преступники удаленно управляют устройством, в том числе в нужный момент (когда будет загружен лоток банкомата) дают команду на начало выдачи наличных денежных средств через диспенсер, которые получают соучастники (обналыцики).

Вредоносные программы - любое программное обеспечение, которое предназначено для скрытного (несанкционированного) доступа к персональному компьютеру с целью хищения конфиденциальных данных, а также для нанесения любого вида ущерба, связанного с его использованием.

Существует много классификаций вредоносных программ, однако основная масса из них является чисто техническими, которые не могут быть использованы для решения стоящих перед криминалистикой задач.

Ряд классификаций вредоносных программ приводится и в юридической литературе. Так, В. В. Крылов предлагает классифицировать все вредоносные программы «на базе представлений о цели создания программы и последствиях ее действия»: «безвредные» инфекции, «опасные инфекции», «инфекции проникновения». Последние предназначены «для организации неправомерного доступа к чужим информационным ресурсам («люки» («back door») или «Троянские программы (кони)», «логические бомбы и бомбы с часовым механизмом»)».

Для целей настоящей работы представляется возможным ограничиться выделением следующих видов вредоносных программ: самораспространяющиеся - компьютерные черви, компьютерные вирусы (или вирусы); а также троянские программы (банковские троянские программы), вредоносные утилиты.

Сетевые черви - это вредоносные программы, которые размножаются, но не являются частью других файлов, представляя собой самостоятельные файлы. Сетевые черви могут распространяться по локальным сетям и Интернету (например, через электронную почту).

Особенность червей - чрезвычайно быстрое «размножение». Червь без ведома пользователя может, например, отправить «червивые» сообщения всем респондентам, адреса которых имеются в адресной книге пользователя почтовой программы. Помимо загрузки сети в результате лавинообразного распространения, сетевые черви способны выполнять опасные действия.

Компьютерные вирусы (Вирусы, Virus) - вредоносные программы, обладающие способностью к несанкционированному пользователем саморазмножению по локальным ресурсам компьютера и внедрению своих копий в другие компьютерные программы (напр., Worms and Viruses; Worm; Email-Worm и т.п.), т.е. заражению уже существующих файлов, путем включения своего программного кода или некоторой его части в программный код файлов, системные области или иное рабочее пространство электронных носителей информации, с сохранением всех первоначальных свойств или некоторой их части. Обычно это исполняемые файлы (*.exe, *.cot) или файлы, содержащие микропроцедуры (*.doc, *.xls), которые в результате заражения становятся вредоносными.

Существует значительное число классификаций компьютерных вирусов: по типам объектов, в которые они внедряются (по среде обитания), по способу заражения среды обитания, по деструктивным возможностям, по особенностям функционирования вируса и другие. Многие из них чисто технические и не имеют для криминалистики особого значения.

В отличие от червей, вирусы не используют сетевых сервисов для своего распространения и проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том случае, если заражённый объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например: при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе; вирус скопировал себя на съёмный носитель или заразил файлы на нем; пользователь отослал электронное письмо с зараженным вложением.

Троянские программы (Trojan) - вредоносные программы, предназначенные для осуществления несанкционированных пользователем действий, влекущих уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей, и при всём при этом не попадающая ни под одно из других троянских поведений. Также такие программы могут обеспечить удаленный доступ к компьютерной информации пользователя без его согласия.

К Trojan также относятся «многоцелевые» троянские программы, т.е. программы, способные совершать сразу несколько несанкционированных

пользователем действий, присущих одновременно нескольким другим поведениям троянских программ, что не позволяет однозначно отнести их к тому или иному поведению.

К разновидностям троянских программ относятся Trojan-ArcBomb, Trojan-Banker, Trojan-Clicker, Trojan-DDoS, Trojan-Downloader, Trojan-Dropper, Trojan-GameThief, Trojan-Notifier, Trojan-Proxy, Trojan-Spy, Trojan-PSW (Password-Stealing-Ware), Trojan-Mailfinder и т. п.

Например, Trojan-Banker представляет собой вредоносную программу, предназначенную для кражи пользовательской информации, относящейся к банковским системам, системам электронных денег и пластиковых карт. Найденная информация передается злоумышленнику. Для передачи данных «хозяину» могут быть использованы электронная почта, FTP, HTTP (посредством указания данных в запросе) и другие способы. Trojan-Notifier -для несанкционированного пользователем сообщения своему «хозяину» о том, что заражённый компьютер сейчас находится «на связи». При этом на адрес преступника отправляется информация о компьютере, например, IP-адрес компьютера, номер открытого порта, адрес электронной почты и т.п. Отсылка осуществляется различными способами: электронным письмом, специально оформленным обращением к веб-странице злоумышленника, ICQ-сообщением. Trojan-Spy - для ведения электронного шпионажа за пользователем (вводимая с клавиатуры информация, снимки экрана, список активных приложений и т.д.). Найденная информация передается преступнику. Для передачи используются электронная почта, FTP, HTTP (посредством указания данных в запросе) и другие способы. Trojan-Mailfinder - для несанкционированного пользователем сбора адресов электронной почты на компьютере с последующей передачей их злоумышленнику через электронную почту, HTTP, FTP или другими способами. Похищенные адреса используются преступниками при проведении последующих рассылок вредоносных программ и спама.

Банковские троянские программы - это вредоносные программы, предназначенные для похищения конфиденциальной информации и обеспечения несанкционированного доступа к банковской информационной системе (напр., системе ДБО). Многие банковские трояны сочетают в себе функции бэкдора и шпионских программ.

Наиболее распространенными методами проникновения банковских троянских программ в операционную систему, являются их загрузка на компьютер жертвы:

1) другими вредоносными программами - троянами-загрузчиками;

2) при просмотре инфицированных веб-страниц (с использованием различных уязвимостей прикладного программного обеспечения);

3) при открытии вложений, содержащихся в сообщениях массово рассылаемые по каналам электронной почты, на инфицированных съемных носителях;

4) с использованием методов социальной инженерии.

Банковские троянские программы условно можно разделить на управляемые и неуправляемые.

Неуправляемые троянские программы - являются самыми простыми вредоносными программами. После их установки в компьютере потерпевшего они не ждут команд с сервера преступника, их нельзя обновить до более новой версии или использовать их для установки других вредоносных программ. Такие программы используются для совершения хищений у физических лиц.

Управляемые троянские программы - являются наиболее распространёнными и сложными. Их постоянное использование требует поддержки со стороны их авторов, которые обладают высоким уровнем программирования. В некоторых случаях автор вредоносной программы может входить в состав преступной группы, тогда вредоносная программа может использоваться только одной преступной группой. После установки в компьютере потерпевшего вредоносная программа обязательно сообщает о своей успешной установке на сервер, управляемый преступником. Постоянное взаимодействие вредоносной программы с сервером управления дает возможность преступнику управлять этой программой, например, обновлять ее в случае обнаружения средствами антивирусной защиты, выполнять команды на компьютере пользователя, загружать модули, расширяющие функционал вредоносной программы. Модуля вредоносной программы могут разрабатываться другими авторами, например, для работы со специфичными для конкретного региона системами ДБО кредитных организаций.

Типичными видами семейства банковских троянских программ являются: Trojan. Carberp; Trojan.PWS.Ibank; Trojan.PWS.Panda (также известен как Zeus и Zbot); Troj an.PWS. Spy Sweep (также известен как SpyEye). Для мобильной платформы Android банковским трояном является Android.SpyEye.

По данным компании «Лаборатории Касперского» TOP 10 семейств вредоносных программ, использованных для атак на пользователей онлайн-банкинга в 2015 году, состоит из Trojan-Downloader.Win32.Upatre, Trojan-Spy. Win32.Zbot, Trojan-Banker.Win32.ChePro, Trojan-Banker.Win32.Shiotob, Trojan-Banker.Win32.Banbra, Trojan-Banker. Win32.Caphaw, Trojan-Banker.AndroidOS.Faketoken, Trojan-Banker. AndroidOS.Marcher, Troj an-Banker. Win32.Tinba и Troj an-Banker. J S. Agent.

Подавляющее большинство семейств вредоносных программ, попавших в TOP 10, используют классическую для банковских троянцев технику внедрения произвольного HTML-кода в отображаемую браузером веб-страницу и последующего перехвата платежных данных, вводимых пользователем в оригинальные и добавленные троянцем веб-формы.

Основной задачей банковских троянцев является компрометация платежных данных пользователей систем онлайн-банкинга и модификации содержимого банковских веб-страниц.

Некоторые банковские троянцы используют несколько уровней шифрования своих конфигурационных файлов и при этом сам расшифрованный файл конфигурации не хранится в памяти целиком, а загружается по частям (например, Trojan-Spy.Win32.Zbot).

Некоторые банковские троянцы позволяют делать снимки экрана, регистрировать клавиатурные нажатия и читать содержимое буфера копирования, т.е. имеют функционал, дающий возможность использовать

вредоносную программу для атаки практически на любые системы онлайн-банкинга (например, Trojan-Banker.Win32.ChePro).

Специализированные вредоносные программы семейства Faketoken и Marcher предназначены для компрометации платежных данных с мобильных устройств под управлением операционной системы Android.

Вредоносные программы семейства Trojan-Banker.AndroidOS.Faketoken работают в паре с компьютерными банковскими троянцами. Для их распространения киберпреступники используют технологии социальной инженерии: когда клиент банка с зараженного компьютера посещает страницу онлайн-банкинга, троянская программа модифицирует эту страницу, предлагая загрузить Android-приложение, которое якобы будет защищать транзакции. На самом деле ссылка ведет на вредоносное приложение Faketoken. После того как такая программа оказывается на смартфоне жертвы, преступники через зараженный банковским троянцем компьютер пользователя получают доступ к банковскому счету, а зараженное мобильное устройство позволяет им перехватывать одноразовый пароль двухфакторной аутентификации (mTAN).

Вредоносные программы семейства мобильных банковских троянцев -Trojan-Banker. AndroidOS.Marcher, заразив мобильное устройство, отслеживают запуск всего двух приложений: клиента мобильного банкинга одного из европейских банков и Google Play. В случае если пользователь входит в магазин Google Play, Marcher демонстрирует пользователю фальшивое окно для ввода данных о платежной карте, которые затем попадают к преступникам. Аналогичным образом троянская программа действует и в случае открытия пользователем банковского приложения.

Использование в преступных целях банковских троянских программ возможно по следующим причинам:

ежедневное появление (создание) большого количества новых банковских троянов, системы защиты которых становятся все более совершенными. Так, преступники нередко используют различные файловые упаковщики для избегания обнаружения антивирусными программами. Таким образом, одновременно может существовать до нескольких сотен образцов одного и того же опасного приложения, отличающихся только способом упаковки исполняемого файла. В результате банковский троян может проникнуть в операционную систему, если в вирусных базах пока еще отсутствует сигнатурная запись для какой-либо отдельной его модификации;

перед выпуском (использованием) банковские троянцы тестируются на актуальных антивирусах, в связи с чем некоторое время после релиза не обнаруживаются ими. Этого времени достаточно для похищения денежных средств;

разработка все более изощренных путей распространения вредоносных программ, в том числе с применением методов социальной инженерии, а также с использованием уязвимостей прикладного программного обеспечения (например, пакета уязвимостей BlackHole Exploit Kit различных версий). При отсутствии достаточных мер для обеспечения защиты компьютера, момент заражения может остаться для пользователя незамеченным;

непринятие пользователями мер информационной безопасности. Использование банковских троянских программ позволяет преступникам:

похищать сертификаты систем защищенного документооборота и паролей от программ с целью обеспечения несанкционированного доступа к банковским компьютерным системам (напр., система ДБО) и торговым платформам (напр., Trojan.Carberp, Trojan.PWS.Panda);

осуществлять перевод денежных средств на счета, подконтрольные им через системы ДБО;

похищать конфиденциальную информацию (напр., Trojan .PWS. SpySweep, Android. SpyEye);

перехватывать данные нажатия клавиш или вводимые с использованием экранной клавиатуры, создание снимков экрана и т. п.;

включать (встраивать) зараженные компьютеры в систему управления ботнета, координируемые из одного (или нескольких) командных центров (Trojan.Carberp);

запускать и удалять различные программы на инфицированном компьютере (Trojan.Carberp, Trojan.PWS.SpySweep, Trojan.PWS.Panda);

выполнять на инфицированном компьютере поступающие из удаленного центра команды, в том числе команды на удаление операционной системы.

Банковские троянские программы обладают развитым вредоносным функционалом. Например, трояны семейства Trojan. Carberp имеют функционал по приему команд от управляющего центра, способны служить прокси-сервером, с помощью которого преступники могут анонимно работать в сети Интернет.

Прокси-сервер (от англ. Proxy - «представитель, уполномоченный») - сервер (комплекс программ) в компьютерных сетях, позволяющий клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-сервер} и запрашивает какой-либо ресурс (например, e-mail), расположенный на другом сервере.

Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэща - промежуточный буфер с быстрым доступом, содержащий информацию, которая может быть запрошена с наибольшей вероятностью (в случаях, если прокси имеет свой кэш). В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях. Прокси-сервер позволяет защищать компьютер клиента от некоторых сетевых атак и помогает сохранять анонимность клиента

Таким образом, банковские троянские программы на современном этапе обеспечивают преступникам возможности удаленно на компьютере жертвы осуществлять: встраивание в отображаемую в браузере веб-страницу постороннего содержимого, в частности, полей форм (веб-инжекты); похищение файлов cookies((от англ. Cookie - печенье) - небольшой фрагмент данных, отправленный веб-сервисом и хранимый на компьютере пользователя. Веб-клиент (обычно веб-браузер) всякий раз при попытке открыть страницу соответствующего сайта пересылает этот фрагмент данных веб-серверу в составе HTTP-запроса. Применяется для сохранения данных на стороне пользователя, на практике обычно используется для: аутентификации пользователя; хранения персональных предпочтений и настроек пользователя; отслеживания состояния); установку в

инфицированную систему поддельных цифровых сертификатов; запись нажатий пользователем клавиш; перехват и анализ сетевого трафика; создание и передачу снимков экрана; перехват и передачу изображения с подключенной к компьютеру веб-камеры; перехват и передачу аудиопотока с подключенного к компьютеру микрофона; перехват сохраненных в системе паролей; встраивание в процессы программ системы «Банк-Клиент» (Trojan.Carberp).

При этом банковские троянские программы обладают функционалом маскировки от средств контроля и наблюдения, а именно: отслеживание запущенных в инфицируемой системе приложений-отладчиков, средств виртуализации, брандмауэров и антивирусных программ; завершения процессов антивирусных программ и брандмауэров ((межсетевой экран или сетевой экран) - комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях в соответствии с заданными правилами); противодействие попыткам запуска процессов антивирусных программ в инфицированной системе; блокировка доступа пользователей к веб-сайтам компаний-производителей антивирусного программного обеспечения и сайтам, распространяющим обновления систем безопасности; шифрование вирусными упаковщиками.

Вредоносные утилиты - вредоносные программы, разработанные для автоматизации создания других вирусов, червей или троянских программ, организации DoS-атак на удаленные сервера, взлома других компьютеров и т.п. В отличие от вирусов, червей и троянских программ, представители данной категории не представляют угрозы непосредственно компьютеру, на котором исполняются. Например, Constructor представляет собой программы, предназначенные для изготовления новых компьютерных вирусов, червей и троянских программ. Подобные программы позволяют генерировать исходные тексты вредоносных программ, объектные модули и непосредственно зараженные файлы. Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вредоносной программы, наличие или отсутствие самошифровки, противодействие отладчику и т.п.

HackTool - для организации атак на локальный или удаленный компьютер (например, несанкционированное пользователем внесение нелегального пользователя в список разрешенных посетителей системы; очистка системных журналов с целью сокрытия следов присутствия в системе; снифферы с выраженным вредоносным функционалом и т.д.).

Hoax (вирусные мистификаторы) - для вывода сообщения о том, что якобы причинен вред компьютеру пользователя, либо будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности.

Exploit - для использования одной или нескольких уязвимостей в программном обеспечении на локальном или удаленном компьютере с заведомо вредоносной целью. Обычно эксплойты используются злоумышленниками для проникновения на компьютер-жертву с целью последующего внедрения туда вредоносного кода (например, заражение всех посетителей взломанного веб-сайта вредоносной программой). Также эксплойты интенсивно используются

программами типа Net-Worm для проникновения на компьютер-жертву без участия пользователя.

Широко известны также так называемые программы-Nuker, которые отправляют на локальный или удаленный компьютер специальным образом сформированные запросы, в результате чего система прекращает свою работу.

VirTool - для модификации других вредоносных программ таким образом, чтобы они не детектировались антивирусным программным обеспечением.

К программам, обеспечивающим функционирование вредоносных программ, можно отнести Rootkit, Backdoor и др. Так, Rootkit представляет собой программу, предназначенную для сокрытия в системе определенных объектов, либо активности. Сокрытию, как правило, подвергаются ключи реестра (например, отвечающие за автозапуск вредоносных объектов), файлы, процессы в памяти зараженного компьютера, вредоносная сетевая активность. Сам по себе Rootkit ничего вредоносного не делает, но данный тип программ, в подавляющем большинстве случаев, используется вредоносными программами для увеличения собственного времени жизни в пораженных системах в силу затрудненного обнаружения. Backdoor - для скрытого удалённого управления пораженным компьютером. По своей функциональности бэкдоры во многом напоминают различные системы администрирования, разрабатываемые и распространяемые фирмами-производителями программных продуктов. Эти вредоносные программы позволяют производить штатные операции: принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т.д. Представители этого типа вредоносных программ очень часто используются для объединения компьютеров-жертв в так называемые «ботнеты», централизованно управляемые преступниками.

Новым орудием подготовки хищения денежных средств являются «прокси программы». Так, если в ходе стандартных фишинговых атак преступники вынуждены создавать реалистичную копию легитимного web-сайта, пользователей которого они намерены скомпрометировать, то специальная «прокси программа» позволяет ретранслировать трафик между web-сайтом и жертвой, а также управлять отображаемым контентом независимо от используемого устройства (персональный компьютер, ноутбук, смартфон, планшет) или браузера. Таким образом, пока потенциальная жертва лишь просматривает ресурс, она видит его оригинальное содержание. Как только осуществляет покупку, упомянутая «прокси программа» перенаправляет его на поддельную страницу, где и происходит компрометация конфиденциальных данных.

Ботнет (бот-сети) - это сеть компьютеров, зараженных вредоносной программой, позволяющая преступным группировкам удаленно управлять зараженными компьютерными устройствами без ведома пользователя. Так, например, в 2011 году, была выявлена группа бот-сетей на основе троянской программы «Оригами». В середине года суммарное количество ботов в этих сетях превышало 2 500 ООО штук. К концу года сети были отключены владельцами, а боты из них переведены в сети на основе троянской программы «Карберп». В мае 2012 г. часть членов группы, работавшей с бот-сетями «Оригами», были задержаны сотрудниками УЭБиПК ГУ МВД России по г. Москве.

В июне 2012 г. сотрудниками Управления «К» БСТМ МВД России был задержан владелец ряда крупнейших бот-сетей на основе вредоносной троянской программы «Карберп» различных модификаций. Общая сумма ботов в этих сетях на момент их отключения сотрудниками полиции превышала 5 500 000 штук. 95% из этих ботов находились на территории России.

На более чем 20 000 из них были обнаружены средства или следы доступа к различным системам дистанционного банковского обслуживания или виртуальным счетам разных типов. «Проработкой» этих компьютеров занимались полтора десятка партнеров организатора. Поступление новых зараженных компьютеров в бот-сети обеспечивалось группой профессиональных продавцов «трафика», и в отдельные дни в сети поступало до 30 000 новых ботов, а ежедневные расходы на эти цели превышали 10-20 тысяч долларов США. В конце 2012 г. по сведениям сотрудников компании «Доктор Веб» другими преступными группами продолжали использоваться не менее двух сетей на основе троянской программы «Карберп», к каждой из которых было «привязано» более 1 000 000 зараженных компьютеров.

Банковские бот-сети состоят из следующих элементов: вредоносная программа; панель управления бот-сетью; билдер для создания исполняемых файлов вредоносной программы с заданными настройками; связка эксплойтов, которая будет использоваться для установки вредоносной программы пользователям; трафик; арендованные серверы для установки различных панелей управления; доменные имена для настройки вредоносных программ; серверы-прокладки, которые будут использоваться для скрытия реального местонахождения сервера управления бот-сетью; крипт-шифрование вредоносной программы и связки для обхода средств обнаружения средств антивирусной защиты.

Процесс создания бот-сети включает несколько этапов подготовки ее инфраструктуры.

После разработки или покупки вредоносной программы у преступника могут быть следующие составляющие: панель управления и билдер76, либо вместо билдера сам экземпляр вредоносной программы. Если автор вредоносной программы не выдал покупателю билдер, то каждый раз, когда будет требоваться перенастройка вредоносной программы, покупатель будет вынужден обращаться к автору.

При использовании троянской программы, будь она управляемой или неуправляемой, происходит взаимодействие с удаленным сервером. Управляемая троянская программа взаимодействует с сервером, на котором установлена панель управления, а неуправляемая - с сервером, на котором находится фишинговый сайт.

Фишинговый сайт - сайт, который полностью или частично копирует дизайн другого сайта, с целью хищения конфиденциальных данных пользователя (логин, пароль, номер счета, почтовый адрес и т. д. Создают фишинговые сайты, например, для сайтов известных мобильных операторов (Мегафон, Билайн, МТС, Yota и др.), для банковских сайтов (Сбербанк, ВТБ24 и т. д.), для социальных сетей (ВКонтакте, Одноклассники и др.), для сайтов электронных денег (Яндекс.Деньги, WebMoney и т. д.), для известных порталов (РЖД, Apple, Avito) и другие варианты.

Поэтапно процесс подготовки инфраструктуры может быть представлен следующим образом:

1 этап: покупка сервера под панель управления;

2 этап: покупка доменных имен;

3 этап: настройка серверов прокладок - это серверы, которые стоят перед серверами управления и используются для сокрытия их реальных IP-адресов;

4 этап: создание (сборка) троянской программы - преступник указывает в файле настроек вредоносной программы необходимые параметры;

5 этап: крипт троянской программы - после того, как исполняемый файл создан перед его распространением его необходимо зашифровать (сделать ее крипт).

Преступники используют ботнеты (бот-сети) для решения следующих задач по подготовке и сокрытию фактов хищений денежных средств:

загрузка и установка на инфицированный компьютер по команде с удаленного сервера других вредоносных программ;

осуществление DDoS-атак (Distributed Denial-of-Service) на отдельные сайты и веб-сервисы. Сетевые атаки могут использоваться в целях вымогательства, давления на конкурентов, дискредитации перед потенциальными клиентами.

удаленное управление инфицированными компьютерами, возможность хищения хранящихся на локальных дисках файлов;

хищение конфиденциальной информации методом анализа трафика, осуществления веб-инжектов, похищения файлов cookies, кейлоггинга (перехвата нажатий клавиш), пересылки снимков экрана, иных методов (Win32.Rmnet.12, Win32. Rmnet.16);

хищение информации для доступа к системам ДБО (Trojan.PWS.Panda, Trojan.Carberpj:

перенаправление браузера пользователя на принадлежащие преступникам веб-страницы, в том числе для фишинга, загрузки на компьютер пользователя вредоносной программы с использованием уязвимостей;

использование инфицированных компьютеров в качестве прокси-серверов для анонимизации доступа преступников в сети Интернет. С помощью инфицированного компьютера, преступники могут:

установить на этом компьютере необходимую для себя программу (в том числе вредоносную);

просматривать любые хранящиеся на компьютере файлы и совершать с ними различные действия;

использовать данный компьютер в качестве промежуточного узла при работе в сети Интернет, а также совершать различные противоправные действия, в том числе хищения денежных средств с банковских счетов. В файлах журналов атакованных узлов при этом останется IP-адрес инфицированного компьютера;

перехватывать пароли от различных приложений, FTP-клиентов, интернет-сервисов, служб электронной почты;

получать снимки экрана и перехватывать изображение с подключенной к компьютеру веб-камеры;

анализировать и перенаправлять сетевой трафик с различными целями. Перенаправление может происходить в зависимости от заданных условий и от введенных пользователем поисковых запросов;

подменять открываемые в браузере веб-страницы, в том числе для получения несанкционированного доступа к системам ДБО;

отдавать установленной на таком компьютере вредоносной программе различные команды;

полностью уничтожить операционную систему компьютера. К типичным способам инфицирования (заражения) компьютеров относятся:

саморепликации вредоносной программы - самостоятельное (без участия пользователя) копирование вредоносной программы на сменные носители и общедоступные ресурсы локальной сети с заражением исполняемых файлов, динамических библиотек и других типов файловых объектов. Подобным образом распространяются файловые вирусные программы, такие как Win32.Rmnet.16 или Win32.Rmnet.12; инфицирование компьютера другими вредоносными программами (Backdoor.Andromeda. 22);

инфицирование компьютера при посещении пользователем зараженных веб-сайтов и в момент просмотра веб-страниц, содержащих известные уязвимости браузеров или операционной СНСТеМbi(Backdoor.Flashback.39);

инфицирование компьютера при открытии вложений в сообщения электронной почты, полученные в спам-рассылке;

инфицирование компьютера при помощи методов социальной инженерии. Например, для просмотра размещенного на сайте видеоролика пользователю предлагается загрузить кодек или обновление, под видом которого распространяется вредоносная программа;

инфицирование компьютера посредством специально «забытых» и заранее инфицированных электронных носителей информации (флешки и т. п.).

Некоторые вредоносные программы могут использовать следующие методы противодействия их обнаружению:

Антиотладка, при которой вредоносная программа определяет, не запущена ли она в виртуальной машине, не загружен ли на инфицируемом компьютере отладчик или антивирусная программа (например, методом перечисления запущенных процессов);

руткит-технологии (специальные драйверы файловой системы), использование которых позволяет вредоносной программе скрыть присутствие своих компонентов на диске зараженного компьютера;

заражение главной загрузочной записи (MBR), хранение компонентов за пределами таблиц разделов позволяет вредоносным программам инфицировать главную загрузочную запись (MBR) и сохранять свои компоненты в свободной области дискового пространства. Получив управление в процессе загрузки операционной системы, такая программа считывает хранящиеся за пределами файловых таблиц модули непосредственно в оперативную память инфицированного компьютера;

исполнение в контексте других запущенных процессов (встраивание вредоносных программ в запущенные процессы и функционирование их «внутри» данных процессов);

обфускация и криптование позволяет вредоностной программе сбить сигнатурный детект путем шифрования ее тела с использованием различных программных упаковщиков. Иногда насчитывается до нескольких сотен зашифрованных различными упаковщиками модификаций одной и той же вредоносной программы.

организация шифрованного виртуального диска (BackDoor.Tdss); блокировка и обход файерволов обеспечивает беспрепятственное получение управляющих сообщений, в том числе использование протокола SOCKS для получения доступа к сервисам;

постоянное изменение реальных адресов управляющего сервера, генерация доменных имен по псевдослучайному принципу, благодаря этому все ботнеты одновременно формируют один и тот же перечень имен и обращаются к ним.

Методы перехвата информации с использованием вредоносных программ:

перехват нажатий клавиш и получение скриншотов в реальном времени - для перехвата ввода с виртуальной клавиатуры;

получение скриншота в области экрана, где была нажата левая кнопка мыши, после захода на нужный URL;

анализ трафика и перехват интересующих данных; получение любых импортируемых сертификатов, или использованных при удачной авторизации логинов/паролей; перехват HTTP/HTTPS запросов;

анализ и подмена страниц, используемых для ввода банковской информации. Кража TAN-кода (кода активации для проведения платежной операции);

анализ передаваемых (POST) на определенные адреса данных; получение данных из буфера обмена;

поиск интересующих файлов и данных с дальнейшим их удалением или закачкой на удаленный сервер;

анализ файлов cookie (данных, связанных с определенным вебсервером и хранимых на компьютере) и данных сохраненных форм; веб-инжекты (встраивание в веб-страницы постороннего кода); сбор и отправка на удаленный сервер информации о программно-аппаратной конфигурации компьютера.

Способы хищения денежных средств, совершаемых с использованием компьютерных технологий

Значение способа хищений рассматриваемого вида исключительно велико. Как было отмечено, способ хищений детерминирован предметом преступного посягательства, а точнее его формой (безналичные денежные средства), доступ к которой обеспечивается автоматизированной информационной системой кредитной организации.

Давая общую характеристику способам хищений денежных средств, совершаемых с использованием компьютерных технологий, следует отметить, что они представляют собой систему целенаправленных взаимосвязанных действий (операций), направленных на подготовку, совершение и сокрытие преступления данного вида.

В зависимости от разновидности хищений денежных средств, совершаемых с использованием компьютерных технологий, различаются способы их подготовки, совершения и сокрытия.

Способами подготовки рассматриваемого вида хищений могут быть: уничтожение компьютерной информации; блокирование компьютерной информации; создание компьютерных программ; модификация компьютерных программ; неправомерный доступ к компьютерной информации; использование компьютерных программ либо иной компьютерной информации, в том числе заведомо предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшие уничтожение, блокирование, модификацию либо копирование компьютерной информации;

аппаратная модификация - модификация устройств для их использования в неправомерном получении конфиденциальной компьютерной информации (модификация мобильных телефонов, кредитных карточек, POS-терминалов, банкоматов, систем спутниковой связи, кассовых аппаратов и т. п.).

Отметим, что дифференциация способов подготовки хищений денежных средств, совершаемых с использованием компьютерных технологий, является условной, так как нередко реализация одного способа напрямую связана с реализацией другого. С учетом данного обстоятельства рассмотрим некоторые из перечисленных способов подготовки таких хищений.

Характеризуя способы неправомерного доступа к компьютерной информации (банковским счетам или системам управления банковскими счетами), как способы подготовки хищения денежных средств, совершаемых с использованием компьютерных технологий, отметим, что в большинстве случаев программное обеспечение любой системы, функционирующей в компьютерных устройствах, состоит из трех основных компонентов: операционной системы (ОС), сетевого программного обеспечения (СПО) и системы управления базами данных (СУБД). В зависимости от этого исследователи выделяют три соответствующих вида метода неправомерного (несанкционированного) доступа (НСД): на уровне операционной системы; на уровне сетевого программного обеспечения; на уровне систем управления базами данных. Также возможен и комбинированный способ НСД.

В криминалистической литературе можно обнаружить следующие три способа НСД: непосредственный, опосредованный и смешанный.

Первая группа - это способы непосредственного доступа к такой информации, осуществляемые пользователем компьютера (например, работник индивидуального предпринимателя (бухгалтер), кредитной организации или

иного юридического лица), а также иными лицами (например, сослуживцы пользователя компьютером и т. п.). В последнем случае способ доступа к компьютерной информации связан, в том числе, с использованием технических отходов информационного процесса, оставленных пользователем после работы с компьютером. Такие отходы могут быть получены путем обследования рабочих мест пользователей компьютерами, подключенными к автоматизированной банковский информационной системе, содержимого мусорных баков, емкостей для технологических отходов для сбора оставленных или выброшенных физических носителей информации, а также обследования различной документации, оставленной на рабочих и в иных местах (ежедневников, книг рабочих записей, перекидных календарей и т. п.) в целях поиска черновых записей, паролей доступа в систему и т. п., а также путем просмотра и последующего исследования данных, находящихся в памяти компьютера, в том числе с использованием специальных программных комплексов восстановления стертых файлов (напр., программный комплекс PC Tools Deluxe).

Отметим, что использование технических отходов информационного процесса не является типичным для способов неправомерного доступа компьютерной информации, как способов подготовки хищения денежных средств, совершаемых с использованием компьютерных технологий.

Вторая группа - способы опосредованного (удаленного) доступа к компьютерной информации. В данном случае неправомерный доступ к определенному компьютеру и находящейся на нем информации осуществляется с другого компьютера, находящегося на определенном расстоянии, через компьютерные сети. Способы опосредованного доступа к компьютерной информации, в свою очередь, можно разделить на две подгруппы: способы преодоления парольной, а также иной программной или технической защиты, и последующего подключения к чужой системе; способы перехвата информации.

Преодоление парольной, а также иной программной или технической защиты, и последующее подключение к чужой системе, преступниками осуществляется путем подключения к линии связи законного пользователя (например, к телефонной линии) и получения тем самым доступа к его системе. Подключившись, преступник дожидается сигнала, означающего окончание работы, перехватывает его «на себя», а потом, когда законный пользователь закончил сеанс работы, осуществляет доступ к его системе. Данный способ сравним с работой двух параллельных телефонных аппаратов, подключенных к одному абонентскому номеру: если один телефон находится в активном режиме (ведется разговор с абонентом) и на другом аппарате поднимается трубка, то когда разговор по первому телефону закончен и трубка положена, он может быть продолжен по второму.

Проникновение в чужие информационные сети путем автоматического перебора абонентских номеров с последующим соединением с тем или иным компьютером (перебор осуществляется до тех пор, пока на другом конце линии не «отзовется» чужой компьютер). Поскольку в подобном случае один несанкционированный пользователь может быть легко обнаружен, подобный «электронный взлом» осуществляется одновременно с нескольких рабочих мест: в заданное время несколько (более десяти) персональных компьютеров одновременно предпринимают попытку несанкционированного доступа. Это может привести к тому, что несколько «атакующих» компьютеров отсекаются

системой защиты, а остальные получают требуемый доступ. Один из «прорвавшихся» компьютеров блокирует систему статистики сети, которая фиксирует все попытки доступа. В результате этого другие «прорвавшиеся» компьютеры не могут быть обнаружены и зафиксированы. Часть из них приступает к «взлому» нужного сектора сети, а остальные занимаются фиктивными операциями в целях дезорганизации работы компьютерной системы и сокрытия преступления.

Проникновение в компьютерную систему с использованием чужих паролей, выдавая себя за законного пользователя. При подобном способе незаконный пользователь осуществляет подбор пароля для доступа к чужому компьютеру. Подбор паролей может осуществляться двумя методами.

Первый: подбор паролей путем простого перебора всех возможных сочетаний символов до тех пор, пока не будет установлена нужная комбинация. Для реализации такого подбора существуют уже специально разработанные программы, которые можно приобрести на «черном» компьютерном рынке. Алгоритм их действия основан на использовании быстродействия современных компьютеров при переборе всех возможных комбинаций букв, цифр и автоматического соединения специальных символов, имеющихся на стандартной клавиатуре персонального компьютера, и в случае совпадения комбинации символов с оригиналом произведения.

Второй: «интеллектуальный» подбор паролей на основе имеющихся «словарей» наиболее распространенных паролей, систематизированных по определенным тематическим группам. При этом наиболее распространенными тематическими группами паролей являются следующие: имена, фамилии и производные от них; последовательность клавиш компьютера, повтор символов; даты рождения пользователя и его близких, а также их комбинации; интересы, хобби (9,5 %); адрес, место рождения; номера телефонов или документов: паспортов, удостоверений личности и пр.

Подобрав необходимый пароль (для подбора восьмизначного пароля требуется несколько часов), незаконный пользователь получает доступ к компьютерной информации и может проводить с ней любые действия под видом законного пользователя: копировать ее, модифицировать, удалять, заставлять программы производить требуемые операции, например, по переводу денежных средств на свои счета, фальсификации платежных документов и пр.

Разновидностью способа получения пароля для последующего незаконного вхождения в компьютерную систему является так называемый социальный инжиниринг («обратный социальный инжиниринг»). Это метод основан на недостаточной бдительности пользователей, когда информация получается в процессе беседы (телефонной, посредством обмена электронными сообщениями) преступников с пользователями системы. При этом способе правонарушитель представляется либо системным администратором, либо сотрудником обслуживающей компьютерной фирмы, либо сотрудником, вновь поступившим на работу, и запрашивает у собеседника данные о паролях доступа к системе.

Данный способ широко применяется для получения данных (имя, пароль) в целях подключения к компьютерной сети Интернет за счет законных пользователей.

Ко второй подгруппе относятся способы опосредованного (удаленного) доступа к компьютерной информации (электромагнитный и другие виды перехвата).

Непосредственный перехват осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного «подслушивания» являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи.

Электромагнитный перехват. Современные технические средства позволяют получить информацию без непосредственного подключения к компьютерной системе: за счет перехвата излучений центрального процессора, дисплея, коммуникационных каналов, принтера и т. д. Все это можно осуществить, находясь на достаточном удалении от объекта перехвата. Например, используя специальную аппаратуру, можно «снимать» информацию с компьютера, расположенного в соседнем помещении, здании.

К методам перехвата информации относится также аудиоперехват и видеооптический перехват.

Аудиоперехват, или снятие информации по вибро-акустическому каналу, имеет две разновидности: заходовую (заносную) и беззаходовую.

