МВД России

Федеральное государственное казенное учреждение
дополнительного профессионального образования
«Всероссийский институт повышения квалификации сотрудников
Министерства внутренних дел Российской Федерации»

СФЕРА ТЕЛЕКОММУНИКАЦИЙ И КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК ПЛАТФОРМА ДЛЯ СОВЕРШЕНИЯ СОВРЕМЕННЫХ ВИДОВ ПРЕСТУПЛЕНИЙ

Учебно-практическое пособие

Под общей редакцией начальника БСТМ МВД России
генерал-лейтенанта М.Ю. Литвинова

Домодедово
ВИПК МВД России
2022

ББК 67.408.135
С 91

Авторский коллектив:

В.И. Алескеров, ***кандидат юридических наук, доцент,***
О.Н. Колокольчикова, Л.В. Василенко, С.Н. Ломакин

Рецензенты: **В.В. Аверин –** начальник БСТМ по Республике Татарстан полковник полиции;
А.И. Антонов – заместитель начальника БСТМ ГУ МВД России по Краснодарскому краю полковник полиции;
М.В. Герасимов – заместитель начальника БСТМ – начальник отдела (4 отдел) УМВД России по Владимирской области подполковник полиции;
А.Ю. Коновалов – заместитель начальника БСТМ УМВД России по Забайкальскому краю полковник полиции;
С.Л. Шелудько – заместитель начальника БСТМ ГУ МВД России по Новосибирской области – начальник отдела «К» полковник полиции;
В.С. Коваль – заместитель начальника БСТМ – начальник отдела «К» УМВД России по Омской области полковник полиции;
О.Н. Гарибов – заместитель начальника БСТМ ГУ МВД России по Ставропольскому краю полковник полиции.

С 91 **Сфера телекоммуникаций и компьютерной информации как платформа для совершения современных видов преступлений** : учебно-практическое пособие / В.И. Алескеров, О.Н. Колокольчикова, Л.В. Василенко, С.Н. Ломакин; под общей редакцией М.Ю. Литвинова. – Домодедово: ВИПК МВД России, 2022. – 360 с.

ISBN 978-5-9552-0775-9

В учебно-практическом пособии раскрывается уголовно-правовая и криминалистическая характеристика преступлений, совершаемых в сфере телекоммуникаций и компьютерной информации, рассматриваются проблемные вопросы раскрытия преступлений данной направленности, особое внимание уделено раскрытию преступлений в системе дистанционного банковского обслуживания. Представлен обзор преступлений, совершаемых с использованием компьютерных технологий.

Учебно-практическое пособие охватывает все основные вопросы как теоретического, так и практического характера, знание которых необходимо для эффективного использования в ходе раскрытия и расследования преступлений данной направленности. В пособии отражены актуальные вопросы практической деятельности сотрудников оперативных подразделений органов внутренних дел. Включены лабораторные работы для усвоения представленного материала путем отработки практических навыков слушателей, студентов и других категорий учащихся в зависимости от направления их обучения. Материал учебно-практического пособия позволит преумножить и систематизировать сведения, полученные во время аудиторных занятий.

Пособие предназначено для руководителей и сотрудников подразделений специальных технических мероприятий и других оперативных подразделений органов внутренних дел Российской Федерации. Может быть адресовано курсантам, адъюнктам, профессорско-преподавательскому составу высших учебных заведений юридического профиля системы МВД России.

ISBN 978-5-9552-0775-9

ГЛОССАРИЙ

Автоматизированное рабочее место клиента Банка России (АРМ КБР) – программа, необходимая любому банку, действующему на территории Российской Федерации, для предоставления финансовой отчетности в Банк России за определенный период времени.

Анонимизация – совокупность действий, направленных на сокрытие личности пользователя путем маскировки или подмены характеристик пользователя и его устройств.

Анонимизированная личность – замаскированная виртуальная сущность, используемая для создания анонимности.

Банк-эквайер – уполномоченный банк (член платежной системы), осуществляющий первичную обработку транзакций и берущий на себя обязательства, которые находятся в его сфере деятельности, всего спектра операций с банковскими картами.

Банк-эмитент – кредитная организация, участник платежной системы, осуществляет выпуск и обслуживание банковских карт. Выступает гарантом выполнения финансовых обязательств, возникающих в ходе использования карт держателями.

Банковские трояны (Trojan-Banker) – вредоносные программы, предназначенные для кражи учетных данных систем интернет-банкинга, систем электронных платежей и кредитных или дебетовых карт.

Биллинг – информация, полученная по техническому каналу связи, включающая в себя периоды времени соединения технических устройств, в том числе и средств информационного обмена, предоставленной услуги осуществления обмена и передачи информации (вне зависимости от ее вида), а также определения места передачи до пункта ее получения.

Процесс (получение) биллинга – определение (установление) по техническому каналу связи периода времени соединения технических устройств, в том числе и средств информационного обмена, предоставленной услуги осуществления обмена и передачи, объема произошедшей информации (вне зависимости от ее вида), а также определения места передачи до пункта ее получения.

БИН (BIN) – первые шесть цифр номера банковской карты; расшифровывается данная аббревиатура как «банковский идентификационный номер».

Блокирование информации – действие, искусственно затрудняющее доступ пользователей к компьютерной информации, не связанное с ее уничтожением, а также создание условий (в том числе, с помощью специальных программ), исключающих использование компьютерной информации ее законным владельцем.

Ботнет (англ. botnet, произошло от слов robot и network, синоним: «зомби-сеть») – это сеть компьютеров, зараженных вредоносной программой,

позволяющей киберпреступникам удаленно управлять зараженными машинами (каждой в отдельности, частью компьютеров, входящих в сеть, или всей сетью целиком) без ведома пользователя.

Бэкдоры (англ. backdoor) – разновидность вредоносных программ, предоставляющая злоумышленникам возможность удаленного управления зараженными компьютерами. Такие программы позволяют автору выполнять на зараженном компьютере любые действия, включая отправку, получение, открытие и удаление файлов, отображение данных и перезагрузку компьютера. Трояны-бэкдоры часто используются для объединения группы компьютеров-жертв в ботнет или зомби-сеть для использования в криминальных целях.

Виртуальная личность **–** совокупность данных, характеризующих пользователя и представляющих его в Интернете: логин, фотоизображение, почтовый адрес, подпись на форуме.

Виртуальная машина **–** программа, которая эмулирует реальный (физический) компьютер со всеми его компонентами (жесткий диск, привод, сетевые адаптеры и прочее).

Виртуальный сервер **–** услуга предоставления в аренду так называемого виртуального выделенного сервера. В плане управления операционной системой по большей части она соответствует физическому выделенному серверу.

Виртуальная частная сеть (VPN) **–** обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) «поверх» другой сети (например, Интернет).

Вирус – вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Как правило, целью вируса является нарушение работы программно-аппаратных комплексов: удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей или же приведение в негодность аппаратных комплексов компьютера и т.п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют некоторые другие ресурсы системы.

Вирусописатели – лица, создающие вредоносные программы с целью превращения компьютеров пользователей в машины для рассылки спама. Пользователи при этом могут даже не догадываться, что их машины используются спамерами. Уже семнадцать лет назад – в 2004 году – основная масса спама рассылалось не напрямую с почтовых серверов, а посредством зараженных пользовательских компьютеров, объединённых в ботнеты.

Вредоносная программа – программа, объективным свойством которой являются модификация, уничтожение, копирование с последующей переда-

чей информации, блокирование информации, нарушение работы компьютера или компьютерных систем без санкции уполномоченных лиц (обладателя информации либо оператора информационной системы).

Выемка – следственное действие, направленное на добровольное либо принудительное изъятие дознавателем, следователем материальных объектов и/или документов из законного или незаконного владения у граждан, учреждений, организаций, предприятий. Выемка проводится в случае необходимости изъятия определенных предметов, имеющих значение для уголовного дела, если точно известно, где и у кого они находятся. Отличительной особенностью выемки от обыска является запрет на производство каких-либо поисковых действий.

Дамп памяти – это копия содержимого оперативной памяти, находящаяся на жёстком диске или другом энергонезависимом устройстве памяти.

Даркнет – (DarkNet), также известен как «скрытая сеть», «темная сеть», «Теневая сеть», «Темный веб» – скрытая сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов. Анонимная сеть представляет собой систему несвязанных между собой виртуальных туннелей, представляющая передачу данных в зашифрованном виде.

Деанонимизация – совокупность действий, совершаемых лицом или автоматизированной системой, направленных на раскрытие реальной личности пользователя и характеристик его устройств.

«Добросовестные спамеры» – чаще всего маркетинговые сотрудники обычных компаний, которые используют возможности рекламы электронной почты. Обычно адреса они берут с сайтов, указывают свои подлинные координаты, настоящий обратный адрес и т.д.

Домен – адрес веб-ресурса в сети Интернет.

DoS-атака (от англ. Denial of Service – «отказ в обслуживании») и DDoS-атака (Distributed Denial of Service – «распределённый отказ обслуживания») – разновидности атак злоумышленника на компьютерные системы, целью которых является создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднён.

Разница же между обычным (DoS) отказом в обслуживании и распределённым (DDoS) состоит в географии трафика: обычный DoS (трафик, приводящий к отказу) приходит с одного компьютера, распределённый – из множества. Термин «DDoS-атака» можно дословно расшифровать как «Атака, направленная на отказ обслуживания системы».

DDoS-атака – как правило, осуществляется посредством «ботнет»-сетей, состоящих из сотен, тысячей «зомби»-компьютеров, которые одновременно отсылают запросы на получение данных из атакуемого сайта. В этом случае происходит перегрузка сайта, что приводит его в нерабочее состояние, так как дамп памяти переполняется информацией, создаются благоприятные

условия для осуществления SQL-инъекции и получения расширенной конфиденциальной информации, находящейся (хранящейся) на атакуемом сервере.

DDoS-трояны – программы, предназначенные для проведения атак типа «отказ в обслуживании» (от англ. Denial of Service, DoS) по целевым веб-адресам. При такой атаке с зараженных компьютеров системе с определенным адресом отправляется большое количество запросов, что может вызвать ее перегрузку и привести к отказу в обслуживании.

Дроп – лицо, непосредственно осуществляющее обналичивание похищенных денег, снимающее денежные средства с банковской карты и других платежных систем, ранее переведенные со счета жертвы, за определенное денежное вознаграждение.

Дроповод – руководитель дропов, является администратором, отвечающим за направление денежных средств, полученных преступным путем, в адрес организатора преступления.

Залив – перевод денежных средств со счета клиента банка либо со счетов самого банка на реквизиты, заранее подготовленные злоумышленником.

Заливщик – лицо, осуществляющее непосредственное хищение денежных средств клиентов банков.

Злоумышленник (личность преступника) – лицо, обладающее совокупностью социально-психологических свойств и качеств, являющихся причинами и условиями совершения преступлений.

Игровые трояны – вредоносные программы этого типа крадут информацию об учетных записях участников сетевых игр.

IM-трояны – вредоносные программы Trojan-IM крадут логины и пароли к программам мгновенного обмена сообщениями, таких как ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype и многие другие.

IM-Worm – вредоносная программа, способная к саморазмножению в системах мгновенного обмена сообщениями, таких как Facebook Messenger, Skype или WhatsApp.

Для этих целей «черви», как правило, рассылают контактам жертвы сообщения, содержащие URL-ссылку на файл с «телом червя». Данный прием практически полностью повторяет способ рассылки, который используют «почтовые черви».

IRC-Worm – вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению через Internet Relay Chats.

У этого типа «червей» существует два способа распространения по IRC-каналам, напоминающие способы распространения «почтовых червей». Первый способ заключается в отсылке URL на копию «червя». Второй способ — отсылка зараженного файла какому-либо пользователю IRC-канала. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диск и открыть (запустить на выполнение).

Интернет **–** всемирная информационная компьютерная сеть, связывающая между собой как пользователей компьютерных сетей, так и пользователей индивидуальных компьютеров для обмена информацией.

IP-адрес (ай-пи адрес, сокращение от англ. Internet Protocol Address) – сетевой адрес узла в компьютерной сети, построенной по протоколу IP. При связи через сеть Интернет требуется глобальная уникальность адреса, в случае работы в локальной сети требуется уникальность адреса в пределах сети.

IP-телефония – голосовая связь, которая осуществляется по сетям передачи данных, в частности по IP-сетям (IP – Internet Protocol). На сегодняшний день IP-телефония все больше вытесняет традиционные телефонные сети за счет легкости развертывания, низкой стоимости звонка, простоты конфигурирования, высокого качества связи и сравнительной безопасности соединения.

IP-телефония – это общий термин, обозначающий передачу голоса и факса, а также связанные с этим сервисы, частично или полностью через пакетные сети на основе протокола IP (Internet Protocol – протокол межсетевого взаимодействия).

Термин IP-телефония эквивалентен термину VoIP (Voice over IP). Internet-телефония – более узкое понятие, когда в роли транспортной среды выступает сеть Internet.

Кардинг (англ. carding) – род мошенничества (самый вредоносный вид хакерства), при котором производится операция с использованием банковской карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Реквизиты платежных карт, как правило, берут со взломанных серверов интернет-магазинов, платежных и расчётных систем, а также с персональных компьютеров (либо непосредственно, либо через программы удаленного доступа, так называемые, «трояны» и «черви»).

Кардселлер **–** лицо, осуществляющее приобретение банковских карт с последующей перепродажей с целью наживы (покупает за меньшую цену и перепродает дроповоду за повышенную цену).

Киберпреступность **–** совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, а также против компьютерных систем, компьютерных сетей и компьютерных данных.

Таким образом, понятие «киберпреступление» не ограничивается только рамками сети Интернет, оно распространяется на все виды преступлений, совершаемых в информационно-телекоммуникационной сфере[1].

Кодер – разработчик вредоносного программного обеспечения.

Контент-провайдер **–** компания, осуществляющая предоставление информации в сетях сотовой связи с использованием коротких номеров.

---

[1] Чекунов И.Г. Киберпреступность: понятие и классификация // Российское должностное лицо ОЛПС. 2012. № 2. С. 37.

Корсчет **–** основной банковский счет, используемый банком для всевозможных финансовых операций.

Криптор **–** лицо, осуществляющее шифрование кода вредоносного программного обеспечения с целью его дальнейшего сокрытия от обнаружения антивирусными программами за отдельное вознаграждение.

MAC-адрес (от англ. Media Access Control – управление доступом к среде) – это уникальный идентификатор, сопоставляемый с различными типами оборудования для компьютерных сетей, присваиваемый каждой единице активного оборудования (устройства).

Мул **–** лицо, которое нанимают через сеть Интернет с условием открытия банковского счета, в последующем выступавшее посредником для получения наличных денежных средств путем хищения в системе дистанционного банковского обслуживания. Данное лицо при помощи безналичных переводов может переводить оставшиеся деньги на другие счета и при этом удерживать комиссию.

Несанкционированный доступ к информации – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т.д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т.д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

Объект деанонимизации **–** объект, персональные данные которого были опубликованы в сети Интернет, тот объект, деанонимизацию кого осуществляют.

Обыск – действие, относящееся к разряду следственных, направленное на принудительное обследование участков местности, жилищ, предметов и документов по отысканию объектов, имеющих отношение к расследуемому преступному событию, а также обнаружению лиц, скрывающихся от правосудия, и объектов, запрещенных соответствующим законодательством в свободном обороте.

Организатор **–** лицо, осуществляющее координацию преступных действий со стороны участников преступной группы и распределение ролей между указанными лицами, а также определение последующих выплат денежных средств, добытых участниками преступной группы.

Осмотр – самый распространенный метод обнаружения путем восприятия должностным лицом улик-объектов, которые в последствии могут быть признаны доказательством в ходе расследования того или иного преступления. Данное действие является единственным, которое законодатель позволяет проводить как до момента возбуждения уголовного дела, так и после него.

Отклик – время реакции устройства при поступлении сигнала или команды на электронное устройство.

Платежная система сети Интернет («электронный кошелек») **–** система расчетов между финансовыми организациями, бизнес-организациями и интернет-пользователями при купле-продаже товаров и за различные услуги через интернет.

Преступления в сфере компьютерной информации – общественно опасные деяния, совершаемые в сфере компьютерной информации, признаваемые преступлениями уголовным законодательством Российской Федерации. В теории и на практике не выработано единого определения подобных преступлений. Объясняется это, в первую очередь, различием российского законодательства и законодательств других стран о преступлениях с использованием компьютера.

Провайдер – специализированная компания или фирма, обеспечивающая доступ к информационным сетевым службам (сотовая телефонная связь, интернет и т.п.).

Регистратор доменного имени – организация, имеющая полномочия создавать (регистрировать) новые доменные имена и продлевать срок действия уже существующих доменных имен в домене, для которого установлена обязательная регистрация. Таковыми доменами являются: домен нулевого уровня (корневой домен); все домены верхнего уровня (первого уровня).

Редирект (от англ. redirect – «перенаправление») – это автоматическая переадресация пользователей с одного URL-адреса на другой.

Руткиты – программы, предназначенные для сокрытия в системе определенных объектов или действий. Часто основная их цель – предотвратить обнаружение вредоносных программ, чтобы увеличить время работы этих программ на зараженном компьютере.

Руткит (англ. rootkit, то есть «набор root'a») – набор программных средств (например, исполняемых файлов, скриптов, конфигурационных файлов), для обеспечения маскировки объектов (процессов, файлов, директорий, драйверов), управления (событий, происходящих в системе), сбора данных (параметров системы). В системе Windows под термином «руткит» принято считать программу, которая внедряется в систему и перехватывает системные функции или производит замену системных библиотек. Перехват и модификация низкоуровневых API функций в первую очередь позволяет такой программе достаточно качественно маскировать свое присутствие в системе, защищая ее от обнаружения пользователем и антивирусным программным обеспечением (ПО).

Кроме того, многие «руткиты» могут маскировать присутствие в системе любых описанных в его конфигурации процессов, папок и файлов на диске, ключей в реестре. Многие руткиты устанавливают в систему свои драйверы и сервисы (они естественно также являются «невидимыми».

Сервер – специализированный компьютер или оборудование, предназначенное для выполнения сервисного программного обеспечения без непосредственного участия в работе самого человека.

Сетевой трафик – это объем информации, передаваемой через компьютерную сеть за определенный период времени.

Символика экстремистской организации – символика, описание которой содержится в учредительных документах организации, в отношении которой по основаниям, предусмотренным законодательством

Российской Федерации, судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности.

Скимминг – снятие информации с финансового инструмента пользователя с целью последующего хищения денежных средств и других противоправных действий.

Скриншот **–** мгновенный снимок экрана, осуществляемый нажатием клавиши «PrtScr» на клавиатуре.

Создание компьютерной программы **–** результат творческой деятельности, выразившийся в полном описании алгоритма данной деятельности, то есть логически связанных команд, с дальнейшим преобразованием в машиночитаемый язык (пункт 2 части 1 статьи 1225 Гражданского кодекса Российской Федерации, статья 1228 настоящего Кодекса). Программа считается созданной с момента, когда компьютер способен ее исполнить и поставленная задача автором может быть решена.

СОРМ (система технических средств для обеспечения функций оперативно-розыскных мероприятий) – комплекс технических средств и мер, предназначенных для проведения оперативно-розыскных мероприятий в сетях телефонной, подвижной и беспроводной связи и радиосвязи.

Социальная инженерия – это метод несанкционированного доступа к информации или системам хранения информации без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным.

Социальная сеть – платформа, онлайн-сервис или веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений, визуализацией которых являются социальные графы.

Спам (от англ. Spiced ham – «анонимная массовая незапрошенная рассылка сообщений»). Термин «спам» возник в 1936 году. На долю электронной почты приходится более двух третьих всего потока спама. Среди других средств распространения спама следует особо отметить мгновенные сообщения, SMS-сообщения и социальные сети. Спам может преследовать рекламные цели, может представлять из себя мошенническую спам-рассылку («нигерийские» письма, фишинговые сообщения), быть рассылкой политической информации, благотворительной спам-рассылкой и т.д.

Спамеры – профессиональные службы рассылок. Это группы весьма квалифицированных людей, вооруженных совершенным программным обеспечением, которое умеет рассылать письма с огромной скоростью и использовать последние достижения спамерской мысли.

Субъект деанонимизации **–** тот, кто осуществляет деанонимизацию.

Тайминг **–** точное расписание и планирование времени работы устройства. Временной промежуток, в течение которого необходимо выполнить определенное действие. Данное определение используется в характеристике компьютерного оборудования, а также есть определение тайминга рабочего времени.

Терроризм – это идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и/или иными формами противоправных насильственных действий.

Террористическая деятельность – это деятельность, включающая в себя организацию, планирование, подготовку, финансирование и реализацию террористического акта; подстрекательство к террористическому акту; организацию незаконного вооруженного формирования, преступного сообщества (преступной организации), организованной группы для реализации террористического акта, а равно участие в такой структуре; вербовку, вооружение, обучение и использование террористов; информационное или иное пособничество в планировании, подготовке или реализации террористического акта; пропаганду идей терроризма, распространение материалов или информации, призывающих к осуществлению террористической деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности.

Террористический акт − совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях воздействия на принятие решения органами власти или международными организациями, а также угроза совершения указанных действий в тех же целях.

Террористическая организация – организация, созданная в целях осуществления террористической деятельности или признающая возможность использования в своей деятельности терроризма.

Технический канал связи – одна из составляющих частей телекоммуникационной сети, состоящая из технических средств и устройств, обеспечивающих проводную и беспроводную связь по передаче и обмену информацией во времени и в пространстве.

Транзакция – операция, состоящая в переводе денежных средств с одного счета на другой; сделка купли-продажи.

Трафер – лицо, обладающее специальными знаниями в области программирования, осуществляющее распространение вредоносного программного обеспечения за определенную оговоренную сумму.

Удаленная атака – сканирование системы на предмет открытых портов с последующим захватом контроля над компьютером, что грозит финансовыми потерями или в лучшем случае приводит в негодность операционную систему.

Файрвол (межсетевой экран или сетевой экран) – комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.

Фишинг (от англ. phishing – «рыбная ловля, выуживание») – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям, что достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков («Ситибанк», «Альфа-банк»), поисковых («Рамблер»), почтовых («Mail.ru») и других сервисов или в социальных сетях («Facebook», «ВКонтакте»). В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. Оказавшись на таком сайте, пользователь может сообщить мошенникам ценную информацию, позволяющую получить доступ к аккаунтам и банковским счетам. Фишинг – одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности, в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учетные данные, пароль и прочее.

Хостинг – услуга по предоставлению ресурсов для размещения информации на сервере, постоянно находящемся в сети (обычно в сети Интернет). Как правило, хостинг входит в пакет по обслуживанию сайта и подразумевает, как минимум, услугу размещения файлов сайта на сервере, на котором запущено программное обеспечение, необходимое для обработки запросов к этим файлам (веб-сервер). Обычно в обслуживание уже входит предоставление места для почтовой корреспонденции, баз данных, DNS, файлового хранилища на специально выделенном файл-сервере.

Хостинговая компания – организация, оказывающая услуги по предоставлению вычислительных мощностей для размещения информации на сервере, постоянно находящемся в сети Интернет.

Червь (сетевой червь) – тип (составная часть) вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных систем, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, осуществлению иного вредоносного воздействия.

Большинство известных компьютерных червей распространяется следующими способами:

в виде файла, отправленного во вложении в электронном письме;

в виде ссылки на интернет – или FTP-ресурс;

в виде ссылки, переданной через сообщение ICQ или IR;

через пиринговые сети обмена данными P2P (peer-to-peer).

Некоторые черви распространяются как сетевые пакеты. Они проникают в компьютерную память, затем активируется код червя.

Компьютерные черви могут использовать ошибки конфигурации сети (например, чтобы скопировать себя на полностью доступный диск) или бреши в защите операционной системы и приложений.

Шпионские программы – программы типа Trojan-Spy способны скрыто наблюдать за использованием компьютера, например, отслеживая вводимые с

клавиатуры данные, делая снимки экрана и получая список работающих приложений.

Экстремизм – антиобщественное поведение физических или юридических лиц, которое выражается в использовании насилия или иных крайних форм и методов деятельности по мотивам политической, идеологической, расовой, национальной, религиозной ненависти или вражды, ненависти или вражды в отношении какой-либо социальной группы и тому подобным идейным мотивам.

Экстремист – лицо, придерживающееся крайних взглядов и методов достижения социально-политических, экономических и иных целей и допускающее возможность применения насилия.

Экстремистская группировка – это группа лиц, организованная для подготовки или совершения по мотивам идеологической, политической, расовой, религиозной или национальной ненависти либо вражды преступлений экстремистской направленности.

Экстремистская организация – общественное или религиозное объединение либо иная организация, в отношении которых по основаниям, предусмотренным Федеральным законом от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности», судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности .

Экстремистские материалы – предназначенные для обнародования документы либо информация на иных носителях, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии, публикации, обосновывающие или оправдывающие национальное и/или расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы.

Эксплойты – программы с данными или кодом, использующие уязвимость в работающих на компьютере приложениях.

Яндекс. Деньги (ЮMoney)- сервис электронных платежей, который позволяет принимать оплату электронными деньгами, наличными, с банковских карт.

ADWARE – компьютерная программа, находящаяся на компьютере пользователя без его ведома, не несущая деструктивных действий, ее вред выражается в навязчивом показе пользователю рекламы путем изменения стандартной страницы браузера, показа всплывающих окон, баннеров, переадресации на другие сайты.

DEF-код - код мобильного оператора, позволяющий географически определить компанию, обладающую определенным диапазоном номеров.

Email-Worm – вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению по каналам электронной почты. В процессе размножения червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе (например, URL на зараженный файл, расположенный на взломанном или хакерском веб-сайте).

В первом случае код червя активизируется при открытии (запуске) заражённого вложения, во втором – при открытии ссылки на заражённый файл. В обоих случаях эффект одинаков – активизируется код червя.

Почтовые черви для отправки зараженных сообщений используют различные способы, такие как:

прямое подключение к SMTP-серверу (сервер почтовых сообщений), используется встроенная в код червя почтовая библиотека;

использование сервисов MS Outlook;

использование функций Windows MAPI (инструмент обмена сообщениями в сети).