Третью группу способов подготовки совершения рассматриваемых хищений составляют смешанные способы, которые могут осуществляться как путем непосредственного, так и опосредованного (удаленного) доступа. К числу таких способов относятся тайное введение в чужую программу таких команд, которые помогают ей осуществить новые, незапланированные разработчиком функции при одновременном сохранении прежней ее работоспособности. Данный способ может иметь две разновидности. В первом случае программные модули-фрагменты, которые создают троянскую программу, то есть незапланированное разработчиком программное обеспечение, самоликвидируются по окончании исполнения своей задачи. Найти после этого данные программные модули практически невозможно. Во втором случае в алгоритм программы, наряду с ее основными функциями, закладывается алгоритм действий, осуществляющих саморазмножение, автоматическое самовоспроизводство указанной троянской программы. В результате подобные «программы-черви» автоматически копируют себя в памяти одного или нескольких компьютеров (при наличии компьютерной сети).

Модификация программ путем тайного встраивания в программу набора команд, которые должны сработать при определенных условиях через определенное время. Например, как только программа незаконно перечислит денежные средства на банковский счет, подконтрольный преступнику, она самоуничтожится и при этом уничтожит всю информацию о проделанной операции.

Осуществление доступа к базам данных и файлам законного пользователя путем нахождения слабых мест в системах защиты. При их обнаружении появляется возможность читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости.

Использование ошибок в логике построения программы и обнаружение «брешей». При этом программа «разрывается» и в нее вводится необходимое число определенных команд, которые помогают ей осуществлять новые, незапланированные функции при одновременном сохранении прежней ее работоспособности. Именно таким образом можно переводить деньги на банковский счет, подконтрольный преступнику.

В последние годы наиболее распространенным смешанным способом доступа к компьютерной информации как способом подготовки к хищению денежных средств, совершаемых с использованием компьютерных технологий, является направление на электронную почту потерпевшего различных писем. Так, на электронную почту коммерческих организаций, индивидуальных предпринимателей направляются преступниками письма с вложенными файлами якобы от имени налоговых и иных контролирующих органов, контрагентов и партнеров. В то же время на электронную почту работников коммерческого банка могут быть направлены сообщения с вложенными файлами якобы от Банка России.

Сущность данного способа неправомерного доступа к компьютерной информации заключается в компьютерной атаке типа Man-in-the-Middle, направленной на кражу информации, перехват текущей сессии и получение доступа к частным сетевым ресурсам, для анализа трафика и получения информации о сети и ее пользователях. Данные атаки возможны при наличии у преступника доступа к пакетам, передаваемым по сети. Такой доступ ко всем пакетам, передаваемым от провайдера в любую другую сеть, может, к примеру, получить сотрудник этого провайдера. Для атак данного типа часто используются снифферы пакетов, транспортные протоколы и протоколы маршрутизации.

Для примера можно привести сетевую атаку, состоявшуюся 15-16 марта 2016 г.

В ночь с 14 на 15 марта 2016 г. преступники при помощи доменного регистратора REG.ru зарегистрировали два домена (fincert.net и view-atdmt.com). Физически IP-адрес 31.184.234.204 сервера, на котором был размещен домен, находился на хостинге в Санкт-Петербурге.

Около 12 ч. 15 марта с адреса info@fincert.net преступники разослали письма банковским работникам, многие их которых не обратили внимание на тоА что вместо настоящего адреса, с которого Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT) присылает письма (fincert@cbr.ru), письмо пришло совсем с другого. Письма рассылались с адреса info@fincert.net (IP: 194.58.90.56), в то время как настоящий адрес FinCERT - fincert@cbr.ru.

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT) - структурное подразделение главного управления безопасности и защиты информации Банка России (ГУБиЗИ). FinCERT осуществляет сбор информации от финансовых учреждений о кибератаках, анализирует полученные сведения и дает обратную связь кредитно-финансовым организациям о возможных угрозах информационной безопасности, разрабатывает рекомендации по отражению хакерских атак.

Отметим, что преступники хорошо были осведомлены об именах и фамилиях работников коммерческих банков, которым направили письма (очевидно, имея

доступ к специальной базе, возможно составленной из материалов отраслевых конференций или каких-то служебных документов ряда банков), в названии файла-вложения использован цифровой код «20160314 - 001» - именно такой код использует FinCERT для уведомлений об атаках, а сам скачиваемый, после открытия файла-вложения (DOC-файла) при помощи макрос (вредоносная программа), файл fincert.cab был подписан легальным цифровым сертификатом московской транспортной компании «СПЕК-2000».

Макрос (от англ. macros, ед. ч. — macro) — программный объект, при обработке «развёртывающийся» в последовательность действий и/или команд.

Данные обстоятельства, с учетом убедительного доменного имя (fincert.net), удачного времени рассылки письма (предобеденное или обеденное время), свидетельствуют о хорошей (квалифицированной) подготовке преступников (наличия баз данных с персональными данными работников коммерческих организаций и т. п.).

В вежливой форме (назвав получателя по имени и отчеству), преступники предлагали скачать DOC-файл из вложения к письму, в котором якобы находится «важная информация касательно компрометации банковских систем».

Несмотря на внимательность и вежливость, преступники только один раз из трех смогли правильно написать слово «компрометация» — в оставшихся двух всплывала явно лишняя буква «н».

Между тем в файле находилась инструкция для запуска встроенного в него же VBA макроса «NewMacros», исполнение которого как раз и приводило к компрометации банковских систем.

При запуске макроса происходит попытка соединения с удаленным ресурсом http://view-atdmt[.]com для загрузки оттуда файла fincert.cab (MD5 8ac7alfb84357ed82cf99e53d9d89dal).

Файл размером 3 252 624 байта представляет собой самораспаковывающийся NSIS архив. При этом файл подписан легальной цифровой подписью московской компании «СПЕК-2000».

Подпись валидна, и файл был ею подписан 15 - 02 c3 01 £2 63 11 cб ce f5 02 9b 69 92 f7 3f ae) был создан в декабре 2015 года и содержит все реальные данные об этой компании.

После загрузки файла в систему8 и его запуска происходит автоматическая распаковка содержащихся в нем приложений. В результате работы файлы устанавливаются в C:\Documents and Settings\{user name}\AppData\Roaming\Microsoft\MTM.

Устанавливаемые файлы составляют набор удаленного администрирования на базе LiteManager 3.4.

Затем приложение запускается с ключом /HIDETRAY, который используется для сокрытия его присутствия в системе: C:\Documents and Settings\<USER>\Application

Data\Microsoft\MTM\ROMServer.exe/HIDETRAY. В результате происходит регистрация в ключе автозапуска системного реестра для старта при каждом входе в систему:

HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Ru п, а затем вносятся параметры для работы в ключ LiteManager: HKEY_LOCAL_MACHINE\SYSTEM\LiteManager\v3.4\Server\Parameters

Таким образом, на всех этапах данной атаки единственный вредоносный элемент - макрос в doc-файле, что является отличительной чертой современных целевых атак (преступники используют легальные инструменты, чтобы затруднить обнаружение вторжения при помощи традиционных средств защиты, работающих на основе «черных списков»). Атака FakeCERT: Здравствуйте, мы из Центробанка blog.kaspersky.ru/ataka-fakecert-zdravstvujte-my-iz-centrobanka/11279/

Используя перечисленные способы неправомерного доступа к компьютерной информации, преступники могут получить пароли, коды, идентифицирующие шифры, номера банковских счетов и другую конфиденциальную информацию законных пользователей и проникнуть в компьютерную систему, выдавая себя за законного пользователя. Особенно уязвимы в этом отношении системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т. п.).

Таким образом, способы неправомерного удаленного доступа к компьютерной информации, как способ подготовки хищений денежных средств, совершаемых с использованием компьютерных технологий, могут быть связаны с относительно простыми в техническом отношении действиями, не требующими высокого уровня квалификации преступников, а также с высокотехнологичными действиями с использованием чужих сетевых адресов в локальной сети, имеющей выход в Интернет, беспроводного (Wi-Fi) соединения, чужого телефонного номера или компьютера в качестве средства неправомерного доступа путем кратковременного удаленного соединения с ним, услуг провайдера, не фиксирующего данные о своих пользователях. На данное обстоятельство указывают исследователи.

Способы уничтожения компьютерной информации могут быть направлены на подготовку и одновременное сокрытие хищений денежных средств, совершаемых с использованием компьютерных технологий.

Сущность способов уничтожения компьютерной информации заключается в доведении вычислительной системы компьютерного устройства до нестабильного или полностью нерабочего состояния. Наиболее часто для этой цели используются DoS-атаки и DDoS-атаки.

Существует два основных типа DoS-атак: отправка компьютеру-жертве специально сформированных пакетов, не ожидаемых этим компьютером, что приводит к перезагрузке или остановке системы; отправка компьютеру-жертве большого количества пакетов в единицу времени, которые этот компьютер не в состоянии обработать, что приводит к исчерпанию ресурсов системы.

Использование DDoS-атак на компьютерную систему коммерческих банков является, как правило, отвлекающим маневром преступников. Под прикрытием таких атак (пока специалисты занимаются отражением атак),

преступники проникают в банковские системы незамеченными, получают расширенные привилегии в системе и совершают хищение денежных средств.

Следует отметить, что вредоносные программы или троянские программы используются преступниками не только для получения доступа к конфиденциальной информации, находящейся на рабочей станции конечного пользователя (компьютер, сервер и т.п.), но и находящейся на мобильных устройствах (телефоны, планшеты и т.п.), в том числе под управлением операционной системы Android. В последнем случае используются такие способы хищения конфиденциальной информации как фишинг, SMS-банкинг и эмуляция работы банковского приложения на телефоне.

Согласно исследованиям мобильных бот-сетей, 40 % пользователей мобильных устройств имеют банковский счет в банке, привязанный к зараженному мобильному телефону.

Отметим, что современные мобильные троянские программы позволяют преступникам совершать хищения в автоматическом режиме, что приводит к росту числа преступлений в коммерческих банках с большими клиентскими базами.

Кроме совершения хищений, мобильные бот-сети активно используются для шпионажа за владельцами телефонов, перехватывая СМС-сообщения, изображения, историю и запись телефонных переговоров, отслеживая перемещения владельца устройства.

Так, фишинг используется преступником для получения информации о банковской карте либо логинов/паролей в интернет-банке. Технология работы вредоносной программы (телефонный аппарат с операционной системой Android): после попадания на мобильное устройство жертвы она проверяет, запущено ли приложение Google Play. Если пользователь запускает эту программу, то троян показывает поверх окна Google Play свое окно с предложением ввести данные банковской карты. После того как пользователь ввел данные своей банковской карты, они автоматически передаются на сервер, находящийся под контролем преступника, где специальными скриптами осуществляется проверка корректности введенных данных карт. Если введены корректные данные, то в режиме реального времени преступник получает соответствующее уведомление по протоколу Jabber.

Аналогичным образом вредоносная программа может получить логин и пароль на доступ в Интернет-банкинг. Когда пользователь запускает банковское приложение, троянская программа подменяет оригинальное окно на фишинговое, где жертва сама вводит необходимые данные, которые немедленно отправляются на сервер, находящийся под контролем преступника. Обладая логином, паролем, а также доступом ко всем SMS-сообщениям, в том числе от банков с TAN-кодами, преступник может успешно совершать банковские переводы.

Вредоносные программы или троянские программы обладают, в том числе следующими функциями:

Сбор данных платежных карт с помощью вредоносной программы и программы Google Play

Сущность данного способа в следующем. При запуске приложения Google Play открывается системный диалог с запросом ввода данных банковской карты

(без заполнения данного диалогового окна пользователь не сможет в будущем запустить приложение Google Play). После ввода данных с карты они отправляются на сервер, находящийся под контролем преступника. При этом происходит обычный запуск приложения Google Play.

Одной из вредоносных (троянских) программ, используемой для хищения данных платежных карт, является Android.ZBot, различные модификации которой атакуют смартфоны и планшеты с февраля 2015 г. и получили по классификации Dr.Web имя Android.ZBot. I. origin. Как и многие другие Andmid-троянцы, Android.ZBot. I. origin распространяется преступниками под видом безобидной программы (в данном случае -приложения Google Play), которая скачивается на мобильные устройства при посещении мошеннических или взломанных веб-сайтов, либо загружается другой вредоносной программой.

После того как жертва установит и запустит программу Android.ZBot. I.origin, она запрашивает через приложения Google Play доступ к функциям администратора зараженного смартфона или планшета и в случае успеха выводит на экран уведомление: «Ошибка! Приложение не было установлено, файл поврежден. [Удалить]». После того как пользователь нажмет кнопку [Удалить], будет воспроизведена анимация удаления и программа закроется. Однако на самом деле приложение удалено не будет.

Если же пользователь отказывается предоставить вредоносной программе необходимые полномочия, она тут же пытается украсть у него подробные сведения о его банковской карте, включая ее номер и срок действия, трехзначный код безопасности CVV, а также имя владельца. Для этого Android.ZBot. I. origin показывает жертве поддельное окно, имитирующее оригинальную форму ввода соответствующей информации настоящего приложения Google Play. Аналогичное окно данная вредоносная программа отображает и после получения требуемых функций администратора, однако лишь через некоторое время после установки на целевом устройстве.

Далее Android.ZBot. I. origin удаляет свой значок с экрана приложений, «прячась» от пользователя, и начинает контролировать системные события, связанные с загрузкой операционной системы. Тем самым троянская программа обеспечивает себе автоматический запуск при каждом включении инфицированного устройства. Как только вредоносная программа получает управление, она связывается с удаленным узлом, регистрирует на нем зараженный смартфон или планшет и ожидает дальнейших указаний злоумышленников. В зависимости от полученной директивы сервера Android.ZBot. I. origin выполняет следующие действия (реализует функции): получение входящих SMS-сообщений; выполнение USSD-команд; перехват SMS-сообщений; рассылка SMS-сообщений по определенным контактам пользователя; рассылка SMS-сообщений по фильтрам (всем, on-line, избранным, по операторам, по странам); отправка SMS-сообщения на любой номер; SMS-команды: allCMC - пересылка SMS-сообщений с номера, на котором будет получена команда, на номер, с которого будет отправлена команда (если нет доступа к сети Интернет); send [НОМЕР] [ТЕКСТ] - SMS-команда для отправки SMS-сообщения с номера получателя; совершение телефонных звонков; получение текущих GPS-координат; воспроизведение специально сформированного диалогового окна поверх заданного приложения.

Функция по отправке SMS-сообщений на любые номера может быть использована преступниками для отправки сообщений на платные номера в

целях хищения денежных средств с банковского счета пользователя. В связи с возможностью выполнения USSD-команд преступникам становятся доступны конфиденциальные данные жертвы, часть из которых может быть использована для хищения денег с существующих банковских аккаунтов. Функция по перехвату SMS-сообщений может позволить преступникам получать SMS-коды для проведения транзакций со счета жертвы.

Например, сразу после того как на управляющем сервере, находящемся под контролем преступников, регистрируется новое зараженное устройство, Android.ZBot.l.origin получает команду на проверку состояния баланса банковского счета пользователя. Если троянская программа обнаруживает наличие денег, она автоматически переводит заданную преступниками сумму на подконтрольные им банковские счета.

Некоторые коммерческие банки разрешают совершать переводы по SMS-сообщениям только получателям из белого списка, например, по шаблонам, созданным в Интернет-банкинге. Однако в белом списке всегда присутствует номер телефона, привязанный к банковскому счету, чтобы владелец мобильного устройства мог пополнять баланс телефона. В этом случае преступники переводят все деньги с банковского счета на номер мобильного телефона. Впоследствии преступники, обладая доступом к SMS-сообщениям, могут привязать электронный кошелек к этому телефону и сделать перевод денежных средств с баланса телефона на новый электронный кошелек, таким образом, обходя ограничения белого списка.

Таким образом, Android.ZBot.l.origin может получить доступ к управлению банковскими счетами владельцев мобильных Andmid-устройств и незаметно для пользователей похитить деньги при помощи специальных SMS-команд, предусмотренных тем или иным сервисом мобильного банкинга. При этом жертва не будет подозревать о краже, т. к. вредоносная программа перехватывает поступающие от коммерческих банков сообщения с проверочными кодами транзакций.

Как отмечают специалисты «Доктор Веб», часть вредоносного функционала Android.ZBot.l.origin (например, отправка SMS-сообщений) реализована вирусописателями в виде отдельной Linux-библиотеки с именем libandroid-v7-support.so, которая хранится внутри программного пакета троянца. Это обеспечивает троянской программе защиту от детектирования антивирусами и позволяет ей дольше находиться на зараженных устройствах необнаруженной.

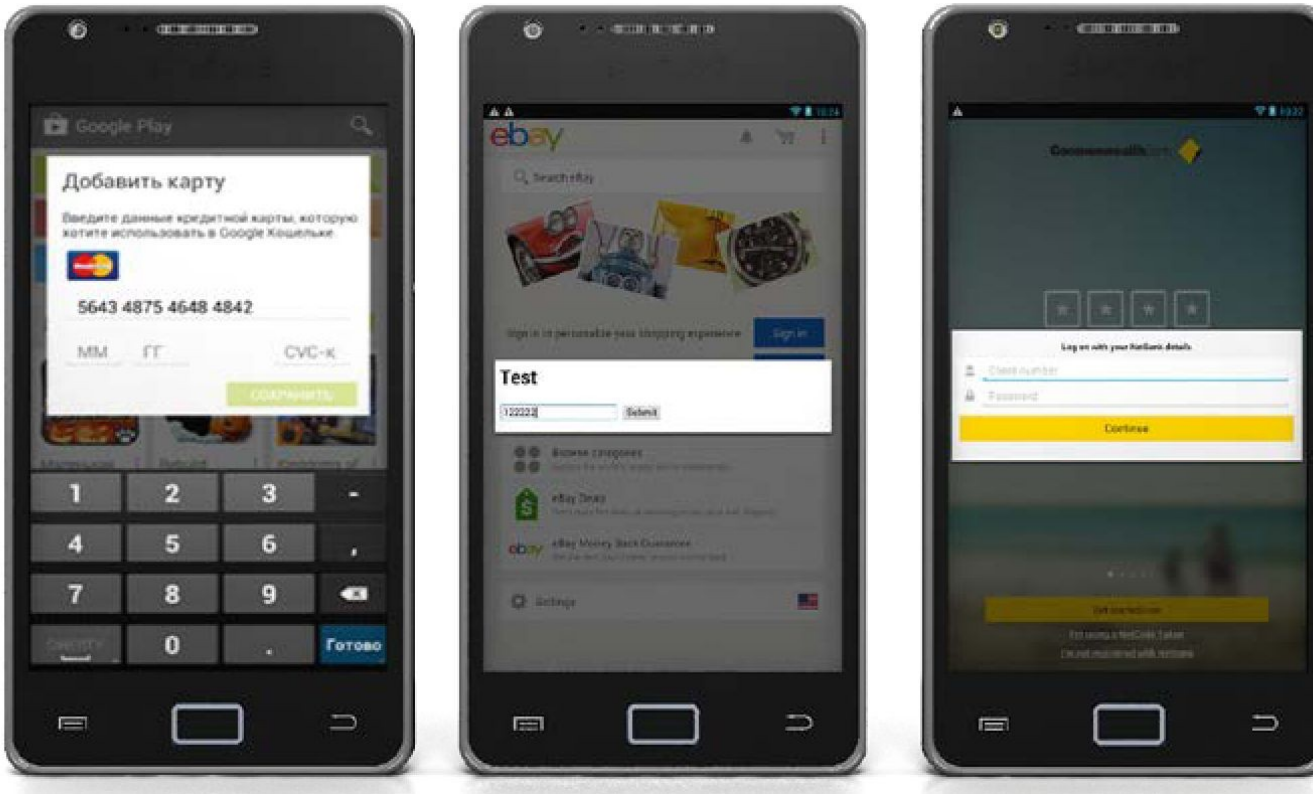
Однако одна из главных особенностей Android.ZBot.l.origin заключается в его способности похищать логины и пароли для доступа к сервисам мобильного банкинга при помощи поддельных форм ввода, генерируемых по указанию управляющего сервера и предназначенных для создания видимости их принадлежности к тем или иным программам.

Данная атака представляет собой классический фишинг, особенности которого состоят в следующем. Вначале троянская программа получает от преступников команду, содержащую название целевого приложения, после чего с определенной периодичностью начинает проверять, запущена ли пользователем соответствующая программа. В конце 2015 г. данная троянская программа контролировала запуск нескольких десятков банковских приложений: m.sberbank.ivom; ru.sberbanksbbol; ru.raiffeisennews; m.vtb24.mobilebanking. android; PSB.Droid; com.idamob.tinkoff.android;

rn.simpls.brs2 .mobbank; ru.kykyryza; com.smpbank.android; m.ftc.faktura.sovkombank; hu.eqlsoft.otpdirektru; m.ftc.faktura.sovkombank; rii.rocketbank.r2d2 и др.

Как только необходимая программа начинает работу, Android.ZBot.l. origin при помощи функции Web View формирует специальную веб-форму, содержимое которой загружает с удаленного узла.

В частности, преступники могут задать размер демонстрируемого окна, его внешний вид, включая заголовок и сопроводительный текст, количество полей для ввода данных, сопутствующие изображения и т. п. При этом выводимая на экран форма «привязывается» к атакуемому приложению: если потенциальная жертва фишинга попытается избавиться от показанного сообщения и вернуться к окну оригинальной программы при помощи аппаратной кнопки «Назад», Android.ZBot.l.origin перенаправит пользователя на главный экран операционной системы, закрыв само приложение. Скриншот примера фишингового окна показан на рис.



В результате у пользователя (жертвы) зараженного мобильного устройства может сложиться впечатление, что увиденный им ранее запрос в действительности принадлежит соответствующей программе, и ему все-таки необходимо ввести требуемую информацию. Как только троянская программа получает от жертвы ее логин и пароль, эти данные загружаются на удаленный узел, после чего преступники обретают полный контроль над учетными записями мобильного банкинга пользователей и могут управлять их счетами.

Другую модификацию вредоносной программы, получившую имя Android.ZBot.2.origin, вирусные аналитики «Доктор Веб» выявили в июне 2015 г. Данная версия троянской программы обладает аналогичным Android.ZBot. l.origin функционалом и отличается от своего предшественника лишь тем, что

ее код зашифрован, чтобы усложнить обнаружение антивирусами. В ноябре 2015 н. Android.ZBot.2.origin был обнаружен специалистами «Доктор Веб» на 6238 смартфонах и планшетах, а с момента внесения его в вирусную базу, антивирусное программное обеспечение Dr. Web для Android зафиксировало 27 033 случая проникновения троянской программы на Andraid-устройства

Сбор информации с помощью системных диалогов

Сущность данного способа в следующем. После установки вредоносная программа проверяет наличие аккаунтов пользователей в интересующих преступника коммерческих банках, сканируя установленные приложения, SMS-сообщения и контакты пользователя. При обнаружении нужного коммерческого банка пользователю показывается системный диалог с текстом «Принять Уведомление от «название банка»?». При согласии пользователю предлагается синхронизироваться с банком и заполнить формы, сгенерированные преступником. Все скомпрометированные данные затем автоматически направляются на сервер, находящийся под контролем преступника.

Сбор информации с помощью HTML/JS-диалогов

Сущность данного способа в следующем. После установки вредоносная программа проверяет наличие аккаунтов пользователей в интересующих преступника коммерческих банках, сканируя установленные приложения, SMS-сообщения и контакты пользователя. При обнаружении нужного коммерческого банка пользователю выводится фишинговое окно, где он должен заполнить данные банковской карты или другую информацию. Скомпрометированные данные автоматически направляются на сервер, находящийся под контролем преступника.

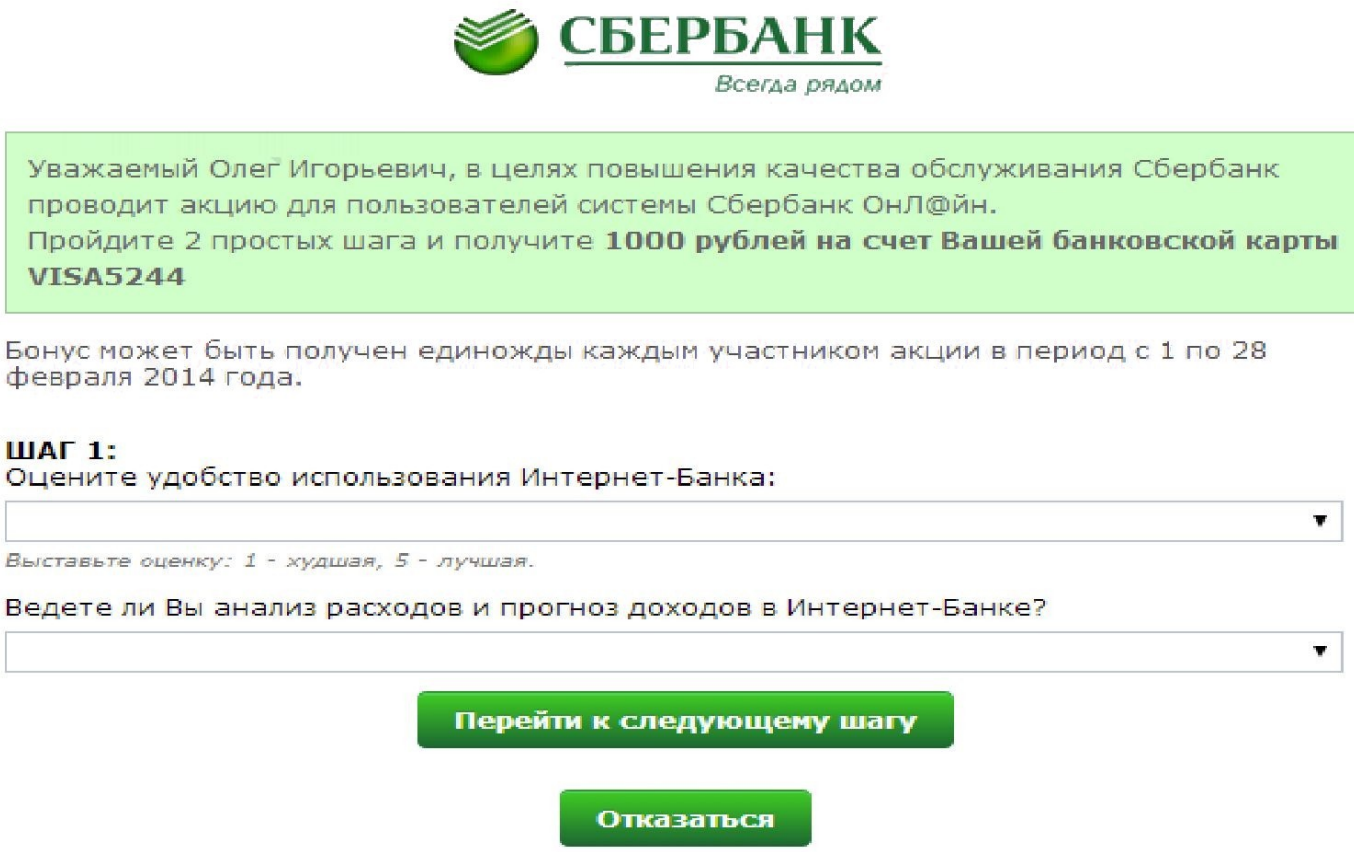
Сбор информации через установленные приложения

Сущность данного способа в следующем. При запуске определенных приложений (например, Facebook, Skype и др.) открывается системный диалог с запросом ввода данных банковской карты (без заполнения данного диалогового окна пользователь не сможет запустить желаемое приложение). Для формирования диалога преступники используют дизайн самого приложения, чтобы пользователь не смог заметить подозрительную активность.

Кроме того, для получения логина и пароля от Интернет-банкинга преступники используют фишинговые сайты. Изучая перехваченные SMS-сообщения, преступник ищет абонентов с необходимым балансом на банковском счете. Таким пользователям преступник от имени банка направляет SMS-сообщения с просьбой пройти анкетирование на сайте, где за заполненную анкету клиенту будут начислены бонусы. Анкета заполняется в несколько шагов, на одном из которых просят указать логин от системы Интернет-банкинга. При этом другую секретную информацию (пароль, номер карты, кодовые слова и т. д.) не запрашивают.

Зная логин от системы Интернет-банкинга, преступник на сайте банка использует процедуру восстановления пароля по SMS-сообщению, в результате чего на зараженный телефон приходит новый пароль, и таким образом преступники получают логин, пароль, а также доступ ко всем SMS-сообщениям, в том числе от коммерческих банков с TAN-кодами, что позволяет им успешно совершать банковские переводы (хищения денежных средств).

Пример фишинговой страницы с анкетой на русском языке, используемой преступниками вместе с мобильной троянской программой, показан на рисунке.



Еще одним способом получения доступа к банковскому счету жертвы является распространение мошеннических приложений от имени коммерческого банка. В данном случае приложение стилизовано под конкретный банк. Преступники упростили процесс создания таких приложений для распространения и в своей панели управления сделали раздел с мастером по созданию этих приложений по шаблону.

Пример такой бот-сети показан на рисунке.

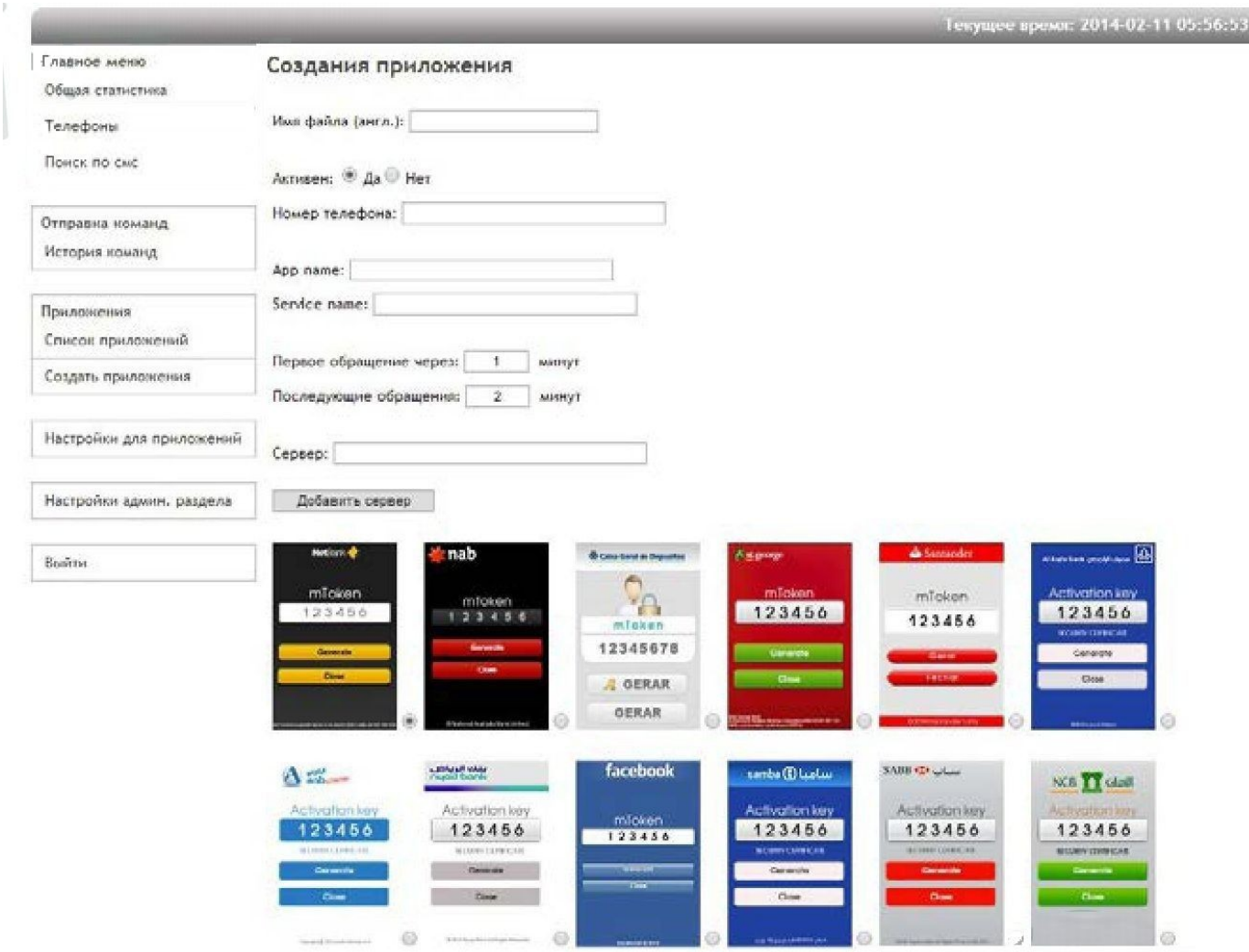


Рисунок. Раздел в панели управления с мастером по созданию этих приложений по шаблону

Подобное приложение также получает логин/пароль во время установки на мобильное устройство, а все TAN-коды в автоматическом режиме направляются на сервер, находящийся под контролем преступников.

Особенностью использования SMS-банкинг для хищений денежных средств с банковских счетов преступнику знать логин/пароль не надо. Под SMS-банкингом понимается процедура перевода денег с банковского счета с помощью отправки специально сформированного SMS-сообщения на номер банка. Подтверждение переводов осуществляется отправкой SMS-сообщения на специальный номер банка с TAN-кодом, который также получается от коммерческого банка по SMS-сообщению. Имея возможность манипулировать SMS-сообщениями, преступники могут осуществлять банковские переводы (хищения денежных средств).

Последовательность операций, образующих технологию хищения, можно представить следующим образом:

1) троянская программа пересылает все SMS-сообщения на сервер, находящийся под контролем преступника.

2) преступник ищет на сервере SMS-сообщения с уведомлениями от банков. Например, такие SMS-сообщения приходят после совершения покупок, и в них

содержится информация о балансе банковского счета. Если преступник находит номер телефона с интересующим балансом и владелец телефона является клиентом банка, который предоставляет услугу SMS-банкинга, то он создает задание вредоносной программе на отправку SMS-сообщения с информацией о переводе денежных средств на номер банка. При этом все дальнейшие уведомления от банка будут скрываться на телефоне владельца счета и передаваться в автоматическом режиме на сервер, находящийся под контролем преступника.

3) банк отправляет код подтверждения операции на перевод денежных средств по SMS-сообщению.

4) троянская программа перехватывает SMS-сообщения от банка, скрывает это SMS-сообщения от пользователя и передает его текст в автоматическом режиме на сервер, находящийся под контролем преступника.

5) преступник создает задание вредоносной программе на отправку SMS-сообщения с кодом подтверждения на номер банка.

6) вредоносная программа выполняет свое задание, в результате чего операция перевода завершается.

Сегодня это наиболее типичный способ совершения хищений, поскольку крупнейшие банки предоставляют услугу SMS-банкинга.

Под сокрытием преступления понимается деятельность (элемент преступной деятельности), направленная на воспрепятствование выявлению, раскрытию и расследованию преступного деяния путем утаивания, уничтожения, маскировки или фальсификации следов преступления и преступника и их носителей.

Способы сокрытия преступлений в значительной степени детерминированы способами их совершения.

По содержательной стороне способы сокрытия преступлений можно классифицировать на следующие группы:

утаивание информации и (или) ее носителей;

уничтожение информации и (или) ее носителей;

маскировка информации и (или) ее носителей;

фальсификация информации и (или) ее носителей (заведомо ложные показания, сообщения, доносы, создание ложных следов, полная или частичная подделка документов, подмена, дублирование объекта, частичное уничтожение объекта с целью изменения его внешнего вида, фальсификация назначения, создание преступником ложного представления о своем пребывании в интересующий следствие момент в другом месте и т.п.).

Перечисленные способы сокрытия преступлений свойственны и хищениям денежных средств, совершаемых с использованием компьютерных технологий. Так, при непосредственном доступе к банковским счетам (например, работником коммерческого банка или иной коммерческой организации) сокрытие следов преступления сводится к воссозданию обстановки, предшествующей совершению преступления, т. е. уничтожению оставленных следов (следов пальцев рук, следов обуви, микрочастиц и пр.).

При опосредованном (удаленном) доступе к банковским счетам сокрытие заключается в самом способе совершения преступления, который затрудняет обнаружение неправомерного доступа. В частности, для сокрытия рассматриваемого вида хищений применяются чужие пароли, идентификационные средства доступа, указываются фиктивные адреса отправителей электронных сообщений, ложные телефонные номера, пароли и анкетные данные и т. п. Средствами сокрытия в таких случаях все чаще выступают специальные компьютерные программы и устройства.