GPRS (от англ. General Packet Radio Service – «пакетная радиосвязь общего пользования») – надстройка над технологией мобильной связи GSM, осуществляющая пакетную передачу данных. GPRS позволяет пользователю мобильного телефона производить обмен данными с другими устройствами в сети GSM и с внешними сетями, в том числе Интернет. GPRS предполагает тарификацию по объему переданной/полученной информации, а не времени, проведенному online.

HTML *(*от англ. HyperText Markup Language – язык «гипертекстовой разметки») – стандартизированный язык разметки веб-страниц во всемирной паутине.

HTTP – широко распространенный протокол передачи данных, изначально предназначенный для передачи гипертекстовых документов (т.е. документов, которые могут содержать ссылки, позволяющие организовать переход к другим документам. На данный момент именно благодаря протоколу HTTP обеспечивается работа всемирной паутины.

IMEI-код (сокр. от англ. International Mobile Equipment Identity – международный идентификатор мобильного оборудования) – это номер, обычно уникальный, для идентификации телефонов различных стандартов радиоинтерфейсов, а также некоторых спутниковых телефонов.

IP или IP-протокол (сокр. от англ. Internet Protocol – «межсетевой протокол») – маршрутизируемый протокол сетевого уровня стека TCP/IP. Именно IP стал тем протоколом, который объединил отдельные компьютерные сети во всемирную сеть Интернет. IP объединяет сегменты сети в единую сеть, обеспечивая доставку пакетов данных между любыми узлами сети через произвольное число промежуточных узлов (маршрутизаторов).

Net-Worm − вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению в компьютерных се-

тях. Отличительной особенностью данного типа червей является отсутствие необходимости в пользователе как в звене в цепочке распространения (т.е. непосредственно для активации вредоносной программы).

Зачастую при распространении такой червь ищет в сети компьютеры, на которых используется программное обеспечение, содержащее критические уязвимости. Для заражения уязвимых компьютеров червь посылает специально сформированный сетевой пакет (эксплойт), в результате чего код (или часть кода) червя проникает на компьютер-жертву и активируется. Если сетевой пакет содержит только часть кода червя, то после проникновения в уязвимый компьютер он скачивает основной файл червя и запускает его на исполнение.

Можно встретить сетевых червей данного типа, использующих сразу несколько эксплойтов для своего распространения, что увеличивает скорость нахождения ими компьютера-жертвы.

P2P-Worm – (от одного человека к другому человеку) вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению по каналам файлообменных пиринговых сетей (например, Kazaa, Grokster, eDonkey, FastTrack, Gnutella и др.).

Пиринговая сеть (одноранговая, децентрализованная сеть) – сеть, созданная поверх другой сети (надстройка над сетью интернет), основанная на равноправии участников.

Механизм работы большинства подобных червей достаточно прост — для внедрения в P2P-сеть червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по распространению вируса P2P-сеть берет на себя: при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла с зараженного компьютера.

Существуют более сложные P2P-черви, которые имитируют сетевой протокол конкретной файлообменной системы и на поисковые запросы отвечают положительно. При этом червь предлагает для скачивания свою копию.

RISKWARE − легальные программы, которые могут причинить вред компьютеру, если используются злоумышленниками для удаления, блокирования, изменения или копирования данных, а также для нарушения работы компьютеров и сетей.

По своему назначению это не вредоносные программы, но некоторые их функции могут быть использованы во вредоносных целях.

Например, программы удаленного администрирования часто используются системными администраторами и службами поддержки клиентов для диагностики и устранения неполадок, возникающих на компьютерах пользователей. Однако если такая программа установлена на Вашем компьютере злоумышленником (без Вашего ведома), он получит удаленный доступ к Ва-

шему компьютеру. Полностью контролируя Ваш компьютер, злоумышленник сможет использовать его практически в любых нужных ему целях.

SMS-сообщения (сокр. от англ. Short Message Service – «служба коротких сообщений») – технология, позволяющая осуществлять прием и передачу коротких текстовых сообщений с помощью сотового телефона.

SMS-трояны – такие программы отправляют текстовые сообщения с мобильного устройства на платные телефонные номера с повышенным тарифом, растрачивая Ваши деньги.

SIM-карта (сокр. от англ. Subscriber Identification Module – модуль идентификации абонента) – идентификационный модуль абонента, применяемый в мобильной связи.

Spyware – компьютерная программа, находящаяся на компьютере пользователя без его ведома и не несущая деструктивных действий, ее вред выражается в шпионских действиях против пользователя с целью получения паролей и другой личной информации.

TOR – система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищенное от прослушивания.

Троянские программы − вредоносные программы, выполняющие несанкционированные пользователем действия. Такие действия могут включать:

удаление данных;
блокирование данных;
изменение данных;
копирование данных;
замедление работы компьютеров и компьютерных сетей.

В отличие от компьютерных вирусов и червей троянские программы неспособны к самовоспроизведению.

Trojan-Downloader – эти программы Trojan-Downloader (загрузчики) способны загружать и устанавливать на компьютер-жертву новые версии вредоносных программ, включая троянские и рекламные программы.

Trojan-Dropper − эти программы используются хакерами, чтобы установить троянские программы и/или вирусы или предотвратить обнаружение вредоносных программ. Не каждая антивирусная программа способна выявить все компоненты троянских программ этого типа.

Trojan-FakeAV − программы типа Trojan-FakeAV (обман) имитируют работу антивирусного программного обеспечения. Они созданы, чтобы вымогать деньги у пользователя в обмен на обещание обнаружения и удаления угроз, хотя угроз, о которых они сообщают, в действительности не существует.

Trojan-Ransom − троянские программы этого типа (выкуп; вымогатель) могут изменить данные на компьютере таким образом, что компьютер перестает нормально работать, а пользователь лишается возможности использовать определенные данные. Злоумышленник обещает восстановить нормальную работу компьютера или разблокировать данные после уплаты запрашиваемой суммы.

Trojan-Mailfinder − такие программы способны собирать на Вашем компьютере адреса электронной почты.

Trojan-ArcBomb − эти трояны представляют собой архивы, специально сформированные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать данные – зависание или существенное замедление работы компьютера или заполнение диска большим количеством «пустых» данных. Особенно опасны «архивные бомбы» для файловых и почтовых серверов, если на сервере используется какая-либо система автоматической обработки входящей информации – «архивная бомба» может просто остановить работу сервера. Встречаются три типа подобных «бомб»:

некорректный заголовок архива;

повторяющиеся данные;

одинаковые файлы в архиве.

Некорректный заголовок архива или испорченные данные в архиве могут привести к сбою в работе конкретного архиватора или алгоритма разархивирования при разборе содержимого архива.

Trojan-Clicker − предназначены для обращения к целевым интернет-ресурсам. Это достигается либо передачей соответствующих команд браузеру, либо заменой системных файлов, в которых указаны «стандартные» адреса сайтов (например, файл hosts в MS Windows).

Злоумышленники могут преследовать различные цели:

увеличение посещаемости каких-либо сайтов, чтобы увеличить показы рекламы;

привлечение потенциальных жертв для заражения вирусами или троянами;

искусственная накрутка «кликов» в рекламных сетях с целью обогащения злоумышленников.

Trojan-Notifier − вредоносная программа, отправляющая злоумышленнику сигнал, что зараженное устройство подключено к сети. При этом в сообщении содержится информация о компьютере или смартфоне и его владельце, например, IP-адрес, номер открытого порта и e-mail. Сигналы высылают различными способами: электронным письмом, специально оформленным обращением к веб-странице злоумышленника, сообщением в мессенджере.

Подобные программы используют в многокомпонентных троянских наборах для извещения злоумышленника о закреплении вредоносных программ в атакуемой системе.

Trojan-Proxy − вредоносная программа, предназначенная для осуществления злоумышленником несанкционированного пользователем анонимного доступа к различным интернет-ресурсам через компьютер-жертву.

Данный тип вредоносных программ обычно используется при рассылке спама через заражённые компьютеры.

Trojan-PSW − вредоносная программа, предназначенная для кражи пользовательских аккаунтов (логин и пароль) с пораженных компьютеров. Название PSW произошло от Password-Stealing-Ware (вор аккаунтов).

При запуске PSW-трояны ищут необходимую им информацию системных файлов, хранящих различную конфиденциальную информацию или реестр. В случае успешного поиска программа отсылает найденные данные «хозяину». Для передачи данных могут быть использованы электронная почта, FTP, HTTP (посредством указания данных в запросе) и другие способы.

Некоторые трояны данного типа воруют регистрационную информацию к различному программному обеспечению.

Примечание: Trojan-PSW, занимающиеся кражей банковских аккаунтов, аккаунтов к интернет-пейджерам, а также аккаунтов к компьютерным играм относятся к Trojan-Banker, Trojan-IM и Trojan-GameThief соответственно. В отдельные типы данные вредоносные программы выделены в силу их многочисленности.

URL – адрес (от англ. Uniform Resource Locator – «единый указатель ресурса») – единообразный локатор (определитель местонахождения) ресурса. Изначально URL предназначался для обозначения мест расположения ресурсов (чаще всего файлов) во Всемирной паутине. Сейчас URL применяется для обозначения адресов почти всех ресурсов Интернета.

WAP (сокр. от англ. Wireless Application Protocol – «протокол беспроводного доступа») – это средство получения доступа к ресурсам Интернета посредством только мобильного телефона, не прибегая к помощи компьютера и/или модема. По сути, это технический стандарт, описывающий способ, с помощью которого информация из Интернета передается на дисплей мобильного телефона.

WebMoney – электронная система расчетов виртуальных денежных средств. Юридически в системе происходит передача имущественных прав, учет которых осуществляется при помощи специальных расчетных единиц – «титульных знаков».

WHOIS – сетевой протокол прикладного уровня. Основное применение – получение регистрационных данных о владельцах доменных имен, IP-адресов и автономных систем.

QIWI – платежный сервис в России и странах СНГ; представляет собой электронную платежную систему, позволяющую производить платежи с использованием различных устройств и каналов связи. Особенностью системы является «привязка» счета к номеру мобильного телефона абонента.

ВВЕДЕНИЕ

В настоящее время анализ складывающейся криминогенной обстановки, а также имеющиеся статистические сведения о совершаемых преступлениях на территории Российской Федерации позволяют сделать вывод о том, что преступления, совершаемые в сфере телекоммуникаций и компьютерной информации, ежегодно имеют тенденцию значительного роста (см. диаграмму 1).

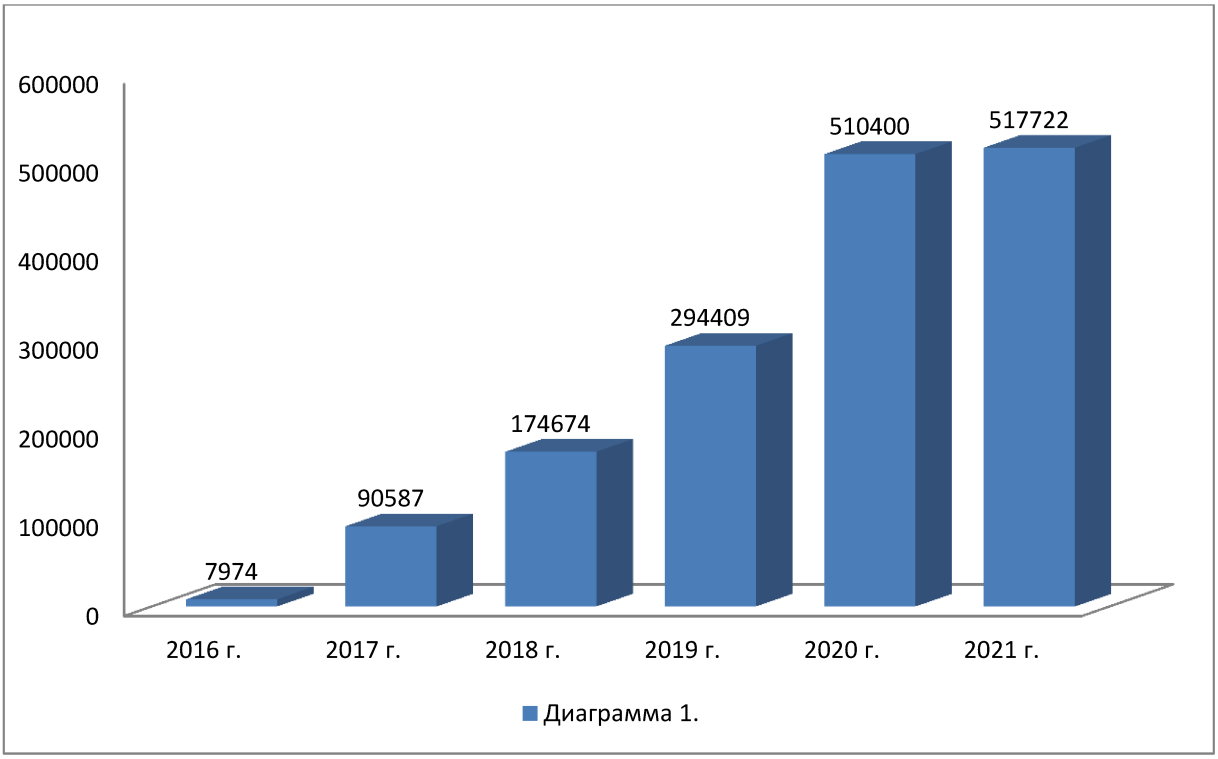


Диаграмма 1. Сведения о количестве зарегистрированных преступлений в сфере телекоммуникаций и компьютерной информации

Приведем сведения о состоянии преступности в России за 2019 год. Каждое седьмое преступление (14,5%), зарегистрированное в 2019 году, совершается с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (всего 294,4 тыс., то есть +68,5%). В общем числе зарегистрированных преступлений их удельный вес увеличился с 8,8 % в 2018 году до 14,5%.

Почти половина таких преступлений (48,5%) относится к категории тяжких и особо тяжких: 142,7 тыс. (+149,0%); половина (53,3%) совершается с использованием сети Интернет: 157,0 тыс. (+45,4%), более трети (39,5%) – средств мобильной связи: 116,2 тыс. (+89,5%).

Четыре таких преступления (80,0%) из пяти совершаются путем кражи или мошенничества: 235,5 тыс. (+83,2%), каждое двенадцатое (8,4%) – с це-

лью незаконного производства, сбыта или пересылки наркотических средств: 24,7 тыс. (+31,2%).[1]

В 2020 году зарегистрировано 510,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или на 73,4 больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 14,5% в январе-декабре 2019 года до 25,0%.

Практически все такие преступления (98,6%) выявляются органами внутренних дел.

Больше половины таких преступлений (52,4%) относятся к категориям тяжких и особо тяжких: 267,6 тыс. (+87,5%); больше половины (58,8%) совершается с использованием сети Интернет: 300,3 тыс. (+91,3%), почти половина (42,9%) – средств мобильной связи: 218,7 тыс. (+88,3%).

Четыре таких преступления (80,4%) из пяти совершаются путем кражи или мошенничества: 410,5 тыс. (+74,3%), почти каждое одиннадцатое (9,2%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 47,1 тыс. (+90,7%).[2]

По данным ГИАЦ МВД России каждое четвертое (25,8%) зарегистрированное в 2021 году преступление было совершено с использованием информационно-телекоммуникационных технологий (всего 517,7 тыс.)[3].

В общем числе зарегистрированных преступлений их удельный вес увеличился с 25,0% в 2020 году до 25,8% в 2021 году.

Больше половины таких преступлений (55,7%) относится к категориям тяжких и особо тяжких (288,3 тыс.; +7,7%), более двух третей (67,9%) совершается с использованием сети Интернет (351,5 тыс.;+17,0%), почти половина (42,0%) – с использованием средств мобильной связи (217,6 тыс.; -0,5%).

Почти четыре пятых таких преступлений (78,4%) совершается путем кражи или мошенничества: 406,0 тыс. (-1,1%), почти каждое десятое (9,9%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 51,4 тыс. (+9,3%).

Исходя из представленных статистических сведений, можно сделать вывод о том, что проблема противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, остается крайне актуальной, требующей особо пристального внимания со стороны правоохранительных органов и государства. Действительно, развитие информационно-телекоммуникационных и компьютерных технологий сопро-

---

[1] Состояние преступности в России за 2019 год / ФКУ «Главный информационно-аналитический центр МВД России». М., 2020.

[2] Состояние преступности в России за 2020 год / ФКУ «Главный информационно-аналитический центр МВД России». М., 2021.

[3] Состояние преступности в России за 2021 год / ФКУ «Главный информационно-аналитический центр МВД России». М., 2022.

вождается активной деятельностью преступников. Однако проблема заключается не только в увеличении числа преступлений в рассматриваемой сфере, но и в повсеместном распространении таких преступлений во всех областях жизнедеятельности граждан Российской Федерации. Новейшие компьютерные и информационные технологии используются при незаконном обороте наркотических средств и психотропных веществ, пропаганде деструктивной идеологии, при совершении различного рода мошеннических действий, дистанционных хищений, незаконных финансовых операций и других видов преступлений.

Исходя из сказанного, считаем необходимым привести некоторые примеры по раскрытию преступлений, совершаемых в сфере телекоммуникаций и компьютерной информации.

9 июня 2021 года закончилась самая масштабная международная полицейская операция, в ней приняли участие агенты ФБР, сотрудники федеральной полиции Австралии, Европола, силовики десятка стран. Задержаны, как минимум, 800 членов организованных преступных группировок. За сутки изъято 8 тонн кокаина, 250 единиц огнестрельного оружия, более 48 млн. дол. в обычной и криптовалюте. Глобальная слежка за фигурантами велась четыре года и стала возможной благодаря мессенджеру «AnOm», который, как выяснилось позже, был разработан спецслужбами. Его продвигали как абсолютно защищенный, он стал популярным среди преступников. «AnOm» устанавливали даже на специальные телефоны, которые международный преступный синдикат считал абсолютно секретными. Контролировалось более 12 тыс. телефонов, с которых было отправлено свыше 27 млн. сообщений в более чем 100 странах и более чем на 45 языках. Все эти телефоны использовались преступниками. Продавцы и пользователи «AnOm» были так уверены в секретности этих телефонов, что рекламировали их как устройства, разработанные преступниками для преступников.

В качестве примера совершения противоправных действий, связанных с использованием информационно-телекоммуникационных технологий, можно привести также пример о задержании граждан Белоруссии и России за совершение преступлений, предусмотренных ст. 207 УК РФ.

При комплексной работе ФСБ России, МВД России, СК России и КГБ Белоруссии были выявлены 8 участников Интернет-сообщества, которые распространяли ложные сообщения о минировании общественных мест. Участниками сообщества являлись граждане в возрасте от 13 до 21 года. С декабря 2021 года злоумышленники массово направляли анонимные сообщения с ложными угрозами о минировании детских садов, школ, торговых центров и других мест массового скопления людей. Преступники публиковали отчеты о своих действиях в социальных сетях. По произошедшим преступным деяниям были возбуждены уголовные дела в различных регионах по факту заведомо ложных сообщений об акте терроризма. Установлено, что

в специально созданном телеграмм-канале злоумышленники за денежное вознаграждение принимали заказы на отправку заведомо ложных сообщений о минировании объектов на территории России, Белоруссии и других государств. С октября 2021 года участники группы сделали более 80 ложных сообщений о факте терроризма.

Таким образом, можно сделать вывод о том, что преступления в сфере информационно-телекоммуникационных технологий создают реальную угрозу общественному строю государств и наносят достаточно большой ущерб государственным и иным структурам. Для пресечения такой деятельности требуется большие затраты сил и средств, направленных на их изобличение.

Рассматриваемый вид преступлений в отечественном уголовном законодательстве появился сравнительно недавно. Данные преступления в подавляющем большинстве совершаются изощренно, носят многогранный и латентный характер, их совершение причиняет огромный вред современному обществу, в результате которого создаются порой непоправимые проблемы правообладателям информации разного рода во многих сферах деятельности.

На сегодняшний день участились случаи незаконного использования компьютерной информации, в связи с чем возникает потребность урегулирования некоторых пробелов в действующем уголовном законодательстве и усиления ответственности в отношении вопроса несанкционированного использования информации, хранящейся на различных электронных носителях.

Уголовные дела, возбужденные по преступлениям в сфере телекоммуникаций и компьютерной информации, имеющиеся в производстве и оконченные расследованием, впоследствии переданные в суд для дальнейшего их рассмотрения и полного разрешения, позволяют сделать вывод, что в сложившейся ситуации во многих организациях, предприятиях, учреждениях и отраслях производства накопленная компьютерная информация остается наиболее уязвимой и создает лицам, склонным к совершению преступлений рассматриваемого вида, благоприятные условия для совершения преступлений.

Анализ положений действующего Уголовного кодекса Российской Федерации говорит о том, что глава 28 «Преступления в сфере компьютерной информации» содержит несколько понятий, ранее не имевших место не только в понятийно–терминологическом аппарате уголовного права, но и в «информационном» законодательстве.

Оперативные сотрудники, наделенные правами раскрывать преступления в сфере телекоммуникаций и компьютерной информации, ранее не имели практических наработок и теоретических рекомендаций по раскрытию и расследованию преступлений в этой сфере.

В целях своевременного документирования преступной деятельности данного вида преступлений и получения необходимой доказательной базы в отношении лиц, их совершивших, в 2001 году в структуре МВД России создано специализированное подразделение – Управление «К» БСТМ

МВД России, основными направлениями оперативно-служебной деятельности которого являются:

1. Борьба с преступлениями, связанными с изготовлением и распространением порнографических материалов с изображением несовершеннолетних.
2. Борьба с неправомерным доступом к компьютерной информации.
3. Борьба с преступлениями, связанными с созданием и использованием вредоносного программного обеспечения.
4. Борьба с нарушениями авторских и смежных прав в сфере информационных технологий.
5. Борьба с преступлениями в электронных платежных системах и системах дистанционного банковского обслуживания.
6. Борьба с мошенничеством в сети Интернет.
7. Борьба с преступлениями в сетях связи общего пользования.
8. Борьба с незаконным оборотом специальных технических средств для негласного получения информации.

Для достижения поставленных задач и принятия решений, исходя из складывающихся оперативно-розыскных и следственных ситуаций в ходе раскрытия преступлений, совершаемых в **сфере телекоммуникаций и компьютерной информации**, было и предложено данное учебно-практическое пособие[1].

Компьютеризация всех слоев населения представляет собой социально значимое явление, ее достижения могут быть использованы не только в хороших намерениях, но и в целях совершения преступлений компьютерной направленности. Компьютерные преступления носят специфичный характер, в настоящее время – это новации в системе уголовного права. Так как способы их совершения настолько многогранны и носят изощренный характер, что порой сотрудникам управлений «К» при документировании и раскрытии данного вида преступлений приходится сталкиваться с определенными трудностями, в связи с чем разрабатываются и внедряются новые формы и методы оперативно-розыскной деятельности. Необходимо заметить, что одним из важнейших составляющих элементов криминалистической характеристики методики раскрытия преступлений в **сфере телекоммуникаций и компьютерной информации** (компьютерных преступлений) является **субъективная особенность личности преступника**, которая на начальном этапе раскрытия преступлений характеризуется лишь скудной информацией, в связи с чем мы абсолютно согласны с мнением, высказанным Т.В. Ворошиловой, которая предлагает учитывать такие составляющие, как пол, возраст, социальное происхождение, уровень образования, род занятий, наличие специальности, семейное положение, социальный статус, уровень материальной обеспеченно-

[1] Историческая и социально-образовательная мысль. Всероссийский научный журнал. 2014. № 4 (26). С. 350.

сти, место жительства, а также места проведения досуга и возможная принадлежность к определенной субкультуре[1]. Иными словами, немаловажное значение в раскрытии любого вида компьютерного преступления играет характерологическая особенность психологии личности преступника. Она позволит при глубоком анализе определить и сузить круг подозреваемых лиц, мотив преступления, установить способ его совершения, а также выдвинуть версии, что, естественно, верно сориентирует и приблизит оперативных сотрудников и следователей к проведению оперативно-розыскных, специальных технических мероприятий[2] и следственных действий, способствующих раскрытию данного вида преступлений. Действующий уголовный закон в настоящее время защищает не только документированную информацию, но и ее разновидности, что расширяет возможности своевременно изобличать лиц, совершающих преступления данной направленности. Из проведенного анализа Уголовного кодекса Российской Федерации[3] следует отметить, что отношения, возникающие в области компьютерной информации, в настоящее время подлежат специальной охране.

В главу 28 УК РФ о преступлениях в сфере компьютерной информации введены термины и понятия, которых ранее не было не только в уголовно-правовой терминологии, но и в законодательстве, регулировавшем информационные отношения[4].

Проанализировав нормы из различных отраслей права, можно сделать ряд выводов[5]:

1. Информация – сведения (сообщения, данные) независимо от формы их представления [6].

2. Правовой защите подлежит любая документированная информация, т.е. информация, облеченная в форму, позволяющую ее идентифицировать[7].

3. Документированная информация является объектом гражданских прав и имеет собственника.

4. Информация может быть конфиденциальной, ознакомление с которой ограничивается ее собственником или нормами закона, и массовой, предназначенной для неограниченного круга лиц[8].

---

[1] Ворошилова Т.В. Социальная и психологическая характеристика личности компьютерного преступника. М., 2009. С. 5.

[2] Далее – ОРМ, СТМ.

[3] Далее – УК РФ.

[4] Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. Домодедово: ВИПК МВД России. 2013. № 2 (26).

[5] Историческая и социально-образовательная мысль. Всероссийский научный журнал. 2014. № 4 (26). С. 351.

[6] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ.

[7] Там же. Ст.2.

[8] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ.

5. Ограничения (установление режима) использования информации устанавливаются законом или собственником информации, которые объявляют уровень ее конфиденциальности.

Конфиденциальной в соответствии с законом является информация:

- содержащая государственную тайну[1];
- передаваемая путем переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений[2];
- содержащая служебную тайну[3], коммерческую тайну[4], банковскую тайну[5], личную тайну и семейную тайну[6], информация, являющаяся объектом авторских и смежных прав[7];
- непосредственно затрагивающая права и свободы гражданина или персональные данные[8] и др.

6. **Любая форма** завладения и пользования конфиденциальной документированной информацией **без** прямо выраженного **согласия** ее собственника является нарушением его прав, т.е. **неправомерной.**

Уголовно-правовой анализ преступлений в сфере компьютерной информации невозможно провести без предварительного уяснения родового понятия «информации». Информация как таковая выступает в качестве сравнительно нового предмета исследования и особого объекта правового регулирования. Именно поэтому необходимо обратиться не только к законодательным понятиям информации, но и к научным ее толкованиям.