Так, к компьютерным программам и устройствам, позволяющим сокрыть следы хищений денежных средств, с использованием компьютерных технологий, относятся:

ремейлеры (Remailers), т. е. компьютеры, получающие сообщения и переправляющие их по адресам, указанным отправителями. В процессе переадресовки вся информация об отправителе уничтожается, что не позволяет конечному получателю выяснить, кто автор сообщения. Ремейлеров в сети Интернет много, некоторые из них позволяют указывать фиктивный адрес отправителя, большинство же прямо указывает в заголовке, что электронное сообщение анонимно;

программы-анонимизаторы. В отличие от ремейлеров, которые фактически осуществляют переадресацию электронной почты, направляя ее с другого компьютера, анонимизаторы позволяют изменять данные об обратном адресе и службе электронной почты отправителя. При этом остается возможность установить электронный адрес (IP-адрес) компьютера отправителя;

вредоносные программы. Так, следы неправомерного доступа к компьютерной информации, в частности, файлы истории, фиксирующие все последние проделанные операции, можно удалить, используя вредоносную программу, которая незаконно распространяется как в сети Интернет, так и на компакт-дисках.

Кроме того, сокрытие следов хищений денежных средств, с использованием компьютерных технологий, осуществляется посредством второго электронного почтового ящика. В сети Интернет существует множество сайтов, где беспрепятственно и бесплатно можно открыть почтовый ящик, откуда отправлять электронную почту под любыми вымышленными исходными данными.

Не теряет актуальности и физическое сокрытие следов преступлений (например, следов пальцев рук на клавиатуре, кнопках дисководов и других объектах, с которыми контактировал преступник). Крайней формой сокрытия следов преступления можно предположить попытки физического уничтожения или повреждения компьютерной техники или ее отдельных узлов (например, жесткого диска).

Единство этапов подготовки, совершения и сокрытия рассматриваемого вида хищений можно проиллюстрировать, например, на технологии хищения денежных средств в системе ДБО. Так, подготовительный этап данной разновидности хищений включает следующие операции:

1) приобретение компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной

информации или нейтрализации средств защиты компьютерной информации (далее - вредоносные программы), в том числе путем их создания.

Приобретение вредоносных программ может быть осуществлено следующими способами:

покупка на различных хакерских форумах доступов к взломанным вебсайтам различной тематики;

покупка трафика (под трафиком в данном случае понимаются посетители веб-сайта) на специализированных электронных биржах, где за деньги продают определенное количество переходов посетителей заданной тематической категории на какую-либо страницу. Биржи трафика во многом похожи на баннерные сети, только в них вместо показов баннеров продаются переходы на сайт. Следует отметить, что биржи трафика обычно противодействуют перенаправлению посетителей на сайты, распространяющие вредоносные программы. Для этого производится регулярная проверка (модерация) ссылок на интернет-ресурсы, предоставляемые клиентами биржи трафика. В то же время преступники находят способы обмануть администраторов и модераторов бирж трафика и перенаправить их переходы на интернет-страницы, не содержащие вредоносного содержимого, хотя остальные посетители перенаправляются на интернет-страницы именно с таким содержимым. Одним из легальных способов использования бирж трафика является раскрутка вебсайтов. В данном случае владелец веб-сайта покупает посетителей из тематической категории, которым его веб-сайт будет интересен.

2) размещение сайтов-двойников в сети Интернет (преступники фабрикуют фишинговые сайты (сайты-двойники) для хищения логинов и паролей);

3) распространение вредоносной программы с целью заражения компьютеров с установленным на них программным обеспечением ДБО (например, «Банк-клиент»);

4) хищение авторизационных данных пользователя в системе ДБО (логина, пароля и ключей электронной подписи (сеансовые ключи).

Для хищения авторизационных данных преступники используют специальное вредоносное программное обеспечение. Чаще всего это модификации хорошо известных банковских троянов ZeuS, SpyEye, Carberp, RDPdoor и Shiz с дополнительным функционалом, обеспечивающим возможность удаленного управления компьютером, что позволяет преступнику работать, в том числе, и с ключами, хранящимися в защищенном хранилище. Кроме описанных выше функций данные вредоносные программы умеют работать с Crypto API операционной системы, что позволяет им самостоятельно взаимодействовать со смарткартами и токенами. Как правило, код вредоносных программ этого типа зашифрован, а сами программы содержат механизмы обхода различного антивирусного программного обеспечения (включая антивирусные продукты Лаборатории Касперского, Avira, AYG, Windows Defender и др.). Для затруднения последующего обнаружения хищений вредоносные программы класса «Win32. Shiz» удаляют все системные точки восстановления, а также позволяют по команде преступника перезаписать первые секторы системного носителя информации.

Этап совершения хищения денежных средств в системе ДБО (основной этап) включает следующие операции:

1) создание подложного распоряжения (платежное поручение и т.п.) и направление его по системе ДБО в кредитную организацию, обслуживающую клиента.

Для отправки подложного платежного распоряжения преступники могут использовать различные возможности вредоносных программ. Например, преступники могут внедрить в компьютер или мобильное устройство потерпевшего троянскую программу, изменяющую в подготовленных к отправке платежных поручениях информацию (например, изменить реквизиты получателя платежа, его расчетного счета, наименования банка получателя, суммы платежа).

Пользователь видит на экране монитора одну информацию, а в кредитную организацию отправляется другая. Параллельно подменяются данные об остатках на счете, выполненных транзакциях и т. д.

Другой способ связан с автоматическим формированием подложного платежного распоряжения вирусом и подменой вредоносной программой реквизитов легитимного платежного поручения за мгновение до его подписания и передачи в кредитную организацию.

Как только подложное распоряжение направлено в кредитную организацию, задачей преступника является скрыть преступление путем ограничения доступа потерпевшего к системе ДБО.

2) кредитная организация идентифицирует подложное распоряжение как подлинное (легитимное) и осуществляет перевод денежных средств клиента по реквизитам, указанным в данном документе;

3) зачисление денежных средств на счет фирмы-однодневки и (или) счет (а) подставных физических лиц, находящихся, как правило, в другой кредитной организации.

Таким образом, пока потерпевший восстанавливает работоспособность компьютера, денежные средства похищаются путем перечисления их на специально созданные преступниками банковские счета и обналичиваются.

Этап сокрытия хищения денежных средств в системе ДБО является неотъемлемой частью этапа подготовки и совершения преступления. Данный этап может быть связан со следующими операциями:

приобретение и использование специального оборудования, а также программного обеспечения для осуществления преступной деятельности;

использование возможностей общедоступных радиосетей Wi-Fi, Wi-Max;

использование серверов, физически расположенных в других странах мира;

уничтожение или маскировка информации о преступлении после его совершения;

хранение информации о преступной деятельности на веб-серверах с использованием «облачного пространства»;

использование номеров мобильных телефонов, оформленных на подставных лиц; использование GSM-модемов и иных информационных систем;

сокрытие информации о своем месте нахождения при подготовке и совершении хищения;

сокрытие хищения от потерпевшего сразу же после направления подложного распоряжения в кредитную организацию.

Для сокрытия информации о своем месте нахождения при подготовке и совершении хищения преступники используют различные методы анонимизации своей активности в сети Интернет. Анонимизация достигается за счет сокрытия реального IP-адреса преступника, по которому можно определить его точное местонахождение. Перечисленные ниже методы различаются технологией, по которой будет происходить замена реального IP-адреса на другой.

1) VPN-серверы - данный метод обеспечивает высокий уровень анонимности и предоставляется большим количеством поставщиков таких Заслуг в сети Интернет. В этом случае весь сетевой трафик с компьютера преступника будет идти через один или несколько серверов в зашифрованном виде. Для использования этого метода канонизации преступник должен купить подписку на использование серверов у поставщика услуги. Как правило, многие VPN-серверы находятся за рубежом, поэтому при доступе в системе ДБО с иностранных IP-адресов, системы выявления преступлений в кредитных организациях могут выдавать предупреждения.

2) HTTP-прокси - самый простой метод. В сети Интернет есть множество ресурсов, на которых публикуются списки таких прокси для открытого использования. Для начала его использования нет необходимости оплачивать доступ к таким серверам, устанавливать дополнительно программное обеспечение на компьютер, достаточно использовать штатные средства Веб-браузера. В данном случае уровень анонимизации низкий и при определенных обстоятельствах реальный IP-адрес преступника может быть установлен. Трафик во время использования HTTP-прокси не шифруется. Преступник может использовать данный метод вместе с использованием VPN-серверов. Данный метод анонимизации используется редко.

3) SOCKS-проски - данный метод обеспечивает более высокий уровень анонимности, чем HTTP-прокси, но более низкий, чем при использовании VPN. SOCKS-прокси могут быть организованы на отдельных серверах, либо с использованием бот-сети. В последнем случае преступник может воспользоваться любым компьютером из бот-сети для сокрытия своего местонахождения. Использование SOCKS-прокси широко применяется при совершении хищений у физических лиц, когда при доступе в систему ДБО необходимо использовать IP-адрес того же города или провайдера, что и у владельца-счета. Для начала использования этого способа анонимизации нет необходимости устанавливать дополнительно программное обеспечение на компьютер, а использовать штатные средства Веб браузера.

4) Выделенные серверы - чтобы повысить уровень анонимизации и не оставлять следов на своем компьютере преступник может осуществлять все действия с выделенного сервера. Такой сервер он может купить, либо использовать чужой скомпрометированный сервер. В последнем случае ему необходимо будет либо скомпрометировать сервер самому, либо купить доступ к нему у поставщика таких серверов.

5) TOR-сеть - является бесплатной, обеспечивает высокий уровень анонимизации и шифрование сетевого трафика. Кроме того, позволяет выбрать IP-адрес в нужном городе. Основными недостатками ее использования являются низкая скорость, низкое доверие к IP-адресам этой

сети со стороны кредитных организаций, невозможность скрывать весь сетевой трафик. При совершении хищений используется редко.

Сокрытие хищения денежных средств в системе ДБО от потерпевшего сразу же после направления подложного распоряжения в кредитную организацию может осуществляться путем: смены пароля входа в систему ДБО, вывода из строя компьютера потерпевшего, DDoS-атаки на сервер кредитной организации, форматирования жесткого диска потерпевшего или удаления одного из компонентов операционной системы (например, NT Loader) и т.п. Рассмотрим некоторые из данных способов.

1) вывод из строя операционной системы компьютера. В данном случае троянская программа удаляет некоторые системные файлы, что приводит к неспособности успешной загрузки операционной системы (ОС) и необходимости ее переустановки. Вывод ОС из строя не позволяет владельцу счета проверить состояние счета и вовремя выявить несанкционированное списание денежных средств. Отметим, что во время переустановки операционной системы криминалистически значимая информация может быть удалена.

2) затирание информации. При затирании информации данные удаляются по специальным алгоритмам, исключающим возможность успешного восстановления информации при проведении криминалистического исследования. Данные могут быть удалены частично, или информация может быть удалена полностью с НЖМД. Для полного затирания информации со всего НЖМД требуется много времени, поэтому преступники, как правило, уничтожают данным способом отдельные файлы, которые могут относиться к преступлению, например, файлы системы ДБО и вредоносных программ.

3) DDoS-атака на клиента. При проведении данной атаки интернет канал потерпевшего, либо его серверы, обеспечивающие доступ в сеть Интернет, будут временно полностью или частично выведены из строя. В результате владелец счета не сможет подключиться к серверам кредитной организации, проверить состояние счета и вовремя выявить несанкционированное списание денежных средств.

4) DDoS-атака на сервер кредитной организации. При проведении данной атаки на сервер кредитной организации, серверы ДБО становятся недоступными для всех клиентов данной организации. В результате владельцы счетов (потерпевшие) не могут проверить их состояние и вовремя выявить несанкционированное списание денежных средств. Данный способ в настоящее время используется редко, поскольку начало такой атаки является сигналом для службы безопасности кредитных организаций к проведению более тщательной проверки платежных распоряжений и в результате вероятность успешного перевода значительно снижается.

Таким образом, способы подготовки хищения с использованием компьютерных технологий в некоторых случаях неразделимы со способом их совершения и сокрытия. Между тем, дифференциация таких хищений на этапы имеет значение для их расследования, так как позволяет следователю представлять технологию рассматриваемых преступных деяний и на этой основе в системном единстве со знаниями о других элементах криминалистической характеристики разрабатывать следственные версии, целенаправленно планировать расследование по уголовному делу в целом и отдельные процессуальные действия в частности.

Механизм следообразования хищений денежных средств, совершаемых с использованием компьютерных технологий

Общим для всех способов хищений денежных средств с использованием компьютерных технологий будет являться механизм следообразования или его отдельные элементы (операции). При этом под механизмом следообразования следует понимать специфическую конкретную форму протекания процесса взаимодействия двух и более объектов, конечная фаза которого представляет собой образование следа.

В основе механизма образования виртуальных следов находятся электромагнитные взаимодействия двух и более материальных объектов -объективных форм существования (представления) компьютерной информации.

Воздействие одной объективной формы существования компьютерной информации на другую (взаимодействие объектов следообразования) может быть обнаружено по наблюдаемому различию между тремя известными их состояниями:

содержание, формат и другие характеристики;

алгоритм работы программы;

автоматически создаваемые компьютерной программой (негласно для пользователя) скрытые файлы, которые используются некоторыми программами и операционными системами для фиксации хода обработки компьютерной информации и ее восстановления на случай аварийного сбоя в работе компьютерного устройства или его программного обеспечения.

Фиксируемые изменения этих состояний и будут следами-отображениями, характеризующими результат взаимодействия.

Основными следообразующими и следовоспринимающими объектами выступают: электромагнитный сигнал; файл; компьютерная программа; база данных; электронное сообщение; электронный документ; электронная страница или сайт в компьютерной сети.

Следами-предметами (частями предметов) и одновременно типичными материальными носителями виртуальных следов следует считать электронные (машинные) носители информации, интегральные микросхемы, микроконтроллеры, пластиковые карты и иные комбинированные документы, компьютеры, в том числе мобильные устройства. Помимо того, что в указанных технических устройствах содержится компьютерная информация, связанная с событием преступления, их отдельные электронные модули при работе излучают в окружающее пространство дополнительную криминалистически значимую компьютерную информацию, которая может быть дистанционно обнаружена и зафиксирована посредством соответствующих радиоэлектронных или иных специальных программно-технических средств. В последующем эта информация с помощью компьютерных программ и устройств может быть расшифрована (раскодирована), представлена в человекочитаемом виде и использована в целях уголовного судопроизводства.

В отличие от традиционно рассматриваемого в криминалистике физического следообразующего воздействия - механического или теплового - в данном случае будет иметь место другой механизм следообразования, а именно физико-химическое воздействие, сопряженное с механическим. Например, механическое движение нажатия пальцем руки на какую-либо клавишу клавиатуры персонального компьютера вызовет изменение напряжения и силы тока в электрической цепи, что может повлечь изменение магнитного поля носителя информации (при сохранении или копировании информации), или передачу этого электрического импульса по каналам коммуникаций к другому компьютеру (при обмене информацией), или же может быть вновь преобразовано в механическое движение головки принтера (при распечатывании информации). Несколько похожая ситуация в отношении механизма следообразования характерна для технического исследования документов, изготовленных на печатной машинке, проводимого в рамках криминалистической экспертизы. Как видно, в криминалистике традиционно к следам относились следы-отображения, возникающие в большинстве случаев в ходе механического воздействия.

Таким образом, для подобного следообразующего воздействия характерны следующие виды следов:

программы и текстовые файлы и (или) их части, не входящие в стандартный состав системы, функционирующей в данном устройстве ранее, до совершения преступления;

наборы команд, отдельных знаков, символов и т. д., содержащихся в программах системы, текстовых и иных документах, которые были намеренно внесены преступником в систему для изменения ее свойств, возможностей, содержания и т. п.;

записи в учетных файлах системы, так называемые log-файлы, в которых содержится информация о пользователях (не только о преступниках), когда-либо использовавших данное устройство, регистрирующие особенности работы пользователя в системе, время его работы и т.д., причем количество регистрируемых служебных параметров зависит как от функционирующей в данном устройстве системы, так и от политики безопасности, проводимой на нем.

Данные следы не являются традиционными и не могут быть отнесены ни к одной существующей в криминалистике группе следов. В связи с этим в литературе можно встретить разные наименования данных следов («виртуальные», «бинарные», «компьютерные», «электронные», «информационные», «радиоэлектронные», «электронно-цифровые» и т.п.). Не вступая в дискуссию по столь сложному вопросу, представляется возможным принять точку зрения, согласно которой такие следы можно именовать виртуальными и понимать под ними следы совершения любых действий (включения, создания, открывания, активации, внесения изменений, удаления) в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей.

Иначе говоря, виртуальными следами будет являться любая криминалистически значимая компьютерная информация, связанная с событием преступления, т. е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе

либо передающиеся по каналам связи посредством электромагнитных сигналов.

Приведенное определение, с одной стороны, не претендует на бесспорность, с другой - ни в коей мере не отрицает традиционного понимания такой криминалистической категории, как след, а лишь уточняет, дополняя его возможностью электромагнитного взаимодействия между следообразующим и следовоспринимающим объектом, а также таким возможным носителем следа-отображения, как электромагнитное поле.

Отметим, что действия с компьютерными, в том числе мобильными устройствами (мобильными телефонами, смартфонами, планшетами и т. д.), получают отображение в их памяти:

1) в журналах администрирования, журналах безопасности отображаются такие действия, как включение, выключение, различные операции с содержимым памяти компьютера;

2) в реестре компьютера (reg-файлах) отражаются действия с программами (установка, удаление, изменение и т.д.);

3) в log-файлах отображаются сведения о работе в сети Интернет, локальных и иных сетях;

4) в свойствах файлов отображаются последние операции с ними (например, даты создания последних изменений).

Виртуальные следы могут послужить доказательствами незаконного проникновения в память компьютера или иного устройства (взлома), создания, использования и распространения вредоносных компьютерных программ, совершения или подготовки совершения преступления лицом или группой лиц.

В то же время виртуальные следы ненадежны (благодаря своей природе), так как их можно неправильно считать (например, используя программно-технические средства, основанные на различных соглашениях, легко подделать). Практически невозможно различить одинаковые информационные объекты и т. п. В данном случае напрашивается характеристика «виртуальных» следов как субъективных, что сближает их с идеальными следами, но опять-таки не отождествляет с ними. «Виртуальные» следы хранятся не в памяти человека, а на материальных объектах - электронных носителях информации и получаются с использованием технических средств, действующих в строгом соответствии с заложенными в них алгоритмами.

Виртуальные следы образуются в результате воздействия (уничтожения, модификации, копирования, блокирования) на компьютерную информацию путем доступа к ней и представляют собой любые изменения компьютерной информации, связанные с событием хищения.

В зависимости от этапа совершения хищений денежных средств с использованием компьютерных технологий будет существовать различный набор следообразующих объектов. Так при использовании в хищении компьютерной техники основными (важнейшими с криминалистической точки зрения) характеристиками следообразующих объектов будут:

размер программ и сообщения электронной почты с присоединенным файлом;

дата и время создания (получения) и (или) модификации файлов и сообщения;

отдельные атрибуты (например, признак архивного, скрытого или системного файла, уровень важности и конфиденциальности полученного сообщения) файла и сообщения;

характерные записи (фрагменты) исполняемых программ или файлов конфигурации, позволяющие идентифицировать конкретный экземпляр вредоносной программы. Например, адрес электронного почтового ящика, куда следует отсылать выкраденные пароли, логины и IP-адреса компьютера.

Виртуальные следы могут оставаться и при опосредованном (удаленном) доступе через телекоммуникационные сети, например, через сеть Интернет. Они возникают в силу того, что система, через которую производится доступ, обладает некоторой информацией, которую эта система запрашивает у лица, пытающегося соединиться с другим компьютером. Она определяет электронный адрес, используемое программное обеспечение и его версию. Кроме того, при доступе в сеть обычно запрашивается адрес электронной почты, реальное имя и другие данные. Данная информация запрашивается системным администратором (провайдером) для контроля обращений на его сервер, и это также способствует идентификации личности проникающего в сеть.

С учетом отмеченного следователь имеет возможность выявить виртуальные следы в сети Интернет следующим образом.

В сети Интернет существует специальная служба Wliois, предназначенная для установления провайдера, через которого произошел неправомерный доступ, для чего необходимо указать электронный адрес (IP) интересующего компьютера. Для связи с этой службой для европейской части сети существует сервис по адресу: www.ripe.net. Время выхода абонента на связь и продолжительность его работы можно установить у провайдера по ведущемуся у него специальному лог-файлу.

При определении номера телефона, с которого была установлена связь с провайдером, следует иметь в виду, что не все провайдеры устанавливают устройства автоматического определения номера на свои телефоны. Также не следует забывать и о том, что существуют широко популяризированные через Интернет различные системы маскировки под другой номер, либо анти-АОНы, позволяющие скрыть свой номер телефона от АТС. Однако пренебрегать этими возможностями нельзя.

Установление номера телефона, с которого был осуществлен звонок, не всегда дает выход на конкретное лицо, поскольку к Интернету может быть подключена и локальная вычислительная сеть. В этом случае установить, с какого рабочего места был осуществлен сеанс связи, можно по лог-файлу сервера локальной сети с теми же ограничениями по времени.

Протокол выхода в Интернет ведется автоматически на каждом компьютере, с которого возможен выход в сеть Интернет (количество дней его хранения определяется пользователем). Представляется, что совпадение данного протокола с лог-файлом провайдера может служить неопровержимым доказательством.

Данные о пользователе электронной почты (фамилия, имя, отчество, дата и место рождения, место жительства, работы и т.п.) в большинстве своем

достоверны, так как сам пользователь заинтересован в получении персонифицированных электронных сообщений.

Большой информационной ценностью обладают разговоры через Интернет, поскольку их содержание автоматически сохраняется во временных файлах, которые даже после стирания могут быть восстановлены (хотя бы частично).

Следует отметить, что многие программы фирмы Microsoft создают резервные копии файлов, файлы-отчеты, сохраняют информацию о последних проделанных операциях и выполненных программах, а также содержат иную информацию, представляющую огромный интерес для расследования. Вот лишь некоторые примеры.

Microsoft Outlook Express 4.0 - в директории \Windows\Aplication\Microsoft\Outlook Express\Mail\ с расширениями IDX и MBX хранит все письма, которые были отправлены, получены или удалены.

Microsoft Internet Explorer 4.0 - в директории \Windows\Temporary Internet Files\ хранит места, которые посетил пользователь, находясь в сети Интернет.

Microsoft Windows 95 - в директории \Windows\History\ хранит все файлы истории, то есть данные о ранее выполнявшихся программах; в директории \Windows\name.pwl хранит имена, телефоны и пароли для соединения с Интернет, которые с помощью специальных программ расшифровываются.

Следами, указывающими на посторонний доступ к информации, могут являться: переименование каталогов и файлов; изменение размеров и содержимого файлов; изменение стандартных реквизитов файлов, даты и времени их создания; появление новых каталогов, файлов и т. п.

Перечисленное может свидетельствовать об изменениях в заданной структуре файловой системы, а также об изменении содержимого файлов. Кроме того, на неправомерный доступ к компьютерной информации могут указывать изменения в заданной ранее конфигурации компьютера, в том числе: изменение картинки и цвета экрана при включении; изменение порядка взаимодействия с периферийным оборудованием (принтером, модемом и др.); появление новых и удаление прежних сетевых устройств.

На неправомерный доступ к компьютерной информации могут указывать и необычные проявления в работе компьютера, в том числе замедленная или неправильная загрузка операционной системы, замедленная реакция компьютера на ввод с клавиатуры, замедленная работа компьютера с дисковыми накопителями при записи и считывании информации, неадекватная реакция компьютера на команды пользователя, появление на экране нестандартных символов, знаков и т. п.

Представляется, что данное классификационное построение согласуется с классификацией следов, описанной выше, и дополняет ее.

Один из наиболее распространенных способов рассматриваемого вида хищений денежных средств сопряжен с вредоносными программами, используемыми для несанкционированного получения информации с компьютеров «жертв». В зависимости от этапа данного вида преступления будет существовать различный набор следообразующих объектов.

На этапе внедрения вредоносной программы - это сообщение электронной почты с прикрепленным исполняемым файлом в специальном формате, а на

этапе активизации к нему добавится еще соответствующий исполняемый файл. При этом криминалистически значимыми характеристиками следообразующих объектов являются:

размер программ и сообщения электронной почты с присоединенным файлом;

дата и время создания/получения и/или модификации файлов и сообщения;

отдельные атрибуты (например, признак архивного, скрытого или системного файла, уровень важности и конфиденциальности полученного сообщения) файла и сообщения;

характерные записи (фрагменты) исполняемых программ или файлов конфигурации, позволяющие идентифицировать конкретный экземпляр вредоносной программы. Например, адрес электронного почтового ящика, куда следует отсылать выкраденные пароли, логины и IP-адрес компьютера.

Помимо самих файлов вредоносной программы следообразующими объектами также будут являться:

1) файлы, использующиеся для электронной рассылки вредоносных программ:

вид используемой стандартной почтовой программы, ее версия и текущие настройки;

текстовые файлы или файлы в специальном формате (согласованном с программой рассылки почтовых сообщений), содержащие списки рассылки и вспомогательные данные (даты и время рассылки), количество попыток повторения и т.п.;

файлы программ, обеспечивающие удаленное соединение компьютера и содержащие номера телефонов, «логины» (учетные имена для входа в сеть), пароли, скрипты (наборы автоматически выполняемой последовательности команд) и т.п.

2) файлы компилятора, использующегося для создания (программирования или настройки) самой вредоносной программы:

версия, настройки и параметры. Такие настройки и параметры в ряде компиляторов автоматически включаются в тело создаваемой с их помощью программы;

используемые библиотеки компилятора, операционной системы или других пакетов прикладных программ. Некоторые программы рассчитаны на обязательное присутствие на компьютере определенных библиотек или пакетов прикладных программ. Например, вредоносные программы для рассылки похищенной парольно-ключевой информации используют коммуникационные средства программы обмена информацией в реальном времени ICQ (фирмы Mirabilis).

При совершении хищений денежных средств, сопряженных с вредоносными программами, используется как минимум два компьютера (преступника и жертвы). В связи с этим следовоспринимающих объектов также будет несколько. На компьютере жертвы такими объектами будут:

таблица размещения файлов (FAT, NTFS или другая в зависимости от типа используемой операционной системы). На компьютере жертвы должны появиться файлы с программами, представляющими собой первую часть

вредоносной программы «троянский конь». Как правило, это два файла: один исполняемый файл (непосредственно сама программа), а второй файл содержит параметры конфигурации и вспомогательные данные, необходимые для работы исполняемого файла. Имена этих файлов могут быть произвольными (легко и без изменения функциональных возможностей программы заменяются преступником), но они должны иметь фиксированную (одну и ту же) длину. Дата и время создания/модификации этих файлов должны соответствовать дате и времени установки этих программ на компьютер -жертву.

системный реестр операционной системы компьютера; отдельные кластеры магнитного носителя информации (винчестера, дискеты), з которых записываются фрагменты исполняемых файлов (программ) и файлов конфигурации. Соответствующие разделы системного реестра должны включать указания на размещение и параметры установленных программных файлов.

файлы и каталоги (папки) хранения входящей электронной почты и прикрепленных исполняемых файлов, конфигурации почтовой программы;

файлы конфигурации программ удаленного соединения компьютера с информационной сетью.

На компьютере преступника такими объектами будут: таблица размещения файлов (FAT, NTFS или другая в зависимости от типа используемой операционной системы). На компьютере преступника должны появиться файлы с программами, представляющими собой вторую (управляющую) часть вредоносной программы «троянский конь».

системный реестр операционной системы компьютера; отдельные кластеры магнитного носителя информации (винчестера, дискеты), с которых записываются фрагменты исполняемых файлов (программ) и файлов конфигурации. Соответствующие разделы системного реестра должны включать указания на размещение и параметры установленных программных файлов.

файлы и каталоги (папки) хранения входящей электронной почты и прикрепленных исполняемых файлов, конфигурации почтовой программы;

файлы конфигурации программ удаленного соединения компьютера с информационной сетью.

На компьютере преступника такими объектами будут: таблица размещения файлов (FAT, NTFS или другая в зависимости от типа используемой операционной системы) На компьютере преступника должны появиться файлы с программами, представляющими собой вторую (управляющую) часть вредоносной программы «троянский конь».

системный реестр операционной системы компьютера;

скопированные с компьютера-жертвы файлы данных и программы, а также так называемые «скриншоты» (графические изображения экрана монитора) с компьютера-жертвы;

файлы и каталоги (папки) хранения входящей электронной почты и прикрепленных исполняемых файлов, конфигурации почтовой программы. Здесь могут быть обнаружены присланные с компьютера-жертвы значения

паролей и «логинов» для входа в информационную сеть, копии украденной электронной корреспонденции и т. п.;

файлы конфигурации программ удаленного соединения компьютера с информационной сетью. В этих файлах могут быть обнаружены логины и пароли компьютер а-жертвы, его адресная книга, используемые скрипты и т.п.;

отдельные кластеры магнитного носителя информации (винчестера, дискеты), в которых записываются фрагменты исполняемых файлов (программ) и файлов конфигурации.

Отметим, что кроме виртуальных следов при хищениях денежных средств, совершаемых с использованием компьютерных технологий, остаются на месте происшествия и иные, так называемые, традиционные, следы: документы на бумажных носителях, в том числе рукописные записи, а также выполненные с использованием средств автоматизации; отпечатки пальцев рук; микрочастицы; идеальные следы и т. д. Механизм следообразования таких следов достаточно подробно описан в литературе, в связи с этим ограничимся сказанным.

Общие рекомендации по организации расследования хищений денежных средств, совершаемых с использованием компьютерных технологий

Организация рассмотрения сообщений о хищениях денежных средств, совершаемых с использованием компьютерных технологий

Организация рассмотрения сообщений о хищениях денежных средств, совершаемых с использованием компьютерных технологий (далее, если не указано иное, хищение), является важным этапом не только стадии возбуждения уголовного дела, но и всего предварительного расследования. Этот этап связан с деятельностью должностных лиц ОВД по выявлению таких преступлений. В связи с этим обратимся к некоторым особенностям выявления хищений.

Согласно поступившей от ОПС информации, в период 2014 - 2015 гг. было выявлено 13032 хищения (2014 г. - 2164, 2015 г. - 10868) или 49,6 % сотрудниками полиции, большая часть из которых - 9088 или 69,7 % -сотрудниками подразделений уголовного розыска. При этом данный показатель 2015 г. (7894 преступления) у соответствующих подразделений выше 2014 г. (1194 преступления) в 6,6 раз. Около 9,3 % - 1211 деяний (2014 г. - 450, 2015 г. - 761) были выявлены сотрудниками БСТМ (управления, отделы, отделения «К»), 689 деяний (2014 г. - 150, 2015 г. - 539) или 5,3 % -сотрудниками подразделений ЭБиПК. Незначительное количество хищений обозначенного вида было выявлено участковыми уполномоченными полиции - всего за 2014-2015 гг. 166 преступлений или 1,3 %. Сотрудниками иных подразделений полиции за обозначенный период времени было выявлено порядка 4 % таких деяний.

Кроме того, немалое количество хищений выявлено сотрудниками органов предварительного следствия в системе МВД России. Так, за два года данный

показатель составил 1116 преступлений (2014 г. - 285, 2015 г. - 831) или 4,2 % от всех зарегистрированных деяний рассматриваемого вида.

Сотрудниками ФСБ России по данным, предоставленным ОПС, за обозначенный период времени было выявлено всего 21 рассматриваемое преступление, а сотрудниками иных правоохранительных органов - 172.

Рассматриваемых преступлений с участием сотрудников ЭКЦ ОВД было всего выявлено за два года 107 (2014 г. - 38, 2015 г. - 69), с участием иных государственных экспертных учреждений - всего 17 деяний, с участием коммерческих организаций, специализирующихся на обеспечении информационной безопасности - 7, с участием негосударственных экспертных учреждений и иных организаций - 3.

При выявлении хищений наиболее активно использовались различные виды учетов. Согласно предоставленным данным, с их помощью было выявлено 691 преступление (2014 г. - 281, 2015 г. - 410), в том числе при помощи учетов: оперативно-справочных - 434 (2014 г. - 211, 2015 г. - 223), криминалистических - 176 (36 и 140 соответственно), экспертно-криминалистических - 164 (14 и 150 соответственно), дактилоскопических -130 (77 и 53 соответственно), розыскных - 63 (16 и 47 соответственно). В ходе реализации оперативно-технических мероприятий было выявлено всего за два года 587 преступлений (2014 г. - 169, 2015 г. - 418), при использовании технических средств - 319 преступлений (2014 г. - 119, 2015г. - 200), а также систем видеонаблюдения - 225 деяний (2014 г. - 81, 2015 г. -144). Как установлено, единичными являются факты выявления рассматриваемого вида хищений по информации, полученной от компетентных органов зарубежных стран - всего 7 деяний за два года.

Обобщение складывающейся практики организации рассмотрения сообщений о хищениях показывает, что обращение с заявлением о таких преступлениях в территориальный орган МВД России может быть осуществлено потерпевшим по телефону или доставлено им лично (письменная форма).

Отметим, что большинство потерпевших с заявлением о хищении рассматриваемого вида обращаются в ближайший территориальный орган МВД России на районном уровне. В штатном расписании данного органа не предусматривается наличие специального отдела, группы или даже сотрудника, специализирующихся на раскрытии преступлений, совершенных с использованием компьютерных технологий. Рассмотрением таких материалов занимаются, в основном, оперуполномоченные уголовного розыска и участковые уполномоченные полиции. Достаточными теоретическими и практическими знаниями в данной области, в силу специфики своей работы, они, как правило, не обладают. В силу данного и иных обстоятельств по результатам проведенной проверки при предоставлении материалов в ОПС решение о возбуждении уголовного дела принять не представляется возможным. Материал возвращается для проведения дополнительных проверочных действий, в том числе оперативно-розыскных мероприятий, производство которых силами органа дознания невозможно. В связи с этим сотрудники вынуждены принимать решение об отказе в возбуждении уголовного дела, которое неоднократно отменяется прокурором как незаконное. Кроме того, при наличии межрегионального характера совершенного преступления имеют место частые случаи направления материалов проверки по месту, где похищенные денежные

средства были обналичены (например, местонахождение банкомата), что неизбежно приводит к затягиванию сроков проверки и утере следов совершения преступления.

Проведенный А.Н. Яковлевым и Н.В. Олиндер анкетированный опрос выявил, что типичными поводами для возбуждения уголовных дел о преступлениях, совершаемых с использованием электронных платежных средств и систем, являются:

1. Заявление о преступлении, поступившее от потерпевшего -представителя юридического лица или от гражданина - физического лица (63 %).

2. Непосредственное обнаружение признаков преступления органом дознания (20 %) (в результате проверки сообщения о совершенном или готовящемся преступлении, поступившего из оперативных источников; в ходе проведения специальных оперативно-технических мероприятий; по результатам анализа материалов контрольно-ревизионных и иных документальных проверок).

3. Непосредственное обнаружение признаков преступления следователем или прокурором при расследовании уголовных дел о преступлениях других видов (9 %).

4. Сообщения в средствах массовой информации и иные поводы (8 %).

Комментируя некоторые из полученных результатов, авторы отмечают, что в опросе не представлен такой повод для возбуждения уголовного дела как явка с повинной, которая применительно к преступлению, о факте совершения которого у правоохранительных органов нет информации, является маловероятной и не встречалась опрошенным лицам в качестве повода для возбуждения уголовного дела.

В отличие от преступлений в сфере компьютерной информации, которые носят преимущественно латентный характер на всех этапах, включая этап совершения преступления, хищения сопряжены с уменьшением денежных средств на банковских счетах клиентов кредитных организаций или иных платежных систем, что свидетельствует об очевидности преступного деяния. Исключение составляют хищения денежных средств в небольших размерах, которые пострадавшими при больших оборотах на их банковских счетах могут быть незамеченными.

Как следствие в большинстве случаев поводами для возбуждения уголовных дел будут заявления о преступлении, поступившие от потерпевшего - представителя юридического лица или от гражданина - физического лица.

Вместе с тем обращению в ОВД с заявлением о преступлении, как правило, предшествуют попытки пострадавшего или его представителя установить причины уменьшения денежных средств на счете, связанные с внутренней проверкой организации факта списания с ее банковского счета денежных средств, в том числе с уведомлением и содействием в проверке коммерческого банка или иной платежной системы.

Такой временной интервал между событием преступления и обращением в ОВД дает преступникам достаточно времени для сокрытия следов хищений.

Несмотря на длительность времени, прошедшего с момента обнаружения хищения до обращения пострадавших с заявлением о преступлении, органы дознания или следователи должны организовать и провести комплекс

мероприятий, включая фиксацию следов преступления на электронных носителях информации, отслеживание соединений с компьютерным устройством и иные.

Как известно, действующее законодательство Российской Федерации связывает возбуждение уголовного дела и все последующее производство по нему с обнаружением признаков преступления. По мнению ряда ученых-криминалистов, в общей форме точнее было бы говорить об обнаружении признаков возможного преступления, поскольку одни и те же признаки бывают свойственны как преступному, так и непреступному деянию. Не вступая в дискуссию по вопросу определения понятия признаков преступления, полагаем возможным привести точку зрения Г. А. Густова и В. Г. Танасевича, определяющих данное понятие как «определенные факты реальной действительности, представляющие собой следы преступления, указывающие на возможность совершения конкретного преступления» При этом отметим, что одни и те же данные о преступном деянии могут иметь различную уголовно-правовую квалификацию. Так, например, операция по списанию денежных средств с банковского счета может образоваться вследствие хищения, нарушения правил эксплуатации банковской компьютерной системы либо ошибок в учете или естественного сбоя в работе данной системы (его программного обеспечения, рабочих органов и т. д.).

В связи с отмеченным, сделать даже предположительный вывод о том, что имело место хищение на основании одного какого-либо признака достаточно проблематично. Необходимо наличие целого ряда признаков, свидетельствующих о возможно совершенном преступном деянии.

Обобщение результатов опосредованного анкетирования следователей (должностных лиц ОПС) показало, что на вопрос о признаках (или их совокупности) хищений, являющихся достаточными для принятия решения о возбуждении уголовного дела, 61 % опрошенных респондентов указали на признаки события преступления, среди которых выделили: перевод денежных средств на другой счет, списание денег со счетов - 11 %; время, место, способ преступления - 10 %; субъект, субъективная сторона, объект, объективная сторона преступления - 4%; незаконное проникновение в источник компьютерной информации, установление вредоносных программ - 4 %; снятие денежных средств с карты потерпевшего - 2 %; доступ у лица к дистанционному банковскому обслуживанию - 2 %; установка посторонних устройств для считывания информации; несанкционированное вмешательство в работу банковской системы - 1 %.

На признаки виновности лица в совершении преступления указали 18 % опрошенных респондентов, среди которых выделили: наличие прямого умысла - 4 %; введение в заблуждение путем обмана потерпевшего - 2 %; наличие у лица доступа к объекту -2%.

На признаки, характеризующие личность лица, причастного к деянию, указали 9 % опрошенных респондентов, среди которых выделили: профессионализм лица, наличие у него навыков в сфере компьютерных технологий - 4 %; высокий уровень знаний в сфере банковской деятельности - 1 %; наличие прямого умысла - 1 %.

На признаки вреда (ущерба), причиненного преступлением, указали 28 % опрошенных респондентов, среди которых выделили: размер причиненного ущерба - 10%, неправомерное изъятие денежных средств -4 %,

значительность размера причиненного ущерба - 3 %, движение денежных средств на счете - 2 %.

На признаки обстоятельств, которые способствовали совершению преступления, указали 17 % опрошенных респондентов, среди которых выделили: легкомыслие, доверчивость потерпевших, их неграмотность в данной сфере - 6 %, несовершенство средств информационной безопасности -6%.

Среди иных признаков респонденты указали на недостаточную защищенность средств сотовой связи от вирусов - 1 %.

Как несложно убедиться, следователи в ходе анкетирования нередко отвечали не на поставленный вопрос, а о причинах и условиях совершения хищений. Пожалуй, только этим можно объяснить столь широкую палитру мнений по вопросу о признаках, достаточных для принятия решения о возбуждении уголовного дела.

Как представляется, в целом признаки рассматриваемых хищений аналогичны тем, которые свойственны любым кражам, мошенничествам, присвоениям или растратам, но с учетом организационно-правовой формы предмета посягательства (безналичные денежные средства). Независимо от разновидности хищений перечень признаков, данные о которых образуют основание возбуждения уголовного дела, включает: списание денежных средств со счета (изъятие денежных средств); противозаконное перечисление этих средств без согласия и вопреки воле собственника или владельца (противоправность); зачисление этих средств на счета иных лиц без эквивалентной компенсации (безвозмездность)

Безвозмездность заведомо предполагается, поскольку денежные средства со счета пострадавшего переводятся на счета, оформленные, как правило, на чужие похищенные паспорта; перечисление средств осуществляется по «цепочке» аналогичных счетов; отдельные счета в электронной платежной системе, использованные при хищении денежных средств, достаточно быстро закрываются преступниками. Сам факт перечисления со счета пострадавшего денежных средств всегда предполагает наличие их получателя, в качестве которого выступает фактический владелец счета, на который переведены денежные средства. Отслеживанием цепочки счетов, участвующих в перечислении похищенных денежных средств, данный фактический владелец счета может быть установлен.

Инициирование соответствующих операций с целью завладения этими средствами, т. е. получение материальной выгоды (корыстная цель); уменьшение баланса счета (причинение ущерба собственнику или владельцу). При этом данные о признаках способа хищения, т. е. каким-образом преступники осуществили операции по счету собственника или владельца числящихся на нем денежных средств (напр., путем модификации, копирования, блокирования и (или) уничтожения информации), а также об орудиях преступления (вредоносная программа, скимминг и т. п.) являются необходимыми для принятия решения о возбуждении уголовного дела.

Невозможно согласиться в полном объеме с позицией, согласно которой перечень признаков хищений ограничен данными, подтверждающими модификацию либо копирование информации. В перечень таких признаков, в зависимости от разновидности хищений, могут входить уничтожение или

блокирование информации, о чем подробно было сказано в настоящей работе (раздел, посвященный криминалистической характеристике хищений).

В соответствии с положениями УПК РФ и ведомственными нормативными актами должностное лицо, правомочное либо уполномоченное проводить проверку или организацию проверки сообщения о преступлении, с учетом содержащихся в сообщении сведений, требующих неотложного реагирования, обязано в пределах своей компетенции принять незамедлительные меры:

по предотвращению и пресечению преступления;

по обнаружению признаков преступления, сохранению и фиксации следов преступления, а также доказательств, требующих закрепления, изъятия и исследования;

по проведению розыскных и оперативно-розыскных мероприятий по установлению и задержанию с поличным или «по горячим следам» лиц, подготавливающих, совершающих или совершивших преступление.

О принятых мерах неотложного реагирования по сообщению о преступлении и их результатах должно быть в максимально короткий срок, не более чем в течение 24 часов, доложено соответствующему начальнику ОПС или органу дознания для организации дальнейшей проверки этого сообщения.

Поскольку проверка сообщений о любом преступлении проводится в сроки, жестко регламентированные действующим уголовно-процессуальным законом (ч.ч. 1 и 3 ст. 144 УПК РФ), целесообразно составить план ее проведения, в который включить:

1) организацию мероприятия по ознакомлению с сообщением и исходной информацией о хищении, содержащихся в представленных потерпевшим материалах;

2) выдвижение версий, определение вопросов, подлежащих выяснению;

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

В юридической литературе сотрудники правоохранительных органов зачастую именуют проверку сообщений о преступлениях предварительной или доследственной проверкой.

Несмотря на то, что проверки проводят, как правило, сотрудники оперативных подразделений и даже службы участковых уполномоченных полиции, следователь должен принять участие в составлении плана проверки.

В план проверки заявления о хищении рекомендуется включать следующие действия (операции):

1) получение письменного объяснения у потерпевшего (его представителя),

2) осмотр места происшествия (точка размещения банкомата, помещение с компьютером, подключенным к системе ДБО и т. п.)

3) истребование в ходе осмотра места происшествия или путем направления запроса пострадавшему документов и сведений, относящихся к событию

хищения. Ознакомление с перечисленными и иными документами и осуществление их анализа.

4) получение письменных объяснений;

5) истребование в кредитных организациях сведений и документов, относящихся к хищению. Ознакомление и анализ изъятых в кредитных организациях отправителя (потерпевшего) сведений и документов;

6) получение письменных объяснений от работников кредитных организаций;

7) истребование у Интернет-провайдера или оператора связи соответствующих документов и сведений;

8) получение объяснения от работника Интернет-провайдера или оператора связи (при необходимости);

9) анализ результатов осмотра места происшествия, полученных объяснений, документов и сведений для решения вопроса о необходимости производства исследований либо назначения и производства СКЭ и других судебных экспертиз;

10) дача поручений органам, осуществляющим оперативно-розыскные мероприятия (далее - ОРМ).

В плане могут быть предусмотрены и другие проверочные и ознакомительные действия. В очередность перечисленных следственных действий, оперативно-розыскных, проверочных и организационных мероприятий могут быть внесены коррективы.

В ходе проверки сообщений о рассматриваемых преступлениях как уже отмечено, могут проводиться ОРМ, определенные ч. 1 ст. 6 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее - Закон об ОРД) по поручению следователя (дознавателя). Организация и тактика производства ОРМ регламентируется ведомственными нормативными актами, в том числе содержащими сведения, отнесенные к государственной тайне. В связи с этим в настоящей работе возможно указать только некоторые общие требования производства ОРМ.

Наиболее распространенными (типичными) ОРМ в стадии возбуждения уголовного дела являются: снятие информации с технических каналов связи; наблюдение; контроль почтовых отправлений, телеграфных и иных сообщений; прослушивание телефонных переговоров; наведение справок; исследование предметов и документов.

Исследование, проведенное А.В. Рыбкиным, позволило ему сделать вывод, что при осуществлении ОРД, направленной на выявление преступлений в сфере компьютерной информации, чаще всего проводятся следующие ОРМ: опрос граждан (в 93% случаев); наведение справок (61%); исследование документов (57%); наблюдение (50%); исследование машинных носителей информации (26%); оперативный осмотр СВТ (24%). Реже используются: контроль почтовых отправлений, телеграфных и иных сообщений (в т. ч. «электронной почты») - в 18% случаев; отождествление личности (в 15% случаев); обследование помещений, зданий, сооружений, участков местности и транспортных средств (13%); исследование СВТ (12%). Практически не используются такие мероприятия как: прослушивание телефонных переговоров (7%) и оперативное внедрение (4%). Одновременно с указанным, стоит подчеркнуть,

что такое важное, применительно к рассматриваемым преступным деликтам, оперативно-разыскное мероприятие как снятие информации с технических каналов связи не было обнаружено исследователем при изучении материалов практики.

Кратко рассмотрим некоторые из них

Снятие информации с технических каналов связи - это ОРМ, направленное на конспиративное получение с последующим документированием субъектами оперативно-розыскной деятельности фактической или оперативно-значимой информации, путём съёма (перехвата) с помощью специальных технических средств текстовой, графической и иной информации, передаваемой проверяемыми лицами по телексным, факсимильным, селекторным, радиорелейным каналам передачи данных, системам персонального радиовызова (пейджинговая связь), а также линиям абонентского телеграфирования, IP-телефонии, электронной почте и иным каналам связи.

Для технического обеспечения проведения данного мероприятия на сетях электросвязи, используемых для услуг передачи данных телематических служб, включая Интернет, создана Система технических средств по обеспечению ОРМ (СОРМ) «технические требования», которая регламентирована приказом Министерства информационных технологий и связи РФ от 16 января 2008 г. № 6 «Об утверждении требований к сетям электросвязи для проведения оперативно-розыскных мероприятий». Данное ОРМ осуществляется только на основании соответствующего судебного решения с использованием оперативно-технических сил и средств подразделений МВД России и ФСБ России.

Наблюдение - состоит в тайном, целенаправленном, систематическом, непосредственном (визуальном) или опосредованном (с помощью использования специальных технических средств) восприятии и фиксации фактической или оперативно-значимой информации для решения конкретных задач оперативно-розыскной деятельности.

В зависимости от метода получения информации (непосредственно или с помощью удаленного доступа) выделяют три основных вида наблюдения: физическое, электронное и смешанное. Физическое - основано на визуальном методе получения информации и заключается в негласном, непосредственном восприятии наблюдателем деятельности изучаемого лица или объекта. Наблюдателем является, как правило, сотрудник оперативно-поискового подразделения субъекта оперативно-розыскной деятельности или агент.

Электронное - проводится с помощью специальных технических средств с удаленного контрольного пункта и заключается в негласном, направленном восприятии деятельности изучаемого лица или материального объекта посредством аудио - и видео - средств, с целью слухового или визуального контроля, а также документирования преступных действий.

Электронное наблюдение, как оперативно-техническое мероприятие, проводится сотрудниками оперативно-технических подразделений субъектов оперативно-розыскной деятельности. Его не стоит смешивать с электронным наблюдением, осуществляемым в публичных местах (вокзалы, метро, магазины, автомобильные стоянки и т. п.). В данном случае преследуются совершенно другие цели, не ограничиваются конституционные права граждан и не привлекаются субъекты оперативно-розыскной деятельности. Но

относиться наблюдение с использованием сетей связи при помощи специальных компьютерных программ и компьютерных устройств. Разновидностями такого наблюдения являются:

электронное наблюдение на сетях связи общего пользования;

электронное наблюдение на выделенных сетях связи;

электронное наблюдение на технологических сетях связи, присоединенных к сети связи общего пользования.

Сеть связи общего пользования предназначена для возмездного оказания услуг электросвязи любому пользователю услугами связи на территории Российской Федерации и включает в себя сети электросвязи, определяемые географически в пределах обслуживаемой территории и ресурса нумерации, и не определяемые географически в пределах территории Российской Федерации и ресурса нумерации, а также сети связи, определяемые по технологии реализации оказания услуг связи. Сеть связи общего пользования представляет собой комплекс взаимодействующих сетей электросвязи, в том числе сети связи для распространения программ телевизионного вещания и радиовещания. Сеть связи общего пользования имеет присоединение к сетям связи общего пользования иностранных государств (ст. 13 Федерального закона «О связи»)

Выделенными сетями связи являются сети электросвязи, предназначенные для возмездного оказания услуг электросвязи ограниченному кругу пользователей или группам таких пользователей. Выделенные сети связи могут взаимодействовать между собой. Выделенные сети связи не имеют присоединения к сети связи общего пользования, а также к сетям связи общего пользования иностранных государств. Технологии и средства связи, применяемые для организации выделенных сетей связи, а также принципы их построения устанавливаются собственниками или иными владельцами этих сетей. Выделенная сеть связи может быть присоединена к сети связи общего пользования с переводом в категорию сети связи общего пользования, если выделенная сеть связи соответствует требованиям, установленным для сети связи общего пользования. При этом выделенный ресурс нумерации изымается и предоставляется ресурс нумерации из ресурса нумерации сети связи общего пользования. Оказание услуг связи операторами выделенных сетей связи осуществляется на основании соответствующих лицензий в пределах указанных в них территорий и с использованием нумерации, присвоенной каждой выделенной сети связи в порядке, установленном федеральным органом исполнительной власти в области связи (ст. 14 Федерального закона «О связи»)

Технологические сети связи предназначены для обеспечения производственной деятельности организаций, управления технологическими процессами в производстве. Технологии и средства связи, применяемые для создания технологических сетей связи, а также принципы их построения устанавливаются собственниками или иными владельцами этих сетей. При наличии свободных ресурсов технологической сети связи часть этой сети может быть присоединена к сети связи общего пользования с переводе м в категорию сети связи общего пользования для возмездного оказания услуг связи любому пользователю на основании соответствующей лицензии. Такое присоединение допускается, если: часть технологической сети связи, предназначаемая для присоединения к сети связи общего пользования,

может быть технически,^ или программно, или физически отделена собственником от технологической сети связи; присоединяемая к сети связи общего пользования часть технологической сети связи соответствует требованиям функционирования сети связи общего пользования. Части технологической сети связи, присоединенной к сети связи общего пользования, выделяется ресурс нумерации из ресурса нумерации сети связи общего пользования в порядке, установленном федеральным органом исполнительной власти в области связи (ст. 15 Федерального закона «О связи»),

В зависимости от способа передачи сигнала и используемых при этом средств связи (могут использоваться на любой из категорий сетей электросвязи):

1) электронное наблюдение на электронных (цифровых) автоматических телефонных станциях. Проводится на всех отечественных и импортных электронных автоматических телефонных станциях, устанавливаемых на территории России и входящих в состав единой сети электросвязи Российской Федерации («проводная» электросвязь). Включают в себя сельские, городские, управленческие, междугородние, международные и комбинированные электронные автоматические телефонные станции независимо от формы собственности и ведомственной принадлежности. Предназначено для получения информации в различных режимах времени, как следственными органами, а в случае необходимости и судом, так и правоприменительными органами на основании действующего законодательства.

2) электронное наблюдение на сетях подвижной радиотелефонной связи;

3) электронное наблюдение в транкинговых системах подвижной радиотелефонной связи. Позволяет осуществлять контроль абонентских соединений и местоположение пользователей транкинговой подвижной радиосвязи в соответствии с действующим законодательством (название данного вида связи происходит от английского слова «trunk» ствол). Проводится на всех отечественных и импортных коммутаторах рассматриваемого вида связи стандарта SmartTrank, MPT-1327, SmartNet, LTR, ESAS, ED ACS, TETRA и др.

4) электронное наблюдение на сетях персонального радиовызова общего пользования. Пейджинговая связь происходит от английского слова «page» - страница. Позволяет осуществлять мониторинг сообщений абонентов передаваемых операторами связи в стандарте FLEX, POGSAC и др.

5) электронное наблюдение на сетях документальной электросвязи. Сети документальной электросвязи включают себя такие трансграничные информационно-телекоммуникационные сети, как Интернет (World Wide Web -«всемирная информационная паутина»), электронную почту, факсимильную связь, системы передачи данных различной направленности, IP- телефонию (весь комплекс информации в электронном виде передаваемой по единой сети электросвязи России).

6) электронное наблюдение на системе глобальной подвижной персональной спутниковой связи. Позволяет осуществлять контроль информации, передаваемой по каналам спутниковой связи.

В качестве отдельного вида электронного наблюдения необходимо выделить видеозапись с использованием мультимедиа-технологий. Во всех больших

городах постепенно увеличивается число видеокамер, объективы которых направлены не только на транспортные узлы, но и на пешеходные зоны, магазины, офисы, автостоянки, жилые помещения и т. д. На одной только Трафальгарской площади вокруг Колонны Нельсона установлено более 40 видеокамер наружного наблюдения. Как правило, управление видеонаблюдением является удаленным. Технологии позволяют пользователю контролировать события через Интернет с помощью веббраузера с любого компьютера и из любой точки мира.

Смешанное (комплексное) - основано на применении двух вышеназванных видов наблюдения одновременно.

Контроль почтовых отправлений, телеграфных и иных сообщений -заключается в действиях по конспиративной перлюстрации (перлюстрация (от лат. perlustrare) - вскрытие и просмотр без ведома адресата) письменной или иной зафиксированной на материальном носителе корреспонденции с целью обнаружения сведений о преступной деятельности изучаемого лица, проводимой специальными подразделениями органов, осуществляющих оперативно-розыскную деятельность, посредством личного участия в организации и проведении непосредственно в учреждениях связи по месту отправления или поступления объектов контроля, используя при этом помощь должностных лиц и специалистов, обладающих научными, техническими и иными специальными знаниями, а также отдельных граждан с их согласия на гласной и негласной основе.

Субъектом рассматриваемого оперативно-технического мероприятия в соответствии с ч. 4 ст. 6 Закона об ОРД является ФСБ. Детализацию этой нормы см.: п. 1 Указа Президента РФ от 01.09.1995 г. № 891 «Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств» // Собрание законодательства РФ. 1999. № 24. Ст. 2954.

Прослушивание телефонных переговоров - комплексное оперативно-техническое мероприятие по конспиративному слуховому контролю с обязательным использованием специальных технических средств переговоров, ведущихся лицами оперативной заинтересованности субъектов оперативно-розыскной деятельности, с использованием названными лицами линий единой сети электросвязи России и услуг операторов связи России, их документированием с целью получения фактической или оперативнозначимой информации о преступной деятельности изучаемого лица.

Прослушивание телефонных переговоров с подключением к станционной аппаратуре предприятий, учреждений и организаций независимо от форм собственности, физических и юридических лиц, предоставляющих услуги и средства связи, со снятием информации с технических каналов связи проводится с использованием оперативно-технических сил и средств, в том числе органов ФСБ России, МВД России в порядке, определяемом межведомственными нормативными актами или соглашениями между органами, осуществляющими оперативно-розыскную деятельность.

Отметим, что проведение ОРМ, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, допускается на основании судебного решения.

В связи с тем, что хищения могут носить международный (трансграничный) характер, в ходе документирования должно осуществляться взаимодействие с правоохранительными органами иностранных государств по каналам Интерпола и др.

В соответствии с Инструкцией по организации информационного обеспечения сотрудничества по линии Интерпола, утвержденной приказом МВД РФ № 786, Минюста РФ № 310, ФСБ РФ № 470, ФСО РФ № 454, ФСКИ РФ № 333, ФТС РФ № 971 от 6 октября 2006 г.129 (далее - Инструкция по линии Интерпола), оперативные подразделения посредством Национального центрального бюро Интерпола при МВД России могут обратиться с запросом к правоохранительным органами иностранных государств - членов Интерпола, Генеральному секретариату с целью получения следующей информации по фактам трансграничных хищений:

о сетевых адресах, именах доменов и серверов организаций и пользователей;

о содержании протоколов, трейсингов, логических файлов; об электронной информации, заблокированной в порядке оперативного взаимодействия правоохранительных органов при пресечении трансграничных правонарушений;

о провайдерах и дистрибьюторах сетевых и телекоммуникационных услуг;

о физических и юридических лицах, имеющих отношение к хищению и др.

Также НЦБ Интерпола МВД России осуществляет международный обмен информацией о преступлениях, связанных с хищением денежных средств с банковских платежных карт. С этой целью в телекоммуникационной сети Интерпола 1-24/7 функционирует директория прямого доступа к базам данных по «BIN» платежных систем «MasterCard» и «Visa» (удаленно - «American Express»).

При проверке 6-значного «BIN» платежной карты база данных выдает информацию о банке-эмитенте и государстве его нахождения.

Кроме того, оперативные подразделения могут воспользоваться возможностями Национального контактного пункта и каналами связи «горячей линии», предназначенных для оперативного взаимодействия с правоохранительными органами государств - участников СНГ управления «К» БСТМ МВД России в целях выявления и раскрытия трансграничных хищений. Каналы связи «горячей линии», предназначенные для оперативного взаимодействия с правоохранительными органами стран Содружества, определены в соответствии с решением Совета министров внутренних дел (полиции) государств - участников СНГ от 7 сентября 2007 г. «О повышении эффективности сотрудничества в борьбе с преступностью в сфере информационных технологий».

Как правило, продуманное и грамотное документирование в рамках исполнения поручений следователей (дознавателей) позволяет выявить данные, указывающие на признаки хищения рассматриваемого вида, всех лиц, причастных к его совершению, формальные и неформальные связи между ними, их характеризующие данные, в том числе клички (сетевые псевдонимы) и посещаемые сайты в сети Интернет, в том числе «хакерской» направленности, средства хищений (компьютеры, программное обеспечение, банковские карты, телефоны, с которых устанавливается связь,

автотранспорт и т. п.), и т. п., что предопределяет успех не только первоначальных следственных действий по закреплению доказательств и задержанию преступников, но и результативность всего предварительного следствия. В частности, документирование позволяет создать предпосылки последующему доказыванию обстоятельств создания, распространения и использования вредоносных программ, предназначенных для блокировки, уничтожения, модификации компьютерной информации и нейтрализации средств защиты при неправомерном доступе к банковским счетам.

Результаты проверки сообщений о хищениях, представляемые должностным лицом ОПС для решения вопроса о возбуждении уголовного дела, должны содержать не только достаточные данные, указывающие на признаки преступления, но и сведения о том, где, когда данные признаки обнаружены, при каких обстоятельствах имело место их обнаружение и очевидцах преступления (если они известны), о местонахождении объектов (компьютеры, банковские карты, документы и т. п.), которые могут быть признаны вещественными доказательствами по уголовному делу.

По информации ОПС, количество рассмотренных следователями проверочных материалов о хищениях, поступивших из органов дознания, за 2014 - 2015 гг. составило 8177. При этом в 2015 г. таких материалов было рассмотрено в 2,8 раза больше, чем в 2014 г. (2014 г. - 2128, 2015 г. - 6049). Основным недостатком качественной составляющей таких материалов является неполнота проверки, что явилось основанием для возвращения в орган дознания всего за два года 2029 материалов, что составило 24,8 % от общего количества рассмотренных. Следует заметить, что в 2015 г. доля материалов, возвращенных в орган дознания по обозначенным основаниям, возросла по сравнению с 2014 г. на 23,9 % и составила 31 % (2014 г. -153, 2015 г. - 1876). Другими основаниями возвращения материалов в орган дознания явились: отсутствие признаков хищения - 31 (2014г.-8,2015г,-13), недостатки в материалах ОРМ - 31 (2014 г. - 15, 2015 г. - 16) и иные основания - 38 (2014 г. - 13, 2015 г. - 25).

Говоря о качестве материалов проверки сообщений о хищениях, которые поступают от органов дознания в ОПС, следует отметить, что по результатам опосредованного анкетирования большинство следователей оценивают его удовлетворительно - 69 %, а согласно мнению 21 % опрошенных качество таких материалов является неудовлетворительным, и всего 6 % респондентов полагают его хорошим.

Выделяя недостатки, имеющиеся в материалах проверки сообщений о хищениях, поступающих от органов дознания в органы предварительного следствия, большинство респондентов отметили следующие:

отсутствие в материалах сведений о движении похищенных средств (данных из коммерческих организаций, процессинговых центров и др.) -36 %;

отсутствие в материалах сведений о средствах совершения и сокрытия преступления (не установлена информация о нахождении «хостинг-сервиса», Интернет-сайта, о мерах защиты компьютерной информации и др.) - 27 %; в частности - отсутствие возможности установления серверов, в т. ч. за пределами РФ - 2 %;

отсутствие в материалах объяснений лиц, имеющих сведения о проверяемом событии (сотрудников Интернет-провайдера, отдела безопасности кредитной или иной коммерческой организации и др.) - 24 %.

Среди иных недостатков, присущих материалам проверки, респонденты также отметили:

недостатки в организации проведения ОРМ - 19 %, среди которых: непроведение ОРМ в полном объеме, в том числе по детализации телефонных звонков - 3 %, неполнота материалов ОРМ - 4 %, непроведение до возбуждения уголовного дела контроля и записи телефонных переговоров и отсутствие оперативности - 1 %;

отсутствие сведений, указывающих на признаки хищения - 9 %; отсутствие ответов из банков и сотовых компаний - 2 %, отсутствие выписок по счетам - 3 %, несвоевременное направление запросов и предоставление документов из кредитных организаций - 1 %;

неправильное определение территориальности и подследственности - 9 %;

нарушения законодательства при проведении ОРМ - 4 %, в том числе не в полном объеме предоставление документов и электронных носителей информации - 2 %;

недостатки в тактике проведения ОРМ - 4 %.

Результаты анкетирования в большей своей части подтверждаются анализом поступившей из ОПС информации. Так, по информации ГСУ ГУ МВД России по Кемеровской области, ГСУ ГУ МВД России по Новосибирской области и некоторых других ОПС характерными (типичными) ошибками (недостатками, проблемами), совершаемыми на стадии возбуждения уголовного дела и (или) документирования, являются невыяснение всех необходимых обстоятельств совершенного преступления, утрата вещественных доказательств, технические ошибки. По информации ГСУ ГУ МВД России по Нижегородской области - возбуждение нескольких уголовных дел по одному факту хищения, в связи с тем, что гражданин может подать несколько заявлений в разные инстанции. По информации СУ УМВД России по Омской области - направление запросов в коммерческие банки о предоставлении документов о наличии у потерпевшего банковского счета, платежной карты и движении денежных средств по ней, а также об адресате получателя похищенных денежных средств, без судебного решения. По информации СУ МВД Республики Хакасия - несвоевременное изъятие сотового телефона у потерпевшего с целью осмотра и проведения судебной технической экспертизы. По информации СУ МВД по Чувашской Республике - неправильное определение места и способов совершения преступного деяния. По информации СУ МВД России по Чукотскому автономному округу - нарушение законодательства при проведении ОРМ, а также непроведение ОРМ, направленных на установление лиц, совершивших хищения, использующих в преступных целях одни и те же абонентские номера и счета на протяжении до двух месяцев. По информации СУ МВД России по Владимирской области - направление запросов в сотовые компании только с целью установления лиц, на которые зарегистрированы абонентские номера, без установления соответствующего IMEI - кода устройств.

Некоторые ОПС обращают внимание на неверную квалификацию преступного деяния по ст. 159.6 УК РФ на стадии возбуждения уголовного дела. Одним из

условий неверной квалификации, согласно информации СУ УМВД по Владимирской области, является то, что по результатам рассмотрения претензий потерпевших Владимирским отделением ПАО «Сбербанк России» высказывается предположение, что мобильные устройства заявителей, с помощью которых происходит дистанционное обслуживание их банковских счетов, поражены вредоносным программным обеспечением (вредоносной программой), позволяющим тайно для владельца счета похищать денежные средства, то есть фактически дистанционно управлять его счетом и мобильным устройством, а именно: направлять и получать SMS-команды от сервисного номера ОАО «Сбербанк России» 900, оставаясь при этом невидимым для владельца счета и мобильного устройства. Далее заявителю разъясняется, что согласно правил пользования банковскими картами, антивирусная безопасность его мобильного устройства полностью возлагается на владельца этого устройства. Ни в одном ответе не было предложено провести исследование мобильного устройства на предмет наличия в нем вредоносной программы.

В связи с отмеченным, представляется необходимым обратить внимание на следующие обстоятельства.

Во-первых, вопрос о квалификации преступного деяния, если о ней вообще уместно говорить в стадии возбуждения уголовного дела, находится в компетенции должностных лиц, осуществляющих проверку сообщений о хищениях денежных средств, совершаемых с использованием компьютерных технологий.

Во-вторых, установление признаков способа хищений находится в компетенции указанных должностных лиц, а не работников ОАО «Сбербанк России».

В-третьих, при наличии данных о совершенном хищении с использованием вредоносной программы следует, на основании ч.1 ст. 144 УПК РФ, провести исследование компьютерного (мобильного) устройства.

Между тем, как справедливо отмечается в информационных письмах ОПС, во многих регионах отсутствуют в системе ОВД необходимое программное обеспечение и специалисты, способные проводить исследование (судебные экспертизы) на предмет выявления в компьютерных устройствах вредоносных программ.

Перечисленные недостатки и ошибки в конечном итоге влияют на объективность, полноту и качество предварительного следствия. Устранение их в большинстве своем связано с надлежащей организацией деятельности ОВД в целом, разработкой методических рекомендаций и обучением, как следователей, так и иных должностных лиц, осуществляющих проверки по сообщениям о хищениях.

Как представляется, для принятия обоснованного решения о возбуждении уголовного дела о любой разновидности рассматриваемых хищений, в распоряжении следователя должны находиться следующие сведения и документы:

письменное заявление потерпевшего - гражданина или представителя юридического лица либо протокол принятия устного заявления о преступлении, составленный в соответствии с действующим уголовно-процессуальным законодательством;

рапорт об обнаружении признаков преступления и приложенные к нему материалы, полученные в ходе производства оперативно-розыскных мероприятий, и других проверочных действий;

письменное объяснение заявителя, в котором содержатся данные о времени и месте совершения и обнаружения преступления, предмете преступного посягательства и его индивидуальных признаках;

документы либо их копии, подтверждающие право собственности на похищенные денежные средства или их владением, право использования компьютерных технологий (ДБО, платежной карты и т. п.), например: письменный договор на получение услуг сети Интернет, электросвязи по конкретному абонентскому номеру или обслуживание по платежной карте; пластиковая карта; документ о праве обладания (пользования) программным обеспечением ДБО; базой данных, электронным ресурсом сети Интернет, электронной цифровой подписью и т. п;

письменное заключение специалиста и (или) заключение экспертов, проводивших исследование средств компьютерных технологий, в том числе компьютерных программ;

идентификационные данные о владельце (собственнике, пользователе) компьютерного устройства и его программного обеспечения, возможно, осуществившем несанкционированный доступ к информатизационной автоматизированной банковской системе, например: IP-адрес, IMEI или иной идентификатор компьютерного устройства или в информационно-телекоммуникационной сети либо сети электросвязи, а также логин, пароль и номер абонента в сети электросвязи (номер телефона), с помощью которых был осуществлен такой доступ;

протокол осмотра места происшествия, предметов и документов, в т.ч. электронных носителей информации, электронных документов, электронных сообщений, сайта или страницы в сети Интернет;

документы, подтверждающие факт использования орудий хищений (напр., вредоносных компьютерных программ), в том числе протоколы проведения соответствующих оперативно-розыскных мероприятий и приложенных к нему документов.

Представление результатов оперативно-розыскной деятельности должностным лицом ОПС осуществляется в соответствии с положениями Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд, утвержденной приказом МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27 сентября 2013 г.132 (далее - Инструкция о результатах ОРД), с учетом положений которой и методических рекомендаций133, а также специфики рассматриваемых хищений в направляемых для возбуждения уголовного дела материалах должны содержаться следующие сведения и документы:

сопроводительное письмо руководителя органа дознания (оперативной службы);

рапорт сотрудника, проводившего оперативно-розыскные и иные мероприятия;

документы, фиксирующие этапы проведения оперативно-розыскных мероприятий (за исключением сведений, составляющих государственную тайну);

протоколы наблюдений, оперативного эксперимента и контрольных закупок (при продаже, распространении электронных носителей информации с вредоносными компьютерными программами);

протоколы и стенограммы прослушивания телефонных переговоров и иных сообщений (радиообмена, пейджинговых, модемных, иных), перехвата информации с иных каналов связи, свидетельствующие о неправомерной деятельности конкретных лиц (необходимо иметь в виду, что согласно действующему законодательству указанные оперативно-розыскные мероприятия могут проводиться только на основании судебного решения и только в отношении преступлений особо тяжких, тяжких и средней тяжести);

протоколы перехвата и регистрации информации электронной почты лиц, причастных к хищению;

протоколы оперативного наблюдения с приобщенными фото- и видеокадрами;

материалы оперативных экспериментов;

протоколы изъятия образцов для сравнительного исследования с участием специалистов;

протоколы (акты) изъятия компьютерных устройств либо отражение такого изъятия непосредственно в протоколах оперативно-розыскных мероприятий (следует обратить внимание на тот факт, что доказательства, изъятые в ходе проведения оперативно-розыскных мероприятий, в соответствии со ст. 89 УПК РФ должны отвечать требованиям, предъявляемым к доказательствам, указанным Кодексом (разъяснение соответствующих прав лицам, присутствующим при изъятии, присутствие общественных наблюдателей и т. п.);

бумажные распечатки информации с изъятых электронных носителей информации, в том числе информации, находившейся на жестком диске переносного компьютера;

материалы лабораторных исследований носителей информации и находящихся на них компьютерных программ; объяснения должностных и иных лиц; инструкции, справки, другие документы и материалы. При передаче должностным лицом ОПС материалов, документов и иных объектов, полученных при проведении ОРМ, должны быть приняты необходимые меры по их сохранности и целостности (защита от деформации, размагничивания, обесцвечивания, стирания и другие). Фонограммы, полученные в результате прослушивания телефонных и иных переговоров, представляются должностным лицом ОПС в опечатанном виде в условиях, исключающих возможность их прослушивания и тиражирования посторонними лицами с приложением бумажных носителей записи переговоров.

Допускается представление материалов, документов и иных объектов, полученных при проведении ОРМ, в копиях (выписках), в том числе с переносом наиболее важных частей (разговоров) на единый носитель, о чем обязательно указывается в рапорте и на бумажном носителе записи переговоров. При этом оригиналы данных объектов, если они не были в дальнейшем истребованы должностным лицом ОПС, хранятся в органе,

осуществившем ОРМ, до завершения судебного разбирательства и вступления приговора в законную силу, либо до прекращения уголовного дела (уголовного преследования). Так, например, результатом ОРМ - прослушивание телефонных переговоров является соответствующая аудиозапись телефонных переговоров, общий объем которой в оцифрованном виде может превышать десятки гигабайт компьютерной памяти. Как правило, аудиозапись телефонных переговоров содержит, наряду с уголовно-релевантной информацией, в большом количестве нейтральные сведения. В связи с этим в полном объеме представлять запись телефонных переговоров и ее распечатку нецелесообразно. В таком случае должностным лицом ОПС представляются аудиозаписи телефонных переговоров и их распечатки, содержащие наиболее значимые разговоры между членами преступной группы, касающиеся процессов ее формирования и функционирования, распределения ролей между членами группы и вознаграждения каждого, используемых вредоносных программ и их усовершенствования, совершения отдельных преступных действий, вывода и обналичивания похищенных денежных средств, а также осознания членами группы преступного характера совершаемых ими действий, в том числе заливщиками, администраторами, дроппами и т.п.