Понятие «информация» имеет как минимум четыре основных значения:

- сведения, передаваемые людьми любым способом;
- общенаучное понятие;
- обмен сигналами в животном и растительном мире;
- кибернетический термин.

Само слово «информация» происходит от латинского «information» и означает «разъяснение» или «осведомленность»[9]. Начальные шаги в теории информации были сделаны еще в первой половине XX в.: в 1928 г. Р. Хартли впервые дал количественное определение информации, а в 1948 г. вышла знаменитая

---

[1] О государственной тайне: Федеральный закон от 21 июля 1993 г. № 5485-1; УК РФ. Ст. 275, 276, 283, 284.
[2] Конституция РФ. Ст.23. Ч. 2; УК РФ. Ст. 138.
[3] Гражданский кодекс Российской Федерации. Ст.139. Далее – ГК РФ.
[4] ГК РФ. Ст. 139; УК РФ. Ст. 183.
[5] УК РФ. Ст.183.
[6] Там же. Ст.137.
[7] Об авторском праве и смежных правах: Закон Российской Федерации от 09.07.1993 № 5351-1; УК РФ. Ст.146.
[8] Об информации, информатизации и защите информации: Федеральный закон; УК РФ. Ст.140.
[9] Большой энциклопедический словарь. М., 2004. С. 421.

книга К. Шеннона «Математическая теория связи», где информация и дается уже как статистическое определение.

Н. Винер, один из основателей кибернетики, определил информацию как «обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств»[1]. К. Шеннон, который сыграл не меньшую роль в развитии кибернетики, рассматривал информацию как сигнал (сообщение), устраняющий или снижающий неопределенность[2].

А.А. Фатьянов полагает, что «информация есть воспринимаемая живым организмом через органы чувств окружающая действительность в виде распределения материи и энергии во времени и в пространстве и процессов их перераспределения».

Таким образом, информация с точки зрения кибернетики представляется не как общественный феномен, то есть информация, производимая и потребляемая обществом, а в более узком, техническом аспекте – как информация, циркулирующая по электронным каналам связи. Кибернетика доказала, что информация имеет непосредственное отношение к процессам управления и развития, обеспечивающим функционирование любых систем[3].

Информационная сфера сегодня – это одна из наиболее динамичных и быстро развивающихся сфер общественных отношений, нуждающаяся в адекватном правовом регулировании. С этой целью создается «информационное» законодательство, а также система мер уголовно-правовой защиты данной группы отношений. Последние изменения в главу 28 УК РФ вступили в силу 30 декабря 2020 года.

Основное различие правового режима информации состоит в степени ее доступности для пользователей. Так, в зависимости от категории доступа к ней, информация подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)[4]. В соответствии со ст. 5 Федерального закона от 27 июля 2006 года № 149 «Об информации, информационных технологиях и о защите информации», информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

---

[1] Винер Н. Кибернетика и общество. М., 2003. С. 35.

[2] Шеннон К. Работы по теории информации и кибернетике. М., 1963. С. 59.

[3] Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. Домодедово: ВИПК МВД России. 2013. № 2 (26). С. 32-37

[4] Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации: учеб. пособие. М., 2001. С. 10.

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Так, например, правовой режим информации, составляющей государственную тайну, определяется Законом Российской Федерации от 21 июля 1993 года № 5485-1 «О государственной тайне» (в ред. федеральных законов от 30 декабря 2020 года № 481-ФЗ). Перечень сведений, составляющих государственную тайну, определен ст. 5 Закона и включает в себя четыре основных раздела:

1) сведения в военной области;

2) сведения в области экономики, науки и техники;

3) сведения в области внешней политики и экономики;

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты.

Как указывалось ранее, законодателю в каждом нормативном правовом акте требуется найти баланс между обеспеченным Конституцией Российской Федерации правом граждан на информацию и обеспечением ее конфиденциальности. Не стал исключением в этом смысле и Закон «О государственной тайне», который содержит перечень сведений, не подлежащих отнесению к государственной тайне и засекречиванию.

В соответствии со ст. 7 Закона таковыми являются: сведения о чрезвычайных происшествиях, катастрофах, стихийных бедствиях; о состоянии экологии, здравоохранения, санитарии, демографии, а также о состоянии преступности; о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам; о фактах нарушения прав и свобод человека и гражданина; о размерах золотого запаса и государственных валютных резервах Российской Федерации; о состоянии здоровья высших должностных лиц Российской Федерации; о фактах нарушения законности органами государственной власти и их должностными лицами.

Основополагающие принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации заложены Федеральным законом «Об информации, информационных технологиях и о защите информации», в ст. 3 которого четко установлено, что правовое регулирование рассматриваемых отношений основывается на принципах:

1) свободы поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установления ограничений доступа к информации только федеральными законами;

3) открытости информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправия языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечения безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверности информации и своевременности ее предоставления;

7) неприкосновенности частной жизни, недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимости установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Понятие **«компьютерной информации»** является не менее многозначным, чем понятие информации. Ее место в системе правоотношений, возникающих в информационной сфере, до сих пор является предметом научных дискуссий, которые пока не завершились формированием общепризнанного научного и законодательного определения, поскольку многообразие его толкования отображает весьма сложный характер реального мира.

Проблемы в правоприменительной практике связаны с тем, что несмотря на важность точного формализованного представления о сущности и свойствах компьютерной информации (как предмета преступления), на законодательном уровне появилось определение «компьютерной информации» относительно недавно. Однако в специальной и учебной литературе предложено множество определений рассматриваемого термина. Так, например, одними из первых понятие «компьютерной информации» дали: Т.Г. Смирнова, определив компьютерную информацию как «совокупность сведений, представляющих особую ценность для государства, общества и отдельных граждан, производство, хранение и использование которых осуществляется посредством компьютерной техники», и А.А. Петров, предложивший понимать под данным термином «информацию, содержащую сведения, составляющие государственную или коммерческую тайну, сведения конфиденциального характера и общего пользования».

Отметим, что предложенные определения не лишены недостатков. Из определения Т.Г. Смирновой следует, что информация и ее материальный носитель («компьютерная техника») не отделимы друг от друга, а исходя из такого подхода, компьютерная информация, циркулирующая в сети ЭВМ, не будет являться предметом данной категории преступлений, а, следовательно,

останется без надлежащей уголовно-правовой защиты. Из содержания понятия «компьютерная информация», данного А.А. Петровым, вообще невозможно выделить отличительные признаки компьютерной информации как таковой[1].

Более корректными представляются определения, предложенные С.А. Пашиным и В.С. Комиссаровым. По утверждению первого автора, «компьютерная информация – это информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ»[2]. В.С. Комиссаров справедливо указал, что «компьютерная информация может находиться или на машинном носителе (магнитном диске, магнитной ленте, дискете, магнитно-оптическом диске (CD-ROMe), или непосредственно в ЭВМ (в постоянном или оперативном запоминающих устройствах), либо в системе ЭВМ или их сети»[3]. По нашему мнению, понятия, предложенные С.А. Пашиным и В.С. Комисаровым, наиболее точные, четко отражают критерии предмета преступлений в сфере компьютерной информации. Также нельзя не согласиться и с определением «компьютерного преступления», предложенным авторами В.А. Дуленко, Р.Р. Мамлеевым, В.А. Пестриковым, определяющими компьютерное преступление как уголовно-правовое понятие – это предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства[4].

Поэтому с учетом представленных позиций авторов **понятие «компьютерной информации»** как предмета преступления можно сформулировать как организационно упорядоченную совокупность сведений (сообщений, данных), зафиксированных на машинном носителе или находящихся в оперативной памяти компьютера либо в информационно–телекоммуникационной сети с реквизитами, позволяющими их идентифицировать, имеющую собственника либо иного законного владельца.

Телекоммуникационные сети – это технические средства (механизмы, оборудование) и устройства информационного обмена, а также программные средства, при помощи которых субъекты информационного права могут «обмениваться» информацией и «обращать» информацию в пространстве через технические каналы связи (проводной связи, оптические и радиоканалы),

---

[1] См.: Петров А.А. Компьютерная информация как предмет уголовно-правовой защиты реформированного уголовного законодательства // Российское право в период социальных реформ. Н. Новгород. 1998. Вып. 2. С. 132.

[2] Комментарий к Уголовному кодексу Российской Федерации / под общ. ред. Ю.И. Скуратова, В.М. Лебедева. М., 2001. С. 696.

[3] Уголовное право России / под ред. В.С. Комисарова. М., 2006. С. 307.

[4] Дуленко В.А., Мамлеев Р.Р., Пестриков В.А. Преступление в сфере высоких технологий: учебное пособие. М., 2010. С. 196.

представляющие собой технологические системы с различными видами передач (цифровое телевидение, различные виды работы в Интернете, факсимильная, телеграфная, телефонная и др., включая обмен информацией между электронными устройствами и другие виды документальных сообщений) (рис. 1).

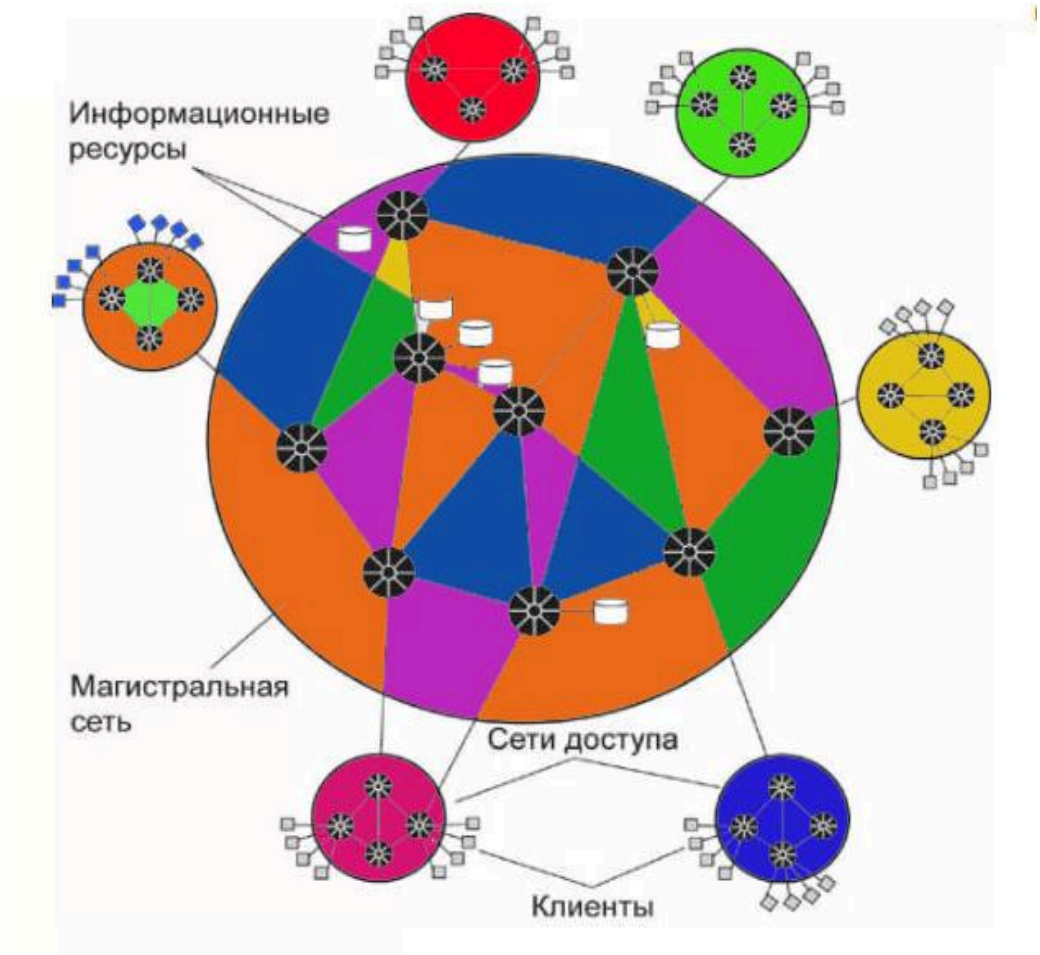


Рис. 1. Телекоммуникационная сеть

Таким образом, уголовно-правовой защите подлежит любая информация, неправомерное обращение с которой может нанести ущерб ее собственнику (владельцу, пользователю). При закреплении предложенных определений в базовом для этой сферы законодательстве, например в Федеральном законе «Об информации, информационных технологиях и о защите информации», оно позволит, на наш взгляд, существенно сократить ошибки в правовом применении рассматриваемых уголовно-правовых норм[1].

[1] Вестник Всероссийского института повышения квалификации сотрудников МВД России. Домодедово: ВИПК МВД России. 2013. № 2 (26). С. 32-37.

Контрольные вопросы

1. Чем вызвана необходимость установления уголовной ответственности за причинение вреда в связи с незаконным использованием компьютерной информации?
2. Какая информация является наиболее уязвимой?
3. Что явилось основанием сделать вывод об уточнении и конкретизации понятия «компьютерная информация»?
4. В каком году создано специализированное подразделение – Управление «К» БСТМ МВД России?
5. Назовите основные направления деятельности специализированного подразделения – Управления «К» БСТМ МВД России.
6. Назовите основные элементы в ходе раскрытия преступлений, совершаемых в сфере телекоммуникаций и компьютерной информации?
7. Что имеет немаловажное значение в раскрытии любого вида компьютерного преступления?
8. Какие выводы можно сделать, проанализировав различные нормы права относительно понятия «информация»?
9. Какие основные значения имеет понятие «информация»?
10. Какие авторы посвятили свои работы трактованию понятия «информация»?
11. В чем заключается различие правового режима понятия «информации»?
12. В каком нормативном документе заложены основополагающие принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации?
13. Дайте свое видение понятию «информация».
14. Согласны ли Вы с понятием «компьютерной информации», представленным в данном учебно-практическом пособии?
15. Согласны ли Вы с понятием «телекоммуникационные сети», представленным в данном учебно-практическом пособии?

ГЛАВА I
УГОЛОВНО-ПРАВОВАЯ И КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СФЕРЕ ТЕЛЕКОММУНИКАЦИЙ И КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В настоящее время одним из современных видов совершаемых преступлений являются преступления в сфере телекоммуникаций и компьютерной информации.

Телекоммуникационные системы и компьютерная информация внедряются во все сферы жизнедеятельности человека, представляют собой сеть развитых технических средств по сбору, передаче, обработке и хранению информации и поэтому наиболее часто подвержены пристальному вниманию со стороны преступников.

В соответствии со ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» и ч. 1 ст. 272 УК РФ, «**информация – это сведения (сообщения, данные) независимо от формы их представления**»[1]. Что же касается определения компьютерной информации, то доцент кафедры криминалистики МГУ им. М.В. Ломоносова В. Крылов рассматривает компьютерную информацию как специальный объект преступного посягательства и считает, что ***компьютерная информация*** «есть сведения, знания или набор команд (программа), предназначенные для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинных носителях – идентифицируемый элемент информационной системы, имеющей собственника, установившего правила ее использования».

Таким образом, правовой защите подлежит главным образом документированная информация (документ), зафиксированная на материальном носителе с реквизитами, т.е. информация, которая облечена в форму, позволяющую ее «идентифицировать»[2].

Кроме того, понятие «документированная информация» основано на «двуединстве – информации (сведений) и материального носителя, на котором она отражена в виде символов, знаков, букв, волн или других способов отображения. В результате документирования происходит как бы материализация и овеществление сведений...»[3]. Отсюда можно сделать вывод, что информация становится объектом гражданского законодательства.

Преступления, совершаемые **в сфере телекоммуникаций и компьютерной информации**, как уже было сказано, являются одной из разновидностей преступлений, входящих в настоящее время в Главу 28 УК РФ «**Пре-**

---

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. №149-ФЗ. Ст.2.

[2] Крылов В.В. Информация как элемент криминальной деятельности // Вестник Московского университета. Сер. 11. М.: Право, 1998. № 4.

[3] Копылов В.А. Информационное право. М.: Юристъ, 1997. С. 23.

ступления в сфере компьютерной информации», а некоторые из них могут тесно взаимодействовать и с иными видами преступлений, входящих в другие главы УК РФ (например, статья 242.1 УК РФ «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних» и статья 242.2 УК РФ «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов», которые входят в Главу 25 УК РФ «Преступления против здоровья населения и общественной нравственности»).

В этих целях сотрудниками БСТМ МВД России постоянно осуществляется комплекс оперативно-поисковых, оперативно-розыскных и специальных технических мероприятий, направленных на выявление, пресечение и раскрытие преступлений, предусмотренных статьями 132 УК РФ (насильственные действия сексуального характера), 135 УК РФ (развратные действия) и 242.2 УК РФ (использование несовершеннолетнего в целях изготовления порнографических материалов или предметов).

Эти виды преступлений обладают следующими ***криминалистическими особенностями***[1]:

1. Компьютерная информация достаточно просто и быстро преобразуется из одной объектной формы в другую, копируется (размножается) на различные виды машинных носителей и пересылается на любые расстояния, ограниченные только радиусом действия современных средств телекоммуникационных сетей.

2. При изъятии (копировании) информации, зафиксированной в телекоммуникационных сетях, а также любого вида компьютерной информации, в отличие от изъятия материального предмета, она может сохраниться в первоисточнике.

3. В большинстве случаев информация, в том числе и телекоммуникационная, становится продуктом общественных отношений, имеет определенную цену и является предметом купли–продажи.

Такого рода общественные отношения закреплены в Федеральном законе «Об информации, информационных технологиях и о защите информации». В связи с этим новые информационные технологии не только дали толчок в плане прогресса общества, но и стимулировали возникновение и развитие новых форм преступности. Прогресс в области компьютерной техники и телекоммуникационной среде предоставил злоумышленникам широкие возможности неправомерного доступа к новым техническим средствам и дальнейшее их использование в противоправных целях.

Как нам известно, виды преступлений в сфере компьютерной информации представлены в главе 28 Уголовного кодекса Российской Федерации:

Статья 272. Неправомерный доступ к компьютерной информации.

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

---

[1] Вестник ВИПК МВД России. Домодедово: ВИПК МВД России. 2012. № 3 (23). С. 69.

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

Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Так как преступления, совершаемые в телекоммуникационных сетях, являются новой разновидностью компьютерных преступлений, законодатель ввел новые нормы неизвестных ранее составов преступлений. Необходимость установления уголовной ответственности за причинение вреда в связи с использованием той или иной информации вызвана возрастающим значением и широким применением ЭВМ во многих сферах деятельности и, наряду с этим, повышенной уязвимостью информации, находящейся в ИТКС (информационно-телекоммуникационная среда) по сравнению, скажем, с информацией, зафиксированной на бумаге и хранящейся в сейфе[1].

Итак, **преступления в телекоммуникационных сетях** – это разновидность преступлений, совершаемых с использованием компьютерной информации. При этом информация, находящаяся в телекоммуникационных сетях является предметом и (или) средством совершения преступления.

Преступления, совершаемые в телекоммуникационных сетях, имеют некоторые характерные особенности:

- неоднородность объекта посягательства;
- выступление телекоммуникационной информации как в качестве объекта, так и в качестве средства преступления;
- многообразие предметов и средств преступного посягательства;
- выступление ИТКС либо в качестве предмета, либо в качестве средства совершения преступления.

На основе этих особенностей можно сделать вывод, что преступления, совершаемые в телекоммуникационных сетях, – это предусмотренное уголовным законом общественно опасное действие, совершенное с использованием телекоммуникационных средств.

Мы абсолютно солидарны и полностью разделяем мнение И.Г. Чекунова, который ранее говорил, что все большее количество государств ставит перед собой **в качестве приоритетной цели создание информационного общества на основе широкого внедрения телекоммуникационных технологий.** Одной из определяющих задач на этом пути является формирование комплексной инфраструктуры для оказания электронных услуг населению. Постановка этой задачи в России вполне оправдана, поскольку сегодня компьютеры, мобильные средства связи, их программное обеспечение, телекоммуникационные системы охватывают практически все сферы жизнедеятельности человека, общества и государства[2]. Однако выстроенные глобальные

---

[1] Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // Рос. юстиция. 1999. № 1. С. 44-45.

[2] Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2012. №1. С. 9-10.

информационные сети, востребуемые современным цивилизованным обществом, все чаще используются и лицами склонными к совершению различного рода преступлениям и, к нашему сожалению, статистические данные говорят, что такое незаконное использование сферы телекоммуникаций и компьютерной информации из года в год растет (см. диаграмму 2).

Диаграмма 2. Сведения о количестве зарегистрированных преступлений в сфере телекоммуникаций и компьютерной информации

Существенно то, что предметом данных преступлений является информация, находящаяся в телекоммуникационных сетях. По данным «Лаборатории Касперского», ежедневно злоумышленники создают и используют новые способы заражения и обходят установленные, не отвечающие современным требованиям, способы защиты информации, хранящейся на ПЭВМ. Известно, что количество новых вредоносных программ ежедневно доходит до 350 тысяч!

Кроме того, **предметом** компьютерных преступлений является и оборудование, обеспечивающее информационно-телекоммуникационные процессы. Непосредственным **объектом** данных преступных деяний является безопасность информационно-телекоммуникационных систем, базирующихся на использовании ИТКС.

Объективная сторона компьютерных преступлений и, в частности, преступлений, совершаемых в телекоммуникационных сетях, характеризуется как действием, так и бездействием. Действие (бездействие) сопряжено с нарушением прав и интересов по поводу пользования информацией, находящейся в телекоммуникационной сети.

Компьютерные преступления имеют материальные составы. Действие (бездействие) должно причинить значительный вред правам и интересам личности, общества или государства (исключением является преступление с формальным составом, предусмотренное ч. 1 ст. 273 УК РФ: создание, использование и распространение вредоносных программ для ЭВМ). Преступные последствия конкретизируются в законе применительно к конкретным видам компьютерных преступлений. Между деянием и последствиями обязательно должна быть установлена причинная связь, относящаяся к элементам криминалистически значимой информации.

Субъективная сторона компьютерных преступлений, а также преступлений, совершаемых в телекоммуникационных сетях, характеризуется умышленной виной. Деяние, совершенное по неосторожности, признается преступлением только тогда, когда это специально предусмотрено соответствующей статьей Особенной части УК РФ. Неосторожная форма вины названа в Особенной части лишь применительно к квалифицированным видам компьютерных преступлений, предусмотренных в ч. 2 ст. 273 и ч. 2 ст. 274 УК РФ.

Субъект компьютерного преступления общий – лицо, достигшее 16 лет. В ст. 274 и ч. 2 ст. 272 УК РФ формулируются признаки специального субъекта: лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети.

Однако необходимо заметить, что перечисленные статьи главы 28 Уголовного кодекса Российской Федерации в зависимости от создаваемой криминогенной обстановки и появления новых способов совершения преступлений иногда требуют существенных исследований и новых дополнений.

Сравнительный анализ сложившегося положения о преступлениях, совершаемых в сфере телекоммуникаций и компьютерной информации позволяет нам констатировать определенную трансформацию взглядов на данную группу преступлений, которая выражается, в первую очередь, в отказе законодателя от использования формулировки «компьютерные преступления» и появлении в УК РФ главы 28 «Преступления в сфере компьютерной информации», что не всеми учеными признается правильным. Так, К.С. Скоромников, говоря о частом использовании термина «компьютерные преступления» в правоприменительной практике в отношении общественно опасных деяний с применением средств вычислительной техники и об отсутствии данного термина в УК РФ, предлагал, «учитывая, что он прочно вошел в профессиональный лексикон у нас в стране и за рубежом»[1], сохранить его и ввести в официальную судебную статистику как условное наименование не только преступлений, предусмотренных гл. 28 УК РФ, но и совокупности с ними по другим статьям УК РФ. На наш взгляд, с таким выводом согласиться нельзя, так как использование терминов, отсутствующих в действующем законодательстве, в том числе и в судебной статистике, создаст нестабильность понятийно-терминологического аппарата, вызовет сложности при отграничении

[1] Скоромников К.С. Неправомерный доступ к компьютерной информации и его расследование // Прокурорский надзор и следственная практика. 1998. № 1. С. 168.

одних составов от других. Кроме того, зарубежная и отечественная правоприменительная практика свидетельствуют о появлении новых деяний в рассматриваемой сфере, которые осуществляются не только посредством ЭВМ, системы ЭВМ или их сети, но и с помощью телекоммуникационного оборудования, перечень которого постоянно расширяется. При этом телекоммуникационное оборудование, с использованием которого совершаются противоправные деяния, не всегда признается ЭВМ или системой ЭВМ.

Таким образом, в уголовно-правовой литературе применительно к наименованию, а, следовательно, и к понятию рассматриваемой группы преступлений существовали две позиции, когда одни ученые предлагали именовать эту группу деяний «компьютерные преступления», другие – «преступления в сфере компьютерной информации». Однако преступления, совершаемые в сфере телекоммуникаций, не всегда возможно квалифицировать, как «компьютерные преступления» или «преступления в сфере компьютерной информации». Вместе с тем количество выявляемых преступлений в сфере телекоммуникаций и компьютерной информации имеет *тенденцию роста* и постоянной модификации. В связи с этим **глава 28 УК РФ периодически дополняется отдельными статьями и видоизменяется**, что позволяет более точно рассматривать данные правонарушения, проводить дефиницию преступного деяния и способствовать квалифицированному документированию и дальнейшему успешному расследованию указанных преступлений.

Предлагаем рассмотреть статьи указанной главы.

Статья 272 УК РФ «Неправомерный доступ к компьютерной информации».

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации:

- наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности:

- наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения:

- наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления:

- наказываются лишением свободы на срок до семи лет.

В примечании 1 данной статьи дается следующее определение, под **компьютерной информацией** понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

В примечании 2 данной статьи говорится, что **крупным ущербом** в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Неправомерный доступ к компьютерной информации – это не санкционированное собственником или иным законным пользователем информации проникновение к ней, в том числе с возможностью ознакомления, которое позволяет распоряжаться этой информацией (уничтожать, блокировать, модифицировать и т.д.), и создающее опасность как для самой информации, так и для интересов собственника или иного законного пользователя.

В данном случае (дефиниция) под **предметом преступления** будет признаваться вещь, элемент материального мира, на который осуществляется воздействие в ходе совершения преступления.