Также большой объем информации может содержаться по результатам ОРМ - снятия информации с технических каналов связи по электронным почтовым ящикам (копии входящих и исходящих писем). В связи с этим должностным лицом ОПС предоставляется справка, включающая распечатку наиболее значимых писем (текстовое содержание письма, приложения и технические заголовки). В частности, такие письма могут содержать электронные сообщения одной кредитной организации другой по факту перечисления денежных средств, которые явились предметом хищения, подложные платежные поручения, копии документов членов преступной группы и (или) подставных лиц и т. п.

Все вышеуказанные документы и содержащиеся в них сведения необходимо оценить с позиций законности получения, достоверности и достаточности для принятия того или иного процессуального решения. В этих целях, как подчеркивается в литературе, исключительно важное значение имеют консультации следователей со специалистами. Между тем, по мнению авторов настоящей работы, специалисты должны привлекаться не только для оценки собранных материалов в ходе проверки сообщения о хищении, но и во время ее проведения. В частности, специалисты могут консультировать сотрудников ОВД по вопросам обнаружения, идентификации и изъятия электронных носителей информации в конкретной ситуации, участвовать в проверочных действиях (напр., в осмотре места происшествия и т.п.), в том числе в ОРМ, с целью оказания содействия в обнаружении, идентификации и изъятии электронных носителей информации и документов, поиске компьютерной информации в соответствии с указанными характеристиками, копировании криминалистически значимой компьютерной информации с их носителей, которые по каким-либо причинам не могут быть изъяты, в идентификации и опросе лиц, которые могут располагать сведениями, имеющими отношение к проверяемому событию, в составлении протокола (по вопросам, требующим специальных знаний), а также в проведении компьютерных исследований.

При необходимости начальники ОПС и начальники органа дознания вправе по мотивированному ходатайству соответственно следователя, дознавателя

продлить до 10 суток срок проверки сообщения о хищениях, а для проведения судебных экспертиз, исследований документов, предметов, а также проведения оперативно-розыскных мероприятий начальник ОПС по ходатайству следователя, а прокурор по ходатайству дознавателя вправе продлить этот срок до 30 суток с обязательным указанием на конкретные, фактические обстоятельства, послужившие основанием для такого продления (ч. 3 ст. 144 УПК РФ).

Отметим, что по поступившей от ОПС информации, в порядке ст. 144 УПК РФ следователями в течение 2014 - 2015 гг. рассмотрено 19421 сообщение о хищениях. При этом в 2015 г. нагрузка на ОПС в данной части возросла практически в 3,3 раза (2014 г. - 4517, 2015 г. - 14904).

Наибольшее количество материалов было рассмотрено в срок до трех суток - 8625, что составило 44,4 % от общего количества рассмотренных (2014 г. - 1678, 2015 г. - 6947), до десяти суток рассмотрено 6345 материалов или 32,6 % (2014 г. - 1662, 2015 г. - 4683), до тридцати суток - 4344 или 22,3 % (2014 г. - 1051, 2015 г. - 3293). С положительной стороны следует отметить, что доля материалов, рассмотренных в срок, не превышающий трех суток, ежегодно увеличивается и в 2015 г. составила 46,6 % в сравнении с 37,1 % в 2014 г.

С учетом данных, полученных в результате предварительной проверки сообщения о хищении, принимается решение о возбуждении уголовного дела, об отказе в его возбуждении или передаче сообщения о преступлении по подследственности в соответствии с положениями ст. 151 УПК РФ. Так, если при проверке поступившего и зарегистрированного сообщения о хищении будет установлено, что с учетом территориальности оно подлежит передаче в другой орган по подследственности, орган дознания, дознаватель, следователь, а также иное должностное лицо, уполномоченное осуществлять прием и проверку сообщений о преступлениях, обязано вынести постановление о передаче сообщения по подследственности.

Иным должностным лицом, уполномоченным осуществлять прием и проверку сообщений о преступлениях, является лицо, на которое начальником органа дознания или его заместителем посредством издания организационно-распорядительного документа возложены полномочия органа дознания.

При этом по сообщениям о преступлениях, требующим неотложного реагирования, информация, содержащаяся в сообщении, либо постановление с этим сообщением должны быть предварительно переданы в соответствующий орган по подследственности по каналам экстренной связи.

Обращаясь к практике путем анализа поступившей информации от ОПС, установлено, что по сообщениям о хищениях следователями принято 20304 решения (2014 г. - 4609, 2015 г. - 15695), из которых, в основном, о возбуждении уголовного дела - 19590 или 96,4 % (2014 г. - 4579, 2015 г. -15011). О передаче по подследственности или подсудности принято всего 623 решения (2014 г. - 176, 2015 г. - 447). Об отказе в возбуждении уголовного дела - 480 (2014 г. - 69, 2015 г. - 411), в том числе, за отсутствием события или состава преступления - 183, что составляет 38,1 % от общего количества отказных материалов (2014 г. - 43, 2015 г. - 140).

Как уже отмечалось, в деятельности следователей существуют сложности при принятии решения о возбуждении уголовного дела о хищении, связанные с определением подследственности. В результате материалы проверок

сообщений о хищениях продолжительное время (до 1,5 - 2 лет) перенаправляются из одного территориального органа МВД России в другой, за это время следы преступлений утрачиваются, возможности раскрыть преступления и привлечь виновных лиц к ответственности практически сводятся к «нулю».

Данные сложности предопределены проблемой установления в стадии возбуждения уголовного дела места совершения хищения, а точнее его окончания. Эта проблема усугубляет тем, что в ходе проверки сообщений о хищениях зачастую невозможно быстро установить принадлежность абонентских номеров телефонов или других мобильных устройств, места открытия банковских счетов, на которые были перечислены похищенные денежные средства, IP - адресов компьютерных устройств, с использованием которых совершаются такие преступления. Например, анализ представленных материалов доследственных проверок в Республике Адыгея показал, что хищение денежных средств у потерпевших в основном сопряжено с зачислением их на абонентские номера различных операторов сотовой связи (например, ОАО «Мобильные ТелеСистемы» (МТС), ОАО «ВымпелКом» (Билайн), ОАО «Мегафон», ОАО «Санкт-Петербург Телеком» (Теле2), ОАО «Смартс» (Самара) и т.д.), осуществлением переводов (блиц-переводов) через системы «Колибри» Сбербанка России, «Юнистрим», «Золотая корона» и электронные платежные системы «Лидер», «Контакт» (Contact), ЗАО «Киви» и другие организации. При этом в ходе проведения доследственной проверки оперативные сотрудники обращаются в суд с ходатайством о получении информации о соединениях между абонентами и абонентскими устройствами с указанием местонахождения абонентов в момент соединений. Однако суды республики не дают разрешение на проведение оперативно-розыскного мероприятия «Снятие информации с технических каналов связи», поэтому не представляется возможным установить место совершения преступления, либо постановление суда на проведение оперативно-розыскного мероприятия выносится судом с грифом «секретно», что исключает возможность получения интересующей информации напрямую у оператора сотовой связи либо в кредитной организации.

По информации ГСУ ГУ МВД России по Нижегородской области, длительность получения ответов на запросы в сотовые компании и банковские организации нередко сопровождается отсутствием в них необходимой информации (например, абонентский номер, на который перечислялись денежные средства может быть не указан вообще, очень часто указывается только название компании - провайдер и регион). В некоторых случаях невозможность определения пользователей мобильными устройствами связана с объективными причинами (например, абонентский номер зарегистрирован на юридическое лицо, либо он зарегистрирован на несуществующее лицо).

Отметим, что в некоторых регионах существуют разногласия с операторами связи о правовом порядке представления информации, которые перерастают в конфликтную ситуацию, препятствующую проведениям проверок сообщений о хищениях в разумные сроки. Так, за непредставление информации филиал ОАО «МТС» в Республике Татарстан был привлечен к административной ответственности Отделом «К» МВД по Республике Татарстан по ст. 19.7 КоАП РФ за непредставление информации. Вместе с тем и в настоящее время данная организация продолжает не представлять требуемые сведения уполномоченным сотрудникам ОВД.

Справедливости ради заметим, что, обозначая рассматриваемую проблему, некоторые ОПС внесли свои предложения по ее разрешению. Так, ГСУ ГУ МВД России по Саратовской области предлагает проблему определения места проведения доследственных мероприятий и возбуждения уголовных дел решать следующим образом: «место производства предварительного расследования определяется в соответствии со ст. 152 УПК, однако, в законодательстве нет определения места совершения преступления. Это обусловлено невозможностью отражения всех конкретных обстоятельств, которые могут иметь значение для его установления. В связи с этим место совершения устанавливается в каждом конкретном случае самостоятельно правоприменителем, исходя из особенностей конструкции состава преступления, характера совершенного деяния, примененных средств и способов причинения вреда охраняемым общественным отношениям.

Во многих случаях действия, входящие в объективную сторону состава преступления, могут совершаться в разных географических точках, каждая из которых, в npumfune, может быть признана местом совершения преступления. Однако, исходя из того, что объективная сторона мошенничества, как и любого хищения, заключается в противоправном изъятии чужого имущества, а также в приобретении права на чужое имущество, местом совершения преступления является место изъятия чужого имущества (банк, банкомат и т. п.) или место получения права на чужое имущество (например, IP-адрес, с которого осуществляется несанционированный доступ в «Личный кабинет» «он-лайн банка» потерпевшего).

По вопросу о времени окончания совершения преступления: временем окончания преступления, в соответствии с п. 12 постановления Пленума Верховного Суда Российской Федерации № 51 от 27.12.2007 «О судебной практике по делам о мошенничестве, присвоении и растрате» является момент зачисления денег на банковский счет лица, когда оно получает реальную возможность распоряжаться поступившими денежными средствами по своему усмотрению. Например, осуществлять расчеты от своего имени или от имени третьих лиц, не снимая денежных средств со счета, на который они были перечислены в результате мошенничества. Вместе с тем, этот момент сам по себе не может изменить место совершения общественно-опасного деяния, которым является место изъятия имущества, то есть место причинения ущерба собственнику или иному владельцу».

Рассматривая проблему возбуждения уголовного дела в контексте определения места совершения хищения, Следственный департамент МВД России в указаниях от 20 июня 2014 г. № 17/3-16230 «О реализации решений коллегии МВД России» рекомендовал при наличии достаточных оснований принимать процессуальное решение о возбуждении уголовного дела по месту поступления заявления о совершенном преступлении, проводить первоначальные следственные действия и, руководствуясь действующим уголовно-процессуальным законодательством Российской Федерации, определять дальнейшее место производства предварительного расследования.

Несмотря на данные рекомендации, проблема установления в предусмотренные УПК РФ сроки проверки сообщений о хищениях места его совершения, в том числе в связи с отсутствием сведений об абонентских номерах мобильных устройств и их владельцев, банковских счетах на которые были перечислены похищенные денежные средства, IP - адресов

компьютерных устройств и др. остается. В результате сотрудниками оперативных подразделений или следователями принимаются решения об отказе в возбуждении уголовного дела.

Полагаем, многочисленные процессуальные решения об отказе в возбуждении уголовного дела по указанным причинам являются недопустимыми, нарушают конституционные права граждан на доступ к правосудию, а зачастую негативно сказываются на результате предварительного следствия в связи с утратой возможности формирования доказательств по делу (например, срок хранения видеозаписи с банкомата истек и т. п.). В то же время, нарушение конституционных прав граждан находится во взаимосвязи с формированием негативного облика сотрудника ОВД в целом и ОПС в частности.

Представляется, что процессуальные решения по материалам проверок по сообщениям о хищениях в случае невозможности выявления в установленный УПК РФ срок места окончания таких преступлений, должны приниматься с учетом выявленных иных признаков хищений (противоправное безвозмездное изъятие денежных средств с банковских счетов, точное время, место и способ списания (хищения) денежных средств, лицевые счета, абонентские и электронные номера получателей похищенных денег, причинение ущерба собственнику этих средств и т.п.) и положений ст. 150 - 152 УПК РФ. В частности, согласно положениям ст. 152 УПК РФ, предварительное расследование производится по месту совершения деяния, содержащего признаки рассматриваемого вида хищения (п. 1). Если хищение было начато в одном месте, а окончено в другом, то уголовное дело расследуется по месту окончания преступления (п. 2). Если преступления совершены в разных местах, то по решению вышестоящего руководителя следственного органа уголовное дело расследуется по месту совершения большинства преступлений или наиболее тяжкого из них (п. 3), а по мотивированному постановлению руководителя вышестоящего следственного органа уголовное дело может быть передано для производства предварительного расследования в вышестоящий следственный орган с письменным уведомлением прокурора о принятом решении (п. 6).

В то же время предварительное расследование может производиться по месту нахождения обвиняемого или большинства свидетелей в целях обеспечения его полноты, объективности и соблюдения процессуальных сроков (п. 4). Если хищение денежных средств совершено с использованием компьютерных технологий вне пределов Российской Федерации, уголовное дело расследуется по основаниям, предусмотренным ст. 12 УК РФ, или в соответствии со ст. 459 УПК РФ, по месту жительства или месту пребывания потерпевшего в Российской Федерации, либо по месту нахождения большинства свидетелей, либо по месту жительства или месту пребывания обвиняемого в Российской Федерации, если потерпевший проживает или пребывает вне пределов Российской Федерации (п. 4.1.).

Кроме того, в силу положений ст. 152 УПК РФ, следователь, дознаватель, установив, что уголовное дело ему не подследственно, производит неотложные следственные действия, после чего следователь передает уголовное дело руководителю следственного органа, а дознаватель - прокурору для направления по подследственности (п. 5).

Отметим, процессуальные проблемы определения места совершения и окончания рассматриваемого вида хищений и связанные с ними определения места производства предварительного расследования, сопряжены с проблемами статистического их учета.

Исходя из положений межведомственных нормативных актов, в случаях, когда все мероприятия по установлению места окончания хищения денежных средств, совершенного с использованием компьютерных технологий, проведены, но по объективным причинам установить место окончания не представляется возможным, данное преступление подлежит учету по месту его выявления. В данном случае руководители ОПС должны руководствоваться требованиями, указанными в разделе III Положения о едином порядке регистрации уголовных дел и учета преступлений, утвержденного совместным приказом Генеральной Прокуратуры Российской Федерации, МВД России, МЧС России, Минюста России, ФСБ России, Минэкономразвития России, ФСКН России от 29 декабря 2005 года №39/1070/1021/253/780/353/399, согласно которым учет преступлений осуществляется ИЦ, на территории оперативного обслуживания которого совершено преступление. В случае если не представляется возможным определить место совершения преступления, оно подлежит учету по месту его выявления. Преступления, совершенные на территории нескольких субъектов Российской Федерации, выявленные при расследовании уголовного дела в одном субъекте Российской Федерации, учитываются по месту их совершения путем направления учетных документов в ИЦ по месту совершения каждого преступления (п. 7). Учет преступлений, уголовные дела о которых возбуждены следователями и дознавателями центральных аппаратов субъектов учета, осуществляется в ИЦ по месту проведения расследования (п. 8).

В соответствии с действующими ведомственными нормативными актами следователь имеет право заблаговременно ознакомиться с проверочными материалами, в том числе с материалами документирования, и на этой основе совместно с оперативным сотрудником выбрать в тактическом отношении наиболее оптимальный момент для возбуждения дела, а также определить характер и последовательность первоначальных следственных действий, организационных и иных мероприятий.

Если представленных материалов для возбуждения уголовного дела, по мнению руководителя следственного органа (начальника ОПС), недостаточно, постановление о возбуждении уголовного дела должно быть отменено.

Организация расследования хищений денежных средств, совершаемых с использованием компьютерных технологий

Приступая к рассмотрению организации расследования хищений, отметим, что по информации ОПС, за 2014 - 2015 гг. следователями принято к производству 18490 уголовных дел о рассматриваемом виде преступлений, в том числе в 2014 г. - 3728, в 2015 г. - 14762. Остаток неоконченных уголовных дел на начало 2014 г. составил 537, а на начало 2014г. -1314.

В исследуемом периоде ОПС всего окончено уголовных дел (без повторных) 1491, при этом в 2015 г. окончено 1052 уголовных дела, что в 2,4 раза больше, чем в 2014 г. (439 уголовных дел).

Как положительный момент следует заметить, что за последние два года более половины (51,3 %) уголовных дел окончены в срок, не более 2 месяцев - 765 (2014 г. - 242, 2015 г. - 523). Однако в 2015 г. данный показатель несколько снизился и составил 49,7 % в отличие от 55,1 % в 2014 г. соответственно, в 2015 г. возросла, по сравнению с 2014 г., доля уголовных дел, оконченных в срок свыше 2-х месяцев. Вместе с тем, применительно к определенному сроку расследования показатели 2014 г. и 2015 г. складывались различно:

свыше 2 месяцев, но не более 3 месяцев окончено 472 зтоловных дела или 31,6 % (2014 г. - 96 или 21,8 %, 2015 г. - 376 или 44,8 %);

свыше 3 месяцев, но не более 6 месяцев окончено 166 уголовных дел или 11,1 % (2014 г. - 65 или 14,8 %, 2015 г. - 101 или 9,6 %);

свыше 6 месяцев, но не более 12 месяцев окончено 101 уголовное дело или 6,7 % (2014 г. - 26 или 5,9 %, 2015 г. - 75 или 7,1 %);

свыше 12 месяцев окончено всего75уголовных дел или 5 % (2014 г. -37 или 8,4 %, 2015 г. - 38 или 3,6 %).

В течение двух лет всего окончено уголовных дел (с повторными) 2498, в том числе 2014 г. - 722, 2015 г. - 1776 (более чем в 2,4 раза).

Из оконченных уголовных дел направлено прокурору с обвинительным заключением (актом, постановлением о применении принудительных мер медицинского характера) всего 2374 дела, в том числе 2014 г. - 689, 2015 г. -1685, из которых 97 % или 2303 дела направлены в суд с обвинительным заключением либо актом (2014 г. - 640, 2015 - 1663). При этом в 2015 г. соответствующий показатель улучшился на 5,8 % и составил 98,6 % по сравнению с 92,8 % в 2014 г. В суд с постановлением о применении принудительных мер медицинского характера направлено за два года 24 уголовных дела, что составляет всего 1 % от общего количества направленных прокурору.

Из представленных ОПС сведений следует, что положительной оценки заслуживает качество расследования уголовных дел о хищениях рассматриваемого вида, поскольку доля уголовных дел, возвращенных прокурором для дополнительного следствия за два обозначенных года, составила всего1,3 % или 30 уголовных дел (2014 г. - 14, 2015 г. - 16) Основной причиной возвращения уголовных дел для дополнительного следствия явились: неполнота следствия - 20 дел (66,6 %). По причине нарушения прав обвиняемого в ходе расследования за два года было возвращено всего 6 уголовных дел, по иным основаниям - 1.

Незначительной является и доля уголовных дел, возвращенных судом в порядке ст. 237 УПК РФ - всего 0,3 % или 9 дел, причинами чему, в большей части (55,5 %), явились технические ошибки, допущенные при оформлении процессуальных документов.

В ходе предварительного следствия 110 уголовных дел были прекращены производством, в том числе в 2014 г. - 30, 2015 г. - 80. Большинство уголовных дел были прекращены вследствие акта амнистии (п. 3 ч. 1 ст. 27 УПК РФ) - 36

уголовных дел или 32,7 % (2014 г. - 5, 2015 г. -31).На основании отсутствия в деянии состава преступления (п. 2 ч. 1 ст. 24 УПК РФ) прекращено 23 уголовных дела или 20,9 %, при этом в 2015 г. соответствующий показатель значительно улучшился и составил 12,5 % или 10 уголовных дел в отличие от 43,3 % или 13 дел в 2014 г.

В связи с примирением сторон (ст. 25 УПК РФ) было прекращено 21 уголовное дело или 19 %, в том числе в 2014 г. - 5 дел, в 2015 г. - 16 дел. За истечением сроков давности уголовного преследования в отношении установленного лица (п. 3 ч. 1 ст. 24 УПК РФ) в течение двух исследуемых лет прекращено 15 уголовных дел или 13,6 % (2014 г. - 5, 2015 г. - 10); в связи со смертью подозреваемого, обвиняемого (п. 4 ч. 1 ст. 24 УПК РФ) - 7 дел или 6,3 % (2014 г. - 1, 2015 г. - 6); за отсутствием события преступления (п. 1 ч. 1 ст. 24 УПК РФ) - 2 уголовных дела или 1,8 %; в связи с деятельным раскаянием (ст. 28 УПК РФ) - 1 или 0,9 %; по другим основаниям - 4 или 3,6 %.

Из предоставленной ОПС информации видно, что обжалование постановлений прокурора о возвращении дел для производства дополнительного следствия носит единичный характер.

Количество лиц, в отношении которых уголовное преследование прекращено за непричастностью к совершению преступления, за два исследуемых года составило 18 человек, в том числе в 2014 г. - 7 и в 2015 г. -11; в связи с изменением закона - 17 человек (2014 г. - 6, 2015 г. - 11).

Количество лиц, производство по делу о которых прекращено за отсутствием события, состава преступления, а также уголовное преследование прекращено за непричастностью, составило 11 человек, в том числе в 2014 г. - 4, в 2015 г. - 7. При этом по инициативе руководителя следственного органа - всего 5 (2014г. - 3, 2015 г. - 2), а по инициативе прокурора - всего 2.

В течение 2014-2015 гг. всего было приостановлено 19651 уголовных дела, в том числе в 2014 г. - 6038, в 2015 г. - 13613. Большинство уголовных дел, а именно 18968 или 96,5 % приостановлены по п. 1 ч. 1 ст. 208 УПК РФ. Следует заметить, что в 2015 г. доля приостановленных уголовных дел по обозначенному основанию по сравнению с 2014 г. снизилась на 3,5 % (2014 г. - 5975 или 98,9 %; 2015 г. - 12993 или 95,4 %).

По основаниям, предусмотренным п. 2 ч. 1 ст. 208 УПК РФ, всего было приостановлено 9 уголовных дел, в том числе в 2014 г. - 6, в 2015 г. - 3; по основаниям, предусмотренным п. 3 ч. 1 ст. 208 УПК РФ - всего 7,в том числе в 2014 г.-3, в 2015 г.-4.

Согласно полученным сведениям, в указанном периоде времени уголовные дела о хищениях, совершенных с использованием компьютерных технологий, по п. 4 ч. 1 ст. 208 УПК РФ не приостанавливались.

Остаток приостановленных дел на начало2016 г. (без повторных за все годы) составил 15409, в том числе 2014 г. - 3537, 2015 г. - 11872.

С непринятыми процессуальными решениями на конец 2014 г. в ОПС находилось 888 уголовных дел, в том числе со сроками следствия: свыше 2 месяцев, но не более 3 - 1455; свыше 3 месяцев, но не более 6-134; свыше 6 месяцев, но не более 12 - 21; со сроками свыше 12 месяцев, согласно предоставленным данным, уголовных дел в производстве не было. С непринятыми процессуальными решениями на конец 2015 г. в ОПС

находилось 2705 уголовных дел, что в 3 раза больше, чем в 2014 г., в том числе со сроками следствия: свыше 2 месяцев, но не более 3 - 2824; свыше 3 месяцев, но не более 6 - 395; свыше 6 месяцев, но не более 12 - 45; свыше 12 месяцев - всего 2 уголовных дела.

Количество дел, по которым внесены представления о принятии мер по устранению обстоятельств, способствующих совершению преступления или другим нарушениям закона, всего за два года составило 8985, в том числе 2014 г.- 1345, 2015 г.-7640.

Следует отметить, что в ходе расследования уголовных дел о хищениях решения прокурора и суда почти не обжаловались. Так, за два года обжалованию подвергались всего 17 решений прокурора, в том числе в

2014 г. - 11, в 2015 г. - 6; решений суда - 7, в том числе в 2014 г. - 4, в

2015 г. - 3, которые удовлетворены не были.

Как правило, предварительное расследование по ним осуществлялось исключительно следователем. Таких фактов выявлено 37, что составляет 90,2 % от общего количества таких уголовных дел. Специализированных следственно-оперативных групп было создано для расследования 3 уголовных дел. Производство предварительного следствия следственной группой без привлечения должностных лиц, осуществляющих ОРД, осуществлялось по 2 уголовным делам и следственной группой с привлечением должностных лиц, осуществляющих ОРД - по 1 уголовному делу.

По 5 уголовным делам выделялись в отдельное производство другие дела и по 5 - материалы, содержащие сведения о новом преступлении.

Из изученных уголовных дел решения о прекращении уголовного дела (уголовного преследования) не принимались.

По 24 уголовным делам или 58,5 % производство приостанавливалось поп. 1 ч. 1 ст. 208 УПК РФ.

Для производства дополнительного следствия уголовные дела не возвращались.

Исходя из представленных данных, уголовные дела оканчивались производством, в первую очередь, по ст. 158 УК РФ - 7, что составило 17 % от всех изученных уголовных дел; по ст. 159 УК РФ - 5 или 12 %; по ст. 159.6 УК РФ - 4 или 9,7 %. Дополнительные эпизоды преступной деятельности квалифицированы: по ст. 183 УК РФ - 2, ст. 272 УК РФ - 1 и ст. 273 УК РФ-1.

Уголовных дел, находящихся в производстве на момент заполнения анкеты со сроком предварительного следствия свыше 30 суток, но не более 2 месяцев, установлено 6; со сроком свыше 2 месяцев, но не более 3 - 11; со сроком свыше 3 месяцев, но не более 6 - 6; со сроком свыше 6 месяцев, но не более 12 - 8 и свыше 12 месяцев - 4.

Из изученных уголовных дел в суд с обвинительным заключением либо актом направлено - 16, из которых половина (8 уголовных дел) рассмотрена в общем порядке, в особом порядке при согласии обвиняемого с предъявленным ему обвинением - 6. По результатам рассмотрения по 10 уголовным делам состоялся обвинительный приговор, фактов оправдательных приговоров не установлено.

Относительно сведений о потерпевших по уголовным делам о хищениях денежных средств, совершенных с использованием компьютерных технологий, установлено, что их общее количество за рассматриваемый период времени составило 20880 лиц. При этом в 2015 г. (16168) их количество по сравнению с 2014 г. (4712) увеличилось более чем в 3 раза.

Приведенные сведения о результатах расследований хищений со всей очевидностью свидетельствуют о наличии известных трудностей, проблем и ошибок в деятельности следователей, что нашло подтверждение в обобщенных результатах анкетирования. Так, опрос следователей показал, что трудностями предварительного расследования хищений являются:

недостаточный у следователей уровень специальных знаний следователя (32 %);

продолжительность производства отдельных следственных действий (31 %);

получение информации и документов, содержащих банковскую тайну (29 %);

отсутствие у следователей информации об основах методики расследования данных преступлений (27 %);

отсутствие желания сотрудничества со стороны работников (руководства) кредитных организаций (23 %);

отсутствие надлежащего взаимодействия с компетентными органами зарубежных стран (17 %), оперативными сотрудниками (13%), со специалистами и (или) экспертами (11 %).

Конкретизируя трудности, с которыми приходится сталкиваться при расследовании уголовных дел о хищениях, респонденты, в первую очередь, указали на длительность получения сведений о счетах и их владельцах из банков - 21 %.

Остальные ответы респондентов в данной части ввиду их немногочисленности не позволяют установить их системный характер.

Отчасти, повторяя ответ на предыдущий вопрос, некоторые респонденты отметили, что такие трудности проявляются в следующем:

отсутствие у следователя специальных знаний в области программного обеспечения, осуществления электронных платежей и т. п. (6 %);

продолжительность исполнения поручений в других регионах (4 %); несоответствие методик расследования современным реалиям (3 %); длительность производства компьютерных экспертиз (3 %); удаленность местонахождения потерпевшего от места совершения преступления (места расследования уголовного дела) (2 %);

регулярное совершенствование способов совершения преступлений (2 %);

нахождение IP-адреса, с которого запущен вирус, за рубежом (2 %); длительность получения информации от сотовых компаний (2 %). Обобщая и систематизируя поступившую из ОПС информацию, можно сделать промежуточный вывод о том, что она отражает большинство из обозначенных опрошенными следователями проблем расследования хищений. При этом некоторые проблемы носят производный характер, т.е. являются следствием

неразрешенных проблем рассмотрения сообщений о хищениях, другие - свойственны только стадии предварительного расследования.

Авторами настоящей работы предпринята попытка сгруппировать проблемы, с которыми сталкиваются следователи, содержащиеся в информационных письмах ОПС, на проблемы организации банковских автоматизированных информационных систем, проблемы, связанные со способами подготовки, совершения и сокрытия хищений и собственно проблемы организации и производства расследования хищений.

К проблемам оргаигасщгш банковских автоматизированных информационных систем, а также предоставления услуг операторами сотовой связи и провайдерами, относятся:

низкий уровень компьютерной грамотности населения, в том числе отсутствие у граждан знаний о банковских автоматизированных информационных системах, которое, в совокупности с их беспечностью, повышает виктимный уровень поведения потерпевших. Беспечность граждан проявляется в неотключении услуги удалённого доступа, предоставляемой коммерческими банками к своим счетам, при смене/прекращении пользования абонентским номером сотовой связи, неотслеживании состояния своих счетов, непринятии должных мер по сохранности защитных кодов доступа к своим банковским картам, расчётным счетам, а также в позднем обращении в ОВД с момента совершения преступления.

неконтролируемый оборот банковских пластиковых карт, оформленных на вымышленных людей, либо лиц, ведущих асоциальный образ жизни, студентов. Пример, где мы столкнулись с подобным, уже приводился;

анонимность пользователей сети Интернет, в которой при этом представлены инструменты перераспределения материальных благ, что в совокупности является главной и вполне естественной предпосылкой совершения хищений денежных средств, связанных с использованием компьютерных технологий, т. к. позволяет при наличии определенных познаний реализовать корыстные цели с минимальным риском привлечения к ответственности;

отсутствие должной защиты программного обеспечения и компьютерных устройств (программное обеспечение, банкоматы, платежные терминалы и т. д.), позволяющее преступникам осуществлять неправомерные действия (внедрять вирусные программы, устанавливать скиминговые устройства и т. д.);

реализация операторами сотовой связи SIM-карт в нарушение норм действующего законодательства без удостоверения личности абонента (на выдуманных, несуществующих либо подставных лиц).

К проблемам, связанным со способами подготовки, совершения и сокрытия хищений, относятся:

внедрение (распространение) вредоносных программ через различные зарубежные файловые хранилища, интернет ресурсы, виртуальные платежные системы электронные счета и т. п., находящиеся на территории зарубежных стран, в том числе Европы и США;

совершение преступления на территории других регионов, использование при совершении преступлений зарегистрированных в других регионах на «подставных» лиц электронных адресов, счетов, абонентских номеров,

использование для выхода в сеть Интернет открытых точек доступа Wi-fi или операторов мобильной связи, предоставляющих один IP-адрес сразу нескольким абонентам, что препятствует идентификации преступника, использование при хищении многократных переводов денежных средств посредством электронных кошельков Qiwi, WebMoney и др.;

осуществление виртуального общения с преступниками через почтовые ящики @google.com, @yahoo.com, @aol.com, сервера которых находятся только на территории США, либо с использованием TOR-сети (браузера), в связи с чем не имеется возможности получения информации о владельце;

использование в случае перечисления денег потерпевшими виртуальной криптовалюты (Биткоин, Лайткоин, Праймкоин и т. п.), не имеющей единого центра хранения сведений о владельцах виртуальных счетов, не рекомендованной Банком России к обороту на территории Российской Федерации и изначально разработанной с функцией анонимности сведений о владельце;

лица, совершающие преступления, в подавляющем большинстве случаев, находятся в других регионах страны, и похищенные денежные средства перечисляются в указанные регионы. Так, 90 % лиц, совершающих такие хищения в Чувашской Республике, и места окончания таких преступлений находятся за пределами республики (в других регионах страны);

использование для совершения хищений виновными лицами поддельных (зарегистрированных на иных лиц) платежных карт, телефонных номеров, программных средств, позволяющих заменять номера телефонов, IP-адреса и т.д. Данное обстоятельство по информации некоторых ОПС (например, СУ МВД по Республике Бурятия и др.) является существенным препятствием в расследовании. Так, согласно поступившей информации СУ УМВД России по Рязанской области основной проблемой расследования по уголовным делам о хищения денежных средств, совершенных с использованием компьютерных технологий, в случаях, когда источником информации о преступлении являются сообщения граждан, является фактическая невозможность изобличения виновного лица. Процессуальные действия, проводимые по уголовному делу в целях установления движения похищенных денежных средств и конечного способа распоряжения ими, а также данных пользователей пластиковых карт не позволяют установить как место совершения преступления, так и сведения о лицах, его совершивших.

К проблемам организации и производства расследования уголовных дел о хищениях относятся:

низкое качество материалов проверок - отсутствуют объяснения лиц, на чье имя зарегистрированы абонентские номера, IP-адреса, счета, отсутствуют акты исследований (заключения эксперта) компьютерной техники. Доследственная проверка, как правило, сводится к установлению факта списания денежных средств у потерпевшего путем его опроса и приобщения банковской выписки;

различные толкования положений постановления № 51 следователями, прокурорами и судами. Так, например, при направлении уголовного дела № 1136005 по подсудности, по которому установлено, что преступления совершались в двух субъектах Российской Федерации (Адыгея и Краснодарский край), между судами двух субъектов возник неофициальный

спор о подследственности, в результате которого уголовное дело дважды по надуманным основаниям возвращалось прокурору в порядке ст. 237 УПК РФ;

сложность при установлении вредоносных программ в компьютерных устройствах, с помощью которых происходит снятие денежных средств (зачастую потерпевшие удаляют Интернет ссылки);

невозможность получения в кратчайшие сроки информации из коммерческих банков, у сотовых операторов и провайдеров (например, о месте снятия денежных средств, либо месте их перевода, о Log-файлах и IP-адресах компьютерах, обращавшихся к расчетным счетам и т.п.). Ответы данные организации представляют в течение от 1 до 3 месяцев. Так, на территории Забайкальского края услуги сотовой связи представляют три оператора: ОАО «Мегафон», ОАО «Билайн», ОАО «СИБИНТЕРТЕЛЕКОМ». В соответствии с распоряжением руководства Дальневосточного Филиала ОАО «Мегафон», исполнение запросов осуществляется специализированной группой Департамента безопасности Дальневосточного Филиала ОАО «Мегафон», расположенной в г. Хабаровске, что значительно увеличило сроки предоставления требуемой информации. В офисе ОАО «Мегафон» в г. Чите постановления суда не принимаются. Оператор связи предупредил, что срок исполнения постановлений следователей в среднем будет составлять 1 месяц, без учета времени доставки почтой, однако, фактически данный срок превышает два месяца. В то же время неустановление в кратчайшие сроки принадлежности абонентских номеров телефонов, банковских карт, IP -адресов, с использованием которых совершаются преступления, не дает возможности установить виновных и пресечь противоправную деятельность преступных групп;

трудности при проведении следственных и оперативно-розыскных действий с выездом в служебные командировки на продолжительный срок (от 1 месяца и более) в субъекты Российской Федерации. При этом поручения по уголовным делам зачастую выполняются сотрудниками ОВД других регионов некачественно, формально либо не выполняются вообще. Решить данную проблему, по мнению руководства СУ УМВД России по Мурманской области, поможет разработка с закреплением в соответствующем нормативном акте МВД РФ единого алгоритма проведения доследственных проверок по указанной категории преступлений.

длительность получения информации о местонахождении и принадлежности IP-адресов, находящихся на территории иностранных государств, которые используются преступниками для сокрытия следов хищения. Практика свидетельствует о том, что следственные органы направляют международные запросы в исключительных случаях.