Предметом преступлений, предусмотренных настоящей статьей, является охраняемая законом компьютерная информация. Согласно примечанию 1 к статье под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. При этом указанная информация охраняется законом, т.е. она относится к сведениям ограниченного доступа в виде государственной тайны или в виде сведений конфиденциального характера (персональных данных, тайны частной жизни, коммерческой, налоговой или банковской тайны, профессиональной тайны и др.). Действия виновного, который наряду с неправомерным доступом к компьютерной информации посягает на информацию ограниченного доступа, следует квалифицировать по совокупности ст. 272 УК РФ и соответствующей статьи, предусматривающей ответственность за посягательства на ту или иную тайну.

Под объектом преступления необходимо понимать один из элементов состава преступления, представляющий собой общественные институты, которым причиняется ущерб вследствие совершения преступления.

Объектом преступления в данной статье являются общественные отношения, обеспечивающие сохранность и конфиденциальность компьютерной информации.

Объективной стороной преступления будет являться один из элементов состава преступления, представляющий собой внешнее проявление преступления в реальной действительности.

К числу **признаков объективной стороны** относятся:

- общественно опасное деяние (действие или бездействие, посягающее на тот или иной объект);
- общественно опасные последствия;
- причинно-следственная связь между действием (бездействием) и последствиями;
- способ, место, время, обстановка, средства и орудия совершения преступления.

К обязательным признакам **объективной стороны** неправомерного доступа к компьютерной информации относятся:

- общественно опасное деяние, которое заключается в неправомерном доступе к охраняемой законом компьютерной информации;
- общественно опасные последствия в виде уничтожения, блокирования, модификации или копирования компьютерной информации, нарушения работы ЭВМ, системы ЭВМ или их сети;
- причинная связь между совершенным деянием и наступившим последствием.

Отсутствие одного из перечисленных признаков исключает уголовную ответственность за преступление, предусмотренное настоящей статьей. Общественно опасное деяние проявляется в форме действия. Совершение данного преступления путем бездействия невозможно.

Состав данного **преступления** носит **материальный** характер и предполагает обязательное наступление одного из последствий:

а) **уничтожение информации** – это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое «вытеснение» старых версий файлов последними по времени;

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

в) **модификация информации** – внесение изменений в компьютерную информацию (или ее параметры). Законом установлены случаи легальной мо-

дификации программ (баз данных) лицами, правомерно владеющими этой информацией, а именно: модификация в виде исправления явных ошибок; модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя; модификация в виде частной декомпиляции программы для достижения способности к взаимодействию с другими программами;

г) **копирование информации** – создание копии имеющейся информации на другом носителе, то есть перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме – рукописным видом, фотографированием текста с экрана дисплея, а также считыванием информации путем любого перехвата информации и т.п.

Необходимо установить, что указанные последствия наступили именно в результате неправомерного доступа к компьютерной информации.

Квалифицирующими признаками состава преступления являются крупный ущерб (примечание 2 к статье – «**Крупным ущербом** в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей») или совершение деяния из **корыстной заинтересованности** (ч. 2 ст. 272 УК РФ). Указанное примечание означает стремление виновного получить для себя или других лиц выгоду имущественного характера (деньги, имущество или право на его получение и т.п.) либо избавиться от материальных затрат (освобождение от каких-либо имущественных затрат, погашения долга, оплаты услуг, уплаты налогов и т.п.).

Особо квалифицирующими признаками выступают совершение деяния группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения (ч. 3 ст. 272 УК РФ).

Согласно ч. 2 ст. 35 УК РФ преступление признается совершенным **группой лиц по предварительному сговору**, если в нем участвовали лица, заранее договорившиеся о совместном совершении преступления.

Согласно ч. 3 ст. 35 УК РФ преступление признается совершенным **организованной группой**, если оно совершено устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений.

Неправомерный доступ к компьютерной информации, совершенный организованной группой, должен содержать следующие признаки: устойчивость; наличие в ее составе организатора (руководителя); заранее разработанный план совместной преступной деятельности; распределение функций между членами группы при подготовке к совершению преступления и осуществлении преступного умысла.

Об устойчивости организованной группы может свидетельствовать следующее: большой временной промежуток ее существования; неоднократность совершения преступлений членами организованной группы; техническая оснащенность; длительность и тщательность подготовки даже одного преступления; иные обстоятельства (например, специальная подготовка участников организованной группы).

Под **совершением преступления лицом с использованием своего служебного положения** понимается использование возможности доступа к компьютерной информации, возникшей в результате выполняемой работы (по трудовому, гражданско-правовому договору) или влияния по службе на лиц, имеющих такой доступ, то есть тех, кто на законных основаниях использует компьютерную информацию и средства ее обращения (программисты, пользователи, а также администраторы баз данных, инженеры, ремонтники, специалисты по эксплуатации электронно-вычислительной техники и прочие).

В ч. 4 предусмотрена ответственность за совершение указанных в законе действий, если они повлекли тяжкие последствия или создали угрозу их наступления.

В данной ситуации под **тяжкими последствиями** следует понимать крупные аварии, длительные остановки транспорта или производственного процесса, причинение значительного материального ущерба, причинение смерти по неосторожности, самоубийство или покушение на самоубийство потерпевшего и т.п.

Субъективная сторона преступления – это психическое отношение лица к совершаемому им преступлению, которое характеризуется конкретной формой вины, мотивом и целью.

Субъективная сторона неправомерного доступа к компьютерной информации характеризуется виной в форме умысла.

Субъект преступления – это лицо, совершившее предусмотренное уголовным законом общественно опасное деяние и способное нести за него уголовную ответственность.

Субъект преступления – вменяемое физическое лицо, достигшее 16-ти лет на момент совершения преступления.

Субъект преступления, предусмотренный частью 3 рассматриваемой статьи, – специальный: лицо, использующее свое служебное положение.

Статья 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ».

Федеральный закон от 07.12.2011 № 420-ФЗ внес изменения в статью 273 УК РФ, которая ранее звучала, как «Создание, использование и распространение вредоносных программ для ЭВМ», а в новой редакции она была представлена в следующем варианте: ***«Создание, использование и распространение вредоносных компьютерных программ».***

Использование в названии термина «вредоносные программы» не случайно. Если бы средством совершения данного преступления были только программы, которые принято называть «компьютерные вирусы», это существенно ограничило бы применение рассматриваемой уголовно-правовой нормы. Во-первых, компьютерный вирус может быть безвредным, и подвергать его создателя уголовному преследованию было бы бессмысленно, а во-вторых, существует множество программ другого типа (например, троянский

конь), приводящих к столь же нежелательным последствиям, как и в случае действия вредоносных вирусов[1].

Программа для ЭВМ – объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ с целью получения определенного результата[2].

Создание вредоносной программы – написание ее алгоритма и преобразование его в машинный язык. Соответственно, внесение изменений в программу означает исключение отдельных частей, внесение новых фрагментов или изменение алгоритма.

Вредоносность или полезность соответствующих программ для ЭВМ определяется не в зависимости от их назначения, способности уничтожать, блокировать, модифицировать, копировать информацию (это вполне типичные функции абсолютно легальных программ), а в связи с тем, предполагает ли их действие, во-первых, предварительное уведомление собственника компьютерной информации или другого добросовестного пользователя о характере действия программы, а во-вторых, получение его согласия (санкции) на реализацию программой своего назначения. Нарушение одного из этих требований делает программу для ЭВМ вредоносной[3].

Объектом данного вида **преступления** являются отношения в сфере обеспечения компьютерной безопасности.

Субъектом преступления является лицо, достигшее 16 лет[4]. Квалифицирующим обстоятельством данного преступления является наступление тяжких последствий (ч. 2 ст. 273 УК РФ). При фиксации последствий в данном составе преступления законодатель использует оценочное понятие. Следовательно, их тяжесть должна определяться с учетом конкретных обстоятельств дела: имущественный ущерб, сопряженный с восстановлением информации; упущенная выгода при срыве заключения крупного контракта или соглашения; дезорганизация работы предприятий или учреждений и т.п. Форма вины по отношению к тяжким последствиям может быть только неосторожной.

Объективная сторона выражается в совершении одного из следующих действий:

- создание вредоносной программы, приводящей к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети;

- внесение изменений в существующие программы, заведомо приводящие к указанным последствиям;

---

[1] Ляпунов Ю.И., Максимов С.В. Указ. соч. С.12.

[2] О правовой охране программ для электронных вычислительных машин и баз данных: Закон Российской Федерации от 23 сентября 1992 г. № 3523-I // Российская газета. 1992. 20 октября.

[3] Комментарий к Уголовному кодексу Российской Федерации / под общ. ред. Ю.И. Скуратова и В.М. Лебедева. С. 704.

[4] Комментарий к Уголовному кодексу Российской Федерации [Электронный ресурс]. URL: http://rfuk.ru/comment_273.html (дата обращения: 15.01.2021).

- использование вредоносной программы или машинного носителя с такой программой;

- распространение вредоносной программы или машинного носителя с такой программой.

Субъективная сторона преступления, содержащегося в ч. 1 ст. 273 УК РФ, выражается только в прямом умысле, то есть лицо осознает общественную опасность своих деяний, предвидит возможность наступления общественно-опасных последствий и желает их наступления. Для данного преступления характерен признак заведомости – очевидность для виновного того, что созданная им программа может причинить указанные в законе общественно-опасные последствия. Если же лицо не знало об опасности распространяемых им программ, то лицо не должно быть подвергнуто уголовному преследованию.

Помимо «компьютерного вируса» к вредоносным можно отнести также и такие программы, как «троянский конь», «логическая бомба», «люк» и другие. Такие средства не способны к воспроизведению, и внесенные в компьютерную систему они лишь ожидают наступления определенного времени или наступления определенных условий.[1]

Непосредственным объектом данного преступления является неприкосновенность и стабильность компьютерной информации и ее материального носителя – ЭВМ.

Предлагаем рассмотреть примеры выявленных преступлений, раскрытых в тесном взаимодействии сотрудников Управления «К» со службой безопасности ОАО «Сбербанка России» и ЦИБ ФСБ России, взятые из практики.

В результате проделанной работы сотрудниками БСТМ МВД России во взаимодействии со Службой безопасности ОАО «Сбербанка России» пресечена противоправная деятельность членов организованной преступной группы, причастных к более чем 200 хищениям, совершенным с использованием вредоносной программы «Stels APK», нацеленной на компроментацию профессиональных данных, размещенных на планшетах и телефонах под управлением оперативной системы Android. Данная вредоносная программа после успешного внедрения на устройство пользователя скрытно осуществляла отправку СМС – сообщения на номер «900» (технический номер ОАО «Сбербанка России») с затребованием баланса счета пользователя, после чего пересылала полученный ответ на сервер злоумышленников, в последующем осуществляла переводы денежных средств с банковского счета на заранее подготовленные счета мобильных телефонов и банковских карт, подконтрольные преступникам.

В целях разоблачения преступной деятельности подозреваемого лица БСТМ МВД России совместно с ЦИБ ФСБ России в целях декриминализации сетей связи осуществлен комплекс организационных, оперативно-розыскных и специальных технических мероприятий в отношении жителя г. Ярославля гражданина Н., 1980 года рождения, специализирующегося на организации

[1] Смирнова Т.Г. Указ. соч. С. 26.

преступной деятельности в различных регионах Российской Федерации и Украины, связанной с разработкой, распространением и использованием вредоносных программ для операционной системы «Андроид» с целью последующего хищения денежных средств, привязанных к абонентским номерам сотовых телефонов банковских карт ОАО «Сбербанк России».

Распространение программы для ЭВМ возможно как в активной (внедрение вредоносной программы в ЭВМ, их систему или сеть любым способом, предоставляющим свободный доступ к ней), так и пассивной формах (невоспрепятствование самораспространению вредоносной программы или распространению ее третьими лицами).

Распространение машинного носителя с программой для ЭВМ – это передача его третьим лицам в любой форме.[1]

Статья 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей».

Объектом преступления являются отношения в сфере обеспечения безопасности.

Субъектом преступления является лицо, имеющее законный доступ к эксплуатации упомянутых технических средств, достигшее 16 лет[2]. Это могут быть программисты, операторы ЭВМ, техники-наладчики и другие лица, имеющие к ним доступ по работе. О тяжких последствиях, наступивших по неосторожности, сказано выше в статье 273. Квалифицирующим признаком ч. 2 ст. 274 УК РФ является наступление тяжких последствий, а субъективная сторона характеризуется неосторожной формой вины по отношению к этим последствиям.

Объективную сторону преступления образует нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это причинило существенный вред[3].

Субъективную сторону характеризует преступление, которое может быть совершено как умышленно, так и по неосторожности в виде, как небрежности, так и легкомыслия. При установлении умысла на нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, предусмотренное ст. 274 УК РФ, становится лишь способом совершения преступления. Данное преступное деяние в этом случае подлежит квалификации по наступившим последствиям, которые предвидел виновный, по совокупности с преступлением, предусмотренным данной статьей УК РФ.

---

[1] Смирнова Т.Г. Указ. соч. С. 26.

[2] Комментарий к Уголовному кодексу Российской Федерации [Электронный ресурс]. http://rfuk.ru/comment_274.html (дата обращения: 15.01.2021).

[3] Там же.

Под охраняемой законом информацией следует понимать информацию, изъятую из публичного (открытого) оборота на основании закона, других нормативных (включая ведомственные) актов, а также правил внутреннего распорядка, основанных на упомянутых нормативных документах. По общему правилу такая информация имеет гриф ограниченного пользования[1].

Правила эксплуатации компьютерной системы – это правила одной из перечисленных ниже разновидностей:

- правила, содержащиеся в общих требованиях по технике безопасности и эксплуатации компьютерного оборудования;
- правила, установленные изготовителями компьютерного оборудования;
- правила, установленные разработчиками программного обеспечения;
- правила внутреннего распорядка, установленные владельцами компьютерной системы или сети и т.д.

Нарушение этих правил (несоблюдение, ненадлежащее соблюдение, либо прямое несоблюдение) может быть осуществлено как путем активного действия, так и бездействия. Состав ч. 1 ст. 274 УК РФ сформулирован как материальный. При этом общественно опасные последствия заключаются в одновременном наличии двух факторов:

1) уничтожении, блокировании или модификации охраняемой законом информации в ЭВМ;
2) вызванного этим существенного вреда.

Нарушения правил эксплуатации могут выражаться в блокировке системы защиты от несанкционированного доступа, нарушении правил электро- и противопожарной безопасности, отключении сигнализации, длительном оставлении без присмотра, нарушении температурного режима в помещении, неправильном подключении ЭВМ к источникам питания, нерегулярном техническом обслуживании, нарушении порядка ведения диалога с компьютером и т.д.

Из рассмотренного следует, что если преступления, квалифицируемые статьей 272 УК РФ «Неправомерный доступ к компьютерной информации», а также статьей 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», осуществляются только путём совершения действий, то преступления, квалифицируемые статьей 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» – путём как действий, так и бездействием.

Неправомерный доступ к компьютерной информации и нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей сформулированы как преступления с материальным составом, а создание либо использование вредоносных программ для ЭВМ – с формальным. В качестве последствий в статьях 272 и 274 УК РФ указываются: уничтожение, модификация,

---

[1] Комментарий к Уголовному кодексу Российской Федерации [Электронный ресурс]. http://rfuk.ru/comment_274.html (дата обращения: 15.01.2021).

блокирование либо копирование информации, нарушение работы ЭВМ или системы ЭВМ, причинение существенного вреда и т. п.

Статья 274.1. УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

1. Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации.

2. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации.

3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации.

4. Деяния, предусмотренные частью первой, второй или третьей настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения.

5. Деяния, предусмотренные частью первой, второй, третьей или четвертой настоящей статьи, если они повлекли тяжкие последствия.

Прежде чем проанализировать данную статью, необходимо обратиться к **статье 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ, которая определяет следующие основные понятия**:

Критическая информационная инфраструктура – это объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Объекты критической информационной инфраструктуры – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Порядок и правовые критерии отнесения объектов к критической информационной инфраструктуре России определяется упомянутым Федеральным законом № 187–ФЗ.

Субъекты критической информационной инфраструктуры – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Безопасность критической информационной инфраструктуры – состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении нее компьютерных атак.

Рассмотрев данные ключевые понятия, предлагаем проанализировать ст. 274.1 УК РФ.

В данном случае предмет преступления – это вещь, элемент материального мира, на который осуществляется воздействие в ходе совершения преступления.

Предметом преступлений, предусмотренных настоящей статьей, является критическая информационная инфраструктура Российской Федерации, в том числе составляющие её объекты – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, сети электросвязи, относящиеся к критической информационной инфраструктуре Российской Федерации, а также охраняемая компьютерная информация, содержащаяся в критической информационной инфраструктуре Российской Федерации.

Объект преступления – один из элементов состава преступления, представляющий собой общественные институты, которым причиняется ущерб вследствие совершения преступления.

Объектом преступления в данной статье является безопасность критической информационной инфраструктуры Российской Федерации, т.е. состояние защищенности, обеспечивающее её устойчивое функционирование при

проведении в отношении неё компьютерных атак. Поскольку критическая информационная инфраструктура Российской Федерации может функционировать в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, объектом может быть информационная безопасность в любой сфере деятельности государства и общества.

Объективная сторона преступления – один из элементов состава преступления, представляющий собой внешнее проявление преступления в реальной действительности.

К числу признаков объективной стороны относятся:

- общественно опасное деяние (действие или бездействие, посягающее на тот или иной объект);
- общественно опасные последствия;
- причинно-следственная связь между действием (бездействием) и последствиями;
- способ, место, время, обстановка, средства и орудия совершения преступления.

Объективная сторона по части 1 статьи 274.1 УК РФ характеризуется действиями, состоящими в создании, распространении и (или) использовании компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации.

Состав преступления по части 1 статьи 274.1 УК РФ – **формальный**, т.е. преступление является оконченным в момент совершения любого из перечисленных действий: создания, распространения или использования соответствующих программ, вне зависимости от его последствий.

Объективная сторона по части 2 статьи 274.1 УК РФ заключается в неправомерном доступе к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации.

Преступление в этой форме имеет **материальный состав**, т.е. считается оконченным при наступлении общественно опасных последствий – причи-

нение вреда критической информационной инфраструктуре Российской Федерации.

Объективная сторона по части 3 статьи 274.1 УК РФ выражается в действиях или бездействии, выражается в нарушении правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи.

Преступление в этой форме имеет материальный состав – является оконченным с наступлением последствий в виде причинения вреда критической информационной инфраструктуре Российской Федерации.

Объективная сторона по части 4 статьи 274.1 УК РФ предусматривает те же деяния, предусмотренные частью 1, 2 или 3 настоящей статьи, однако, в качестве **отягчающего, квалифицирующего признака** указывает на совершение данного преступления группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения.

Согласно ч. 2 ст. 35 УК РФ преступление признается совершенным группой лиц по предварительному сговору, если в нем участвовали лица, заранее договорившиеся о совместном совершении преступления.

Согласно ч. 3 ст. 35 УК РФ преступление признается совершенным организованной группой, если оно совершено устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений.

Под совершением преступления лицом с использованием своего служебного положения следует понимать совершение преступного деяния лицом постоянно, временно или по специальному полномочию осуществляющим функции представителя власти или выполняющим организационно-распорядительные, административно-хозяйственные функции в государственном органе, органе местного самоуправления, государственном или муниципальном учреждении, государственной корпорации, государственных компаниях, государственных и муниципальных унитарных предприятиях, акционерных обществах, контрольный пакет акций которых принадлежит Российской Федерации, субъектам Российской Федерации или муниципальным образованиям, а также в Вооруженных Силах Российской Федерации, других войсках и воинских формированиях Российской Федерации, путем злоупотребления или превышения своих служебных полномочий.

Объективная сторона по части 5 статьи 274.1 УК РФ определяет те же деяния, предусмотренные частью 1, 2, 3 или 4 настоящей статьи, однако ука-

зывает на наступление тяжких последствий (квалифицированный, а также материальный состав преступления).

Субъективная сторона преступления – это психическое отношение лица к совершаемому им преступлению, которое характеризуется конкретной формой вины, мотивом и целью.

Субъективная сторона преступлений, предусмотренных частями 1 и 2, характеризуется **прямым умыслом** (ст. 25 УК РФ – Преступление признается совершенным с прямым умыслом, если лицо **осознавало** общественную опасность своих действий (бездействия), **предвидело** возможность или неизбежность наступления общественно опасных последствий и **желало** их наступления), а деяние, предусмотренное частью 3, может совершаться и **по неосторожности** (ст.26 УК РФ – Преступлением, совершенным по неосторожности, признается деяние, совершенное по легкомыслию или небрежности).

Субъект преступления – это лицо, совершившее предусмотренное уголовным законом общественно опасное деяние и способное нести за него уголовную ответственность.

Субъект преступления – вменяемое физическое лицо, достигшее 16-ти лет на момент совершения преступления.

Субъект преступления, предусмотренного частью 3, — специальный: лицо, на которое возложена обязанность соблюдать правила эксплуатации соответствующих средств, систем и сетей, а также обязанность соблюдать правила доступа к соответствующим информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи.

Условно, все преступления в сфере телекоммуникаций и компьютерной информации можно разделить на 2 категории:

1. Преступления, связанные с противоправным вмешательством в работу компьютеров:

- неправомерный доступ к компьютерной информации;
- разработка и распространение компьютерных вирусов;
- ввод в программное обеспечение вредоносных программ;
- преступная небрежность в нарушении правил эксплуатации ЭВМ, систем ЭВМ или их сетей;
- хищение компьютерной информации;
- уничтожение компьютерной информации;
- подделка компьютерной информации.

Рассмотрим перечисленные виды более детально.

Неправомерный доступ к компьютерной информации.

Неправомерный доступ к компьютерной информации осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспече-

ния, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Хакеры или компьютерные пираты – так называют компьютерных правонарушителей, осуществляющих противоправный несанкционированный доступ в чужие информационные сети.

Несанкционированный противоправный доступ к файлам и информации законного пользователя осуществляется также нахождением слабых мест в компьютерной защите системы. Однажды обнаружив их, преступник может не спеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней много раз, подобно покупателю, изучающему товары на витрине.

Программисты иногда допускают ошибки в программах, которые не удается обнаружить в процессе их написания и дальнейшего применения. Авторы больших сложных программ могут не заметить некоторых слабостей компьютерной логики. Уязвимые места иногда обнаруживаются и в электронных цепях. Все эти небрежности, ошибки приводят к появлению возможности совершения противоправного деяния. Обычно они все-таки выявляются при проверке, редактировании, отладке программы, но абсолютно избавиться от них невозможно.

Бывает, что правонарушитель проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам, по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т.п.), оказываются без защиты против этого способа совершения преступления. Самый простейший путь его осуществления – это получить коды и другие идентифицирующие шифры законных пользователей. Это возможно путем:

- приобретения (обычно подкупом персонала) списка пользователей со всей необходимой информацией;

- обнаружения такого документа в организациях, где не налажен достаточный контроль за их хранением;

- незаконного, несанкционированного подслушивания через телефонные линии.

Разработка и распространение компьютерных вирусов.

Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Известны случаи, когда вирусы блокировали работу организаций и предприятий. Более того, несколько лет назад был зафиксирован случай, когда **компьютерный вирус стал причиной гибели человека.** В одном из госпиталей Нидерландов пациент получил летальную дозу морфия по той причине, что компьютер был заражен вирусом и выдавал неверную информацию (вирус произвёл модификацию).

Компьютерный вирус – это специально написанная, как правило, небольшая по размерам программа, которая может записывать (внедрять) свои копии (возможно, изменённые) в компьютерные программы, расположенные

в исполняемых файлах, системных областях дисков, драйверах, документах и т.д., причём эти копии сохраняют возможность к «размножению». Процесс внедрения вирусом своей копии в другую программу (системную область диска и т.д.) называется *заражением,* а программа или иной объект, содержащий вирус, – *заражённым.*

Ввод в программное обеспечение вредоносных программ. Одним из типов вредоносных программ является «логическая» бомба. Если ей создать некоторые условия, то **она может полностью или частично повредить** систему компьютерной сети. Одной из разновидностей вредоносных программ является «временная бомба». Она начинает свое пагубное действие при достижении определенного временного периода. Данный преступный метод заключается в несанкционированном проникновении вышеперечисленных вредоносных программ в лицензионную. Эти программы **порождают абсолютно новые функции**, не запланированные владельцем, которые не вредят работе старым. Таким образом, лица криминальной направленности, используя возможности вредоносных программ, перечисляют денежные суммы на свои, временно открытые банковские счета. В связи с тем, что **содержание вирусной программы** в своем текстовом обличии **весьма многогранно** и имеет **огромное количество** команд, их определение, естественно, требует большого профессионализма лиц, имеющих навыки в данной области.

В настоящее время нашла свое место еще одна *разновидность вредоносной программы*. Сущность ее проявления определяется в ходе производства определенных команд, порождающих другие команды, а по завершению их происходит уничтожение предыдущих. Отыскание такой вредоносной программы весьма затруднительно, так как необходимо в данном случае искать **специально** разработанную команду, например, в виде «**троянского коня**», а не вредоносную программу.

Имеется еще одна *разновидность вредоносных программ*. Ее особенность заключается в том, что в обычную часть программы вставляются команды, формирующие другие команды и после выполнения уничтожающие их. В этом случае программисту, пытающемуся найти вредоносную программу, необходимо искать не ее саму, а команды, ее формирующие. Развивая эту идею, можно представить себе вредоносные команды, которые создают команды и т.д. (сколь угодно большое число раз), создающие вредоносную программу по типу «троянского коня».

Преступная небрежность в нарушении правил эксплуатации ЭВМ, систем ЭВМ или их сетей.

В данном случае всегда необходимо соблюдать правила бережного использования компьютерной техники, так как при несоблюдении этого требования может произойти технологичный сбой в ее работе. При использовании компьютерной техники или при транспортировке необходимо быть предельно

внимательным и оберегать ее от различного рода повреждений, так как возможные последствия равноценны неосторожной вине.

В связи с тем, что в настоящее время разработкой нового программного обеспечения занимаются лица, цель которых направлена не только на правомерное ее использование и получение эффективных показателей, но и на достижение абсолютно противоположных замыслов, **поэтому разработать совершенно неуязвимое программное обеспечение практически невозможно**. Ведь на всякий яд, при желании, можно найти свое противоядие.

Хищение компьютерной информации.

Следует заметить, что классифицировать преступление в виде хищения компьютерной информации согласно нормам действующего уголовного законодательства достаточно проблематично.

Когда похищается компьютерная информация, не обязательно злоумышленники ее удаляют у объекта преступления, а воспользуются лишь функцией копирования. Таким образом, **совершается хищение необходимой информации**, в результате чего законному пользователю **наносится значительный вред**.

Уничтожение компьютерной информации.

Когда субъект преступления путем незаконного внедрения в компьютерную сеть чужого пользователя копирует себе информацию, а затем ее уничтожает у законного пользователя, последнему наносится существенный вред. Для восстановления уничтоженной информации законному пользователю приходится изыскивать имеющиеся возможности по восстановлению украденной информации путем специальных компьютерных программ. В случае обнаружения злоумышленника и доказывания его преступной деятельности он будет нести ответственность согласно нормам действующего законодательства.

В тех случаях, когда недоброжелатели путем несанкционированного доступа внедряются в чужую компьютерную сеть, ознакомившись с информацией, под любым предлогом переименовывают файл или создают новую версию изначального файла, то данное действие не будет являться уничтожением имеющейся ранее информации.

При блокировании информации она не уничтожается, но к ее доступу искусственно **создается затруднение**, в связи с чем воспользоваться ею не всегда возможно.

Подделка компьютерной информации.

Этот вид компьютерной преступности является разновидностью несанкционированного доступа с той разницей, что пользоваться им может, как правило, не посторонний пользователь, а сам разработчик, имеющий достаточно высокую квалификацию в области компьютерных технологий.

Масса пользователей, получая искаженную информацию, формируют в своем сознании представление об окружающей действительности в заданном

злоумышленником направлении. Соответственно формируется и поведение, которое будет соответствовать желаниям самого объекта манипуляции. В результате подделывания компьютерной информации пользователи будут думать, что они самостоятельно делают свой выбор, однако выбор за них делают те, кто ими управляют, т.е. злоумышленники.

Примером подделки компьютерной информации является гонка предвыборных компаний, при подсчете результатов всевозможных голосований. Об этом красноречиво свидетельствует проведение предвыборной президентской компании подсчета голосов в США.

2. Преступления, совершаемые с использованием ЭВМ (преступления, в которых компьютер является средством достижения цели):

- разработка сложных математических моделей, которые в последующем будут использованы при осуществлении преступного замысла злоумышленника;

- ввод в программное обеспечение «логических бомб»;

- «логические бомбы» – программы, которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя программное обеспечение компьютерной системы;

- преступления с общим названием «воздушный змей» и др.

Рассмотрим пример данного вида преступления. В нескольких банках открывают небольшие счета, и деньги «перегоняются» из одного банка в другой и обратно с естественной процентной надбавкой. Цель данной финансовой махинации направлена на то, чтобы информация о сумме перевода в первый банк доставлялась быстрее, чем поступающее платежное поручение из другого банка, до того, как будет обнаружено, что перевод не обеспечен необходимой денежной суммой. Данные денежные манипуляции осуществляются неоднократно, с каждым разом увеличивая конечную сумму, пока процентная ставка денежных переводов не будет устраивать преступников и их преступный замысел не будет удовлетворен. В результате достижения преступной цели деньги с конечного счета присваиваются мошенниками, которые впоследствии скрываются. В данной афере, чем больше задействовано количество банков, тем больше и быстрее накапливается желаемая денежная сумма. Такой вид совершения преступления возможен при осуществлении операций при помощи компьютера.

Некоторые инструменты и способы (средства) совершения преступлений в сфере компьютерной информации:

Вирус – компьютерная программа, находящаяся на компьютере пользователя без его ведома и выполняющая какое-либо действие, чаще всего деструктивное (удаление, перемещение, изменение файлов).

ADWARE – компьютерная программа, находящаяся на компьютере пользователя без его ведома, не несущая деструктивных действий, ее вред выражается в навязчивом показе пользователю рекламы путем изменения

стандартной страницы браузера, показа всплывающих окон, баннеров, переадресация на другие сайты.

Spyware – компьютерная программа, находящаяся на компьютере пользователя без его ведома и не несущая деструктивных действий, ее вред выражается в шпионских действиях против вас (пользователя), с целью получения паролей и другой личной информации.

Удаленная атака – это негативное информационное воздействие, направленное на распределенную вычислительную систему, осуществляемое программным образом по каналам связи.

Скимминг – кража данных с электронной банковской карты при помощи специального считывающего устройства (скиммера). (см. рис. 2)

Рис. 2. Один из видов устройства скимминга

В настоящее время к наиболее активным видам преступлений, совершаемым в сети ИНТЕРНЕТ (киберпреступлений), необходимо отнести стремительно развивающийся «FISHING» – поддельные письма якобы от имени банков или платежных Интернет-систем, с просьбой к клиентам сообщить данные для авторизации и доступа к их персональной информации. В случае если пользователь оставляет свои данные, то они используется мошенниками для немедленного снятия с его счета имеющихся денежных средств. Данный вид преступления активно внедрен и применяется преступниками в сетях операторов сотовой связи.

Используемые или предполагаемые меры, при помощи которых возможно разоблачение преступника:

Разоблачение

Основными средствами идентификации пользователя (в том числе и киберпреступника) в сети Интернет является его IP–адрес (уникальный адрес

регистрации абонента в сети Интернет, может быть как статическим, так и динамическим) и MAC–адрес (уникальный идентификатор, присваиваемый каждой единице активного оборудования (устройства) или некоторым их интерфейсам в компьютерных сетях Ethernet). Информацию об указанных данных можно получить посредством СОРМ либо на прямую у провайдера (фирма, предоставляющая пользователю доступ в Интернет).

В подразделение «К» Северной Осетии поступила информация о том, что у гр-на Сидорова всю ночь снимались с его лицевого счета денежные суммы, о которых автоматически передавалась информация путем смс на его телефон.

Данный гражданин Сидоров обратился в письменном виде в Сбербанк, где ему было сказано, что в недалеком прошлом к его текущему счету были привязаны через «мобильный банк» два абонентских телефонных номера. Один из этих ранее привязанных номеров принадлежит ему самому, а другой телефонный номер принадлежал его бывшей супруге Ивановой Н.В.

После этого Сидоров обращается в полицию с заявлением о том, что с его лицевого банковского счета похищены деньги в размере 50000 рублей. В ходе проведения проверочных действий по факту хищения денежных средств с лицевого банковского счета заявителя был установлен номер сотового телефона, ранее принадлежащий его бывшей супруге Ивановой Наталье Владимировне. В ходе беседы с ней было выяснено, что она данным телефонным номером уже давно не пользуется, так как потеряла сим-карту и приобрела новую с другим телефонным номером. Об этом она нигде ранее не сообщала.

В процессе отработки полученной информации был установлен ранее принадлежащий бывшей супруги Ивановой телефонный номер.

В ходе проведения соответствующих мероприятий был установлен IMEI – код телефона, а так же были установлены лица, у которых таким же способом систематически снимались с лицевых банковских счетов денежные суммы. В процессе проведенного глубокого анализа поступающей информации о совершаемых преступлениях путем снятия денежных сумм с лицевых банковских счетов клиентов в поле зрения попали большое количество сим-карт и мобильные сотовые телефоны, которые использовались при совершении преступлений.

Далее в ходе отработки лиц, причастных к совершению преступлений, был установлен факт активной работы мобильного телефона. По данному мобильному телефону было проведено соответствующее мероприятие, в ходе которого была получена информация о причастности лиц, ведущих с этих телефонов постоянные переговоры.

Затем были установлены места их проживания. Лица, причастные к содеянным преступлениям, были задержаны.

В результате совершения данных преступлений пострадало около 20 человек и ущерб от совершения хищений денежных средств превысил 3 млн рублей.

По данному факту было возбуждено уголовное дело по ч. 4 ст. 159 УК РФ и виновные лица осуждены к 10 годам лишения свободы.

Защита компьютерной информации и данных

Защита данных, защита информации – совокупность мер, обеспечивающих защиту прав собственности владельцев информационной продукции, в первую очередь – программ, баз и банков данных от несанкционированного доступа, использования, разрушения или нанесения ущерба в какой-либо иной форме.

Уже в первых публикациях по защите информации были изложены **основные постулаты**, которые не утратили своей актуальности и по сей день.

Первый постулат гласит: абсолютно надежную, непреодолимую защиту создать нельзя. Система защиты информации может быть в лучшем случае адекватна потенциальным угрозам. Поэтому при планировании защиты необходимо представлять, кого и какая именно информация может интересовать, какова ее ценность для вас и на какие финансовые жертвы ради нее способен пойти злоумышленник.

Из первого постулата вытекает второй: система защиты информации должна быть комплексной, т.е. использующей не только технические средства защиты, но также административные и правовые.

Третий постулат состоит в том, что система защиты информации должна быть гибкой и адаптируемой к изменяющимся условиям. Главную роль в этом играют ***административные*** (или организационные) мероприятия – такие, например, как

– регулярная смена паролей и ключей,

– строгий порядок их хранения,

– анализ журналов регистрации событий в системе,

– правильное распределение полномочий пользователей и многое другое.

Человек, отвечающий за все эти действия, должен быть не только преданным сотрудником, но и высококвалифицированным специалистом, как в области технических средств защиты, так и в области вычислительных средств вообще.

Сегодня известно много мер, направленных на **предупреждение** преступлений в сфере телекоммуникаций и компьютерной информации. Выделим из них три:

- технические,

- правовые,

- организационные.

К техническим мерам можно отнести:

• защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем;

• организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев;

• установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды;

• принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов;

• установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

К правовым мерам следует отнести:

• разработку норм, устанавливающих ответственность за компьютерные преступления,

• защиту авторских прав программистов,

• совершенствование уголовного и гражданского законодательства, а также судопроизводства.

К организационным мерам относят:

• охрану вычислительного центра;

• тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком;

• наличие плана восстановления работоспособности центра после выхода его из строя;

• организацию обслуживания вычислительного центра посторонней организацией или лицами, не заинтересованными в сокрытии фактов нарушения работы центра;

• универсальность средств защиты от всех пользователей (включая высшее руководство);

• возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п.

Перечислим **основные способы защиты**:

• наличие актуального антивирусного программного обеспечения, установленного на ЭВМ пользователя. В настоящее время лидерами рынка антивирусного программного обеспечения являются:

- лаборатория Касперского;
- корпорация ESET;
- фирма McCAFE;

• использование различных видов межсетевых экранов (файрволов), программного обеспечения, предназначенного для настройки операционной системы в целях повышения уровня сетевой безопасности при взаимодействии различных сетевых приложений (исключение уязвимости операционной системы);

• установка аппаратных средств защиты направлена на использование различных систем аппаратной защиты ЭВМ от несанкционированного доступа (например, система электронных ключей);

• использование всевозможных видов шифрования информации выражается в шифровании информации на ЭВМ пользователя (например, присвоение парольной защиты архивам и документам пользователя);

• резервирование особо важных компьютерных подсистем;

• организация вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев;

• постоянное обновление операционной системы.

Контрольные вопросы

1. Что такое телекоммуникационные системы?
2. Что такое документированная информация?
3. Какие криминалистические особенности имеют преступления, совершаемые в телекоммуникационных сетях?
4. В какой главе УК РФ отражены статьи, относящиеся к преступлениям, совершаемых в сфере компьютерной информации?
5. Перечислите номера статей и их названия.
6. Какие некоторые характерные особенности включают в себя преступления, совершаемые в телекоммуникационных сетях?
7. Какой можно сделать вывод, исходя из особенностей преступлений, совершаемых в телекоммуникационных сетях?
8. Разделяете ли Вы мнение И.Г. Чекунова, который говорит, что в настоящее время все большее количество государств ставит перед собой в качестве приоритетной цели создание информационного общества на основе широкого внедрения телекоммуникационных технологий? Если да, то обоснуйте свою точку зрения.
9. Что является предметом преступлений, совершаемых в сфере телекоммуникационных сетей?
10. Какие вы знаете способы совершения преступлений в телекоммуникационных сетях?
11. Что является непосредственным объектом данных преступных деяний?
12. Что является объективной стороной компьютерных преступлений и, в частности, преступлений, совершаемых в телекоммуникационных сетях?
13. Что является субъективной стороной компьютерных преступлений, а также преступлений, совершаемых в телекоммуникационных сетях?
14. Что является субъектом компьютерного преступления?
15. Что вызывает необходимость в существенных дополнениях Главы 28 УК РФ?
16. Что вызывает сложность при отграничении одних составов преступлений от других при квалификации преступной лиц, совершивших преступления в сфере телекоммуникаций и компьютерной информации?
17. Какая информация является «охраняемой законом информацией»?
18. Перечислите правила эксплуатации компьютерной системы.
19. Назовите факторы общественно опасных последствий заключающиеся как путем активного действия, так и бездействия при несоблюдении правил эксплуатации компьютерной системы.
20. На какие категории условно можно разделить все преступления в сфере телекоммуникаций и компьютерной информации?
21. Назовите основные виды преступлений, связанных с противоправным вмешательством в работу компьютеров.

22. Назовите основные виды преступлений, совершаемых с использованием ЭВМ (преступления в которых компьютер является средством достижения цели).

23. Назовите основные постулаты по защите информации.

24. Перечислите меры, направленные на предупреждение преступлений в сфере телекоммуникаций и компьютерной информации.

25. Какие компании и фирмы являются лидерами рынка антивирусного программного обеспечения?

ГЛАВА II
РАСКРЫТИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СФЕРЕ ТЕЛЕКОММУНИКАЦИЙ И КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В настоящее время невозможно представить функционирование любого министерства, ведомства, управления, какой-любо организации или компании без современного информационного-телекоммуникационного обеспечения. В этих целях для эффективного функционирования выше названных организаций ведется постоянная работа по подбору квалифицированных кадров. Принятые на работу сотрудники должны обладать специальными знаниями по использованию возможностей современных информационных сетей. Однако не всегда отдельные руководители, а также сотрудники уделяют должное внимание безопасности накапливаемой информации, что создает благоприятные условия и возможности для различных несанкционированных проникновений злоумышленников к данной информации посредством создания различных вредоносных программ и компьютерных вирусов. Впоследствии вирусописатели, в большинстве случаев имея корыстный замысел, совершают завуалированными действиями преступления в сфере телекоммуникаций и компьютерной информации.

Как было сказано ранее, данные преступления носят скрытый характер, и для их своевременного раскрытия необходим высокий профессиональный уровень подготовки сотрудников отдельных оперативных и следственных подразделений органов внутренних дел. Так как рассматриваемые преступления носят изощренный характер, оперативным сотрудникам необходимо иметь специальные знания в сфере телекоммуникаций и компьютерной информации. Предлагаем рассмотреть некоторые виды вредоносных программ и компьютерных вирусов.

2.1. ВРЕДОНОСНЫЕ ПРОГРАММЫ И КОМПЬЮТЕРНЫЕ ВИРУСЫ

По экспертным оценкам исследовательской группы «CNews Analytics», общее число частных пользователей систем дистанционного банковского обслуживания в России по состоянию на начало 2016 года составляло около 90 миллионов человек, в 2017 году составило 108,48 миллионов человек, в 2018 году – 133,6 миллиона, в 2019 году – 150,1 миллиона человек, в 2020 году – 168 миллионов человек и в 2021 году – 170 миллионов человек (см. диаграмму 3). Эксперты прогнозируют, что в ближайшие годы подключение пользователей к системе российского рынка ДБО (дистанционное банковское обслуживание) будет только расти. Уверенный рост рынка будет обусловлен

как распространением банковских продуктов среди населения, так и развитием сервисов дистанционного банковского обслуживания (см. диаграмму 4).[1]

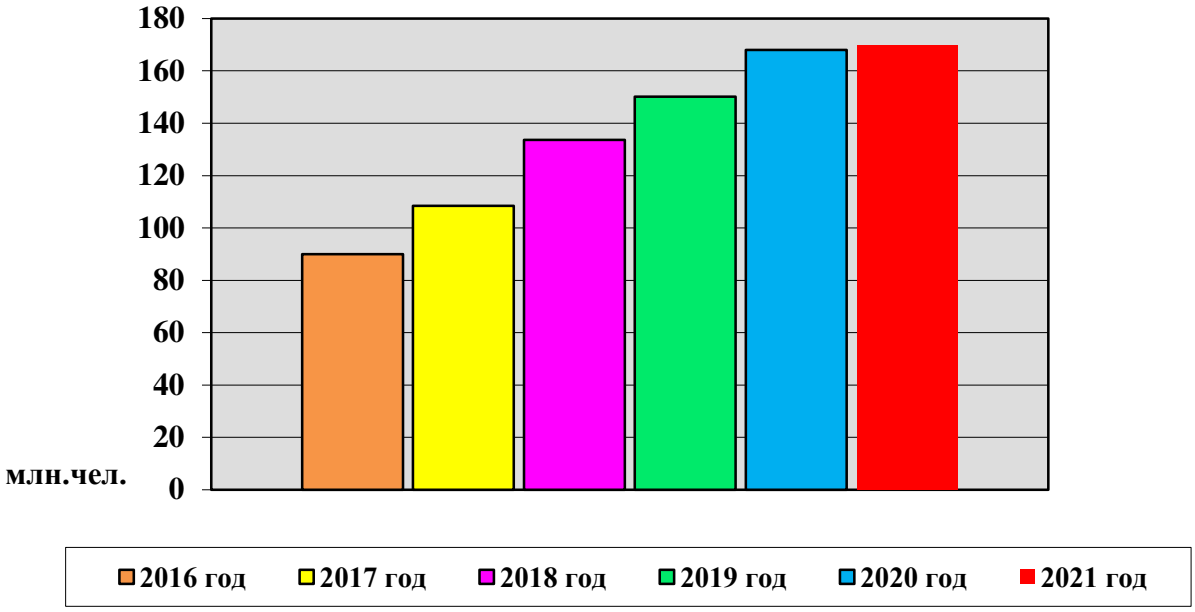


Диаграмма 3. Число частных пользователей систем дистанционного банковского обслуживания в России

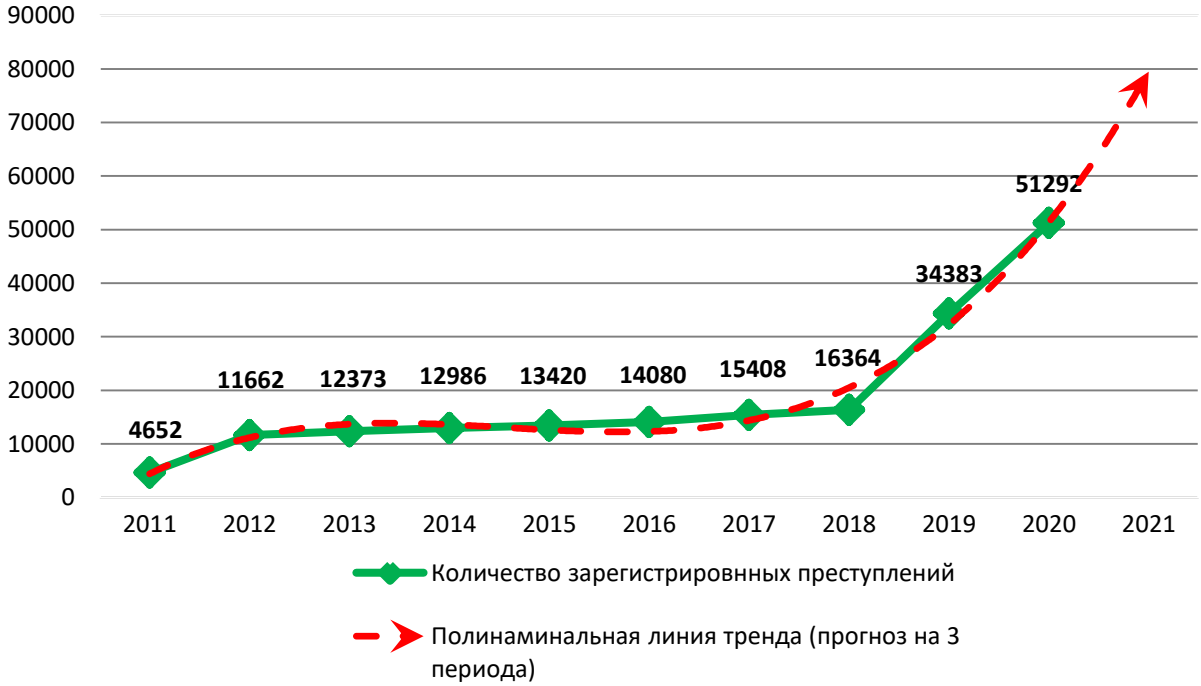


Диаграмма 4. Прогноз количества преступлений, совершаемых в системе ДБО[2]

[1] Научно-практический электронный журнал Аллея Науки. 2020. № 9 (25). URL: Alley-science.ru (дата обращения: 15.11.2021).

[2] Комплексный анализ состояния преступности в Российской Федерации, расчетные варианты ее развития.- ФГКУ «Всероссийский научно-исследовательский институт Министерства внутренних дел Российской Федерации». Москва, 2018.

Предлагаем рассмотреть конкретный пример, взятый из практической деятельности Управления «К» БСТМ МВД России.

Для стабилизации оперативной обстановки в сфере дистанционного банковского обслуживания, кардинга и платежных систем в октябре-декабре 2019 года БСТМ МВД России организован и проведен комплекс оперативно-розыскных и специальных технических мероприятий по выявлению и пресечению преступной деятельности членов международной преступной группы, в состав которой входил гражданин Украины Лысенко Юрий Сергеевич, 1987 года рождения.

Данная организованная преступная группа объединяла и координировала деятельность нескольких преступных групп, действовавших независимо друг от друга, но являвшихся звеньями последовательной цепи при совершении преступлений, инициировала целевые хакерские атаки не только на процессинговые центры отдельно взятых банков, но и на мировые системы обмена межбанковскими финансовыми сообщениями, создала и зарегистрировала по всем международным стандартам свою платежную систему «Multipayment systems», заключив партнерские соглашения с основными процессинговыми центрами нескольких стран, использовала для обналичивания похищенных денежных средств российские и европейские криминальные сервисы, способные за несколько часов привлечь до нескольких сотен человек.

В настоящее время доказана причастность данной группы к следующим хищениям денежных средств в ОАО «Промсвязьбанк» (ущерб 36 млн. руб.), ОАО «Уралсиб» (36 млн. руб.), ОАО НБ «Траст» (110 млн. руб.), ОАО «БанкЗенит» (ущерб 22 млн. руб.), а также к попытке похитить 882 млн руб. Кроме этого, данной группой предпринимались попытки совершить аналогичные хищения еще в двух десятках кредитных организаций, среди которых «Сбербанк России», «Росбанк», «Банк Москвы», «Газпромбанк», «Тинькофф» и др.

Компьютерная техника, изъятая у задержанных преступников, содержит информацию о сотнях хищений денежных средств, совершенных ими со счетов европейских и американских юридических лиц за период 2012-2018 гг., а также базы данных с указанием подготовленных для хищений реквизитов банковских карт европейских кардселлеровских проектов.

В настоящее время ведется работа по выявлению остальных эпизодов преступной деятельности данной группы.

В жизненных ситуациях лиц, пишущих вирусные программы, которые они затем используют при совершении преступлений в сфере телекоммуникаций и компьютерной информации, образно называют **хакерами**. Когда компьютеры только появились, слово «хакер» было уважительным. Его использовали для обозначения компьютерных гениев, способных переписать часть ядра операционной системы, чтобы она стала лучше работать или «сбросить» всеми забытый администраторский пароль. Хакеров уважали за умение нестандартно мыслить и находить разумные решения самым сложным проблемам.

Однако с течением времени оригинальное значение слова было утеряно, поскольку далеко не все «хакеры» ограничивались изменениями ядер ОС и восстановлением паролей по просьбам своих коллег. Некоторые из них начали вторгаться в плохо защищенные компьютерные системы, чтобы «доказать, что это возможно» и, наконец, перешли зыбкую границу взлома с целью кражи какой-либо важной информации или системных ресурсов.

Компьютерное сообщество, столкнувшееся с размыванием значения термина «хакер», ввело в обиход несколько дополнительных терминов, например, «script kiddie» и «cracker». Термин «script kiddie» используется для обозначения людей, не обладающих существенными познаниями в области хакерства и просто использующих для взлома чужие хакерские утилиты — скрипты, эксплойты и т.п. Термин «cracker» обозначает человека, находящегося где-то между script kiddie и хакером по уровню своих знаний. Он умеет взламывать программы и, например, избавляться от защиты от копирования, но недостаточно умен, чтобы самостоятельно находить новые уязвимости или писать хакерские утилиты.

Все еще более усложнилось, когда некоторые «кандидаты» в хакеры начали использовать хакерские утилиты, созданные кем-то другим, взламывать программы и воровать сервисы, в то же время, делая нечто общественно полезное, а «крэкеры» перестали ломать программы и удалять защиту от копирования, а принялись взламывать компьютеры в интернете. Из-за всех этих пертурбаций значение термина «хакер» стало гораздо менее «черно-белым», и в итоге были представлены термины «black hat», «white hat» и «grey hat».

Black hat — плохой, «черный» хакер, который взламывает программы и иные системы с целью кражи информации, запускает DDoS-атаки и крадет номера кредитных карт. «White hat», «белый» хакер, наиболее близок к оригинальному значению термина «хакер» — много знающий программист и эксперт по безопасности, использующий свои таланты чтобы помогать повышать безопасность компьютерных систем и ловить преступников. Где-то между ними находятся «grey hat», серые хакеры, которые занимаются всем понемногу.

Термины «хакер», «крэкер» и «script kiddie» часто используются в интернете и других средствах массовой коммуникации, хотя люди, занятые в области обеспечения информационной безопасности, предпочитают разделение хакеров на «белых» и «черных». Наконец, все эти термины субъективны, зависят от причастности пользующегося ими человека к одной или другой группе и могут провоцировать долгие споры о том, кто же на самом деле «черный», а кто — «белый» хакер.[1] Обычно хакеры используют схему двоичного кода.

---

[1] Материал электронной энциклопедии ЗАО «Лаборатория Касперского». URL: https://encyclopedia.kaspersky.ru/ (дата обращения: 20.12.2021).

Рис 3. Схема двоичного кода

Классификация компьютерных вирусов

Рассмотрим детально, что собой представляет указанная выше классификация (см. рис. 4).