Так, в ходе проведения экспертизы в рамках уголовного дела № 412023, находящегося в производстве ОПС Омской области, по факту хищения денежных средств с банковской карты, было установлено наличие вредоносной программы на мобильном устройстве, которая маскировалась под программу для бесплатных SMS-сообщений и звонков Viber. В свою очередь, анализ обнаруженного программного обеспечения показал, что команду на действия по переводу денежных средств с карты потерпевшей данная программа получала с IP-адресов, зарезервированных в Китайской народной республике. В связи с чем в КНДР был направлен международный запрос об истребовании соответствующей информации;

необходимость и длительность получения судебных решений о наложении ареста на расчетные счета организаций, куда были перечислены похищенные денежные средства, что в итоге приводит к невозможности заблокировать их перечисление и, соответственно, вернуть потерпевшим;

сотрудники ОВД не обладают достаточными знаниями в области компьютерных технологий в целом и банковских автоматизированных информационных систем в частности, что приводит к утрате следов совершения хищений, к неэффективному использованию оперативно значимой информации, полученной в ходе проведения оперативно-технических мероприятий;

длительные сроки проведения судебно-компьютерных экспертиз, в том числе из-за недостатка специалистов ЭКП ОВД, а также ограниченные технические возможности проведения исследований и судебных экспертиз вредоносного программного обеспечения, в том числе на различного рода объектах (смартфоны, планшеты и т.п.). Например, в ЭКЦ МВД по Республике Алтай проводятся компьютерные экспертизы по изъятым у потерпевших телефонным аппаратам, в которых были установлены SIM-карты, подключенные к номеру банковского счета (услуга «Мобильный банк»), с которого были похищены денежные средства. При проведении исследований эксперты обнаруживают вредоносные программы («Trojan-SMS.AndroidOS.Fakeinst.san», «Trojan-SMS.AndroidOS.Opfake.san», и др.), которые копируются и записываются на диск. Дальнейшее исследование вредоносных программ с целью установления IP-адресов, с которых осуществлялось вхождение в систему и установления лиц, совершивших преступление, не производится, в связи с отсутствием в ЭКЦ МВД по Республике Алтай оборудования и специалистов в указанном направлении, в результате чего хищения, совершенные с использованием вредоносных программ, остаются нераскрытыми;

установление владельцев всех скомпрометированных банковских карт и сумм похищенных денежных средств;

большое количество потерпевших, проживающих в различных регионах Российской Федерации. Данное обстоятельство объективно осложняет производство процессуальных действий на заключительном этапе расследования;

производство процессуальных действий с обвиняемыми, в случае если они являются гражданами зарубежных государств;

отсутствует единая финансовая организация (Росфинмониторинг не рассматривает запросы по ч. 2 ст. 158 и ст. 159 УК РФ), в которую следователь мог бы направить один обширный запрос и получить всю необходимую информацию о транзакции похищенных денежных средств по разным кредитным организациям, в том числе и осуществляющим свою деятельность за пределами Российской Федерации. По информации СУ МВД Чувашской Республики проблемой расследования хищений денежных средств, совершаемых с использованием компьютерных технологий, является отсутствие единого источника информации о движении денежных средств от потерпевшего до лица, подлежащего привлечению в качестве обвиняемого (сбор доказательств и его сроки увеличиваются пропорционально количеству этапов в схеме по выводу и обналичиванию денежных средств.

отсутствие технического обеспечения ОПС необходимой техникой, ограниченный доступ следователей к базам данных (ИБД) и отсутствие в ряде территориальных ОПС доступа к сети Интернет;

не в полном составе осуществляется выезд следственно-оперативных групп на осмотр места происшествия, в ходе которого не выявляются и не изымаются следы хищений и иные объекты;

ограниченная возможность получения сведений с IT - сервисов, находящихся за территорией России, поскольку по линии «Интерпола» большинство Государств информацию в корректном виде не предоставляет;

длительное ознакомление обвиняемого и защитника с материалами уголовного дела. Так, по уголовному делу № 12270025, находившемуся в производстве ОПС Забайкальского края, ознакомление обвиняемого и защитника происходило в течение 8 месяцев.

Предлагая конкретные рекомендации по расследованию хищений независимо от их разновидностей, следует обратить внимание, что прежде чем приступить к расследованию, необходимо уяснить ситуацию на конкретный момент времени, что обеспечивает целенаправленное планирование следственных и иных действий.

Значение следственных ситуаций для эффективной организации расследования и разработки его методики применительно к отдельным видам преступлений общепризнано. Р. С. Белкин отмечал, что «активизация исследований в области криминалистической методики выявила ключевое значение ряда понятий криминалистической тактики и среди них понятие следственной ситуации».

Особое внимание обращает на себя мнение В. П. Лаврова, которое состоит в том, что следственная ситуация может рассматриваться в двух аспектах: теоретическом (будучи типизированной применительно к определенному виду преступления и даже шире - как научная, абстрагированная категория) и практическом (как конкретная жизненная ситуация по уголовному делу, находящемуся в производстве у следователя, которая характеризует первоначальный этап расследования и включает, в первую очередь, информацию о результатах предварительных проверок, неотложных следственных действий и оперативно-розыскных мероприятий).

В настоящее время в криминалистической литературе представлено несколько научно обоснованных систем классификации следственных ситуаций, построенных на различных основаниях. Так, В. В. Крылов принимает за основание классификации категорию субъекта, обнаружившего признаки преступления в сфере компьютерной информации, и его первоначальные действия. А. В. Остроушко в своей диссертационной работе типизирует следственные ситуации по способу совершения преступления. Ю.В. Гаврилин и А.В. Кузнецов выделяют типичные следственные ситуации по уголовно-правовой квалификации преступлений в сфере компьютерной информации. Имеются и другие авторские классификации. Например, А.Н. Яковлев и Н.В. Олиндер, учитывая содержание криминалистической характеристики преступлений, совершенных с использованием электронных средств и систем, предложили условно подразделить следственные ситуации, складывающиеся на первоначальном этапе расследования таких преступлений, на две наиболее характерных группы:

ситуация, в которой известно событие преступления и необходимо установить лицо, совершившее преступление, и обстоятельства по данному делу.

ситуация, в которой известно событие преступления и лицо, совершившее преступление, и необходимо установить обстоятельства по данному делу.

Между тем, существующие научные подходы к классификации следственных ситуаций имеют существенный недостаток, заключающийся в том, что они основываются, как правило, только на одном факторе, а система рекомендаций должна разрабатываться с учетом взаимосвязи факторов, образующих такие ситуации. К таким факторам традиционно относят:

первоначальную информацию, полученную при проверке заявлений, сообщений и сразу после возбуждения уголовного дела, о событии, содержащем признаки преступления, о лицах, причастных к этому событию;

объективные условия, характеризующие получение этой информации (место, время, использование технических и аппаратных средств);

силы и средства, имеющиеся в распоряжении следователя для дальнейшей работы по использованию исходной информации в этих условиях;

позицию подозреваемого, потерпевшего, свидетелей, а также результаты их противодействия установлению истины в начале расследования и потенциальной возможности противодействия;

иные факторы, препятствующие или способствующие успешному решению криминалистических задач.

Как представляется, диалектический принцип познания, системный подход позволяет определить факторы, влияющие на следственную ситуацию по делам о хищениях. Так, по результатам анкетирования следователей установлены следующие факторы:

возможность использования следователем информационных баз данных (42 %);

уровень осведомленности следователя об обстоятельствах преступления (30 %);

установленные источники доказательств (23 %);

допущенные ошибки при документировании или рассмотрении сообщений о преступлении (23 %);

процессуальные нормы, создающие благоприятные или неблагоприятные условия расследования (18 %);

позиция надзирающего прокурора по уголовному делу (17 %); установленные источники ориентирующей информации (17 %); оказываемое участниками уголовного судопроизводства противодействие расследованию (16 %);

организационно-управленческие меры, создающие благоприятные или неблагоприятные условия расследования (12 %);

конфликтная ситуация между субъектами расследования и сотрудниками отделов безопасности кредитной или иной коммерческой организации (10 %);

позиция начальника ОПС по уголовному делу (7 %); наличие конфликта между следователем и другими участниками расследования (3 %);

оказываемое иными лицами противодействие расследованию (1 %); взаимодействие служб (1 %);

иные факторы (объективные и субъективные причины) (2 %). В то же время к факторам, оказывающим влияние на первоначальном этапе расследования, респонденты не отнесли допущенные ошибки при документировании или рассмотрении сообщений о преступлении; наличие возможности производить следственные и иные действия в запланированные время и месте; процессуальные нормы, создающие благоприятные или неблагоприятные условия расследования (напр., необходимость получения санкции суда на производство следственных действий и сложности при получении информации по запросам (без производства выемки).

На вопрос о противодействии расследованию уголовных дел о хищениях следователи указали, что такое противодействие, в большинстве своем, оказывается подозреваемым (обвиняемым) (31 %) следующими способами:

предоставление недостоверной или неполной информации (14 %);

отказ от дачи показаний (14 %);

заявление необоснованных ходатайств (4 %);

отказ от сотрудничества (4 %);

сокрытие своего имущества, на которое может быть наложен арест (2 %);

сокрытие сведений об орудиях преступления, в том числе компьютерах и иных технических устройствах (1 %);

замена защитника на стадии ознакомления с материалами уголовного дела (1 %);

уничтожение доказательств (1 %); давление на следователя (1 %).

Также следователи указали, что противодействие расследованию оказывают защитники (адвокаты) (17 %) следующими способами: заявления необоснованных ходатайств и жалоб (6 %); неявки на следственные действия (2 %);

затягивание ознакомления с материалами уголовного дела (1 %); давление на следователя (1 %).

К числу субъектов, оказывающих противодействие следователю, отнесли работников кредитных организаций (13 %), затягивающих представление ответов на запросы или предоставляющих неполные сведения.

Кроме того следователи указали следующих субъектов противодействия:

потерпевшие (3 %) и свидетели (2 %) путем неявки по вызову, отказа участия в следственных действиях, изменения показаний;

должностных лиц ОВД (3 %) путем формального подхода к исполнению поручений следователя и ОРМ, несогласованных выступлений в СМИ и т. п.;

представителей СМИ (3 %) путем отвлечения следователя от расследования, размещения недостоверной или преждевременной информации;

родственников подозреваемого (обвиняемого) (2 %), специалиста (эксперта) (1 %);

государственных и общественных деятелей (1 %) путем привлечения СМИ к факту совершенного деяния, тогда как оглашение данных нежелательно для следствия.

Сложившаяся следственная ситуация предопределяет особенности планирования и осуществления расследования рассматриваемого вида хищения. Перед началом планирования следователю необходимо определить полноту проверочного материала с учетом рекомендаций, содержащихся в предыдущей части настоящей работы.

Также необходимо отметить, что особенности хищений, отраженные в рассмотренной криминалистической характеристике, предопределяют необходимость привлечения специалистов уже на этапе планирования расследования данного вида преступлений.

Таким образом, планирование расследования хищений должно основываться на криминалистической характеристике данных преступлений, складывающейся следственной ситуации при активном участии специалиста.

В настоящее время в криминалистической литературе содержится множество подходов к определению понятия «планирование расследования преступлений». По нашему мнению, заслуживает внимания комплексный подход к формулированию этого понятия, заключающийся в определении его как метода и процесса достижения цели расследования путем постановки задач и заранее намеченной последовательности (программы) их решения150. При этом основными функциями планирования расследования любых категорий преступлений, в том числе рассматриваемого вида хищений, являются: упорядочение доказательств, моделирование, организационно-управленческая функция. Результатом планирования является план расследования преступления, представляющий собой перспективную прогностическую модель будущих действий и мероприятий следователя, детальную программу реализации тактических задач.

Следует разделить позицию, согласно которой система планирования расследования с определенной условностью может быть представлена следующим образом:

анализ информации (внутренних и внешних факторов расследования); построение следственных версий и определение задач расследования; определение путей и способов решения поставленных задач; составление письменного плана (программы и иной документации) расследования.

Рассмотрим кратко содержание каждого из этапов планирования расследования хищений.

На первом этапе осуществляется комплексное исследование исходной информации о хищении. Следователь анализирует данные о субъекте преступления; способе совершения преступления; преступном результате; месте, времени и других обстоятельствах, относящихся к обстановке места происшествия и образующих предмет доказывания; после чего «прибегает» к мысленному моделированию события, выдвигая следственную версию произошедшего и т. п.

Источниками получения информации о расследуемом событии могут быть различные документы, содержащиеся в материалах уголовного дела на момент начала планирования. Объем таких источников зависит от

особенностей конкретной разновидности хищений и этапа расследования. В то же время, как справедливо отмечается в литературе, знание особенностей структуры, работы и документооборота организации, предприятия или учреждения помогает разработать план расследования, и избрать верное направление в проведении следственных действий по обнаружению и изъятию доказательств. Тем самым деятельность органа расследования на данном этапе планирования должна быть направлена на изучение указанных особенностей.

Следует отметить, что в процессе анализа имеющейся информации, содержащейся в перечисленных и иных документах, следователь обязан оценивать такие документы с точки зрения доброкачественности с целью определения возможности использовать их в процессе расследования, не планируя изъятие (истребование) других экземпляров или копий этих документов. Практика показывает, что следователи, не вникая в содержание документов и не определяя необходимость для производства расследования тех или иных из них, зачастую изымают несколько экземпляров (копий) одного и того же документа и, тем самым, необоснованно увеличивают объем уголовного дела.

На первом этапе планирования также следует предварительно оценить возможность проведения расследования теми ресурсами, которые имеются в распоряжении следователя.

Исследование показало, что для эффективного расследования хищений целесообразно создавать следственные группы или следственно-оперативные группы.

Как непосредственно следует из положений ст. 163 УПК РФ, решение о производстве предварительного следствия следственной группой принимает руководитель следственного органа. В постановлении должны быть перечислены все следователи, которым поручено производство предварительного следствия, в том числе указывается, какой следователь назначается руководителем следственной группы. В свою очередь, руководитель следственной группы наделен рядом полномочий, в том числе о самостоятельном принятии решения о выделении уголовных дел в отдельное производство в порядке, установленном ст. 153-155 УПК РФ. При этом следует отметить, что согласно позиции Генеральной прокуратуры Российской Федерации, которая была изложена в постановлении о возвращении уголовного дела для производства дополнительного расследования, следует, что руководитель следственной группы, приняв решение о выделении в отдельное производство уголовного дела, должен приступить к расследованию только после того, как принял это дело к своему производству на основании дополнительного решения руководителя следственного органа.

Необходимо отдельно выделить и такой информационный элемент, как осведомленность следователя о наличии противодействия расследованию.

Таким образом, на первом этапе планирования расследования хищений проводится анализ внутренних и внешних условий, определяющих следственные ситуации.

Вторым этапом планирования является построение следственных версий и определение задач расследования. Значение данного этапа

предопределяется недостаточностью имеющейся информации о расследуемом деянии.

В литературе отмечается, что следственная версия - это идеальная информационно-логическая модель обоснованного предположения следователя относительно отдельных обстоятельств, которые имеют или могут иметь значение для расследования преступлений, или их совокупности (полной или частичной), выдвигаемого с целью объяснения происхождения этих обстоятельств и связи между собой.

Построение следственных версий способствует определению пути преодоления информационной неопределенности. Отметим, что при построении следственных версий нельзя сосредоточиваться исключительно на следственных ситуациях, основанных на имеющейся информации о хищении. Важно учитывать и вероятность наличия иных эпизодов преступной деятельности, присутствие соучастников преступления, а также возможной коррупционной составляющей расследуемого хищения.

В зависимости от характера исходной информации о предполагаемом хищении, можно выделить:

- версии о событии преступления;

- версии о субъекте и субъективной стороне преступления;

- версии об иных обстоятельствах преступления.

В связи с отмеченным заслуживает внимания следующая технология построения следственных версий. Выдвижение общей версии о событии хищения; разработка общих версий, выдвижение частных версий о способе, лицах совершивших хищение и т. п.; выведение следствий из версий на основе посылки «если, то...».

Приведем пример разработки одной из типовых версий при расследовании хищений денежных средств граждан с использованием компьютерных технологий платежной системы. После проведения доследственной проверки возбуждено уголовное дело по факту хищения денежных средств из электронного кошелька пользователя платежной системы. Для построения на первоначальном этапе расследования версий, следователю необходимо предположить, кто и каким образом мог совершить данное деяние, у кого был доступ к компьютерному устройству пользователя или реквизитам доступа к электронному кошельку, каким образом было совершено преступление - путем прямого доступа к компьютерному устройству, либо через удаленный доступ. Если компьютерное устройство находилось дома, то доступ к нему могли иметь члены семьи, либо лица, имеющие доступ в дом. Если компьютерное устройство находилось на рабочем месте, доступ к нему имеет потенциально более широкий круг лиц (сослуживцы, работники других отделов, службы охраны и т. п.). Также следователь, руководствуясь криминалистической характеристикой хищений денежных средств граждан с использованием компьютерных технологий платежной системы при построении версии, должен учитывать не только возможность совершения такого преступления путем прямого доступа, но и удаленного.

При прямом доступе к компьютеру преступник находится в непосредственной близости от компьютерного устройства потерпевшего и пользуется им, как и обычный пользователь. При этом он получает возможность найти на носителе

информации реквизиты доступа к электронному кошельку, отослать такие реквизиты на свой электронный почтовый ящик или скопировать на портативное устройство внешней памяти (например, USB флэш-носитель). Если же на экране монитора отображается рабочий сеанс работы с электронной платежной системой (за некоторое время до этого клиент системы инициировал соединение, и потом вышел из помещения), то преступник может осуществить дополнительные транзакции в своих интересах непосредственно в ходе этого сеанса.

При удаленном доступе к компьютерному устройству преступник находится в иной части города (в ином городе, стране). С использованием вредоносных программ он либо удаленно заражает компьютерное устройство потерпевшего и копирует с него реквизиты доступа к электронному кошельку (такие реквизиты скрытно отсылаются на электронный почтовый ящик подконтрольный преступнику), либо организовывает себе такой удаленный доступ, который позволяет видеть экран монитора потерпевшего и управлять программами на его компьютере. Во втором случае преступник может наблюдать удаленно рабочий сеанс работы потерпевшего с электронной платежной системой, а потом попытаться осуществить дополнительные транзакции в своих интересах также непосредственно в ходе этого сеанса.

Общим для рассматриваемого вида хищений является то, что они связаны с другими преступлениями (напр., незаконное образование (создание, реорганизация) юридического лица, незаконное использование документов для образования (создания, реорганизации) юридического лица, легализация (отмывание) денежных средств или иного имущества, приобретенных преступным путем, незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, неправомерный оборот средств платежей и т. п.), а также с действиями, направленными на обналичивание похищенных денежных средств. В связи с данным обстоятельством следователю необходимо разрабатывать соответствующие следственные версии и на их основе формулировать задачи расследования.

Следует отметить, что решение задач расследования должно обеспечить достижение цели расследования - установление обстоятельств, подлежащих доказыванию, которые в общем виде определены в ст. 73 УПК РФ.

В соответствии с положениями ст. 73 УПК РФ, при производстве по уголовному делу подлежат доказыванию:

1) событие преступления (время, место, способ и другие обстоятельства совершения преступления);

2) виновность лица в совершении преступления, форма его вины и мотивы;

3) обстоятельства, характеризующие личность обвиняемого;

4) характер и размер вреда, причиненного преступлением;

5) обстоятельства, исключающие преступность и наказуемость деяния;

6) обстоятельства, смягчающие и отягчающие наказание;

7) обстоятельства, которые могут повлечь за собой освобождение от уголовной ответственности и наказания;

8) обстоятельства, подтверждающие, что имущество, подлежащее конфискации в соответствии со ст. 104.1 УК РФ, получено в результате совершения преступления или является доходами от этого имущества либо использовалось или предназначалось в качестве орудия преступления, либо для финансирования терроризма, организованной группы, незаконного вооруженного формирования, преступного сообщества (преступной организации). Подлежат выявлению также обстоятельства, способствовавшие совершению преступления.

При расследовании конкретного вида преступных деяний, в том числе рассматриваемых хищений, данные обстоятельства конкретизируются.

Третий этап планирования заключается в определении путей и способов проверки следственных версий, решения поставленных задач. На этом этапе планирования принимаются следующие организационные решения:

разработка, анализ и оценка вариантов возможных процессуальных и иных действий (мероприятий) и/или их комплексов, направленных на подтверждение или опровержение следственных версий, а также разрешение поставленных задач.

принятие окончательного решения следователем о привлечении/использовании определенных ресурсов.

Фактически на этом этапе планирования составляется программа предстоящего расследования, разрабатывается алгоритм процессуальных и иных действий (мероприятий) и/или их комплексов, представляющий собой детальный перечень, а также прорабатывается содержание запланированных тактических приемов, необходимых для практической реализации таких действий. Программа служит подробной инструкцией для следователя и членов СО! и одновременно является средством контроля качества производства процессуальных и иных действий (мероприятий) и/или их комплексов и всего расследования.

В зависимости от изменений следственной ситуации по уголовному делу, прежде всего, в результате проведенных процессуальных и иных действий (мероприятий) и/или их комплексов, программа может меняться, в том числе и без относительного пересмотра всего плана. Причины и результаты изменений следует документировать.

Немаловажным обстоятельством при определении путей и способов проверки следственных версий, решения поставленных задач являются сроки производства процессуальных и иных действий в ходе расследования хищений.

Представляется, что сроки производства тех или иных процессуальных действий следует учитывать как при рассматриваемом (третьем) этапе планирования, так и в целом при составлении плана (на других этапах).

При разработке, анализе и оценке вариантов возможных процессуальных и иных действий (мероприятий) и/или их комплексов, направленных на подтверждение или опровержение следственных версий, а также разрешение поставленных задач, следует учитывать типовые описанные выше проблемы, разрешение которых вызывает определенные трудности.

Систематизация и анализ проблем расследования хищений позволяют сформулировать актуальные задачи расследования, независимо от

разновидности данных преступлений, к которым, с учетом разработанных исследователями - криминалистами рекомендации, следует отнести:

определение последовательности и порядка производства следственных действий, в том числе первоочередных, направленных на сохранение источников доказательственной информации. При решении этого вопроса необходимо учитывать особенности механизма следообразования и способы совершения преступлений - с использованием электронных платежных средств и систем, а также в сфере компьютерной информации;

определение момента или условия, наиболее целесообразного для задержания преступника, личность которого установлена. При решении этого вопроса необходимо учитывать взаимно противоречивые цели: осуществить как можно быстрее задержание преступника для лишения его возможности скрыть следы преступления и, одновременно, отсрочить такое задержание с целью повышения эффективности предпринятых мер, направленных на установление сообщников, сбор доказательств в условиях, когда преступником не предприняты дополнительные меры противодействия расследованию;

обеспечение перспективы дела, в частности, позволить установить всех лиц, совершивших хищение, раскрыть их связи, выяснить обстоятельства, способствовавшие его совершению;

установление и обоснование последовательности допроса свидетелей и подозреваемых, при которой обеспечена полнота и всесторонность расследования, исключена возможность влияния подозреваемых на соучастников, потерпевших и свидетелей;

установления и обоснование последовательности проведения обысков и выемок (у кого, где, когда). При этом конкретизируются предметы, подлежащие выемке, или их категория, специализация лиц, обладающих специальными знаниями и привлекаемых в качестве специалистов для производства этих следственных действий, подлежащие применению научно-технические методы и средства, обеспечивающие получение доказательств с учетом требований закона;

определение перечня мероприятий, направленных на установление размера материального ущерба. При разработке перечня таких мероприятий необходимо учитывать тот факт, что хищения конечной целью имеют материальную выгоду, т. е. похищенные денежные средства должны быть обналичены;

определение порядка взаимодействия следователя с оперативным сотрудником, со специалистами (экспертами);

определение допустимости использования в уголовном деле материалов, полученных в результате осуществления оперативно-розыскной деятельности.

В свою очередь, такие задачи конкретизируются в зависимости от разновидности хищений.

Систематизация представленной ОПС информации позволяет сделать вывод, что следственная практика выработала общий порядок (алгоритм) расследования хищений, включающий следующую последовательность действий:

ознакомление с материалами доследственной проверки, на основании которых возбуждено уголовное дело;

вынесение постановления о признании потерпевшим; допрос потерпевшего или его представителя; допрос свидетелей;

производство выемки, осмотра и приобщение в качестве доказательств документов, содержащих охраняемую законом тайну, в том числе документов, отражающих принадлежность платежной карты конкретному лицу, выписки по счетам физических и юридических лиц, которые фигурируют в уголовном деле;

проведение оперативно-розыскных мероприятий, направленных на установление личности лиц, совершивших хищение, их розыск и задержание;

проведение обыска с участием соответствующих специалистов по месту регистрации либо фактического проживания лиц, причастных к хищению;

проведение опознания свидетелями (очевидцами) держателя карты как лица, причастного к хищению;

оценка собранных по уголовному делу доказательств для решения вопроса о предъявлении обвинения подозреваемому лицу, непосредственное предъявление обвинения, избрание меры пресечения.

Производство каждого отдельного следственного действия, и в своей совокупности, должно быть направлено на установление: факта хищения, в том числе способа, места и времени несанкционированного доступа в компьютерную систему или сеть, повлекшие хищение денежных средств; лица, совершившего неправомерный доступ к компьютерной информации и (или) хищение, а также выявление обстоятельств, способствовавших неправомерному доступу к компьютерной информации, в том числе наличия и надежности средств защиты компьютерной информации.

Между тем приведенный порядок (алгоритм) расследования хищений приобретает конкретный вид, когда следователь проводит анализ следственной ситуации при расследовании конкретной разновидности такого преступления, в том числе нормативного регулирования безналичных расчетов или электронных средств платежа.

Четвертый этап заключается в составлении письменного плана (программы и иной документации) расследования. При этом, если планирование строится на основе отдельных планов, разработанных по каждому направлению, версии (эпизоду) и т. п., то, несмотря на предварительную оптимизацию, следователь вновь корректирует отдельные разделы (составные части) единого плана расследования. Внесение изменений и дополнений в сформированный план расследования некоторыми авторами выделяется в самостоятельный этап планирования, либо выносится за рамки планирования и структурно включается в процесс реализации плановых решений.

В литературе предлагается следующая структура планов расследования преступлений: фабула дела, версии по делу, наименование процессуальных действий и иных мероприятий, исполнители, сроки исполнения, отметка об исполнении и примечание. Подобного рода структуры, в большинстве своем, встречаются в практической деятельности следователей, расследующих мошенничества, связанные с расходованием бюджетных средств. В некоторых случаях к плану прилагаются схемы и другая вспомогательная документация.

Изучение практики расследования хищений позволяет констатировать необходимость совершенствования структуры плана. Прежде всего, это вызвано многоэпизодностью уголовных дел, сложными схемами, реализуемыми при совершении рассматриваемого вида преступлений, что предопределяет большие объемы работ и длительные сроки предварительного расследования по таким делам. Практика расследования хищений выработала требования к структурам соответствующих планов расследования.

С учетом складывающейся практики составления планов расследования хищений и осознания необходимости их совершенствования, представляется возможным предложить следующую структуру плана расследования:

- титульный лист с наименованием документа - «План расследования по уголовному делу № 0000» и отметкой о согласовании и утверждении данного плана;

- краткая фабула дела;

- характеристика следственной ситуации;

- следственные версии и задачи расследования;

- анализ доказательств по уголовному делу с указанием эпизодов, перечня доказательств по каждому эпизоду;

- перечень процессуальных действий и организационных мероприятий по делу с указанием их наименования, вопросов, подлежащих разрешению, исполнителей и сроков проведения, отметки об исполнении. В зависимости от сложности уголовного дела, процессуальные и иные действия могут быть разбиты по эпизодам, построенным версиям и т. п.

Неотъемлемой частью плана должны стать схемы движения денежных средств с указанием связей между участниками преступления и т. п.

Представляется, что подобный план расследования будет способствовать повышению эффективности расследования хищений и сопряженных с ними преступных деяний. Кроме того, данная структура плана позволит более целенаправленно осуществлять процессуальный контроль начальников ОПС за ходом расследования преступлений.

Рассмотренные этапы планирования являются основной схемой формирования планов на первоначальном и последующих этапах расследования, а также по уголовному делу в целом. На завершающем этапе процесс планирования, как правило, приобретает упрощенную структуру (указываются порядок и предполагаемые сроки ознакомления с материалами уголовного дела, сроки производства дополнительных следственных действий и т. п.).

Планирование отдельных процессуальных и иных действий (мероприятий) и/или их комплексов, по существу, имеет такую же структуру, но меньший объем по содержанию.

Таким образом, конечный результат процесса планирования - готовый (сформулированный) план расследования.

Организация взаимодействия при расследовании хищений денежных средств,

совершаемых с использованием компьютерных технологий

Организации взаимодействия при расследовании хищений следователями и начальниками ОПС уделяется самое пристальное внимание, так как от его результатов зависит не только своевременное и полное раскрытие данного вида преступлений (установление виновных лиц), но и формирование по уголовному делу доказательств (доказательственной базы), а также эффективность профилактической деятельности.

Ключевыми субъектами, с которыми взаимодействуют следователи при расследовании хищений, являются сотрудники оперативных подразделений и экспертно-криминалистических подразделений органов внутренних дел, сотрудники контролирующих и надзорных органов, работники государственных и негосударственных судебно-экспертных учреждений и отдельные специалисты, работники кредитных и провайдерских организаций, платежных систем.

В целом взаимодействие при расследовании хищений организуется следователями и начальниками ОПС (каждый на своем уровне) в соответствии с положениями УПК РФ, Закона об ОРД, ведомственными нормативно правовыми актами, в том числе Инструкцией по организации совместной оперативно-служебной деятельности подразделений органов внутренних дел Российской Федерации при раскрытии преступлений и расследовании уголовных дел, утвержденной приказом МВД РФ от 29 апреля 2015 г. № 495-дсп, а также локальными документами (территориальных органов МВД России на окружном, межрегиональном, региональном и районном уровнях). Например, взаимодействие следователей с оперативными сотрудниками органов внутренних дел Владимирской области по противодействию указанному виду преступлений регламентировано приказом УМВД России по Владимирской области от 5 ноября 2015 г. № 556дсп, утверждающим Инструкцию об организации взаимодействия и порядке передачи материалов из оперативных подразделений полиции в следственные органы при выявлении, раскрытии и расследовании преступлений экономической и коррупционной направленности, совместным распоряжением Следственного управления и БСТМ УМВД России по Владимирской области от 17 декабря 2014 г. № 15-р/2-р «О повышении эффективности взаимодействия при рассмотрении материалов доследственных проверок, раскрытии и расследовании преступлений в сфере компьютерной информации», регламентирующим сроки и порядок рассмотрения материалов доследственных проверок, поступивших из БСТМ УМВД России по Владимирской области.

Следует отметить, что согласно полученной от ОПС информации, основной формой взаимодействия с оперативными сотрудниками, используемой следователями, является направление и исполнение поручений о проведении ОРМ, совместная работа в рамках созданных следственно-оперативных групп или рабочих групп (встреч) либо внештатных групп.

Как известно, согласно положениям ст. 11 Закона об ОРД «результаты оперативно-розыскной деятельности могут быть использованы для подготовки и осуществления следственных и судебных действий, проведения оперативно-розыскных мероприятий по выявлению, предупреждению,

пресечению и раскрытию преступлений, выявлению и установлению лиц, их подготавливающих, совершающих или совершивших, а также для розыска лиц, скрывшихся от органов дознания, следствия и суда, уклоняющихся от исполнения наказания и без вести пропавших, имущества, подлежащего конфискации, для принятия решений о достоверности представленных государственным или муниципальным служащим либо гражданином, претендующим на должность судьи, предусмотренных федеральными законами сведений», а также ст. 89 УПК РФ также посвящена использованию в доказывании результатов оперативно-розыскной деятельности в части установления запрета использования результатов оперативно-розыскной деятельности, если они не отвечают требованиям, предъявляемым к доказательствам.

Таким образом, результаты оперативно-розыскной деятельности могут использоваться в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства при условии, что вовлекаемые в уголовный процесс оперативно-розыскные сведения, как и любое доказательство, должны обладать свойствами относимости и допустимости.

Под результатами оперативно-розыскной деятельности, согласно п. 36.1 ст. 5 УПК РФ, понимаются сведения, полученные в соответствии с федеральным законом об оперативно-розыскной деятельности о признаках подготавливаемого, совершаемого или совершенного преступления, лицах, подготавливающих, совершающих или совершивших преступление и скрывшихся от органов дознания, следствия или суда.

Между тем обращает на себя внимание значительно более сдержанная позиция Конституционного Суда Российской Федерации, согласно которой результаты ОРД являются лишь сведениями об источниках тех фактов, которые, будучи полученными с соблюдением требований Закона об ОРД, могут стать доказательствами только после закрепления их надлежащим процессуальным путем, а именно на основе соответствующих норм уголовно-процессуального закона, т.е. так, как это предписывается ч. 1 ст. 49 и ч. 2 ст. 50 Конституции Российской Федерации.

Отражаются такие сведения в оперативно-служебных документах (рапоотах, .справках, справках-меморандумах, сводках, отчетах, актах). При этом к оперативно-служебным документам могут прилагаться предметы и документы, полученные при проведении ОРМ, которые, исходя из смысла п. 36.1 ст. 5 УПК РФ, не являются результатами ОРД, поскольку отражают лишь информацию, полученную субъектом ОРМ, и фиксируют итог его действий.

Отдельными учеными высказывается обоснованное, на наш взгляд, мнение, что «материалы, полученные в результате использования современных научно-технических средств, могут выступать в уголовном процессе как документы, как вещественные доказательства и как самостоятельный источник доказательств - в зависимости от совокупности характерных признаков»

В связи с отмеченным, интерес представляют положения Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд (далее - Инструкция о представлении результатов ОРД), согласно которым полученные (выполненные) при проведении ОРМ материалы фото- и киносъемки, аудио-и видеозаписи и иные

носители информации, а также материальные объекты, могут быть признаны вещественными доказательствами (п. 16), а к результатам оперативно-розыскной деятельности отнесены «достаточные данные, указывающие на признаки преступления, а именно: сведения о том, где, когда, какие признаки и какого именно преступления обнаружены; при каких обстоятельствах имело место их обнаружение, сведения о лице (лицах), его совершившем (если они известны), и очевидцах преступления (если они известны); о местонахождении предметов и документов, которые могут быть признаны вещественными доказательствами по уголовному делу; о любых других фактах и обстоятельствах, имеющих значение для решения вопроса о возбуждении уголовного дела» (п. 18) и «сведения (при установлении таковых) о местонахождении лиц, скрывающихся от органов предварительного расследования и суда; о лицах, которым известны обстоятельства и факты, имеющие значение для уголовного дела; о возможных источниках доказательств; о местонахождении предметов и документов, которые могут быть признаны вещественными доказательствами по уголовному делу; о других фактах и обстоятельствах, позволяющих определить объем и последовательность проведения процессуальных действий, выбрать наиболее эффективную тактику их производства, выработать оптимальную методику расследования по онкретному уголовному делу» (п. 19).

Следственным управлением УМВД России по Омской области осуществляется взаимодействие с внештатным подразделением полиции по противодействию мошенничествам общеуголовной направленности, созданным приказом УМВД России по Омской области от 29 июня 2015 г. № 555, осуществляющим сбор и формирование единой базы использования автоматизированной системы учета абонентских номеров, IP-адресов, идентификационных номеров (IMEI).

Учет преступлений в сфере «телефонных мошенничеств» с помощью специализированных компьютерных программ, либо баз данных в УМВД России по Омской области не ведется, учет данного вида преступлений осуществляется в общем порядке.

Для решения проблем взаимодействия следователей с сотрудниками оперативных подразделений разных ведомств эффективными продолжают оставаться организационные меры, принимаемые руководителями ОПС, направленные на проведение рабочих встреч и оперативных совещаний по конкретным материалам доследственной проверки и уголовному делу. При этом руководители ОПС и следователи должны исходить из возможностей оперативных подразделений каждого ведомства в отдельности, в том числе основанных на рабочих контактах с организациями, оказывающими услуги по защите компьютерной информации и разработке компьютерного программного обеспечения, и при их межведомственном взаимодействии, а также возможностей, которые закреплены в нормах международного права. Так, например, основными направлениями работы Управления «К» БСТМ МВД России являются: борьба с преступлениями в сфере компьютерной информации, в том числе выявление и пресечение фактов неправомерного доступа к компьютерной информации, изготовления, распространения и использования вредоносных программ для компьютерных устройств, а также противодействие мошенническим действиям с использованием возможностей электронных платежных систем; пресечение противоправных действий в информационно-телекоммуникационных сетях, включая сеть Интернет; борьба с незаконным оборотом радиоэлектронных и специальных технических

средств; борьба с международными преступлениями в сфере информационных технологий путем противодействия преступлениям в сфере информационных технологий, носящим международный характер, и взаимодействие с национальными контактными пунктами зарубежных государств; международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных технологий, путем взаимодействия с правоохранительными органами иностранных государств как на двусторонней, так и многосторонней основе (ООН, «восьмерка», СНГ, СЕ, ЕС, ШОС, АТР и др.). Так, в соответствии с соглашениями государств «восьмерки», подписанными в США, в каждой из Учет преступлений в сфере «телефонных мошенничеств» с помощью специализированных компьютерных программ, либо баз данных в УМВД России по Омской области не ведется, учет данного вида преступлений осуществляется в общем порядке.

ее стран созданы национальные координирующие центры (в Германии это БКА, в США - ФБР, в России - на базе МВД). Основной задачей центров является выполнение совместных мероприятий по срочному перехвату электронных данных и взаимный обмен этой информацией. Кроме того, еще с 2000 года между странами - членами СНГ действует «Соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации».

Также правоохранительные органы Российской Федерации, в том числе органы внутренних дел, осуществляют международный обмен информацией о преступлениях, связанных с хищением денежных средств с банковских платежных карт, по линии Интерпола, через НЦБ Интерпола МВД России. С этой целью в телекоммуникационной сети Интерпола 1-24/7 функционирует директория прямого доступа к базам данных по «BIN» платежных систем «MasterCard» и «Visa» (удаленно - «American Express»). При проверке 6-значного «BIN» платежной карты база данных выдает информацию о банке-эмитенте и государстве его нахождения.

Направлениями организации взаимодействия при расследовании хищений с сотрудниками экспертно-криминалистических подразделений ОВД, работниками государственных и негосударственных судебно-экспертных учреждений и отдельными специалистами, являются обеспечение участия соответствующих специалистов в производстве следственных действий, судебных экспертиз, использовании экспертно-криминалистических учетов.

Как уже отмечалось, на современном этапе существуют проблемы в организации производства СКЭ и, так называемых, предварительных компьютерных исследований.

По данным ЭКЦ МВД России в 2015 г. СКЭ выполнялись в 78 региональных и 10 межрегиональных ЭКП территориальных органов МВД России. При этом в 24 ЭКП производством СКЭ и исследований занимается по одному сотруднику. Всего в системе ОВД 333 сотрудника производят СКЭ и компьютерные исследования, из которых 266 имеют соответствующие права.

В 2015 г. силами сотрудников ЭКП территориальных органов МВД России было выполнено 12861 (+31,7 %) СКЭ, 6660 (-2,2 %) исследований, 3830 (+13,6 %) следственных действий и оперативно-розыскных мероприятий. Средняя нагрузка на одного сотрудника составила 58 СКЭ и исследований в год (существующие научно-обоснованные нормативы 30 СКЭ и исследований в

год). Существенное превышение нагрузки способствует снижению качества выполняемой работы (эксперты не успевают обнаружить всю искомую информацию, найденную информацию проверить на корректность, по нетиповым объектам и т.п.). В результате эксперты вынуждены делать выводы о невозможности исследований представленных объектов.

Остается сложная ситуация с привлечением сотрудников ЭКП в качестве специалистов для участия в следственных действиях и оперативно-розыскных мероприятиях, которые могут проводиться от нескольких часов до суток и более. При этом согласно позиции ЭКЦ МВД России, далеко не всегда присутствие профильного специалиста необходимо, а также не во всех ЭКП имеется мобильное оборудование, которое может им помочь в осмотре и копировании компьютерной информации, а то которое имеется укомплектовано не в соответствии с потребностями (в рамках гособоронзаказа в регионы поставлено 32 мобильных стенда; в комплект поставляемого стендового оборудования не входят все необходимые программные и программно-аппаратные средства (например, торговых марок Ufed и XRY); отсутствуют в ОВД системы обновления (продления лицензий) имеющегося программного обеспечения криминалистического назначения).

Отмеченные негативные тенденции находят подтверждение в информации ОПС. Так, например, по информации СУ УМВД России по Курганской области, в связи с отсутствием необходимого количества специалистов, методик проведения данного вида исследований в ЭКЦ УМВД России по Курганской области, экспертизы по уголовным делам о хищениях денежных средств с использованием компьютерных технологий не назначались.

На официальном сайте УМВД России по Курганской области между тем еще 5 октября 2015 г. размещена следующая информация: «В текущем году специалистами ЭКЦ УМВД России по Курганской области проведено более 150 компьютерных экспертиз. Кропотливому исследованию подверглись около 450 объектов: это системные блоки, ноутбуки, планшетные компьютеры, сотовые телефоны, жесткие диски, сим-карты и другие носители цифровой информации».

По информации СУ МВД России по Еврейской автономной области, в ЭКЦ данного территориального органа в штате имеется один эксперт с допуском для производства компьютерных исследований.

По информации СУ УМВД России по Владимирской области, одной из основных проблем расследования хищений денежных средств, совершаемых с использованием компьютерной информации, является невозможность установления в ходе проведения судебных экспертиз и исследований сведений о наличии в мобильных устройствах потерпевших какого-либо вредоносного программного обеспечения, непосредственно используемого для совершения хищения принадлежащих им денежных средств. Специалисты ЭКЦ УМВД России данного региона могут установить в ходе проведения судебной экспертизы только наличие на компьютерном устройстве вредоносного программного обеспечения, без описания его свойств и механизма воздействия.

Следует отметить, что некоторые ЭКЦ территориальных органов МВД России на региональном уровне обеспечены аппаратно-программными комплексами для производства съема и исследования данных из мобильных устройств, в том числе вирусных программ. Например, с декабря 2013 г. сотрудники ЭКЦ

УМВД России по Амурской области в своей работе стали использовать аппаратно-программный комплекс, который позволяет считывать информацию с любых электронных носителей (персональных компьютеров, оборудования сотовой связи, планшетов, пластиковых банковских карт, смарт-карт и т. п.). С использованием данного комплекса специалисты ЭКЦ могут распознать всю информацию, которая когда-либо существовала в памяти электронного носителя: фото-, видео документы, активность использования Сети, подробная история личной переписки, список контактов, а также данные владельца того или иного носителя.

Вместе с тем, спецификация этого комплекса, как отмечают ОПС (напр., СУ УМВД России по Омской области), не предусматривает дальнейшего разбора или анализа вирусного программного обеспечения, обнаруженного в мобильном устройстве.

К актуальным задачам, которые следует решать с использованием возможностей СКЭ, по информации ОПС относятся: определение алгоритма вредоносной программы; извлечение из вредоносной программы списка управляющих серверов; документирование функциональных особенностей вредоносной программы (например, особенностей ее взаимодействия с системами дистанционного банковского обслуживания); определение и документирование реализованных в программе способов противодействия криминалистическому исследованию и обнаружению; документирование изменений, вносимых программой в системный реестр и файловую систему в целом; определение и описание иных действий программы с информацией, которые могут иметь значение для уголовного дела; исследование конфигурационных файлов и дополнительных программных модулей, загружаемых вредоносной программой из сети Интернет; корреляция полученной информации с другими экземплярами вредоносных программ; установление абонентских номеров, с которых поступает SMS-сообщение со ссылкой на загрузку вирусной программой; установление Интернет-сайта, с которого осуществлена загрузка вредоносной программы, а также IP-адреса, с которого вирусная программа поступила на сайт.

Отсутствие у следователя возможности оперативно и в полном объеме решать перечисленные и иные задачи с использованием возможностей СКЭ непосредственным образом влияет на качество и сроки предварительного расследования хищений. Так, по уголовным делам № 2-711/15 и № 2-712/15, возбужденным ОПС МВД по Республике Тыва 7 мая 2015 г. по фактам хищения денежных средств организаций в системе ДБО, были назначены СКЭ, производство которых 2 июля 2015 г. поручено сотрудникам ЭКЦ ГУ МВД России по Красноярскому краю, но до 5 февраля 2016 г. (дата направления информации) не исполнены в связи с большой загруженностью эксперта.

В связи с невозможностью проведения в ЭКЦ УМВД России по Курганской области экспертиз по установлению вида вредоносной программы, с помощью которой осуществлялось хищение денежных средств, времени и способа ее внедрения, у ОПС данного региона отсутствует возможность установления интернет-сайта, с которого осуществлена ее загрузка, а также IP-адреса, с которого вирусная программа поступила на сайт. Проверка всех сайтов, посещенных потерпевшими и указанных в их допросах, путем направления запросов владельцам затруднительна или невозможна, так как большинство из них зарегистрированы за границей Российской Федерации.

В качестве способов решения обозначенных проблем организации взаимодействия следователей с сотрудниками ЭКП предлагается:

увеличить количество специалистов в ЭКП соответствующей специализации;

назначение СКЭ сотрудниками оперативных подразделений при рассматривании сообщений о хищениях, а не предварительных компьютерных исследований;

поручение производства СКЭ специалистам иных государственных и негосударственных судебно-экспертных учреждений или организаций. Например, СКЭ в настоящее время могут проводить следующие организации (учреждения):

автономная некоммерческая организация «Научно-исследовательский центр экспертизы и сертификации» (АНО НИЦЭС), расположенный по адресу: 121596, г. Москва, ул. Толбухина, д. 13/2, офис 5;

автономная некоммерческая организация «Центр информационной безопасности, экспертизы и сертификации» - 127560, г. Москва, ул. Коненкова, д. 19 «Г», кв. 23. Стоимость проведения исследования или экспертизы 1 объекта (носителя информации - мобильного телефона, жесткого диска и т.п.) составляет 65 (шестьдесят пять тысяч) рублей.

«Group-IB» - 115088 г. Москва, ул. Шарикоподшипниковская, д. 1, БЦ «Прогресс Плаза», 9 этаж. Group-IB - международная компания по предотвращению и расследованию кибер преступлений и мошенничеств. Имеет сертификаты CISSP, CIS A, CISM, CEH, CWSP, GCFA и свидетельство государственного образца в области защиты информации. Стоимость проведения исследования или экспертизы 1 объекта (носителя информации -мобильного телефона, жесткого диска и т.п.) составляет 300 ООО (триста тысяч) рублей.

ООО «Доктор Веб» - 125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12 «А». Стоимость проведения исследования или экспертизы 1 объекта (носителя информации - мобильного телефона, жесткого диска и т.п.) договорная и зависит от объема исследования и (или) экспертизы.

«Лаборатории Касперского» - 125212, г. Москва, Ленинградское шоссе, д. 39 «А», стр. 3, БЦ «Олимпия Парк». Проведение экспертиз бесплатно, только при наличии фигурантов по уголовному делу, по согласованию с отделом проведения экспертиз.

Согласно поступившей от ОПС информации, основными формами взаимодействия при расследовании хищений следователей с работниками коммерческих организаций, в том числе коммерческих банков, платежных систем, сотовых операторов и провайдеров, а также с сотрудниками контролирующих органов являются направление и получение ответов на запросы и представления об устранении обстоятельств, способствующих хищениям. Между тем практические все ОПС отмечают проблему длительности исполнения направленных в указанные организации и органы запросов, а также предоставление информации не в полном объеме (не в строгом соответствии с вопросами, указанными в запросах). При этом некоторые ОПС подчеркивают, что инструментов воздействия, кроме направления повторных запросов, требований и представлений не имеется.

Для решения проблем взаимодействия следователей, а также оперативных сотрудников органов внутренних дел с кредитными и иными организациями некоторые начальники территориальных органов, в том числе по инициативе руководителей ОПС, организуют рабочие встречи с представителями таких организаций. Между тем справедливости ради отметим, что далеко не во всех случаях такого рода встречи приводят к положительным результатам. Так, по инициативе УМВД России по Омской области проводятся рабочие встречи с отделением по информационной безопасности УФСБ России по Омской области, руководством Омского отделения ПАО «Сбербанк России». Как констатируется в информации СУ УМВД России по Омской области, совместные совещания не позволили решить ряд стратегических задач. Продолжается негативная практика взаимодействия с работниками ПАО «Сбербанк России» в одностороннем порядке, которые не проявляют должной заинтересованности и не оказывают посильную помощь в раскрытии хищений денежных средств правоохранительными органами, а сроки предоставления информации ПАО «Сбербанк России» затянуты.

Поддерживая предложение о закреплении на законодательном уровне степени ответственности за сроки и качество предоставляемой информации, авторы настоящей работы обращают внимание на то, что в настоящее время некоторыми ОПС нарабатывается практика административного воздействия на коммерческие организации в подобных ситуациях. Так, СУ УМВД России по Владимирской области обращает внимание на то, что некоторые операторы сотовой связи, такие как «Билайн», «МТС» и представители платежной системы QIWI допускают факты несвоевременного исполнения запросов следователей, что приводит к направлению напоминаний и исполнение данных запросов занимает срок до 3-х месяцев. В 2015 г. следователями ОПС области операторам сотовой связи внесены представления об устранении данных нарушений, в связи с их неисполнением в феврале 2016 г. руководство компании «МТС» решением суда привлечено к административной ответственности по ст. 17.7 Кодекса об административных правонарушениях Российской Федерации (далее, КоАП).

Как представляется, следователям необходимо активней использовать не только ст. 17.7 КоАП, но и другие нормы (ст. 13.29, 13.30).

Кроме того, при расследовании хищений денежных средств, совершаемых с использованием компьютерных технологий, следователями выявляются факты неисполнения операторами связи требований постановления Правительства Российской Федерации от 27 августа 2005 г. в части хранения данных в течение 3 лет. Представляется уместной практика ОПС Саратовской области о направлении при выявлении таких фактов соответствующей информации в порядке, предусмотренном ч. 2 ст. 158 УПК РФ, в Управление Роскомнадзора по Саратовской области для принятия мер реагирования.

Важным направлением организации взаимодействия при расследовании хищений следователей с работниками коммерческих организаций, в том числе коммерческих банков, платежных систем, сотовых операторов и провайдеров, является внесение представлений о принятии мер по устранению обстоятельств, способствующих совершению данного вида преступлений, или других нарушений закона, а также уведомление о принятых мерах.

Анализ поступившей от ОПС информации свидетельствует, что к обстоятельствам, способствующим совершению хищений, относятся слабая работа коммерческих банков, платежных систем и ретейрских организаций, направленная на защиту информации своих клиентов (IT-безопасность), халатность граждан по защите своих мобильных устройств, в том числе неотключение услуг удалённого доступа, предоставляемых коммерческими банками, к своим счетам при смене/прекращении пользования абонентским номером сотовой связи, по сохранности кодов доступа к своим платежным картам, расчётным счетам, или безответственность сотрудников, которые должным образом не соблюдают меры безопасности при работе с программным обеспечением системы ДБО.

В качестве примера можно привести хищение денежных средств в сумме 32 973 357 рублей с банковского счета РОО РТ ГТО, произошедшее 25 декабря 2015 г. Причиной хищения явились действия главного бухгалтера данной организации Л.В. Аглиуллиной, которая в нарушение мер информационной безопасности скопировала электронный ключ для работы в системе ДБО с дискеты, выданной коммерческом банком, на жесткий диск персонального компьютера, с которого осуществляла доступ к сети Интернет без прекращения работы с программой «Клиент-Банк». Кроме того, после получения уведомления о том, что необходимо закрыть все окна и перезагрузить компьютер, она не выполнила данное указание, что и способствовало заражению компьютера вредоносным программным обеспечением. После перезагрузки компьютер не запустился, и Аглиуллина вызвала специалиста, который продиагностировав, запустил его в рабочем состоянии. Проверка на наличие вредоносного программного обеспечения не проводилась, поскольку она посчитала произошедшие события системным сбоем.

В преставлениях, в зависимости от обстоятельств хищения, могут содержаться рекомендации:

1) постоянного обновления антивирусных программ, позволяющих обнаружить вредоносные файлы известных типов, а также вредоносные файлы, неизвестные антивирусу, но действующие в соответствии с известными антивирусному ядру алгоритмами действия

2) проведения периодического антивирусного сканирования на обнаружение ранее неизвестных вирусных программ, находящихся в неакгивированном виде

3) установки Firewall для исключения возможности атак через открытые порты, а также

4) введения: системы ограниченного доступа ограничить количество посещаемых Интернет-ресурсов до необходимого минимума; системы ограничения использования внешних устройств исключить риск заражения с внешних устройств, в том числе флеш-накоиителей; списка разрешенных приложений уменьшить риск запуска неизвестных приложений без их предварительной проверки на безопасность; системы проверки Интернет-трафика исключить использование уязвимостей клиентского программного обеспечения за счет проверки трафика до его поступления в приложения; системы поверки Интернет-ссылок исключить возможность перехода на зараженные и мошеннические ресурсы.

В качестве примера можно привести уголовное дело № 360282, возбужденное 16 февраля 2015 г. СУ У МВД России по г. Барнаул, по которому установлено, что в периоде 6 декабря 2014 г. по 17 февраля 2015 г. участники созданной Райсяном организованной преступной группы Дубовых, Салюков, Ракитнна, Ракитин совершили хищение денежных средств со счетов банковских карт Публичного акционерного общества «Сбербанк России», открытых на имя 32 граждан, проживающих на территории Алтайского края, причинив им ущерб на общую сумму 185 тыс. руб. Указанным лицам предъявлены обвинения по п. «а» ч. 4 ст. 158 УК РФ и в их отношении судом избрана мера пресечения в виде заключения под стражу.

19 апреля 2016 г. по данному уголовному делу заместителем Министра внутренних дел Российской Федерации начальником Следственного департамента МВД России на имя Президента, Председателя Правления ПАО «Сбербанк России» Г.О. Грефа в соответствии со ст. 158 УПК РФ внесено представление об устранении обстоятельств, способствующих совершению преступлений, в котором указано, что совершение хищения денежных средств со счетов банковских карт стало возможным в связи с несовершенством системы информационной безопасности услуги «Мобильный банк», предоставляемой ПАО Сбербанк владельцам платежных карт; отсутствием эффективной системы контроля за операциями, производимыми клиентами с использованием указанной услуги; возможностью доступа посторонних лиц к персональным данным клиентов ПАО Сбербанк.

Особое внимание ОПС в современных условиях следует обратить на такую форму профилактики как внесение, так называемых, обобщенных представлений (информационных писем) в коммерческие банки или соответствующим их руководителям.

Так, 16 ноября 2015 г. СУ УМВД России по Владимирской области, с учетом анализа находящихся в производстве уголовных дел и направленных ОПС на районном уровне представлений по конкретным уголовным делам, с целью профилактики и пресечения данного вида преступлений, на имя Управляющего Владимирского отделения № 8611 ПАО «Сбербанк России» направлено информационное письмо, в соответствии с которым работникам данного коммерческого банка предложено при заключении договоров на оказание услуги мобильного банкинга, в обязательном порядке доводить до сведения клиентов информацию о рисках использования данной услуги и способах обеспечения безопасности операций по лицевым счетам, а также проведении иных мероприятий, направленных на обеспечение экономической безопасности клиентов.

Согласно поступившему ответу Владимирским отделением № 8611 ПАО «Сбербанк России» проводится комплекс мероприятий, направленных на информирование клиентов о наиболее распространенных мошеннических схемах и способах защиты от них. Кроме того, с целью защиты мобильных устройств клиентов, ПАО «Сбербанк России» совместно с АО «Лаборатория Касперского» разработано антивирусное программное обеспечение для операционных систем «Android».

Отметим, что на официальном сайте ПАО «Сбербанк России» для клиентов данного банка - абонентов Билайн и Мегафон, использующих аппараты под управлением Android, бесплатно доступен антивирус (приложение DrWeb for Android Light (доступен для загрузки из Google Play) и Kaspersky Internet

Security for Android (пробная версия доступна на сайте компании, также будет доступна для загрузки из Google Play)

Также эффективным средством профилактики является выступление и публикации следователей, руководителей ОПС в СМИ с целью информирования граждан о способах хищений денежных средств, совершаемых с использованием компьютерных технологий, о мерах безопасности применения ими компьютерных технологий при проведении банковских операций. В качестве положительного примера можно отметить проведение 9 декабря 2015 г. сотрудниками СУ совместно с УР УМВД России по г. Саратову, БСТМ ГУ МВД России по Саратовской области пресс-конференции, посвященной профилактике хищений с банковских счетов граждан в системе ДБО, а также с использованием банкоматов. Информация о проведенной пресс-конференции размещена на сайте ГУ МВД России по Саратовской области. Кроме того, подготовлен видеорепортаж, который 12 декабря 2015 г. вышел в эфир передачи «Вести. Дежурная часть. Саратов» на канале «ВГТРК.Саратов».

21 декабря 2015 г. и 4 апреля 2016 г. заместителем начальника УМВД России по Ярославской области - начальником СУ полковником юстиции А.И. Мешковым проведен брифинг с представителями областных СМИ в целях профилактики рассматриваемого вида преступлений. На данном брифинге И. Мешков, обращаясь к представителям СМИ, обозначил проблему участившихся мошенничеств, совершаемых с использованием компьютерных технологий, и призвал представителей СМИ к проведению совместной профилактической работы по усилению информационной безопасности среди различных категорий граждан.

Также в 2015 г. СУ УМВД России по Ярославской области опубликовало информацию профилактического характера по уголовным делам о рассматриваемом виде хищений в информационных изданиях «Комсомольская правда», «Ярньюс.Нет», «Городской телеканал», «76.RU», «Городские новости», «MONA VISTA», «Без формата.ш», «АиФ Ярославль», подготовило выступления руководителей ОПС УМВД России по Ярославской области на районном уровне в местных СМИ (3 телевизионных выступления, 13 публикаций в печатных изданиях).

В качестве обеспечительной меры профилактической работы следует назвать изучение опыта ОПС других регионов страны. Так, в рамках взаимного сотрудничества СУ МВД Республики Бурятия изучен положительный опыт ГСУ МВД России по Курганской и Иркутской областям в сфере профилактики мобильного мошенничества.

Организация производства отдельных следственных действий при расследовании хищений денежных средств, совершаемых с использованием компьютерных технологий

Проведенный нами анализ следственной практики показал, что основными следственными действиями, востребованными при расследовании хищений и имеющими существенную специфику, явились осмотр (места происшествия, предметов и документов), обыск (в жилище, в ином помещении, личный),

выемка (обычная, предметов - электронных носителей информации, электронной почтовой корреспонденции), допрос (обвиняемого, подозреваемого, потерпевшего, свидетеля, эксперта, специалиста), получение информации о соединениях между абонентами и (или) абонентскими устройствами, назначение экспертизы.

Рассмотрим особенности производства перечисленных следственных действий в процессе расследования хищений рассматриваемого вида.

1. Осмотр (места происшествия, предметов и документов). Особое значение осмотра места происшествия как первого следственного действия, проводимого, как правило, до возбуждения уголовного дела, заключается в том, что это самое близкое во времени и в пространстве соприкосновение следователя с событием преступления.

Осмотр при расследовании хищений позволяет установить ряд важных обстоятельств, а именно:

имеются ли на месте осмотра следы события, подлежащего расследованию;

если да, то содержит ли событие признаки хищения; кто принимал участие и какую функцию выполнял при подготовке, совершении и сокрытии хищении;

какие носители информации, содержащие следы события, подлежащего расследованию, имеются на месте происшествия;

какие технические средства и документы использовались для доступа к предмету посягательства и совершения незаконных действий с ним;

кто мог стать очевидцем подготовки, совершения или сокрытия хищения и т.п.

Известно, что сущность рассматриваемого следственного действия заключается в непосредственном исследовании следователем (дознавателем) и другими участниками осмотра обстановки места происшествия; выявлении, изучении, фиксации и изъятии в установленном законом порядке материальных объектов и следов на них с целью получения сведений и доказательств, имеющих значение для раскрытия и расследования преступлений, а также событий, содержащих признаки преступления.

В настоящей работе обосновывалось, что место рассматриваемого вида преступления (место происшествия) образует:

1) место физического нахождения (пространственное расположение) преступников в период подготовки, совершения и сокрытия хищения

2) мест открытия банковских и иных счетов, с которых списываются (перечисляются, похищаются) денежные средства

3) мест открытия банковских и иных счетов, на которые зачисляются похищенные денежные средства

4) мест нахождения компьютерных устройств потерпевших и т. п. Также нами обосновывалось значение мест обналичивая денежных средств, в тех случаях, когда эти соответствующие действия не образуют самостоятельный этап хищения.

Специфика рассматриваемого вида хищений такова, что место происшествия привязано к IP-адресу компьютерного устройства преступника, IP-адресу

компьютера потерпевшего, IP-адресу некоторого элемента электронной платежной системы, с которым осуществлялось взаимодействие.

Таким образом, на место преступления укажут, например, сведения о привязке GPRS-модема к базовой станции сотовой связи или IP-адрес, которому по договору между пользователем и провайдером сопоставлен конкретный адрес местожительства конкретного лица, если не предпринимались меры по подмене IP-адреса.

В связи с тем, что на месте происшествия могут находиться такие носители информации как внешние накопители на жестких магнитных дисках, компакт-диски, устройства флэш-памяти в разнообразном исполнении, считаем целесообразным указывать факт их наличия в протоколе осмотра места происшествия с указанием следующих данных: места нахождения носителя информации, его тип, название, индивидуализирующую и идентифицирующую объект информацию (маркировочные обозначения, серийные номера и т. п.).

Также на месте происшествия может находиться компьютерная и иная техника (например, мобильные телефоны), на носителях которых могут остаться следы события преступления. Такая техника описывается в протоколе следственного действия с указанием сведений, аналогичных сведениям, приводимым при обнаружении носителей информации; дополнительно указывается комплектация оборудования.

Специфичен осмотр места происшествия, представляющего помещение с сервером (например, в кредитной или иной организации), на котором предположительно имеется информация, относящаяся к событию преступления. В протоколе осмотра необходимо отразить факт наличия технических средств, к которым нет логического доступа непосредственно из осматриваемого помещения, поскольку рабочее место по управлению сервером находится, как правило, в ином помещении. Также целесообразно указать на то, из какого места производится доступ на логическом уровне администраторов к серверу. Указанное место доступа также должно выступать в качестве места происшествия, подлежащего осмотру.

Особенными целями осмотра места рассматриваемого вида хищений дополнительно являются поиск, обнаружение, осмотр и изъятие средств подготовки, совершения и сокрытия преступления, уголовно-релевантной информации: средств электросвязи; специальных технических средств для негласного получения информации с технических средств; вредоносных программ на компьютерных носителях информации; специальной литературы; методических рекомендаций и цифровых видеофильмов, раскрывающих способ преступления; электронных записей, находящихся в памяти компьютера или иного аппаратного средства, и содержащих криминалистически значимые сведения - имена, адреса, телефоны сетевые псевдонимы, сетевые адреса, даты, PIN-коды, реквизиты доступа к электронным счетам, названия вредоносных компьютерных программ и другую идентификационно-справочную информацию.

Отметим, что помимо проблем, предполагающих обязательное привлечение к следственному осмотру специалиста и использование его специальных знаний, существенной является проблема привлечения к осмотру понятых в порядке ст. 177 УПК РФ. Поскольку понятым может выступать любое незаинтересованное в исходе уголовного дела лицо, то такой понятой в

подавляющем большинстве случаев не будет обладать специальными знаниями, позволяющими ему удостоверить содержание, ход и результаты следственного действия.

Представляется, что данное обстоятельство может стать поводом для внесения изменений в ч. 3 статьи 170 УПК РФ, которая оговаривает условия, при которых следственное действие производится без участия понятых. Считаем добавить в перечень таких условий после слов «а также в случаях, если производство следственного действия связано с опасностью для жизни и здоровья людей» фразу «или связано с наличием на месте проведения следственного действия сложных технических устройств, подлежащих отображению в его протоколе». Вместе с тем при отсутствии такого разрешения следственная практика идет по пути привлечения в качестве понятых лиц, обладающих минимально необходимыми специальными знаниями, что вступает в логическое противоречие с фактом участия в следственном действии специалиста, заведомо обладающего требуемым объемом таких знаний.

Важно, что по результатам осмотра следователь может установить, совершено ли преступление с использованием компьютерных технологий, либо происшедшее событие является следствием негативных факторов или правонарушением иного рода.

Осмотр предметов (документов) по делам о преступлениях, совершенных с использованием компьютерных технологий, на первый взгляд не содержит специфики по сравнению с аналогичным осмотром, проводимым по делам о преступлениях в сфере компьютерной информации, порядок и содержание которого детально описаны В. Ю. Агибаловым, В. Б. Веховым, Д. А. Илюшиным, П.В. Костиным, Т.Э. Кукарниковой, А. Н. Яковлевым и другими учеными. Вместе с тем, это не совсем верное утверждение. Специфика осмотра предметов (документов) при расследовании хищений рассматриваемого вида, заключается в том, что осмотру подлежат, как правило, не файлы, содержащие текстовые или графические документы, подготовленные пользователем, а служебные журналы системных и прикладных программ, применяемых для осуществления транзакций. Это предполагает использование в ходе осмотра современных экспертных аппаратно-программных комплексов, оснащенных необходимым экспертным программным обеспечением, позволяющих быстро находить требуемые файлы и интерпретировать их содержимое. Использование в этих целях компьютера, специально не подготовленного для проведения осмотра (например, рабочего компьютера следователя) -нецелесообразно.

Практически при каждом расследовании хищений имеется необходимость провести осмотр обнаруженного и (или) изъятого средства сотовой связи (мольного устройства), который, как правило, делится на несколько этапов:

внешний осмотр, в ходе которого происходит непосредственное изучение и фиксация наружного строения и состояния мобильного устройства, в рамках которого в протоколе указываются марка, модель, тип, форма аппарата, цвет корпуса, размер; наличие объективов тыльной и (или) лицевой фото/видеокамеры (вспышки), фирменных наименований, логотипа, обозначений; количество и расположение функциональных, встроенных, сенсорных клавиш (джойстика); разъемов Mini(Micro)USB, зарядного устройства, стереонаушников; наличие отверстий для динамика, микрофона,

датчика расстояния, внешней освещенности. Отдельно указываются особые приметы наружного строения: повреждения - сколы, царапины, потертости, отсутствие должных элементов; наличие дополнительных атрибутов и технических составляющих - чехла, шнурка, брелока, гарнитуры, полимерных наклеек, графических вставок, надписей, инкрустации драгоценными металлами и др. В ходе внешнего осмотра проводится детальная фотосъемка внешней, оборотной, боковых панелей мобильного устройства. В случае если осматриваемый телефон раскладного («бабочка») или раздвижного типа («слайдер»), то телефон фотографируется в первоначальном и раскладном/раздвижном состоянии;

конструктивный осмотр - осмотр конструкции телефона по частям -задней крышки телефона и (или) аккумуляторной батареи (в определенных моделях аппаратов сотовой связи батарея встроена в корпус либо в заднюю крышку), флеш-карты, SIM-карт(ы). При осмотре аккумуляторной батареи в протоколе следует указать ее идентификационный номер, тип, марку, модель, мощность, иную информацию, указанную на корпусе. Также в протоколе указывается цвет и родовой материал, из которого изготовлена батарея. При осмотре флеш-карты (MiniSD) необходимо обратить внимание на ее идентификационный номер, объем, цвет и родовой материал корпуса. SIM-карта, обнаруженная в телефоне, осматривается аналогичным образом. Как правило, на корпусе SIM-карты имеется логотип оператора сотовой связи, описание которого также обязательно в протоколе. В ходе конструктивного осмотра проводится детальная фотосъемка внешней и оборотной стороны батареи, флеш-карты, SIM-карты, а также тыльной стороны корпуса мобильного телефона (без задней крышки) так, чтобы на снимке был виден IMEI-номер мобильного устройства;

осмотр информационной среды, включающий изучение и фиксацию сведений, которые содержатся в памяти телефона, флеш-карты, SIM-карты. В случае если в ходе осмотра следователю удалось включить мобильный телефон, и получен доступ к сведениям, которые в нем находятся, в протоколе в хронологическом порядке фиксируются все производимые в дальнейшем с устройством манипуляции.

В следственной практике нередко возникают ситуации, в которых в ходе производства первоначальных следственных действий изымается сразу несколько мобильных устройств во включенном состоянии. Выключать их в таких случаях до осмотра нецелесообразно (отключение может произойти при извлечении батареи, SIM-карты, просмотре IMEI-кода на наклейке, расположенной во внутренней части панели телефона и т. д.), т. к. при последующем включении потребуются коды блокировки (PIN-код), которые могут быть известны только его последнему пользователю (подозреваемому, свидетелю или потерпевшему). Отказ последнего в предоставлении информации по разблокировке телефона может исключить возможность незамедлительного полноценного исследования его информационного содержимого (электронной записной книжки, входящих и исходящих соединений, SMS-, MMS-сообщений, E-mail, голосовой почты, фото-, видеофайлов, диктофонных записей, органайзера и др., в зависимости от модели телефона). Поэтому важно подчеркнуть, что если к моменту осмотра мобильное устройство было включено, то конструктивный осмотр следует проводить только после изучения его информационной среды.

В литературе высказывается мнение, что в случае отсутствия согласия законного владельца мобильного устройства осматривать данные о входящих и исходящих сигналах, следователь может осматривать его только по решению Суда.

Обязательность исполнения этого положения корреспондирует с позицией Конституционного Суда Российской Федерации, согласно которой «…информацией, составляющей охраняемую Конституцией Российской Федерации и действующими на территории Российской Федерации законами тайну телефонных переговоров, считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи; для доступа к указанным сведениям органам, осуществляющим оперативно-розыскную деятельность, необходимо получение судебного решения. Иное означало бы несоблюдение требования статьи 23 (части 2) Конституции Российской Федерации о возможности ограничения права на тайну телефонных переговоров только на основании судебного решения»

Таким образом, в случае отказа лица - владельца мобильного устройства в даче согласия на его осмотр, но при необходимости производства осмотра в связи с его неотложностью, следователь может руководствоваться требованиями ч. 5 ст. 165 УПК.

Осмотр информационной среды необходимо начать с указания в протоколе процедуры разблокировки клавиатуры мобильного устройства, перечисления графических и текстовых элементов, которые отобразились на его экране после разблокировки. Затем осуществляется проверка IMEI-номера мобильного устройства нажатием комбинации клавиш *#06# (пятнадцатизначный номер должен отобразиться на экране телефона).

В случае если мобильное устройство не защищено паролем, то в протоколе осмотра последовательно указывается информационное содержимое - список контактов, сообщений, наличие изображений, фотографий, видеороликов и т. д. При описании определенного контакта указывается его вид (входящий, исходящий, неотвеченный), время, длительность, данные абонента, с которым осуществлен контакт, а также его абонентский номер (описание сообщения исключает указание длительности, но включает текстовое (SMS) и (или) графическое содержимое (MMS)).

Описание графических изображений, фотографий состоит из следующих элементов: указание того, что или кто изображен, тип, размер, время создания файла (описание видеороликов включает, помимо указанного, их длительность).

Отметим, что в настоящее время органы внутренних дел обеспечиваются специальной высокотехнологичной криминалистической техникой, позволяющей извлекать полную информацию (включая удаленную) из мобильных устройств, а также электронных накопителей (карт памяти, сим-карт и др.) как в ходе проверки сообщений о преступлениях, так и в ходе их расследования.

К такой технике относятся: универсальное устройство извлечения судебной информации (UFED - Universal Forensic Extraction Device), мобильный криминалист, XRY, MOBILedit, Тарантула и др.). При этом данная

криминалистическая техника позволяет работать почти с любой моделью мобильных устройств, в том числе с поврежденными устройствами, планшетными компьютерами на основе любой операционной системы, навигаторами, а также позволяет войти в операционную систему в обход (либо распознавая) паролей и логинов, работать с мобильными устройствами без аккумулятора, либо отдельно с SIM-картой.

Поэтому в случае если доступ к информационной среде мобильного телефона затруднен, то для участия к осмотру необходимо привлечь специалиста, имеющего навыки пользования данными устройствами.

С помощью указанной и иной высокотехнологичной криминалистической техники в рамках следственного осмотра мобильных устройств с участием специалиста (ч. 2 ст. 176 УПК РФ) либо в процессе производства СКЭ (ст. 195 УПК РФ) можно получить информацию о телефоне (IMEI/ESN); сим-карте (ICCID и IMSI); вызовах, в том числе удаленных (время, имена, фото); об использовании интернет-браузера; закладках интернет-сайтов; файлах Cookie; записях телефонной книги; SMS, MMS и голосовых сообщениях; сообщениях чатов и электронной почты; изображениях; видео- и аудиофайлах; местоположении (сети WiFi, ретрансляторы мобильной связи и навигационные приложения), маршрутах перемещения (можно просматривать в Google Earth и Google Maps), GPS-координатах использования мобильного устройства; введенных в GPS устройствах (навигаторы) местоположения, координатах, избранных расположениях; паролях, журналах вызовов, текстовых сообщениях, контактах в электронной почте, мессенджерах, записях в календаре, медиафайлах, геотегах, приложениях, служебных данных (список IMSI, данные последней сим-карты, коды блокировки); данных журнала «Lifeblog», содержащего список действий с телефоном; переписке в различных социальных сетях («Вконтакте», «Одноклассники», «Twitter», «Facebook»), с помощью таких приложений, как Skype, и др.

Извлеченная из мобильного устройства информация может:

напрямую изобличать лицо в совершении преступления (видео, фото совершенного преступления, SMS-сообщения о совершенном хищении);

косвенно указывать на линию поведения лица, возможную причастность его к совершенному хищению;

способствовать установлению иных обстоятельств, имеющих значение для дела.