Загрузочный вирус – компьютерный вирус, записывающийся в первый сектор гибкого или жёсткого диска и выполняющийся при загрузке компьютера с идущих после главной загрузочной записи (MBR), но до первого загрузочного сектора раздела. Перехватив обращения к дискам, вирус либо продолжает загрузку операционной системы, либо нет (MBR-Locker). Размножается вирус записью в загрузочную область других накопителей компьютера.

Простейшие загрузочные вирусы, находясь в памяти заражённого компьютера, обнаруживают в компьютере незаражённый диск и производят следующие действия:

- выделяют некоторую область диска и делают её недоступной для операционной системы;
- замещают программу начальной загрузки в загрузочном секторе диска, копируя корректную программу загрузки, а также свой код в выделенную область диска;
- организуют передачу управления так, чтобы вначале выполнялся код вируса и лишь затем – программа начальной загрузки.

Загрузочные вирусы очень редко «уживаются» вместе на одном диске по причине того, что используют (возможно) одни и те же дисковые сектора для размещения своего кода/данных. В результате код/данные первого вируса

оказываются испорченными при заражении вторым вирусом, и система либо отказывает в обслуживании, либо зацикливается при загрузке операционной системы.

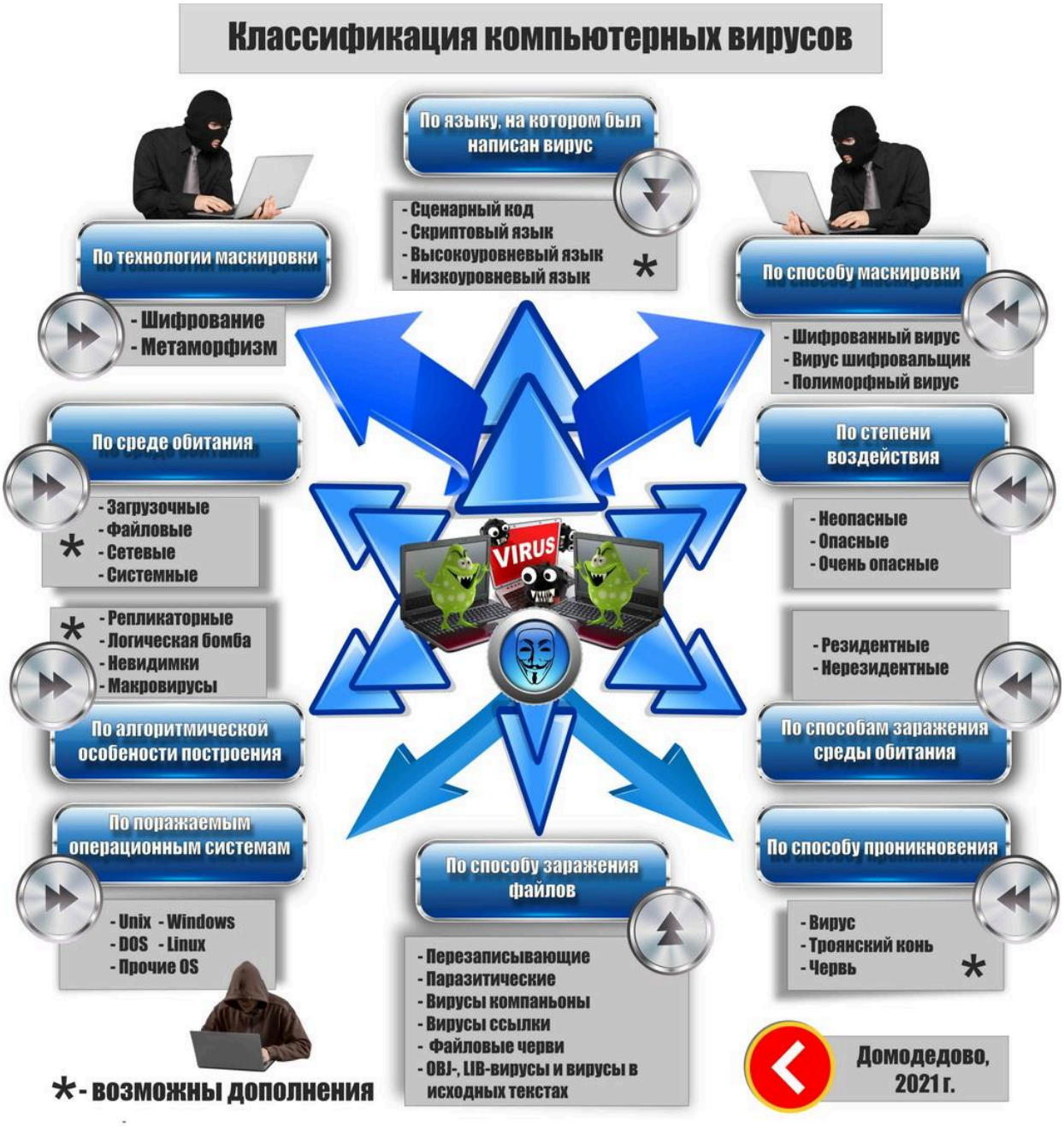


Рис. 4. Классификация современных компьютерных вирусов

Файловый вирус (англ. File infector) – компьютерный вирус, который для своего размножения использует файловую систему, внедряясь в исполняемые файлы практически любой ОС.

Объектом вирусного поражения могут выступать исполняемые двоичные файлы (EXE, COM), файлы динамических библиотек (DLL), драйверы (SYS), командные файлы (BAT, CMD) и тому подобные.

Заражая файл, вирус может внедриться в его начало, конец или середину. Наиболее распространенным способом заражения COM-программ для MS-DOS

является внедрение в конец файла. При этом основной код дописывается в конец файла, а в его начало записывается команда перехода к телу вируса.

Для вирусов, заражающих PE-программы для Windows, характерно размещение тела вируса либо в дополнительной секции, либо в пустых «хвостах» секций, либо в неиспользуемом пространстве между заголовком и секциями. Общая длина файла при этом может оставаться прежней. Похожими приемами пользуются и немногочисленные файловые вирусы, заражающие программы для операционных систем семейства UNIX (например, ELF-программы для Linux).

Чтобы скрыть своё присутствие в системе, файловый вирус может предварительно сохранить дату и время последней модификации и значения атрибутов заражаемого файла, восстановив эти данные уже после заражения.

После того как вирус получил управление, он выполняет следующие действия:

- восстанавливает в оперативной памяти компьютера исходную программу (или её необходимую часть) для последующего её выполнения;
- осуществляет дальнейшее заражение, инфицируя другие файлы или оперативную память компьютера;
- выполняет иные деструктивные действия, если это предусмотрено алгоритмом;
- при этом все действия вируса, как правило, незаметны для пользователя программы.

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Бытует ошибочное мнение, что сетевым является любой вирус, распространяющийся в компьютерной сети. Но в таком случае практически все вирусы были бы сетевыми, даже наиболее примитивные из них: ведь самый обычный нерезидентный вирус при заражении файлов не разбирается – сетевой (удаленный) это диск или локальный. В результате такой вирус способен заражать файлы в пределах сети, но отнести его к сетевым вирусам никак нельзя.

Системные вирусы проникают в системные модули и драйверы периферийных устройств, поражают программы-интер-претаторы.

В компьютерном мире существует особая группа вирусов, предназначенная для отказа системы генерации. Проявления могут быть разными: перезагрузка, зависание, некорректная работа приложений и другое.

Другими словами, программа-вирус умышленно запрограммирована для полной парализации компьютерной системы. Ввиду этого, удаление си-

стемного вируса, вероятно, произойдет вместе с полной переустановкой операционной системы.

На данный момент для операционных систем семейства Windows существуют целая группа вирусов, которая автоматически прописывается в автозагрузку. Узнать среди запущенных системой файлов конкретный вирус не так-то просто – название вражеского объекта является двойником настоящего файла.

Вирусы-репликаторы – вирусы, основная задача которых как можно быстрее размножиться по всем возможным местам хранения данных и коммуникациям. Зачастую сами не предпринимают никаких деструктивных действий, а являются транспортом для других видов вредоносного кода. Репликаторные программы благодаря своему быстрому воспроизводству приводят к переполнению основной памяти, при этом уничтожение программ-репликаторов усложняется, если воспроизводимые программы не являются точными копиями оригинала. В компьютерных сетях распространены программы-«черви». Они вычисляют адреса сетевых компьютеров и «записываются по ним», поддерживая между собой связь. В случае прекращения существования «червя» на каком-либо ПК оставшиеся отыскивают свободный компьютер и внедряют в него такую же программу.

Логическая бомба – программа, которая запускается при определённых временных или информационных условиях для осуществления вредоносных действий. Многие вредоносные программы, такие как вирусы или черви, часто содержат логические бомбы, которые срабатывают в заранее определённое время или при выполнении определённых условий, например, в пятницу 13-го, день смеха или в годовщину аварии на Чернобыльской АЭС (вирус CIH).

К логическим бомбам, как правило, относят код, который приводит к несообщённым заранее последствиям для пользователей. Таким образом, отключение определённой функциональности или окончание работы условно-бесплатных программ, после завершения установленного периода, не считается логической бомбой.

Логическая бомба может вызывать специфическую форму разрушения данных. Бомба активизируется только в случае выполнения какого-то условия. Например, логическая бомба может удалить все файлы любого числа. В отличие от вируса, логическая бомба не делает с себя копии.

Логические бомбы могут нанести нарушение следующих свойств информации с системой защиты: целостность, доступность и конфиденциальность.

Логическая бомба может быть доставлена адресату при помощи электронной почты вместе с вирусом или троянской программой.

Вирус-невидимка или Stealth-вирусы (Стэлс) – файловый вирус, остающийся «невидимым» для антивирусных программ. При проверке системы вирус-невидимка пытается перехватить запросы и выдать сфальсифицированный ответ, сигнализирующий, что все в порядке. Вирусы-невидимки являются разновидностью резидентных вирусов (постоянно находятся в опе-

ративной памяти). Stealth-вирусы фальсифицируют информацию, прочитанную из диска так, что программа, которой предназначена эта информация, получает неверные данные. Эта технология, которую, иногда, так и называют Stealth-технологией, может использоваться как в BOOT-вирусах, так и в файловых вирусах.

Стэлс-вирусы относятся к категории маскирующихся вирусов, которых очень сложно обнаружить.

Основы Stealth технологии

В основе работы Stealth-вирусов лежит тот факт, что операционная система при обращении к периферийным устройствам (в том числе, и к жестким дискам) использует механизм прерываний. При возникновении прерывания управление передается специальной программе – обработчику прерывания. Эта программа отвечает за ввод и вывод информации в/из периферийного устройства.

В такой системе изначально скрыта и уязвимость: управляя обработчиком прерываний, можно управлять потоком информации от периферийного устройства к пользователю. Stealth-вирусы, в частности, используют механизм перехвата управления при возникновении прерывания. Заменяя оригинальный обработчик прерывания своим кодом, stealth-вирусы контролируют чтение данных с диска.

В случае, если с диска читается зараженная программа, вирус «выкусывает» собственный код (обычно код не буквально «выкусывается», а происходит подмена номера читаемого сектора диска). В итоге пользователь получает для чтения «чистый» код. Таким образом, до тех пор, пока вектор обработчика прерываний изменен вирусным кодом, сам вирус активен в памяти компьютера, обнаружить его простым чтением диска средствами операционной системы невозможно. Схожий механизм маскировки используется и загрузочными вирусами.

Виды Stealth-вирусов

Известны стелс-вирусы всех типов – загрузочные вирусы, файловые DOS-вирусы и даже макровирусы.

Загрузочные стелс-вирусы для скрытия своего кода используют два основных способа. Первый из них заключается в том, что вирус перехватывает команды чтения зараженного сектора (INT 13h) и подставляет вместо него незараженный оригинал. Этот способ делает вирус невидимым для любой DOS-программы, включая антивирусы, неспособные «лечить» оперативную память компьютера. Основная идея заключается в том, что несмотря на то, что файл заражен, в оперативную память передаются данные незараженного файла (предварительно вылеченного самим вирусом).

Большинство файловых стелс-вирусов использует те же приемы, что приведены выше: они либо перехватывают DOS-вызовы обращения к файлам (INT 21h) либо временно лечат файл при его открытии и заражают при закрытии. Также как и для загрузочных вирусов, существуют файловые вирусы,

использующие для своих стелс-функций перехват прерываний более низкого уровня – вызовы драйверов DOS, INT 25h и даже INT 13h.

Реализация стелс-алгоритмов в макровирусах является, наверное, наиболее простой задачей – достаточно всего лишь запретить вызов меню File/Templates или Tools/Macro. Достигается это либо удалением этих пунктов меню из списка, либо их подменой на макросы FileTemplates и ToolsMacro. Частично стелс-вирусами можно назвать небольшую группу макровирусов, которые хранят свой основной код не в самом макросе, а в других областях документа – в его переменных или в Auto-text.

К наиболее известным Stealth-вирусам можно отнести такие вирусы, как Exploit.Macro.Stealth, Exploit.MSWord.Stealth, Virus.DOS.Stealth.551.

Макровирус – это разновидность компьютерных вирусов, разработанных на макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office. Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносятся из одного зараженного файла в другие. Большая часть таких вирусов написана для MS Word.

Наибольшее распространение получили макровирусы для Microsoft Word, Excel и Office 97.

Для существования вирусов в конкретной системе (редакторе) необходимо наличие встроенного в систему макроязыка с возможностями:

- привязки программы на макроязыке к конкретному файлу;
- копирования макропрограмм из одного файла в другой;
- получения управления макропрограммой без вмешательства пользователя (автоматические или стандартные макросы). Описанным условиям удовлетворяют редакторы MS Word, MS Office 97 и AmiPro, а также электронная таблица MS Excel. Эти системы содержат в себе макроязыки (MS Word – Word Basic, MS Excel и MS Office 97 – Visual Basic), при этом:
- макропрограммы привязаны к конкретному файлу (AmiPro) или находятся внутри файла (MS Word/Excel/Office 97);
- макроязык позволяет копировать файлы (AmiPro) или перемещать макропрограммы в служебные файлы системы и редактируемые файлы (MSWord /Excel/Office 97);
- при работе с файлом при определенных условиях (открытие, закрытие и т.д.) вызываются макропрограммы (если таковые есть), которые определены специальным образом (AmiPro) или имеют стандартные имена (MS Word/Excel/ Office 97).

В четырех указанных выше программных продуктах вирусы получают управление при открытии или закрытии зараженного файла, перехватывают стандартные файловые функции и затем заражают файлы, к которым каким-либо образом идет обращение. По аналогии с DOS можно сказать, что большинство макровирусов являются резидентными вирусами: они активны не только в момент открытия или закрытия файла, но до тех пор, пока активен сам редактор.

Рассмотрим принципы работы макроавирусов.

Макровирусы, поражающие файлы Word, Excel или Office 97, как правило, пользуются одним из трех нижеперечисленных приемов:

- в вирусе присутствует автомакрос (автофункция);
- в вирусе переопределен один из стандартных системных макросов (ассоциированный с каким-либо пунктом меню);
- макрос вируса автоматически вызывается при нажатии на какую-либо клавишу или комбинацию клавиш.

Бывают также полувирусы, которые не используют перечисленные приемы и размножаются, только если пользователь самостоятельно запускает их на выполнение.

Большинство макровирусов содержат все свои функции в виде стандартных макросов MS Word/Excel/Office 97. Существуют, однако, вирусы, использующие приемы скрытия своего кода и хранящие свой код в виде немакросов. Известны три подобных приема. Все они используют возможность макросов создавать, редактировать и исполнять другие макросы. Как правило, подобные вирусы имеют небольшой (иногда полиморфный) макрос-загрузчик, который вызывает встроенный редактор макросов, создает новый макрос, заполняет его основным кодом вируса, выполняет и затем, как правило, уничтожает, чтобы скрыть следы присутствия вируса. Основной код таких вирусов присутствует либо в теле самого вируса в виде текстовых строк, либо хранится в области переменных документа или в области Auto-text.

Хакер Мак-Намарой был первым, кто создал макровирус, которые заражал документы Word. Далее макровирусы стали писаться регулярно. Основным источником вирусов на сегодняшний день является Internet. Наибольшее число заражений вирусом происходит при обмене письмами в форматах MS Word/Office 97: пользователь зараженного макровирусом редактора, сам того не подозревая, рассылает «инфицированные» письма своим адресатам, а они рассылают новые письма и т.д.

Резидентные вирусы

Под термином «резидентность» (DOS'овский термин TSR – Terminate and Stay Resident) понимается способность вирусов оставлять свои копии в системной памяти, перехватывать некоторые события (например, обращения к файлам или дискам) и вызывать при этом процедуры заражения обнаруженных объектов (файлов и секторов).

Нерезидентные вирусы – вирусы, не оставляющие своих резидентных частей в оперативной памяти компьютера. Существуют вирусы, которые оставляют в памяти некоторые свои фрагменты, не способные к дальнейшему размножению. Такие вирусы считаются не резидентными.

Вредоносный (сценарный) код – это компьютерный код или веб-скрипт, преднамеренно разработанный для создания уязвимостей в системе, с помощью которых он выполняет несанкционированные вредоносные действия, такие как кража информации и данных и другие потенциальные повреждения файлов и вычислительных систем.

Это тип угрозы, которую, по данным «Лаборатории Касперского», могут блокировать далеко не все защитные решения.

Дело в том, что вредоносный код и вредоносное ПО – не одно и то же: под вредоносным ПО имеется в виду исключительно программное обеспечение, тогда как вредоносный код представляет собой скрипты веб-сайта, которые могут использовать уязвимости для загрузки вредоносного ПО.

Это автоматически исполняемое приложение, которое может активировать само себя и принимать различные формы, включая Java-апплеты, элементы управления ActiveX, размещенный контент, плагины, языки сценариев или другие языки программирования, предназначенные для улучшения веб-страниц и электронной почты.

Вредоносный код предоставляет киберпреступникам возможность получить несанкционированный удаленный доступ к атакованной системе (такая программа называется «бэкдор») и похитить важные данные компании.

Используя бэкдор, злоумышленники могут также уничтожить данные компьютера или установить на нем шпионское ПО. Этой угрозе могут подвергаться организации очень высокого уровня.

Скрипты, черви и вирусы могут нанести вред компьютеру, находя точки входа, через которые они получат доступ к ценным данным.

Посещение зараженных сайтов или нажатие на непроверенную ссылку во вложении к электронному сообщению являются основными воротами, через которые вредоносный код проникает в систему.

Антивирусное ПО, которое включает автоматические обновления, возможности удаления вредоносных программ, защиту веб-браузера и функцию обнаружения всех типов заражений, является лучшей защитой.

Скриптовый язык (англ. scripting language, также называют язык сценариев) – язык программирования, разработанный для записи «сценариев», последовательностей операций, которые пользователь может выполнять на компьютере.

Высокоуровневый язык программирования – язык программирования, разработанный для быстроты и удобства использования программистом. Основная черта высокоуровневых языков – это абстракция, то есть введение смысловых конструкций, кратко описывающих такие структуры данных и операции над ними, описания которых на машинном коде (или другом низкоуровневом языке программирования) очень длинны и сложны для понимания.

Высокоуровневые языки программирования были разработаны для платформенной независимости сути алгоритмов. Зависимость от платформы перекладывается на инструментальные программы – трансляторы, компилирующие текст, написанный на языке высокого уровня, в элементарные машинные команды (инструкции). Для каждой платформы разрабатывается платформенно-уникальный транслятор для каждого высокоуровневого языка, например, переводящий текст, написанный на Delphi в элементарные команды микропроцессоров семейства x86.

Так, высокоуровневые языки стремятся не только облегчить решение сложных программных задач, но и упростить портирование программного обеспечения. Использование разнообразных трансляторов и интерпретаторов обеспечивает связь программ, написанных при помощи языков высокого уровня, с различными операционными системами, программируемыми устройствами и оборудованием, и, в идеале, не требует модификации исходного кода (текста, написанного на высокоуровневом языке) для любой платформы.

Такого рода оторванность высокоуровневых языков от аппаратной реализации компьютера помимо множества плюсов имеет и минусы. В частности, она не позволяет создавать простые и точные инструкции к используемому оборудованию. Программы, написанные на языках высокого уровня, проще для понимания программистом, но менее эффективны, чем их аналоги, создаваемые при помощи низкоуровневых языков. Одним из следствий этого стало добавление поддержки того или иного языка низкого уровня (язык ассемблера) в ряд современных профессиональных высокоуровневых языков программирования.

Примеры: C, C++, C#, Delphi, Fortran, Java, JavaScript, Лисп, Паскаль, PHP. Языкам высокого уровня свойственно умение работать с комплексными структурами данных. В большинстве из них интегрирована поддержка строковых типов, объектов, операций файлового ввода-вывода и т.п.

Первым языком программирования высокого уровня считается компьютерный язык Plankalkül, разработанный немецким инженером Конрадом Цузе ещё в период 1942-1946 гг. Однако транслятора для него не существовало до 2000 года. Первым в мире транслятором языка высокого уровня является ПП (Программирующая Программа), он же ПП-1, успешно испытанный в 1954 г. [источник не указан 326 дней] Транслятор ПП-2 (1955 г., 4-й в мире транслятор) уже был оптимизирующим и содержал собственный загрузчик и отладчик, библиотеку стандартных процедур, а транслятор ПП для ЭВМ «Стрела-4» уже содержал и компоновщик (linker) из модулей. Однако, широкое применение высокоуровневых языков началось с возникновением Фортрана и созданием компилятора для этого языка (1957).

Низкоуровневый язык программирования (язык программирования низкого уровня) – язык программирования, близкий к программированию непосредственно в машинных кодах используемого реального или виртуального (например, байт-код, Microsoft .NET) процессора. Для обозначения машинных команд обычно применяется мнемоническое обозначение. Это позволяет запоминать команды не в виде последовательности двоичных нулей и единиц, а в виде осмысленных сокращений слов человеческого языка (обычно английских).

Иногда одно мнемоническое обозначение соответствует целой группе машинных команд, выполняющих одинаковое действие над разными ячейками памяти процессора. Кроме машинных команд языки программирования низкого уровня могут предоставлять дополнительные возможности, такие как макроопределения (макросы). При помощи директив есть возможность управлять

процессом трансляции машинных кодов, предоставляя возможность заносить константы и литеральные строки, резервировать память под переменные и размещать исполняемый код по определенным адресам. Часто эти языки позволяют работать вместо конкретных ячеек памяти с переменными.

Как правило, использует особенности конкретного семейства процессоров. Общеизвестный пример низкоуровневого языка – язык ассемблера, хотя правильнее говорить о группе языков ассемблера. Более того, для одного и того же процессора существует несколько видов языка ассемблера. Они совпадают в машинных командах, но различаются набором дополнительных функций (директив и макросов).

Также к языкам низкого уровня условно можно причислить CIL, применяемый в платформе Microsoft .NET, Форт.

Пример низкоуровневых языков программирования:

- Ассемблер;
- Машинный код.

Шифрование – вирус состоит из двух функциональных кусков: собственно вирус и шифратор. Каждая копия вируса состоит из шифратора, случайного ключа и собственно вируса, зашифрованного этим ключом.

Метаморфизм – создание различных копий вируса путем замены блоков команд на эквивалентные, перестановки местами кусков кода, вставки между значащими кусками кода «мусорных» команд, которые практически ничего не делают.

Шифрованный вирус

Это вирус, использующий простое шифрование со случайным ключом и неизменный шифратор. Такие вирусы легко обнаруживаются по сигнатуре шифратора.

Вирус-шифровальщик

В большинстве случаев вирус-шифровальщик приходит по электронной почте в виде вложения от незнакомого пользователю человека, а возможно, и от имени известного банка или действующей крупной организации. Письма приходят с заголовком типа: «Акт сверки…», «Ваша задолженность перед банком…», «Проверка регистрационных данных», «Резюме», «Блокировка расчетного счета» и прочее. В письме содержится вложение с документами, якобы подтверждающими факт, указанный в заголовке или теле письма. При открытии этого вложения происходит моментальный запуск вируса-шифровальщика, который незаметно и мгновенно зашифрует все документы. Пользователь обнаружит заражение, увидев, что все файлы, имевшие до этого знакомые значки, станут отображаться иконками неизвестного типа. За расшифровку преступником будут затребованы деньги. Но, зачастую, даже заплатив злоумышленнику, шансы восстановить данные ничтожно малы.

Вложения вредоносных писем чаще всего бывают в архивах .zip, .rar, .7z. Если в настройках системы компьютера отключена функция отображения расширения файлов, то пользователь (получатель письма) увидит лишь файлы вида «Документ.doc», «Акт.xls» и тому подобные. Другими словами, фай-

лы будут казаться совершенно безобидными. Но если включить отображение расширения файлов, то сразу станет видно, что это не документы, а исполняемые программы или скрипты, имена файлов приобретут иной вид, например, «Документ.doc.exe» или «Акт.xls.js». При открытии таких файлов происходит не открытие документа, а запуск вируса-шифровальщика. Вот лишь краткий список самых популярных «опасных» расширений файлов: .exe, .com, .js, .wbs, .hta, .bat, .cmd. Поэтому, если пользователю не известно, что ему прислали во вложении, или отправитель не знаком, то, вероятнее всего, в письме – вирус-шифровальщик.

На практике встречаются случаи получения по электронной почте обычного «вордовского» (с расширением .doc) файла, внутри которого, помимо текста, есть изображение, гиперссылка (на неизвестный сайт в Интернете) или встроенный OLE-объект. При нажатии на такой объект происходит незамедлительное заражение.

Вирусы-шифровальщики стали набирать большую популярность, начиная с 2013 года. В июне 2013 известная компания McAfee обнародовала данные, показывающие, что они собрали 250 000 уникальных примеров вирусов-шифровальщиков в первом квартале 2013 года, что более чем вдвое превосходит количество обнаруженных вирусов в первом квартале 2012 года

В 2016 году данные вирусы вышли на новый уровень, изменив принцип работы. В апреле 2016 г. в сети появилась информация о новом виде вируса-шифровальщика Петя (Petya), который вместо шифрования отдельных файлов, шифрует таблицу MFT файловой системы, что приводит к тому, что операционная система не может обнаружить файлы на диске, и весь диск по факту оказывается зашифрован.

Полиморфный вирус

Вирус, использующий метаморфный шифратор для шифрования основного тела вируса со случайным ключом. При этом часть информации, используемой для получения новых копий шифратора, также может быть зашифрована. Например, вирус может реализовывать несколько алгоритмов шифрования и при создании новой копии менять не только команды шифратора, но и сам алгоритм.

Перезаписывающие

Данный метод заражения является наиболее простым: вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать.

Паразитические

К паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными. Основными типами таких вирусов являются вирусы, записывающиеся в начало файлов (prepending), в конец файлов (appending) и в середину файлов

(inserting). В свою очередь, внедрение вирусов в середину файлов происходит различными методами – путем переноса части файла в его конец или копирования своего кода в заведомо неиспользуемые данные файла (cavity-вирусы).

Внедрение вируса в начало файла

Известны два способа внедрения паразитического файлового вируса в начало файла. Первый способ заключается в том, что вирус переписывает начало заражаемого файла в его конец, а сам копируется в освободившееся место. При заражении файла вторым способом вирус дописывает заражаемый файл к своему телу.

Таким образом, при запуске зараженного файла первым управление получает код вируса. При этом вирусы, чтобы сохранить работоспособность программы, либо лечат зараженный файл, повторно запускают его, ждут окончания его работы и снова записываются в его начало (иногда для этого используется временный файл, в который записывается обезвреженный файл), либо восстанавливают код программы в памяти компьютера и настраивают необходимые адреса в ее теле (т.е. дублируют работу ОС).

Внедрение вируса в конец файла

Наиболее распространенным способом внедрения вируса в файл является дописывание вируса в его конец. При этом вирус изменяет начало файла таким образом, что первыми выполняемыми командами программы, содержащейся в файле, являются команды вируса. Для того чтобы получить управление при старте файла, вирус корректирует стартовый адрес программы (адрес точки входа). Для этого вирус производит необходимые изменения в заголовке файла.

Внедрение вируса в середину файла

Существует несколько методов внедрения вируса в середину файла. В наиболее простом из них вирус переносит часть файла в его конец или «раздвигает» файл и записывает свой код в освободившееся пространство. Этот способ во многом аналогичен методам, перечисленным выше. Некоторые вирусы при этом компрессируют переносимый блок файла так, что длина файла при заражении не изменяется.

Вторым является метод «cavity», при котором вирус записывается в заведомо неиспользуемые области файла. Вирус может быть скопирован в незадействованные области заголовок EXE-файла, в «дыры» между секциями EXE-файлов или в область текстовых сообщений популярных компиляторов. Существуют вирусы, заражающие только те файлы, которые содержат блоки, заполненные каким-либо постоянным байтом, при этом вирус записывает свой код вместо такого блока.

Кроме того, копирование вируса в середину файла может произойти в результате ошибки вируса, в этом случае файл может быть необратимо испорчен.

Вирусы без точки входа

Отдельно следует отметить довольно незначительную группу вирусов, не имеющих «точки входа» (EPO-вирусы – Entry Point Obscuring viruses). К ним относятся вирусы, не изменяющие адрес точки старта в заголовке EXE-файлов. Такие вирусы записывают команду перехода на свой код в какое-либо место в середину файла и получают управление не непосредственно при запуске зараженного файла, а при вызове процедуры, содержащей код передачи управления на тело вируса. Причем выполняться эта процедура может крайне редко (например, при выводе сообщения о какой-либо специфической ошибке). В результате вирус может долгие годы «спать» внутри файла и выскочить на свободу только при некоторых ограниченных условиях.

Перед тем, как записать в середину файла команду перехода на свой код, вирусу необходимо выбрать «правильный» адрес в файле – иначе зараженный файл может оказаться испорченным. Известны несколько способов, с помощью которых вирусы определяют такие адреса внутри файлов, например, поиск в файле последовательности стандартного кода заголовков процедур языков программирования (C/Pascal), дизассемблирование кода файла или замена адресов импортируемых функций.

Вирусы-компаньоны

К категории вирусов-компаньонов относятся вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус.

К вирусам данного типа относятся те из них, которые при заражении переименовывают файл в какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на диск под именем заражаемого файла. Например, файл NOTEPAD.EXE переименовывается в NOTEPAD.EXD, а вирус записывается под именем NOTEPAD.EXE. При запуске управление получает код вируса, который затем запускает оригинальный NOTEPAD.

Возможно существование и других типов вирусов-компаньонов, использующих иные оригинальные идеи или особенности других операционных систем. Например, PATH-компаньоны, которые размещают свои копии в основном катагоге Windows, используя тот факт, что этот каталог является первым в списке PATH, и файлы для запуска Windows в первую очередь будут искать именно в нем. Данными способом самозапуска пользуются также многие компьютерные черви и троянские программы.

Вирусы-ссылки

Вирусы-ссылки или link-вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла «заставляют» ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

Файловые черви

Файловые черви никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям «специальные» имена, чтобы подтолкнуть пользователя на запуск своей копии – например, INSTALL.EXE или WINSTART.BAT.

Некоторые файловые черви могут записывать свои копии в архивы (ARJ, ZIP, RAR). Другие записывают команду запуска зараженного файла в BAT-файлы.

OBJ-, LIB-вирусы и вирусы в исходных текстах

Вирусы, заражающие библиотеки компиляторов, объектные модули и исходные тексты программ, достаточно экзотичны и практически не распространены. Всего их около десятка. Вирусы, заражающие OBJ- и LIB-файлы, записывают в них свой код в формате объектного модуля или библиотеки. Зараженный файл, таким образом, не является выполняемым и неспособен на дальнейшее распространение вируса в своем текущем состоянии. Носителем же «живого» вируса становится COM- или EXE-файл, получаемый в процессе линковки зараженного OBJ/LIB-файла с другими объектными модулями и библиотеками. Таким образом, вирус распространяется в два этапа: на первом заражаются OBJ/LIB-файлы, на втором этапе (линковка) получается работоспособный вирус.

Заражение исходных текстов программ является логическим продолжением предыдущего метода размножения. При этом вирус добавляет к исходным текстам свой исходный код (в этом случае вирус должен содержать его в своем теле) или свой шестнадцатеричный дамп (что технически легче). Зараженный файл способен на дальнейшее распространение вируса только после компиляции и линковки.

Рассмотрим примеры распространения вредоносного программного обеспечения:

Пример 1.

Эксперты IBM Trusteer сообщили, что раскрыли масштабную мошенническую операцию, в которой использовались огромные фермы эмуляторов мобильных устройств, при помощи которых преступники выводили миллионы долларов со счетов в онлайн-банках в США и ЕС[1].

Фермы эмуляторов помогали злоумышленникам получить доступ к тысячам взломанных учетных записей (скомпрометированных в результате фишинга или атак малвари) в очень сжатые сроки. Хотя эмуляторы сами по себе не являются вредоносными инструментами стоящая за этой кампанией хак-группа использовала их для эмуляции взломанных устройств. То есть в итоге все выглядело так, будто владельцы скомпрометированных учетных записей перешли на использование новых гаджетов или даже вошли со своего обычного устройства.

[1] Журнал «Хакер» (опубликовано 18.12.2020) www.xakep.ru.

Для настройки эмуляторов мошенники применяли специальный инструмент, способный загружать спецификации устройств из базы ранее скомпрометированных девайсов, сопоставляя каждое при этом поддельные устройства с банковскими учетными данными пострадавших. Ферма могла подделать даже местоположение GPS с помощью VPN, чтобы скрыть вредоносную активность от специалистов банка.

Идентификаторы устройств хакеры, вероятно, получали со взломанных устройств жертв, хотя в некоторых случаях мошенники выдавали себя за клиентов, которые осуществляли связь с использованием новых телефонов. Также злоумышленники могли обойти многофакторную аутентификацию, получив доступ к SMS-сообщениям.

Отчет экспертов гласит о следующем: «Ранее операций таких масштабов еще никогда не обнаруживали. В некоторых случаях более 20 эмуляторов использовались для спуфинга свыше 16 000 взломанных устройств. Злоумышленники применяли эти эмуляторы для многократного доступа к тысячам учетных записей и в конечном итоге похищали миллионы долларов всего за несколько дней».

Во время атак хакеры в режиме реального времени отслеживали активность взломанных банковских счетов, чтобы убедиться, что их активность не была обнаружена. Если что-то шло не так, и атака оказывалась под угрозой раскрытия, злоумышленники могли, резко изменив тактику, либо срочно завершить операцию и немедленно уничтожить все следы.

Когда исследователи IBM Trusteer обнаружили эту вредоносную кампанию, группировка не прекратила свои атаки, а лишь немного изменила тактику.

Данный факт свидетельствует о том, что хакеры не перед чем не останавливаются, а продолжают свою преступную деятельность, несмотря ни на что. В связи с чем напрашивается конкретный вывод о целесообразности ведения постоянной активной работы сотрудниками органов внутренних дел по своевременному разоблачению организованных преступных групп хакерской направленности.

Пример 2.

В интернет-журнале «Хакер» в статье «Rotexy. Как действовал один из опаснейших троянов 2020 года»[1] было указано, что с момента появления трояна Rotexy центр реагирования на компьютерные инциденты BI.ZONE заблокировал более 1000 доменных имен, которые злоумышленники использовали в качестве серверов управления. На протяжении длительного времени специалистами указанного центра внимательно отслеживалась деятельность известного вредоноса для Android. В этой статье описывается активность Rotexy в последние годы и его устройство.

Если разобрать исторический аспект, то Rotexy, по сути, – это помесь банкера и вымогателя. Он появился в 2018 году и провел десятки тысяч атак

[1] Статья опубликована 17.12.2020.

на различные устройства российских пользователей. Исследования функционирования Rotexy показали, что в течение всего 2020 года активность вредоноса постоянно снижалась, но в октябре – ноябре был зафиксировали его рост. Как долго продолжится его активность, покажет время.

Если рассматривать атакующие действия Rotexy, то он распространяется, маскируясь под приложения популярных торговых онлайн-площадок. Его атака начинается вполне обыденно. Так на телефон потенциальной жертвы приходит СМС, которое предлагает пользователю устройства открыть вредоносную ссылку, внешне похожую на адрес той или иной торговой площадки. После чего по ссылке загружается банковский троян и по команде злоумышленников ранее зараженные устройства распространяют такие фишинговые сообщения.

Что же касается функции банкера, то они заключаются в том, что Rotexy побуждает жертву ввести данные банковской карты на фишинговой странице. Кроме того троян действует как вымогатель. По команде с управляющего сервера он может заблокировать экран устройства жертвы. В большинстве таких случаев обычно отображается страница с сообщением о том, что для разблокировки экрана необходимо «оплатить штраф», только после этого будет доступен просмотр контента (например, порнографического).

Свежие семплы вредоносной программы не детектируются антивирусами, поскольку обсфусцируются с помощью приватных крипторов.

У рассматриваемого вредоноса Rotexy имеется отличительная особенность, которая заключается в умении обходить антифрод-системы банков. Программа пополняет баланс мобильного счета с банковской карты жертвы, а затем переводит средства через личный кабинет на другой номер.

С момента создания Rotexy его операторы крайне избирательно относились к распространению своей вредоносной программы. После перехода пользователя по вредоносной ссылке из СМС злоумышленники проверяли User-Agent его устройства. И только если девайс оказывался мобильным, загружалась вредоносная программа.

Кроме того, управляющие серверы настраиваются таким образом, что за одну рассылку они не позволяют скачивать вредоносные файлы больше 2000 раз. Эти ограничения призваны предотвратить детектирование трояна и блокировку домена.

Первым вирусом считается игра Pervading Animal, появившаяся в 1960 году, которая была создана с целью не навредить кому-то, а только лишь выполнять базовую функцию вируса – *размножение*. Однако это была не заслуга ее автора, а являлась чистой случайностью: копии, заполняющие весь жесткий диск, создавались из-за ***ошибки в программном коде***, а не по умыслу создателя. В 1975 году появился вирус The Creeper, который не причинял вреда, лишь выводил сообщение на экран. Но он уже имел такое свойство, как самостоятельно распространяться по сети, став первым сетевым вирусом в истории. Он же породил и первый антивирус – программу Reeper, являющуюся, по сути, таким же сетевым вирусом. Данный вирус Reeper распро-

странялся по сетям, никак себя не проявляя, а если программе удавалось найти на компьютере The Creeper – то она его уничтожала. Первой эпидемией компьютерных вирусов можно считать произошедшую в 1986 году эпидемию достаточно безвредного вируса Brain, который за год своего существования поразил множество компьютеров по всему миру, хотя изначально он создавался для определения уровня компьютерного ***пиратства*** в Пакистане. В 1990-х годах существенно расширился ассортимент вредоносных программ и спектр совершаемых ими действий. В настоящее время у специалистов в области информационно-телекоммуникационных технологий бытует мнение, что любое электронное устройство может быть подвергнуто заражению.

Что же касается компьютерных систем, то с 2000-х годов защищенных систем не осталось, даже такая сильная система как Mac OS X, вирусов для которой не существовало, перестала быть абсолютно безопасной – 16 февраля 2006 года был официально подтвержден факт обнаружения первого вируса для этой операционной системы (для сравнения, первый вирус для IBM PC появился в 70-е годы).

В настоящее время в мире существует порядка 350 – 380 тыс. только активно действующих вирусов, и число их постоянно растет, вызывая создание новых антивирусных программ (ревизоров, детекторов, «вакцин», «фагов»). Примерно с 1990 года проблема вирусов начинает принимать глобальный характер. В начале этого года выходит первый полиморфный вирус ***Chameleon***. Данная технология была быстро взята на вооружение и в сочетании со стелс-технологией (Stealth) и бронированием (Armored) позволила новым вирусам успешно противостоять существующим антивирусным пакетам. Во второй половине 1990 года появились два стелс-вируса – Frodo и Whale. Оба вируса использовали крайне сложные стелс-алгоритмы, а 9-килобайтный Whale к тому же применял несколько уровней шифровки и антиотладочных приёмов. В Болгарии открывается первая в мире специализированная электронная доска объявлений, с которой каждый желающий может скачать свежий вирус. Начинают открываться конференции Usenet по вопросам написания вирусов. В этом же году выходит «Маленькая чёрная книжка о компьютерных вирусах» Марка Людвига. На проблему противостояния вирусам были вынуждены обратить внимание крупные компании – выходит Symantec Norton Antivirus. Начало 1991 года отмечено массовой эпидемией полиморфного загрузочного вируса Tequila. Летом 1991 появился первый link-вирус, который сразу же вызвал эпидемию. В 1993 году появляется всё больше вирусов, использующих необычные способы заражения файлов, проникновения в систему и т.д. Основным примером является вирус PMBS, работающий в защищенном режиме процессора Intel 80386. Shadowguard и Carbuncle, значительно расширившие диапазон алгоритмов компаньон-вирусов. Cruncher – использование принципиально новых приёмов сокрытия своего кода в заражённых файлах. Выходят новые версии вирусных генераторов, а также появляются новые (PC-MPC и G2). Счёт известных вирусов уже идёт на тысячи. Антивирусные компании разрабатывают ряд эффективных алгоритмов для

борьбы с полиморфными вирусами, однако сталкиваются с проблемой ложных срабатываний. В начале 1994 года в Великобритании появились два крайне сложных полиморфик-вируса – SMEG.Pathogen и SMEG.Queeg. Автор вирусов помещал заражённые файлы на станции BBS, что явилось причиной настоящей эпидемии и паники в средствах массовой информации. Автор вируса был арестован. В январе 1994 года появился Shifter– первый вирус, заражающий объектные модули (OBJ-файлы). Весной 1994 было обнаружено SrcVir, семейство вирусов, заражающих исходные тексты программ (C и Pascal). В феврале 1995 года случился инцидент с beta-версией Windows 95, все диски которой оказались заражены DOS-вирусом Form.

В настоящее время постоянно в мире инфицировано около половины всех девайсов, имеющих доступ в сеть Интернет. По сведениям компании «Доктор Веб», широкое распространение на данный момент файлового вируса Win32.Rmnet.12, с помощью которого злоумышленники создали бот-сеть, насчитывающую более миллиона инфицированных компьютеров. По состоянию на 15 апреля 2017 года, ботнет Win32.Rmnet.12 состоит из 1 400 520 зараженных узлов и продолжает уверенно расти. Наибольшее количество зараженных ПК приходится на долю Индонезии – 320 014 инфицированных машин, или 27,12%. На втором месте находится государство Бангладеш с числом заражений 166 172, что составляет 14,08% от размеров всего ботнета. На третьем месте – Вьетнам (154 415 ботов, или 13,08%), далее следуют Индия (83 254 бота, или 7,05%), Пакистан (46 802 бота, или 3,9%), Россия (43 153 инфицированных машины, или 3,6%), Египет (33 261 бот, или 2,8%), Нигерия (27 877 ботов, или 2,3%), Непал (27 705 ботов, или 2,3%) и Иран (23 742 бота, или 2,0%). Достаточно велико количество пострадавших от данного вируса на территории Казахстана (19 773 случая заражения, или 1,67%) и Беларуси (14 196 ботов, или 1,2%). В Украине зафиксировано 12 481 случай инфицирования Win32.Rmnet.12, что составляет 1,05% от размеров всей бот-сети. Относительно небольшое количество зараженных компьютеров выявлено в США – 4 327 единиц, что соответствует 0,36%. Меньше всего случаев приходится на долю Канады (250 компьютеров, или 0,02% от объемов сети) и Австралии (всего лишь 46 компьютеров). По одному инфицированному ПК было выявлено в Албании, Дании и Таджикистане.

Также нельзя оставить без внимания и профессионализм киберпреступников. Если в 1990-е годы почти все вирусы выводили из строя ПО инфицированной машины, тем самым их вред заключался в причинении локального вреда компьютеру, а детектирование таких программ решалось установкой файерволов и антивирусных программ, то ныне **современные вредоносы** (агенты ботнетов) **маскируются**, пытаются не выдать своего присутствия, а захваченные ресурсы (производительность компьютера, место на диске, полоса канала связи) стараются использовать в меру, чтобы пользователь не чувствовал неудобств. Таким образом, **вред от действия вредоносных программ носит глобальный характер, полностью контролировать который уже технически невозможно**.

Однако оставить данную проблему на произвол судьбы так же невозможно. Помимо огромного материального ущерба IT-сегменту бизнеса, влекущего постоянные недоборы в бюджет государства, происходят еще и регулярные нарушения прав человека, таких как **неприкосновенность частной жизни и право на тайну переписки**. Одним из методов борьбы помимо ужесточения санкций за создание, использование и распространение вредоносных программ является постоянное обновление законодательной базы государства, актуализируемой под основные направления вирусописателей и киберпреступников. Таким изменением в Уголовном кодексе Российской Федерации стало преобразование 28 главы в декабре 2011 года, исключающей серьезные системные изъяны в законодательной власти. Впервые глава о преступлениях в сфере компьютерной информации появилась вместе с Уголовным кодексом Российской Федерации в 1996 году. Изначально осуществить криминализацию «компьютерных преступлений» предполагалось посредством внесения ряда статей в Уголовный кодекс РСФСР, в частности,

статья 152-3. «Незаконное овладение программами для компьютерных программ, файлами и базами данных»;

статья 152-4. «Фальсификация или уничтожение информации в автоматизированной системе»;

статья 152-5. «Незаконное проникновение в АИС, совершенное путем незаконного завладения парольно-ключевой информацией, нарушение порядка доступа или обхода механизмов программной защиты информации с целью ее несанкционированного копирования, изменения или уничтожения»;

статья 152-6. «Внесение или распространение «компьютерного вируса»;

статья 152-7. «Нарушение правил, обеспечивающих безопасность АИС»;

статья 152-8. «Промышленный шпионаж с использованием компьютерных программ».

Однако переход к совершенно новому Уголовному кодексу Российской Федерации стал причиной переработки указанных статей и их сведению к нынешним четырем статьям 28-й главы УК РФ.

При расследовании преступлений, связанных с созданием и использованием вредоносных программ, наиболее часто возникают следующие основные задачи.

1. Установление факта и способа создания вредоносной компьютерной программы, ее использования и распространения.

На практике обнаружение факта создания вредоносной программы или компьютерного вируса довольно сложно и, чаще всего, это можно сделать только после фактического выявления результатов ее использования.

Сама по себе направленность действия таких вредоносных программ, равно как и одна из целей их создания, являются проникновение в защищенные компьютерные сети, повреждение их или похищение важной компьютерной информации. Именно поэтому практически при любом факте расследо-

вания неправомерного доступа к компьютерной информации можно вести речь и о преступлении, предусмотренном ст. 273 УК РФ.

Факт использования вредоносной программы, чаще всего, выявляется антивирусными программами, в случае же их отсутствия признаками преступления могут являться особенности функционирования и использования программного обеспечения, повреждение данных и пр.

Таким образом, в большинстве случаев пользователи и не подозревают о наличии вредоносного программного обеспечения в своей оперативной системе.

Так, например, в недалеком прошлом в результате осуществленной хакерской атаки на персональные компьютеры ведомства МВД России, находящиеся под управлением операционной системы Windows, были заражены около тысячи компьютерных устройств. Введенный компьютерный вирус зашифровал все файлы на зараженных устройствах. В последующем на мониторах появлялось сообщение о требовании выкупа в размере 300 долларов США в биткоинах с каждого компьютера.

2. Установление лица, виновного в совершении преступления.

Если методика выявления лица, виновного в использовании или распространении вредоносной программы аналогична методике выявления лиц, совершивших преступление, предусмотренное ст. 272 УК РФ, то с выявлением создателя-автора вредоносной программы все значительно сложнее.

Подтверждение факта создания вредоносной программы требует особой доказательственной базы, которая выражается в выявлении и обнаружении следов создания и использования такой программы и установлении причинной связи между действиями подозреваемого и созданной программой. В процессе доказывания ведущая роль по-прежнему принадлежит экспертам, которые проводят статический и динамический анализ вредоносного программного обеспечения, после которого способны установить принадлежность того или иного подозреваемого к созданию и использованию вредоносной программы, однако получение рабочих материалов для проведения экспертизы зависит именно от сотрудников правоохранительных органов.

Следует отметить, что специфика преступной деятельности и стереотип преступника требуют в случае выявления подозреваемого немедленного его задержания и отстранения от компьютерной техники с целью предотвращения уничтожения им улик преступления, а также изъятия оперативной памяти и жестких дисков компьютеров. Этого можно добиться путем проведения следующих следственных действий: осмотр места происшествия, обыск и выемка.

Дальнейшее изобличение преступника может быть осуществлено как посредством его допроса или допроса иных лиц, причастных к созданию вредоносных программ, так и проведением вышеупомянутой экспертизы с целью установления авторства программы.

3. Установление вреда, причиненного данным преступлением.

Расследуя такие преступления надо иметь в виду, что вредоносные программы могут размножаться в больших количествах, а в отдельных случаях «обходить» и «обманывать» антивирусные программы и системы защиты. В этой

связи установление полного масштаба вреда, причиненного вредоносной программой, а в особенности компьютерным вирусом, практически невозможно.

Вместе с тем ущерб, причиненный конкретным единичным фактом использования вредоносной программы (например, при умышленном проникновении в компьютерную систему и ее заражении вирусной программой), может быть установлен экспертным путем, посредством проведения судебно-бухгалтерской, информационно-технологической и информационно-технической экспертиз.

4. Установление обстоятельств, способствовавших совершению расследуемого преступления.

Как и в случае с неправомерным доступом к компьютерной информации, решение данной задачи помогает более точно квалифицировать деяние, хотя по значимости она является второстепенной.

Помимо всего вышесказанного возникает проблема в признании статуса «вредоносной» экспертом компьютерной программы. Так, в соответствии с комментариями к ст. 273 УК РФ под вредоносными программами в смысле комментируемой статьи понимаются программы, специально созданные для нарушения нормального функционирования компьютерных программ. Под нормальным функционированием понимается выполнение операций, для которых эти программы предназначены, что определено в документации на программу. Таким образом, эксперт не может определить: работоспособна ли программа или нет. Это соответствует признанию абсолютно любой вредоносной компьютерной программы неработоспособной по причине невозможности существования какой-либо документации либо инструкции производителя, где определены критерии и функции интересующей программы.

В ст. 273 УК РФ необходимо подробно рассмотреть части 1 и 2, которые имеют формальный состав, и их содержание вызывает ряд вопросов.

Следует отметить, что в ч.1 и 2 ст. 273 УК РФ законодатель не определяет характер предмета посягательства, как в статьях 272 и 274 УК РФ. Это, на наш взгляд, существенно затрудняет применение данной статьи, так как без указания об информации, как охраняемой законом компьютерной информации, может возникнуть конкуренция между применением ст. 273 УК РФ или ст. 146 УК РФ.

Учитывая положения ч. 1 и 2 ст. 273 УК РФ, можно предположить, что лицо, которое использовало программу для копирования информации, преследовало цель, например, извлечь прибыль, использовало ее в своих интересах, но при этом оно искренне заблуждалось в оценке последствий применения этой программы. В таком случае сама программа, как и, в принципе, компьютер имеет прикладное значение, а мотивы и цели были совершенно иными. Хотя в ст. 273 УК РФ мотивы и цели не имеют квалифицирующего значения, слова «использование компьютерных программ, заведомо предназначенных для...» порождают подобное толкование и понимание данной статьи.

2.2. ВЫЯВЛЕНИЕ И РАСКРЫТИЕ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ВРЕДОНОСНЫМИ КОМПЬЮТЕРНЫМИ ПРОГРАММАМИ

Анализ криминогенной обстановки и имеющиеся оперативные данные свидетельствует о том, что в настоящее время на территории России существует обширный рынок сбыта вредоносных программ. Данная деятельность широко развернута и глубоко законспирирована. Она может быть либо с закрытым доступом, то есть требующим специального «инвайта», либо в «открытых» и «полуоткрытых» Интернет-ресурсах, на которых происходит рекламирование, распространение, обмен и продажа вредоносных программ, в том числе с участием несовершеннолетних. Не стоит забывать и о действующих Интернет-ресурсах бесплатных объявлений, которые являются излюбленным местом распространителей вредоносных программ.

Рассмотрим некоторые примеры, взятые из практической деятельности.

Пример 1. Ст. 273 ч.3 УК РФ «Создание, использование и распространение вредоносных компьютерных программ».

Подсудимый Рыжов А.Н. совершил распространение компьютерных программ, заведомо предназначенных для несанкционированного уничтожения, модификации компьютерной информации и нейтрализации средств защиты компьютерной информации, совершенные организованной группой, в том числе с привлечением несовершеннолетних, из корыстной заинтересованности, повлекшие создание угрозы наступления тяжких последствий, при следующих обстоятельствах:

Рыжов А.Н. вступил в состав созданной лицом N, дело в отношении которого выделено в отдельное производство, организованной группы, целью создания которой являлось осуществление преступной деятельности, связанной с созданием, распространением и использованием на автозаправочных комплексах ОАО «Воронежнефтепродукт» вредоносного программного обеспечения, предназначенного для систематического недолива топлива, отпускаемого клиентам, а также реализации нефтепродуктов клиентам в отсутствии контрольно-кассового учета.