В ходе осмотра информационной среды мобильного устройства проводится поэтапная детальная фотосъемка экрана мобильного телефона с информацией, представляющей значение для уголовного дела. Для визуальной фиксации большого объема сведений, содержащихся в информационной среде, следует применять видеосъемку. При этом следователь в обязательном порядке комментирует все действия, которые направлены на получение той или иной информации с помощью соответствующих манипуляций.

Обыск (в жилище, в ином помещении, автомашине, личный)

Наличие достаточных данных о том, что в каком-либо месте или у какого-либо лица могут находиться орудия преступления, предметы, документы, которые могут иметь значение для уголовного дела, является основанием для

проведения обыска. В качестве отыскиваемых в ходе обыска орудий преступления, предметов, относящихся к событию хищения, выступают компьютерные устройства, в том числе средства мобильной связи, электронные носители информации и иные носители информации, содержащие следы события, подлежащего расследованию.

В ходе обыска необходимо обратить внимание также на следующие документы: черновики с отражением записей о реквизитах доступа к банковским и иным счетам; выписки финансового характера; гарантийные письма об оплате товаров и услуг; записки и письма, в которых затрагиваются вопросы электронных расчетов, договоров; черновые записи о проведенных операциях; при обыске могут быть обнаружены и другие документы, значимые не только для расследуемого дела, но и свидетельствующие о совершении иных преступлений.

При производстве обыска следует иметь в виду, что современные носители информации могут быть интегрированы в различные предметы: рамку с цифровыми фотографиями, наручные часы, кулон, аудиоплеер и т. п. Поэтому обыск целесообразно проводить с применением соответствующих технических средств (приборов нелинейной локации), позволяющих обнаружить мобильные устройства и электронные накопители в помещениях, автотранспорте, в том числе при досмотре людей или личном обыск.

Индивидуальная тактика обыска избирается следователем в зависимости от характера и способа совершенного хищения, условий следственной ситуации. При этом следователю рекомендуется обращать внимание на место нахождения и возможного сокрытия компьютерных устройств и в особенности извлекаемых из них накопителей (например, SIM-карт), а также на поведение участников обысков, пытающихся воспользоваться мобильным устройством для оказания противодействия расследованию.

Выемка (обычная, предметов - электронных носителей информации, электронной почтовой корреспонденции)

Выемка производится в тех случаях, когда следователь располагает точной информацией о том, что нужные ему предметы, документы находятся в определенном месте. Выемка проводится в целях изъятия машинных носителей, содержащих файлы с искомым текстовым и графическим содержимым, а также программы, используемых для подготовки и совершения преступлений рассматриваемой категории. Такие носители информации чаще всего находятся в компьютерах лиц, подозреваемых в совершении преступления.

Целенаправленное и полное изъятие «традиционных» документов на бумажном носителе осуществить достаточно сложно, поэтому следователь может лишь примерно определить состав и объем изымаемых документов. На практике достаточно часто бывают случаи, когда в ходе выемки изымается большой объем документов. Однако в дальнейшем следователь понимает, что многие документы не содержат информацию, относящуюся к событию преступления. Поэтому перед выемкой очень важно получить консультацию специалистов, компетентных в финансовых операциях, осуществляемых с помощью электронных платежных систем, а также в современных компьютерных технологиях, чтобы определить, какие документы необходимо изъять. Такая консультация позволит существенно повысить эффективность данного следственного действия, исключить выемку ненужных документов и,

в то же время, изъять документы, действительно содержащие доказательственную информацию по уголовному делу.

Существенную специфику по преступлениям рассматриваемой категории имеет выемка электронной почтовой корреспонденции.

Во-первых, такая выемка проводится исключительно на основании судебного решения, поскольку электронная почтовая корреспонденция охраняется законом как тайна связи в соответствии со ст. 63 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи». Соответственно в ходатайстве перед судом и в последующем судебном решении должно быть указано, у какой почтовой службы производится выемка; данные из каких ящиков электронной почты подлежат выемке; какая именно электронная корреспонденция подлежит выемке («входящие», «исходящие», иные электронные письма).

Во-вторых, в ходе выемки изымаются файлы, не содержащие в явном виде тексты писем и вложения к ним. Поэтому результатом выемки является лишь носитель информации с записанными на нем базами электронной корреспонденции.

В-третьих, выемке электронной корреспонденции всегда сопутствует последующий осмотр предметов (документов) с участием специалиста, в ходе которого проводятся необходимые программные преобразования баз электронной корреспонденции, имеющихся на носителе информации, представленном по результатам выемки. Результатом таких преобразований является преобразование электронных писем и вложений в формат баз почтовой программы, что позволяет осмотреть непосредственно содержимое писем и вложений, задокументировать (распечатать) такое содержимое на бумажном носителе в виде, понятном всем участникам судопроизводства.

В отличие от электронной почтовой корреспонденции, титульные знаки электронной платежной системы, по мнению А.Н. Яковлева и Н.В. Олиндер, не имеют статуса охраняемой законом компьютерной информации, поэтому при необходимости выемок в организации - электронной платежной системе, отсутствует необходимость получения судебного решения на ее производство: она осуществляется по правилам выемки документов, не содержащих охраняемую законом тайну.

Отметим, что на практике встречаются случаи, когда выемка подменяется истребованием необходимых документов, что может привести к тому, что заинтересованные лица получат возможность скрыть или частично уничтожить искомые документы, либо заменить их другими. Поэтому подмена выемки истребованием документов крайне нежелательна.

Если при производстве выемки в известном следователю месте необходимых документов не оказалось, то действия по их обнаружению в других местах на основании того же постановления будут незаконными, а собранные таким образом доказательства недопустимыми. В этом случае необходимо немедленно вынести постановление о производстве обыска и произвести его для обнаружения скрываемых документов, причем выемка не будет являться частью обыска, а будет представлять собой самостоятельное следственное действие, по результатам которого составляется отдельный протокол, в котором подробно отражаются ее ход и результаты.

При проведении выемки и обысков по делам рассматриваемой категории существенные сложности возникают при изъятии компьютерных устройств в

кредитной или иной организации. Поэтому при подготовке к проведению выемки и обыска, в ходе которых следователь намерен изъять компьютерное устройство, необходимо предварительно установить помещение, в котором находится нужный компьютер, а также получить сведения о его подключении к локальной сети или сети Интернет. Если компьютер находится во включенном состоянии, то следует учитывать возможность срабатывания аппаратных или программных средств уничтожения информации на его носителях, поэтому все действия по корректному выключению средств компьютерного устройства должен осуществлять специалист, участвующий в следственном действии. Считаем устаревшими и не соответствующими современному уровню компьютерных технологий встречавшиеся нам рекомендации по отключению электроэнергии в помещениях организации, поскольку сегодня источниками аварийного питания оснащены практически все компьютеры, что позволяет подозреваемому гарантированно уничтожить компрометирующую его информацию на носителе компьютера. Вместе с тем считаем целесообразным принудительный, предваряющий следственное действие, разрыв сетевых соединений с компьютером, подлежащим выемке, так как в этом случае подозреваемый будет лишен связи с соучастниками посредством программ обмена сообщениями, а также возможности использования своего компьютера для удаления файлов в некотором их хранилище в сети.

При планировании выемки электронных носителей информации следует учитывать, что не допускается назначение выемки неопределенных предметов, т. е. нельзя вынести постановление о выемке «электронных носителей информации» без их конкретизации. Кроме того, недопустимо выносить постановление о выемке «файлов»: так как это понятие не является предметом с точки зрения закона. Для изъятия компьютерной информации в ходе выемки следователь должен вынести постановление о выемке конкретных электронных носителей информации или компьютерных устройств.

Как известно при производстве обыска или выемки электронные носители информации изымаются с участием специалиста (ч. 9.1 ст. 182, ч. 3.1 ст. 183 УПК РФ). В качестве специалиста в данном случае может приглашаться любое лицо, обладающее знаниями в области компьютерных технологий.

Изъятые в ходе следственного действия (обыск или выемка) мобильные устройства, планшетные компьютеры, навигаторы и иные носители электронной информации (следов) упаковываются и опечатываются таким образом, чтобы обеспечить сохранность имеющейся в цифровой памяти информации. Для этого, в зависимости от размеров компьютерного устройства, на практике применяются разные способы упаковки и опечатывания, в том числе: помещение устройства в пластиковый пакет, горловина которого перевязывается крепкой нитью, концы которой опечатываются бумажной биркой; перемежение устройства в коробку или ящик, позволяющий обеспечить физическую целостность носителей; все порты, слоты, входы и выходы устройства опечатываются и другие. При применении перечисленных или иных способов упаковки опечатывание сопровождается проставлением удостоверительных подписей следователя, специалиста и понятых, а также лица, у которого изымается компьютерное устройство (его представитель).

Между тем следует отметить, что в связи с современными возможностями удаленного доступа к памяти компьютерных устройств (прежде всего мобильных устройств) и находящихся в них электронных накопителей с целью удаления собственниками устройств через операторов связи информации, рекомендуется сразу же при обнаружении такого устройства помещать его в специальный чехол (например, «Мешок Фарадея», поставляемый в комплекте с универсальным устройством извлечения судебной информации UFED - Universal Forensic Extraction Device).

В протоколе обыска (выемки) должно быть указано, в каком месте и при каких обстоятельствах были обнаружены компьютерные устройства, выданы они добровольно или изъяты принудительно. Все изымаемые устройства должны быть перечислены с точным указанием их количества, индивидуальных признаков, в том числе модели, серийных номеров, а в необходимых случаях стоимости. Если в ходе обыска были предприняты попытки уничтожить или спрятать мобильные устройства (стереть информацию, хранящуюся в их памяти), то об этом в протоколе делается соответствующая запись, и указываются принятые меры. Также соответствующая запись делается в случаях, если по ходатайству законного владельца изымаемых электронных носителей информации с разрешения следователя осуществляется копирование информации.

Допрос (обвиняемого, подозреваемого, потерпевшего, свидетеля, эксперта, специалиста)

Допрос при расследовании хищений предполагает участие специалиста или в качестве консультанта (перед началом следственного действия) либо в качестве его непосредственного участника, что предопределяется следующими факторами:

подготовка следователя к допросу включает подготовку опросного листа;

допрос обвиняемого, подозреваемого, потерпевшего, свидетеля сопровождается употреблением этими лицами большого количества жаргонизмов;

наличествуют специфичные в техническом аспекте способы хищения, элементы которых с большой вероятностью могут обсуждаться в ходе допроса.

По делам рассматриваемой категории допрос специалиста, эксперта имеет следующие особенности.

Допрос специалиста может производиться для разъяснения следователю вопросов, связанных с техническими, организационными, правовыми аспектами компьютерных технологий, используемых при совершении хищения; особенностей функционирования локальной сети; особенностей подключения к сети Интернет; иных вопросов. Особенность таких допросов в том, что специалист не только дает пояснения следователю по поставленным вопросам, но и выполняет как бы «перевод» сказанного иными участниками судопроизводства (обвиняемым, подозреваемым, потерпевшим, свидетелем) с технического, насыщенного жаргоном языка этих лиц на язык, понятный другим участникам судопроизводства (адвокату, прокурору, судье и т. д.).

Допрос эксперта производится, как правило, для разъяснения данного им заключения. В этом случае также функция допроса заключается не только в

раскрытии существенных деталей, не отраженных в выводах эксперта или исследовательской части экспертного заключения, но и «переводе» написанного техническим языком на язык, понятный всем участникам судопроизводства.

Одним из тактических приемов, используемых при расследовании многоэпизодных хищений, совершенных групповым способом, является досудебное соглашение.

Как следует из закрепленного законодателем в п. 61 ст. 5 УПК РФ определения, «досудебное соглашение о сотрудничестве - это соглашение между сторонами обвинения и защиты, в котором указанные стороны согласовывают условия ответственности подозреваемого или обвиняемого в зависимости от его действий после возбуждения уголовного дела или предъявления обвинения».

Данное процессуальное действие как тактический прием применяется следователем, чтобы получить развернутые показания от одного из соучастников преступной группы, который тем самым содействует в раскрытии и расследовании хищений, изобличении и уголовном преследовании других соучастников преступления, розыске похищенных денежных средств.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами

В соответствии со ст. 186.1 УПК РФ информация о соединениях между абонентами и (или) абонентскими устройствами может быть получена следователем на основании судебного решения, если имеются достаточные основания полагать, что такая информация имеет значение для уголовного дела.

Под категорию «информация о соединениях между абонентами и (или) абонентскими устройствами» применительно к рассматриваемой категории преступлений подпадает:

информация о соединениях между абонентскими устройствами, в качестве которых выступает сетевое оборудование потерпевшего, преступника, иных лиц; провайдера сети Интернет; организации - платежной системы; к такой информации необходимо отнести IP-адреса, интервалы подключений к сети Интернет, иную информацию о сетевых соединениях;

информация о соединениях между абонентскими устройствами, в качестве которых выступают устройства и оборудование мобильной связи -мобильный телефон преступника, иных лиц; оборудование мобильной связи оператора связи; к такой информации необходимо отнести номера IMEI, IMSI, идентифицирующие устройство мобильной связи и сим-карту соответственно; собственно абонентские номера преступника, иных лиц; интервалы связи, иную информацию о сетевых соединениях.

Необходимо отметить, что сами по себе элементы категории «информация о соединениях между абонентами и (или) абонентскими устройствами» не являются охраняемой законом информацией, если получены порознь из других источников. Только полученные провайдером или оператором мобильной связи в ходе оказания услуг, такие данные охраняются законом.

В ст. 186.1 УПК РФ перечислены требования к ходатайству следователя о производстве этого следственного действия. В ходатайстве необходимо указать уголовное дело, при производстве которого необходимо выполнить данное следственное действие; основания, по которым производится данное следственное действие; период, за который необходимо получить соответствующую информацию и (или) срок производства данного следственного действия; наименование организации, от которой необходимо получить указанную информацию.

Уточним, что с учетом потенциально длительной подготовки к преступлению следователь может указать началом периода, за который необходимо получить соответствующую информацию, дату, задолго предшествующую дате совершения преступления. Однако выбор такого интервала должен быть обоснован в ходатайстве следователя и признан судом.

Также важно при составлении ходатайства обращать внимание на правильное наименование организации, от которой необходимо получить запрашиваемую информацию. Многие интернет провайдеры и операторы мобильной связи широко используют в рекламе своих услуг эквивалент названия организации, не фигурирующий в уставных документах организации. При указании такого эквивалента следователем в ходатайстве, суд согласится с доводами следователя и вынесет решение о предоставлении следователю информации о соединениях между абонентами и (или) абонентскими устройствами. В результате этого судебное решение не будет содержать полное или краткое название организации, имеющееся в ее учредительных документах, а последующее исполнение судебного решения может повлечь за собой признание полученных доказательств недопустимыми.

В случае получения копии судебного решения о получении информации о соединениях между абонентами и (или) абонентскими устройствами, руководитель организации - интернет-провайдера или оператора мобильной связи формирует массив данных, содержащий запрашиваемую информацию, распечатывает его на бумажном носителе или записывает на компакт-диск, после чего упаковывает и опечатывает такой носитель, готовит сопроводительное письмо. В сопроводительном письме указывается период, за который предоставлена информация, и номера абонентов и (или) абонентских устройств.

Применительно к расследованию преступлений рассматриваемой категории необходимо иметь в виду, что ч. 4 ст. 186.1 УПК допускает получение следователем информации о соединениях между абонентами и (или) абонентскими устройствами в течение шести месяцев. Такая информация предоставляется интернет провайдером или оператором мобильной связи по мере ее поступления, но не реже одного раза в неделю.

При описании особенностей выемки электронной почтовой корреспонденции было указано, что такой выемке сопутствует последующий осмотр электронной корреспонденции. Аналогичный подход применил законодатель в отношении информации о соединениях между абонентами и (или) абонентскими устройствами: при получении запрашиваемой информации следователь осматривает представленные ему документы с участием понятых и (при необходимости) специалиста, о чем составляет протокол. В протоколе отражается не вся представленная следователю информация, а только та, которая имеет отношение к уголовному делу

К материалам уголовного дела приобщается как полностью документ, представленный следователю интернет провайдером или оператором мобильной связи, так и протокол осмотра этого документа. 6. Назначение экспертизы.

При расследовании хищений денежных средств, совершенных с использованием компьютерных технологий, проводятся разные виды судебных экспертиз (напр., трасологическая, дактилоскопическая, почерковедческая, товароведческая и др.). Однако стоит отметить, что практически по всем уголовным делам вышеуказанной категории назначаются и проводятся следующие судебные компьютерно - технические экспертизы (далее, если не указано иное, судебно-компьютерные экспертизы или СКЭ):

аппаратно-компьютерная экспертиза - назначается для исследования непосредственно компьютерных устройств (персональные компьютеры, моноблоки, ноутбуки, нетбуки, планшеты, мобильные телефоны, сканеры, принтеры и др.);

программно-компьютерная экспертиза - назначается для исследования программного обеспечения (функционального предназначения и характеристик реализуемого алгоритма, структурных особенностей и текущего состояния системного и прикладного программного обеспечения компьютерной системы);

информационно-компьютерная экспертиза - назначается для исследования документации, изготовленной с помощью компьютерных устройств, информации в мультимедийных форматах, информации в базах данных и других приложениях, имеющих прикладной характер и т. п.;

компьютерно-сетевая экспертиза - назначается для исследования физического и функционального состояния компьютерных устройств, которыми обеспечены сетевые и телекоммуникационные технологии.

Следует отметить, что в следственной практике назначаются СКЭ для разрешения соответствующих задач без указаний на их виды.

Принимая во внимание, что назначение, производство и использование результатов СКЭ и других видов судебных экспертиз происходит в рамках взаимодействия следователя (начальника ОПС) с экспертом (экспертными учреждениями), особенности организации которого рассматриваются в отдельном разделе настоящей работы, ограничимся рассмотрением перечней вопросов, которые могут быть поставлены на разрешение СКЭ.

Исследователями предлагаются следующие типичные вопросы при назначении СКЭ:

к какому типу (марке, модели) относится аппаратное средство? Каковы его технические характеристики?

каково функциональное предназначение представленного аппаратного средства?

возможно ли использование данного аппаратного средства для решения конкретной задачи?

каково фактическое состояние (исправен, неисправен) представленного аппаратного средства?

является ли неисправность данного средства следствием нарушения правил эксплуатации?

является ли представленное аппаратное средство носителем информации?

какой вид (тип, модель, марку) имеет представленный носитель информации?

какое устройство предназначено для работы с данным носителем информации? Имеется ли в составе представленной компьютерной системы устройство, предназначенное для работы (чтение, запись) с данным носителем информации?

какие параметры имеет носитель информации?

какова общая характеристика представленного программного обеспечения?

к какому виду (общесистемное, прикладное и т. д.) относится представленное программное обеспечение?

каковы реквизиты разработчика, правообладателя представленного программного средства?

каков состав и параметры файлов представленного программного обеспечения?

какое функциональное предназначение имеет программное обеспечение?

имеется ли на электронных носителях информации программное обеспечение для решения конкретной задачи?

какие системы защиты применялись в представленной на экспертизу системе?

имеются ли на представленных компьютерных носителях информации какие-либо средства для осуществления несанкционированного доступа и средства разграничения прав пользователей?

когда и каким образом осуществлялся несанкционированный (и санкционированный) доступ к информации?

имеется ли в представленных на экспертизу программных средствах возможность фальсифицировать или априорно задавать результат работы программы?

каков алгоритм работы представленного программного средства? подвергалось ли представленное программное средство модификации? В чем это нашло отражение?

имеются ли на представленных образцах с программным обеспечением программы, фрагменты программ, программного обеспечения, свидетельствующие о копировании (полном или частичном) с представленных легитимных образцов?

имеется ли в составе представленного программного обеспечения функции, предназначенные для несанкционированной модификации, уничтожения и распространения информации, нарушения работы аппаратных и программных средств?

какие свойства, характеристики и параметры имеют данные на носителе информации?

к какому типу относятся выявленные данные (текстовые документы, графические файлы и т. д.) и с помощью каких программных средств они могут обрабатываться?

каково содержание обнаруженной информации? какие данные на носителе информации имеют отношение к фактам и обстоятельствам конкретного дела или лица (в том числе и юридического)?

какие данные с представленных на экспертизу образцов и в каком виде находятся на носителе информации?

Перечисленные типичные вопросы конкретизируются с учетом конкретных объектов исследований и складывающейся следственной ситуации. Например, при исследовании мобильных устройств на разрешение эксперту или специалисту могут быть поставлены типовые вопросы общего диагностического характера о наличии в устройстве (включая внешние карты памяти и сим-карты) каких либо файлов (текстовых, графических, музыкальных, видео-, фотофайлов, СМС-сообщений и др.), и эксперт извлекает весь физический дамп памяти. Если же следователя интересует какая-либо конкретная информация, то задаются соответствующие вопросы с указанием временного интервала удаления файлов.

В связи с наличием замечаний по вопросам, выносимым на исследование, необходимо обратить внимание на предлагаемые ЭКЦ МВД России следующие рекомендации:

использовать корректную терминологию (устоявшийся понятийно-категориальный аппарат), исключающий жаргонные или непрофессиональные понятия («проги», «винт», «логи», «взлом», «комп», «банить», «юзать», «коннектить» и т. п.), а так же не использовать всевозможные сокращения. При возникновении затруднений при определении, даче описательной характеристики того или иного объекта (продукта), необходимо использовать ту терминологию, которую используют разработчики конкретного устройства (или иного объекта) в прилагающейся к нему документации (руководство по эксплуатации, справки, памятки и др.);

вопросы не должны касаться этапов исследования, носить справочный характер, выходить за пределы компетенции эксперта;

вопросы должны ставиться конкретно и точно, соответствовать существующей в ЭКП или ином экспертном учреждении методической и технической базе, уровню подготовки его сотрудников (экспертов), быть направлены на установление конкретных обстоятельств расследуемого преступления, а также соответствовать представляемым на исследование объектам;

вопросы должны быть поставлены таким образом, чтобы финансовые, технические и временные затраты на производство экспертизы (исследования) были минимальными или целесообразными.

Представляется важным указать на особенности назначения судебных экспертиз в негосударственные экспертные учреждения, так как их производство в государственных судебно-экспертных учреждениях характеризуется повышенным вниманием к качеству экспертиз, контролем

такого качества; оснащением экспертного подразделения оборудованием; характеризуется разработкой, обменом, использованием новых экспертных методик. В государственных судебно-экспертных учреждениях обеспечен единый научно-методический подход к производству судебных экспертиз: примерно схожи виды выполняемых экспертиз и перечни экспертных специальностей, по которым предоставляется право самостоятельного производства судебных экспертиз. На государственные судебно-экспертные учреждения возложены также научно-методическое обеспечение производства судебных экспертиз, профессиональная подготовка и повышение квалификации экспертов.

К сожалению, анализ практики производства судебных экспертиз в негосударственных экспертных учреждениях показывает невысокое качество выполнения таких экспертиз, что ставит под обоснованное сомнение в суде выводы эксперта. Это заставляет следователя предпринимать при назначении экспертизы в негосударственное экспертное учреждение дополнительные меры по обеспечению качества ее производства. Представляется, что такие меры наиболее полно представлены в постановлении Пленума Верховного Суда РФ от 21 декабря 2010г. №28. Среди них:

запрос сведений, касающихся возможности производства данной экспертизы, а также сведений об эксперте (фамилия, имя, отчество, образование, специальность, стаж работы в качестве судебного эксперта и иные данные, свидетельствующие о его компетентности и надлежащей квалификации);

приобщение к материалам уголовного дела заверенных копий документов, подтверждающих указанные сведения (трудовая книжка, диплом об образовании, приказ о назначении на должность и т. п.);

требование о том, чтобы вопросы, поставленные перед экспертом, и заключение по ним не выходили за пределы его специальных знаний;

требование иметь в распоряжении необходимое экспертное оборудование, если производство экспертизы поручено сотруднику научно-исследовательского учреждения, вуза, иной организации.

При назначении и использовании результатов СКЭ или иного соответствующего предварительного исследования, следователю необходимо иметь общие представления о порядке проведения экспертных исследований, в том числе порядке фиксации их хода и результатов.

Для исследования компьютерных устройств или компьютерной информации экспертом, имеющим соответствующую квалификацию, применяется специальная криминалистическая техника. Например, для извлечения и декодирования значимой для уголовного дела компьютерной информации из мобильных устройств эксперт может применить аппаратно-программные комплексы (напр., UFED и др.). Извлеченные на отдельный компьютер или флэш-карту данные анализируются с помощью специальной программы (напр., UFED Physical Analyzer), которая позволяет создать подробный структурированный отчет с интересующей следствие информацией.

В целях подтверждения получения искомой информации именно с данного мобильного устройства эксперту (специалисту) рекомендуется фиксировать всю процедуру получения информации с помощью видео- или фотосъемки, а видеосъемку или фототаблицу прилагать к заключению эксперта (специалиста).

В последующем полученный и распечатанный отчет об извлеченной из мобильного устройства информации приобщается к материалам Уголовного дела в полном объеме. Компьютерное устройство на основании постановления следователя также приобщается к материалам уголовного дела как вещественное доказательство, хранится в опечатанном виде.

Наложение ареста на имущество

Наложение ареста на имущество в качестве обеспечительной меры исполнения приговора в части гражданского иска при расследовании хищений имеет особенности, связанные с электронными денежными средствами, числящимися на счетах, открытых преступниками на себя или иных лиц в электронных платежных системах («Яндекс. Деньги», «WebMoney» и т. п.).

Электронные денежные средства - денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа. Федеральный Закон от 27.06.2011 № 161-ФЗ (ред. от 05.05.2014) «О национальной платежной системе» // Собрание законодательства РФ. 2011. № 27. Ст. 3872.

Для наложения ареста на электронные денежные средства необходимо, чтобы платежная система была зарегистрирована в России или имелось официальное представительство. В противном случае возможности следователя ограничены. (Например, платежная система «E-gold» создана в 1996 г. и зарегистрирована в США).

Источниками информации о наличии у обвиняемого или подозреваемого электронных денежных средств являются: письменный договор, заключенный с электронной платежной системой; сведения в официальных представительствах электронной платежной системы; информация на электронных носителях информации.

В случае заключения письменного договора с электронной платежной системой, если при производстве обыска или выемки он не найден, необходимо изъять электронный носитель информации для проведения судебно-компьютерной экспертизы, что позволит получить дополнительную информацию о наличии или отсутствии установленного программного обеспечения для доступа к «электронному» кошельку платежных систем и соответствующих номеров. Одновременно с проведением судебно-компьютерной экспертизы направляются запросы в официальные представительства электронных платежных систем на предмет владения обвиняемым, подозреваемым «электронным» кошельком, зарегистрированным на его имя (и может не одним), с указанием о приостановлении операции по нему. В этой ситуации следует учитывать фактор ликвидности электронных денежных средств, а потому необходимо наладить сотрудничество с подразделениями службы безопасности платежной системы.

Сведения об IP-адресе компьютера можно затребовать по официальному запросу, если известна информация о номере «электронного» кошелька или владельца. При получении сведений об IP-адресах, в которых осуществляется доступ к кошельку по запросу к провайдеру (поставщику интернет-услуг, например ОАО «Ростелеком», «Вымпелком» и др.) можно определить владельца IP-адреса, то есть лицо, которое непосредственно имело доступ к электронному кошельку.

При получении данных сведений может быть наложен арест на денежные средства, числящиеся в электронном кошельке.

Вместо заключения

Прогнозируются следующие тенденции в сфере хищений денежных средств с использованием компьютерных технологий:

1) количество использования преступниками вредоносных программ (троянские программ) для хищения с банковских счетов путем модификации информации (подделка электронных платежных документов), находящейся на персональных компьютерах, будет уменьшаться;

2) количество использования преступниками вредоносных программ (троянские программ) для хищения с банковских счетов путем копирования информации (данных банковских карт, логинов и паролей для Интернет-банкинга), находящейся в мобильных устройствах (прежде всего в сотовых аппаратах) на платформе Android, будет увеличиваться;

3) количество использования преступниками вредоносных программ (троянские программ) для хищения с банковских счетов путем модификации, копирования и уничтожения информации (подделка электронных платежных документов), находящейся в банковской системе (банковских компьютерах), будет увеличиваться;

4) количество использования преступниками вредоносных программ (троянские программ) для хищения денежных средств путем модификации и копирования информации платежных карт в POS-терминалах и банкоматах (часть таких программ находится в открытом доступе сети Интернет) будет увеличиваться;

5) количество использования преступниками специальных технических средств (скимминг и т. п.) для хищения денежных средств путем копирования информации платежных карт в POS-терминалах и банкоматах будет уменьшаться.

При этом способы хищения денежных средств с использованием компьютерных технологий будут сопряжены с фишингом, развитием виртуальных организованных преступных групп (преступных сообществ) и автоматизацией процесса совершения таких преступлений.

В то же время эффективность использования вредоносных программ, позволяющих осуществлять операции по переводу денежных средств с банковских счетов посредством подмены реквизитов («автозалива»), для юридических лиц будет снижена за счет внедрения новых систем защиты крупными коммерческими банками.

С учетом обозначенных тенденций в сфере хищений денежных средств с использованием компьютерных технологий необходимо принимать управленческие меры, в том числе направленные на решение задач повышения результативности, качества и сокращения сроков предварительного следствия, соблюдение законности, возмещение причиненного ущерба и профилактику данных преступлений. Обобщение практики управленческой деятельности позволяет выделить следующие меры, принимаемые руководителями ОПС для решения обозначенных задач:

1) обеспечение своевременного ознакомления с поступающими из МВД России и Следственного департамента МВД России распорядительных и иных документов, их систематизация, подготовка на их основе локальных актов, направление их, а в необходимых случаях и распорядительных или иных документов МВД России (Следственного департамента МВД России) в подчиненные ОПС, обеспечение ознакомления с ними уполномоченных сотрудников;

2) обеспечение исполнения следователями в рамках своей компетенции действующего законодательства, распорядительных и иных документов МВД России (СД МВД России) в сфере противодействия хищениям денежных средств, совершаемых с использованием компьютерных технологий;

3) обеспечение постоянного процессуального контроля руководителей ОПС за возбуждением и расследованием уголовных дел о хищениях денежных средств, совершаемых с использованием компьютерных технологий;

4) закрепление за линией расследования преступлений, совершаемых с использованием компьютерных технологий, профессионально подготовленных следователей (установление специализации);

5) создание в структуре следственных частей ОПС на региональном уровне специализированных подразделений по расследованию преступлений, совершаемых с использованием компьютерных технологий;

6) закрепление за линией обеспечения расследования преступлений, совершаемых с использованием компьютерных технологий, сотрудника аппарата управления ОПС (например, сотрудника контрольно-методического подразделения ОПС);

7) проведение оперативных совещаний по результатам организации расследования хищений, совершенных с использованием компьютерных технологий, а при необходимости инициирование проведения оперативных совещаний при начальниках территориальных органов МВД России; проведение оперативных совещаний (рабочих встреч) с представителями банковской и платежной системы, операторов сотовой связи и провайдеров с приглашением представителей СМИ, в ходе которых рассматривать проблемы взаимодействия (представления сведений, видеозаписей и т. п.) и профилактики хищений денежных средств, совершаемых с использованием компьютерных технологий;

8) обеспечение незамедлительного поступления в аппарат управления ОПС информации о возбуждении уголовных дел о хищениях денежных средств, совершаемых с использованием компьютерных технологий, для обобщения, анализа и использования в организации расследования данной категории преступлений. С этой целью целесообразно: разрабатывать и принимать нормативные документы, регламентирующие сбор, систематизацию и

использование информации о преступлениях, совершаемых с использованием компьютерных технологий; разрабатывать электронные таблицы, которые позволяли бы систематизировать и анализировать полученную по всем уголовным делам информацию в части совпадений абонентских номеров, IMEY абонентских устройств, лицевых счетов и номеров банковских карт, IP - адресов, используемых преступниками;

9) обеспечение разработки информационно-аналитических (бюллетени, обзоры, экспресс-информации, письма, сборники нормативно-правовых актов и т. п.) и методических документов (учебные (учебно-практические) пособия, методические рекомендации, макеты уголовных дел и т. п.) по расследованию хищений денежных средств, совершаемых с использованием компьютерных технологий, на основе существующих научных и дидактических материалов, а также региональных особенностей досудебного производства по делам о данной категории преступлений;

10) организация проведения учебных форумов (конференции, семинары, занятия в рамках профессиональной подготовки и т. п.), в том числе в режиме видеоконференции и (или) с участием ученых и специалистов, для следователей, дознавателей, оперуполномоченных, сотрудников экспертно-криминалистических подразделений;

11) обеспечение исполнения качественно и в установленные сроки поручений следователей по делам о хищениях денежных средств, совершаемых с использованием компьютерных технологий, органам дознания или следователям других органов внутренних дел;

12) обеспечение подготовки и направления обобщающих представлений в кредитные организации, платежные системы, провайдерам, операторам сотовой связи с целью профилактики хищений денежных средств, совершаемых с использованием компьютерных технологий. Другим направлением профилактики хищений денежных средств, совершаемых с использованием компьютерных технологий, является привлечение в ходе расследования уголовных дел лиц к административной ответственности по ст. 13.29 КоАП (за заключение от имени оператора связи договора об оказании услуг подвижной радиотелефонной связи лицом, не имеющим полномочий от оператора связи на заключение договора об оказании услуг подвижной радиотелефонной связи), ст. 13.30 КоАП (за невыполнение лицом, действующим от имени оператора связи, требований о включении в договор об оказании услуг подвижной радиотелефонной связи установленных правилами оказания услуг связи сведений об абоненте или включение недостоверных сведений, либо непредставление (несвоевременное) представление оператору связи экземпляра заключенного с абонентом договора, если указанные действия не содержат уголовно-наказуемого деяния), ст. 17.7 КоАП.

Также руководители ОПС с целью обеспечения решения подчиненными сотрудниками задач досудебного производства по делам о хищениях денежных средств, совершаемых с использованием компьютерных технологий, в рамках своих полномочий инициируют:

1) создание в территориальных органах МВД России на региональном уровне специализированных групп, в том числе с участием представителей ОПС, с целью постоянного мониторинга деятельности органов внутренних дел в сфере выявления, раскрытия и расследования преступлений, совершаемых с

использованием компьютерных технологий, разработки организационно-управленческих мер, направленных на повышение эффективности данной деятельности;

2) проведение и (или) принятие участия в координационных совещаниях при прокуроре региона (района). Так, 31 августа 2015 г. руководство СУ УМВД России по Оренбургской области приняло участие в координационном совещании при прокуратуре Оренбургской области, на котором рассмотрено состояние работы и уровень взаимодействия правоохранительных органов по противодействию новым видам мошенничеств, совершенных с использованием средств сотовой связи и в сфере дистанционного банковского обслуживания, по результатам которого выработаны меры по совершенствованию работы по данному направлению;

3) проведение рабочих встреч с прокурорами для обсуждения проблемных вопросов досудебного производства по делам о хищениях денежных средств, совершаемых с использованием компьютерных технологий;

4) своевременное исполнение требований (запросов) следователей о предоставлении сведений и документов кредитными организациями, провайдерами, операторами сотовой связи, или изъятия документов, в том числе путем проведения в данных организациях выемки;

5) создание в территориальных органах МВД России, специализированных следственно - оперативных групп, в состав которых должны входить следователи, сотрудники аппарата управления ОПС и оперативных подразделений территориальных органов МВД России на региональном или межрегиональном уровне;

6) разработку управленческих (распорядительных) документов, регламентирующих действия начальников территориальных органов МВД России на районном уровне при поступлении сообщений о хищениях, совершенных с использованием компьютерных технологий, обязательные процессуальные действия, осуществляемые сотрудниками органа дознания на стадии возбуждения уголовного дела, а также направление следователем запроса в сотовые компании на установление IMEI - кода в течение первых трех суток расследования уголовного дела, с образцами типовых вопросов для составления таких запросов;

7) подготовку плана по профилактике и раскрытию хищений денежных средств, совершаемых с использованием компьютерных технологий, которым предусматриваются мероприятия по организации взаимодействия с органами внутренних дел других регионов Российской Федерации, кредитными организациями, операторами сотовой связи;

8) приобретение и внедрение территориальными органами МВД России программно-аппаратного комплекса, позволяющего получать информацию сотрудниками органов внутренних дел из соответствующих подразделений Сбербанка России по защищенным каналам связи;

9) обеспечение создания автоматизированной информационной системы, обеспечивающей ведение учета преступлений, совершаемых с использованием компьютерных технологий.

Авторский коллектив настоящей работы полагает, что разработанные рекомендации общие положения организации расследования хищений

денежных средств, совершаемых с использованием компьютерных технологий, составят основу для разрабатываемых ОПС методических документов в условиях современного состояния организационно-управленческих и правовых средств обеспечения досудебного производства по делам о преступлениях в сфере высоких технологий.