Подсудимый Рыжов А.Н. совершил тяжкое преступление, вину признал полностью, раскаивается в содеянном, заключил досудебное соглашение о сотрудничестве, по месту жительства и работы.

Суд признал Рыжова виновным в совершении преступления, предусмотренного ст. 273 ч.3 и назначить ему наказание в виде 1 года 6 месяцев лишения свободы.

Под вредоносной программой следует понимать программу, которая была создана для выполнения несанкционированных (неразрешенных) владельцем информации, ЭВМ или системы ЭВМ, определённых функций (алгоритмов, процессов). Под такими функциями можно подразумевать:

- несанкционированное уничтожение информации;
- блокирование информации;

- изменение либо копирование информации;

- нарушение работы ЭВМ или систем ЭВМ, в частности вывод из строя антивируса.

Также к компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств её защиты, относится информация со встроенными в неё вредоносными кодами («компьютерный червь», «логическая бомба», «троянский конь»).

Пример 2. Ст. 273 ч.1 УК РФ «Создание, использование и распространение вредоносных компьютерных программ, заведомо предназначенных для несанкционированного уничтожения, блокирование, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации».

19 сентября 2019 года Евсюков, обладая навыками работы с персональным компьютером и программным обеспечением, обнаружил на одном из Интернет-ресурсов вредоносную компьютерную программу «vzLOM.exe», наделенную функциями неправомерного воздействия на средства вычислительной техники, которая может привести к несанкционированной нейтрализации средств защиты компьютерной информации. 21 сентября 2019 года в период с 20:51:09 по 23:56:15, Евсюков, находясь по месту своего жительства по адресу: г. Иваново, ул. Пушкина, д. 1Е, имея необходимые компьютерные познания, с принадлежащего ему персонального компьютера – ноутбука «Emachines», осуществил соединение с сетью Интернет и запустил вредоносную компьютерную программу «vzLOM.exe», которая в автоматическом режиме совершила 9 сеансов вирусного воздействия на веб-сервер, принадлежащий информационным ресурсам правительства Ивановской области. Вирусное воздействие заключалось в попытках внедрения вредоносного кода в передаваемые Интернет-ресурсу запросы, содержащие команды и параметры для сервера информационного ресурса правительства Ивановской области, что могло привести к несанкционированной нейтрализации средств защиты компьютерной информации, однако ввиду высокой технической защищённости указанного веб-ресурса доступ к компьютерной информации правительства Ивановской области предоставлен не был. Подсудимый Евсюков виновным себя признал полностью. При этом пояснил, что обвинение ему понятно. Суд признал виновным Евсюкова в совершении преступления, предусмотренного ч. 1 ст. 273 УК РФ, и назначил ему наказание в виде лишения свободы сроком на 1 год 6 месяцев со штрафом в размере 10000 рублей.

Пример 3. Ст. 273 ч. 1 УК РФ.

ОРП УМВД СУ УМВД России по г. Борисоглебску 11.02.2019 возбуждено уголовное дело №23 по ч.2 ст. 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности), по фак-

ту того, что 02.02.2019 Крутинин Г.В., находясь в офисном помещении № 406, расположенном по адресу: г. Борисоглебск, ул. Свободы, д. 207, осуществил установку программных продуктов «Microsoft Windows 7 Ultimate», «Microsoft Office Профессиональный 2013» с признаками контрафактности, которые установлены с применением программных продуктов, предназначенных для несанкционированного блокирования и модификации средств лицензионной защиты программных продуктов «Microsoft», из корыстной заинтересованности. Подозреваемым по данному уголовному делу является Крутинин Геннадий Васильевич, 01.04.1998 г.р. После проведения компьютерной судебной экспертизы, изъятых у Крутинина Г.В. ноутбука, флэш-карты и мобильного телефона, вина подозреваемого была установлена.

Подсудимый Крутинин Г.В. свою вину признал полностью, а также активно сотрудничал со следствием.

Суд признал Крутинина Г.В. виновным в совершении преступления, предусмотренного ч.2 ст. 273 УК РФ, и назначил ему наказание в виде 1 года лишения свободы в колонии общего режима.

Пример 4.

В г. Н-ске при слиянии двух банков не была построена система обеспечения информационной безопасности, в том числе на каждом компьютере отсутствовал антивирус. Операционист регулярно посещала Интернет-ресурсы «непристойного содержания». В связи с чем, компьютер подвергся заражению вредоносной программой – «NURA», позволяющей удаленно управлять компьютером. В конце рабочего дня операционист, нарушив требования по информационной безопасности, не выключила и не заблокировала рабочий компьютер. Ночью злоумышленники с использованием вредоносной программы «NURA», завладев управлением компьютера, стали переводить денежные средства на счет банковской карты в одну из стран западной Европы. За ночь преступники совершили хищение денежных средств на общую сумму свыше семидесяти пяти миллионов рублей.

По данному факту было возбуждено уголовное дело № 3 по ч. 3 ст. 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ, повлекшие за собой тяжкие последствия или создали угрозу их наступления). В процессе расследования преступления была назначена и проведена компьютерно-техническая экспертиза, в результате которой были установлены IP-адреса, с которых происходило «вторжение» в банк. В процессе проведения оперативно-розыскных мероприятий и следственных действий был установлен круг подозреваемых лиц. В ходе проведения допросов гражданин К. и гражданин В. сознались в совершении преступления, предусмотренного частью 3 ст. 273 УК РФ. Оба гражданина ходатайствовали о рассмотрении судебного дела в особом порядке, свою вину признали полностью и возместили причиненный ущерб.

Суд признал гражданина К. и гражданина В. виновными в совершении преступления, предусмотренного частью 3 статьи 273 УК РФ. Осужденному гражданину К. суд назначил наказание в виде 6 лет 6 месяцев лишения свобо-

ды с отбыванием срока в колонии общего режима, а осужденному гражданину В. назначил наказание в виде 5 лет 6 месяцев лишения свободы с отбыванием срока в колонии общего режима.

Работу, связанную с выявлением и пресечением фактов преступной деятельности фигурантов по распространению вредоносных компьютерных программ, условно можно разделить на три взаимосвязанных и последовательных этапа:

- получение и проверка оперативной информации в целях установления фактов незаконного распространения вредоносного программного обеспечения, и лиц к ним причастных;
- оперативная разработка и документирование преступной деятельности фигурантов (с использованием имеющихся оперативных возможностей), подготовка и предоставление в следственные органы материалов ОРД, достаточных для возбуждения уголовного дела;
- реализация материалов разработки и оперативное сопровождение расследования по уголовному делу, как правило, вплоть до рассмотрения дела в суде.

Предлагаем к выше сказанному рассмотреть один из характерных примеров.

В отдел «К» БСТМ УМВД России по Н-ской области поступила оперативная информация, о том, что гражданин, имеющий «ник» в сети Интернет и в программе видеозвонков «Skype» «51» (предположительно Иванов Иван Иванович), в группе с неустановленными лицами занимается за денежное вознаграждение созданием и распространением вредоносных компьютерных программ, предназначенных для взлома и неправомерного доступа, а также обучает хакингу. Продажа вредоносных компьютерных программ «51» (Ф.И.О.) осуществляется с использованием возможности сети Интернет (в том числе, через сайты объявлений), через форумы Интернет-ресурсов таких, как «Xakep.ru», «Forum. N-sk.ru», размещенные на ресурсах «Н-скета».В целях конспирации «51» никаких контактных данных в сети не оставлял, кроме почты «51@gmail.ru» и ника в «Skype» «51». Регистрацию и доступ к вышеуказанным ресурсам осуществляет с использованием анонимайзера.

Для достоверности полученной оперативной информации была разработана оперативная комбинация, целью которой являлась попытка войти в доверие и получить дополнительные контактные сведения о распространителе программных продуктов посредствам переписки.

В целях установления причастности фигуранта к распространению вредоносных программ в сети Интернет проведён мониторинг (наблюдение), поиск и анализ информации, размещенной на сайтах, расположенных на информационных ресурсах Н-ских провайдеров сети Интернет, на англо- и русскоязычных сайтах России и иностранных государств. Получены образцы продукции для проведения сравнительного исследования;

Даны соответствующие задания (поручения) подсобному аппарату на установление фигуранта и его связей, причастных к распространению, написанию и распространению вредоносных компьютерных программ, а также конкретных фактов преступной деятельности.

Осуществлены необходимые проверки по оперативно-розыскным, справочно-вспомогательным и криминалистическим учетам УМВД России по Н-ской области и другим информационным базам данных.

Проведен сбор и анализ дополнительно полученной оперативной информации, по результатам которой был намечен последующий план действий по документированию и разоблачению преступной деятельности фигурантов (сбор характерных следов и установления способов совершения данного вида преступлений).

В ходе ОРМ были получены сведения об IP-адресе, с которого фигурант размещал объявления, а также установлен круг лиц, способных освещать деятельность фигуранта.

В ходе переписки, оформленной актом наблюдения в присутствии представителей общественности, с фигурантом посредством компьютерной программы «Skype» установлены контактные номера телефонов, а также назначена встреча для проведения ОРМ «проверочная закупка».

В ходе реализации намеченного плана действий оперативной комбинации на подготовительном этапе перед встречей был составлен ряд вопросов, при ответе на которые фигурант давал бы конкретные ответы, указывающие на осведомленность о нарушении законодательства Российской Федерации и достаточность своих знаний в технической части. В зависимости от складывающейся оперативно-розыскной ситуации определяется список необходимых вопросов:

1. Какое образование имеет фигурант?

2. Его уровень навыков владения компьютером.

3. Осведомленность об уголовной ответственности за распространение вредоносных программ.

4. Имело ли место создание им конкретно данной компьютерной программы? Если да, то при каких обстоятельствах.

5. Где, когда, при каких обстоятельствах имело место завладение данной компьютерной программой?

6. Сколько раз и кому реализовывал фигурант распространяемую программу?

7. Какие функции выполняет интересуемая программа?

8. Осуществлял ли фигурант неправомерный доступ с использованием продаваемой программы? Если да, то в отношении кого именно.

9. Обучал ли кого-нибудь пользоваться данным программным продуктом?

После проведения первой проверочной закупки было назначено исследование в ЭКЦ УМВД России по Н-ской области закупленного образца компь-

ютерной программы. На разрешение исследования поставлены следующие вопросы:

1. Содержатся ли на представленном для исследования USB-флеш-носителе какие-либо программные продукты? Если да, то, какие именно.

2. Является ли находящееся на представленном для исследования USB-флеш-носителе программное обеспечение вредоносным?

3. Детектируются ли антивирусным программным обеспечением программные продукты, содержащиеся на предоставленном USB-флеш-носителе? Если да, то, к какому семейству вредоносных программ относятся данные программные продукты.

4. Какими признаками вредоносности обладают компьютерные программы, находящиеся на представленном USB-флеш-носителе?

После проведения исследования закупленной компьютерной программы на основании постановления заместителя начальника УМВД РФ по Н-ской области – начальника полиции о проведении ОРМ, в соответствии с ФЗ «Об ОРД» в установленном месте сотрудниками отдела «К» БСТМ УМВД России по Н-ской области произведена проверочная закупка образцов вредоносной компьютерной программы «Spy-Net 2.7», распространяемой фигурантом.

По итогам проведенного исследования собранного материала, где следы совершения данного вида преступления были задокументированы, выяснены обстоятельства, указывающие на причастность к преступной деятельности фигуранта, появились достаточные основания полагать, что в действиях разрабатываемого лица (разрабатываемых лиц) имеются признаки преступления, указанные в особенной части УК РФ в статье 273. Данный материал проверки был направлен в следственный орган для решения вопроса о возбуждении уголовного дела.

Предлагаем рассмотреть некоторые примеры раскрытых преступлений, выявленных Управлением «К» БСТМ МВД России.

Пример 1. БСТМ МВД России в рамках международного сотрудничества была проведена межрегиональная операция по ликвидации бот-сети, состоящей более чем из 164 000 компьютеров, зараженных с использованием вредоносной программы «Win32/Dorkbot». Данная работа проводилась посредством реализации скоординированных оперативно-розыскных мероприятий на территории 4 субъектов Российской Федерации. В ходе операции сотрудниками БСТМ МВД России прекращено функционирование 3 серверов, с которых осуществлялось управление данной бот-сетью.

В результате проведенной подразделениями «К» работы Главным следственным управлением ГУ МВД России по Н-ской области возбуждено 12 уголовных дел, связанных с внедрением вредоносных программ в компьютерные системы, повлекшим нарушение правил эксплуатации средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей кредитно-финансовых учреждений, таких

как: ЗАО «ВТБ 24», ОАО «Банк Москвы», ОАО «Альфа-Банка», АКБ «Росбанк», ОАО «ХАНТЫ-МАНСИЙСКИЙ БАНК», ОАО «АК БАРС».

В ходе расследования данных уголовных дел задержаны три члена этнической организованной преступной группы. Документирование противоправной деятельности носило комплексный, межрегиональный характер. Так, только в одном из городов России ущерб от действий виновных в содеянном преступлении лиц составил свыше 4 млн. руб.

В работе по выявлению и раскрытию преступлений, предусмотренных ст. 274 УК РФ, кроме Управления «К» БСТМ МВД России по Свердловской области и Пермскому краю участвовали силы и средства БСТМ МВД России по г. Санкт-Петербургу и Ленинградской области, Нижегородской и Московской областей.

Пример 2. В Управление «К» поступила информация о появлении на территории Российской Федерации нового вида вредоносного программного обеспечения – «Faketoken.b-ruStels2», целью которого являются устройства, работающие на платформе «Android».

В ходе проведения необходимых оперативно-розыскных мероприятий оперативным сотрудникам удалось выйти на след участников преступной группы, в которую входило семь человек.

Злоумышленники использовали программу, которая, после установки на устройство, запрашивала баланс банковской карты, привязанной к номеру абонента, скрывала поступающие уведомления и начинала осуществлять переводы денежных средств с банковского счета на счета, подконтрольные преступникам.

В результате проведенных одновременных обысков сотрудниками следственно-оперативных групп было изъято значительное количество компьютерной техники со следами распространения в сети Интернет вредоносного программного обеспечения, в том числе 25 мобильных телефонов, более 150 сим-карт, электронные носители информации и свыше 100 банковских карт, на которые производилось зачисление похищенных денежных средств.

Все обвиняемые фигуранты, проходящие по уголовному делу, участники преступной группы, были задержаны, им была избрана мера пресечения в виде ареста. В процессе проведения предварительного расследования, подозреваемые лица дали признательные показания, и по его окончанию им предъявлены обвинения по статье 158 УК РФ (Кража).

Сумма предотвращенного ущерба клиентам банка по предварительным оценкам составляет более 5 млн. руб.

Работа по установлению причастности данных лиц к десяткам аналогичных преступлений продолжается.

Пример 3. В Управление «К» поступила информация о появлении на территории Российской Федерации нового вида вредоносного программного обеспечения – «Trojan-Banker.AndroidOS.svpenq.a», целью которого являются устройства, работающие на платформе «Android».

Оперативникам удалось выйти на след создателя вируса, которым оказался 25-летний житель Челябинской области, закончивший девять классов. Кроме него в состав преступной группы входило еще четыре человека.

Программа, которую изъяли оперативные сотрудники, после установки на устройство запрашивала баланс банковской карты, привязанностей к номеру абонента, скрывала поступающие уведомления и начинала осуществлять переводы денежных средств с банковского счета на счета, подконтрольные злоумышленникам.

В настоящее время участники преступной группы задержаны и дают признательные показания. Им предъявлены обвинения по статьям 158 (Кража) и 273 (Создание и распространение вредоносных компьютерных программ) УК РФ.

В результате проведенных обысков было изъято значительное количество компьютерной техники со следами распространения в сети Интернет вредоносного программного обеспечения, мобильные телефоны, сим-карты, электронные носители информации, серверное оборудование и банковские карты, на которые производилось зачисление похищенных денежных средств.

Сумма предотвращения ущерба клиентам банка, по предварительным оценкам, составляет более 50 млн. руб. Ведется работа по установлению причастности данных лиц к десяткам аналогичных преступлений.

Приведенные примеры, взятые из ежедневной практической деятельности сотрудников БСТМ МВД России, позволяют сделать следующие выводы:

1. В настоящее время существует и активно развивается обширный рынок сбыта вредоносных программ.

2. Широко развернута деятельность ряда глубоко законспирированных либо с закрытым доступом Интернет-ресурсов, на которых происходит рекламирование, распространение, обмен и продажа вредоносных программ.

3. Участились случаи вовлечения несовершеннолетних в преступную деятельность, связанную с написанием вредоносных программ.

4. Основной площадкой для распространения вредоносных программ являются бесплатные Интернет-ресурсы (сайты, различные форумы, объявления и т.п.).

В этой связи сотрудникам оперативных подразделений органов внутренних дел рекомендуется:

1. Осуществлять необходимые проверки по оперативно-розыскным, справочно-вспомогательным и криминалистическим учетам МВД России и другим информационным базам данных.

2. Согласно действующим нормативным правовым актам, исходя из оперативно-розыскной, криминалистической и следственной ситуации, необходимо осуществлять соответствующие мероприятия по своевременному выявлению и раскрытию преступлений данной направленности.

3. В каждом конкретном случае необходимо учитывать характерологическую особенность личности разрабатываемого лица, что позволит с

наименьшей затратой времени, сил и средств оперативным сотрудникам и следователям раскрыть совершенное преступление.

4. Постоянно проводить и целенаправлять лиц, осуществляющих содействие правоохранительным органам в раскрытии преступлений, на установление фигурантов и его связей, причастных к распространению, написанию и распространению вредоносных компьютерных программ, а также конкретных фактов преступной деятельности.

Рис. 5. Техническое устройство, при помощи которого совершаются преступления в сфере телекоммуникаций и компьютерной информации

2.3. ОСОБЕННОСТИ ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ТЕЛЕКОММУНИКАЦИЙ И КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В динамичных условиях нашего времени общество постоянно сталкивается с проблемами различного характера, порождение которых зачастую вызвано стремлением к созданию более совершенных и эффективных моделей существования. Это в полной мере относится и к такой специфической сфере, которая все более быстрыми темпами внедряется в современную жизнь мирового сообщества, – как область применения информационных технологий.

Создание компьютерной техники, современных мобильных устройств связи, развитой информационно-телекоммуникационной среды с огромными возможностями, их широкое распространение и применение в экономической, социальной и управленческой сферах, а также появление в быту значительного количества высокотехнологичного оборудования последних поколений явилось не только новым свидетельством технического прогресса, но и неизбежно повлекло за собой негативные последствия, связанные с различного рода злоупотреблениями при использовании средств компьютерной техники и информационных технологий.

Общественная опасность противоправных действий в области информационных технологий выражается в том, что несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы способны вызывать тяжелые и необратимые последствия, связанные не только с имущественным ущербом, но и с причинением физического вреда людям. Опасность компьютерных преступлений многократно возрастает, когда они совершаются в отношении действующих объектов жизнеобеспечения, транспортных и оборонных систем, атомной энергетики и др.

Первым зафиксированным фактом убийства, совершенного посредством компьютерных технологий, был случай, произошедший в недалеком прошлом в США, где тяжело раненный свидетель преступления был спрятан в закрытом госпитале на территории военной базы. Преступники через Интернет изменили режимы работы кардиостимулятора и аппарата вентиляции легких, что привело к смерти охраняемого лица[1] (см. рис. 6).

[1] Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. … канд. юрид. наук: 12.00.08. М., 2002. С. 20.

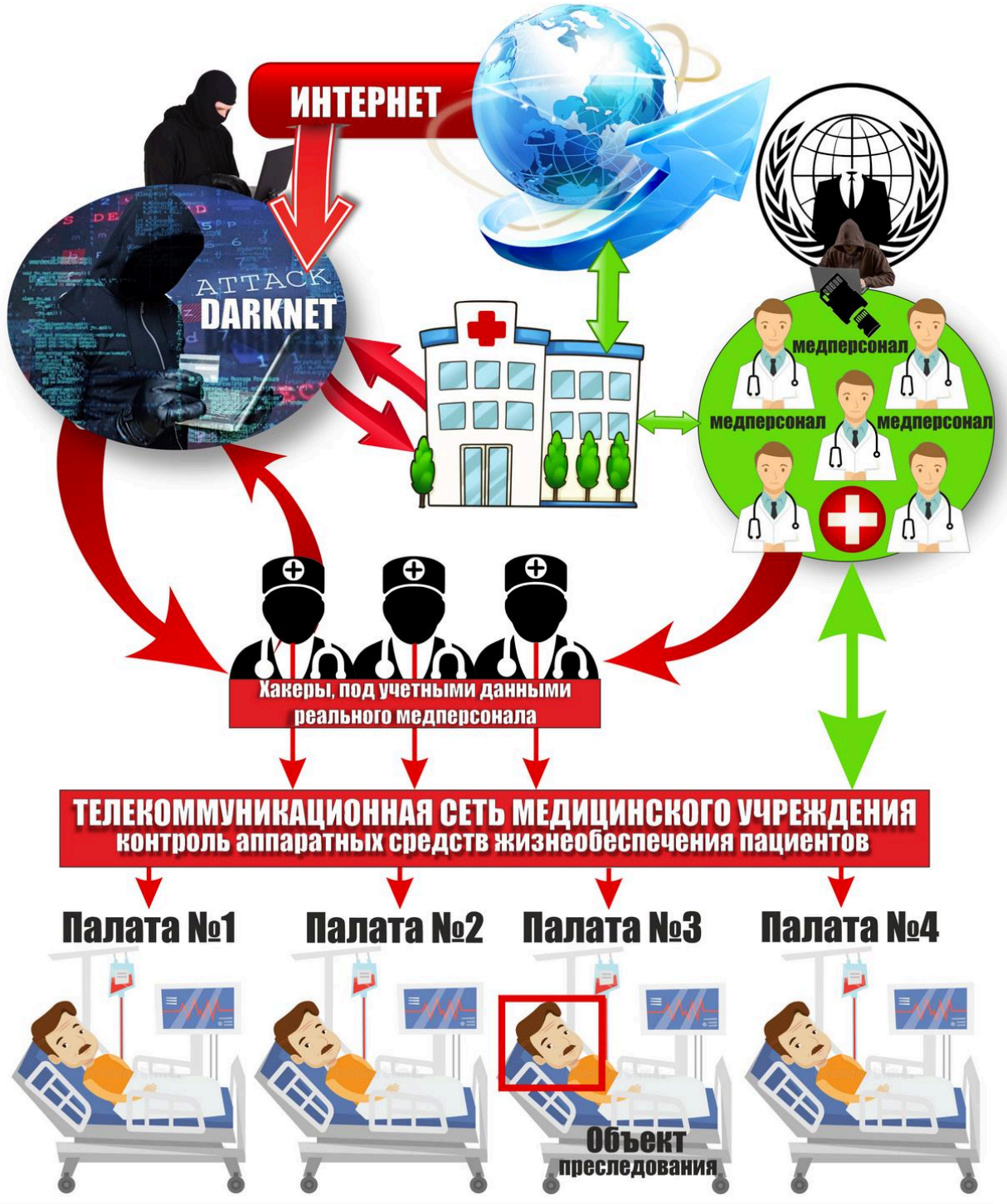


Рис. 6. Первый факт совершения заказного убийства с использованием сферы телекоммуникации и компьютерной информации

Сотрудникам правоохранительных органов довольно сложно расследовать данную категорию дел по ряду объективных и субъективных причин. Так, например, сотрудникам, осуществляющим работу по своевременному раскрытию и дальнейшему расследованию выявленных преступлений, необходимо владеть знаниями компьютерных и информационных технологий, а

также своевременно и тактически грамотно применять нормы действующих нормативных правовых документов.

В данной работе нами предпринята попытка показать особенности производства некоторых оперативно-розыскных мероприятий и проведения следственных действий по делам рассматриваемой категории, а также последовательность их осуществления.

При расследовании компьютерных преступлений, наиболее часто встречающихся, можно выделить **три типичные следственные ситуации**:

1. Собственник информационной системы своими силами выявил нарушение целостности или конфиденциальности информации в системе, обнаружил виновное лицо и заявил об этом в правоохранительные органы.

2. Собственник информационной системы своими силами выявил нарушение целостности или конфиденциальности информации в системе, но не смог обнаружить виновное лицо и заявил об этом в правоохранительные органы.

3. Данные о нарушении целостности или конфиденциальности информации в информационной системе и виновном лице стали общеизвестными или непосредственно обнаружены правоохранительными органами (например, в ходе проведения оперативно-розыскных мероприятий).

При наличии подозреваемого лица первоначальная задача оперативных сотрудников и следствия заключается в полном установлении обстоятельств дела, сборе с помощью собственника информационной системы и процессуальной фиксации доказательств:

а) нарушения целостности или конфиденциальности информации в системе;

б) размера ущерба, причиненного нарушением целостности или конфиденциальности информации;

в) механизма совершения преступления, а именно: причинной связи между действиями, образующими способ совершения, и наступившими последствиями путем детализации способа нарушения целостности или конфиденциальности информации в системе и характера совершенных виновным лицом действий;

г) отношение виновного лица к совершенным действиям и наступившим последствиям.

Если подозреваемые задержаны сразу после совершения преступления, для данной ситуации характерны следующие первоначальные следственные действия:

а) личный обыск задержанных;

б) допрос задержанных;

в) обыск по месту жительства, месту работы и месту задержания.

Осмотр и обыск (выемка) по делам данной категории являются важнейшими инструментами установления обстоятельств расследуемого преступления.

Известно, что в практической деятельности наиболее распространенными процессуальными способами по изъятию вещественных доказательств являются такие следственные действия, как осмотр, обыск и выемка.

Следует напомнить, что **осмотр** – это непосредственное обнаружение, восприятие и исследование следователем (оперативным сотрудником по отдельному поручению следователя) материальных объектов, имеющих отношение к исследуемому событию. **Обыск** – следственное действие, в процессе которого производится поисковые действия и принудительное изъятие объектов, имеющих значение для правомерного решения необходимых на момент расследования задач уголовного судопроизводства.

Выемка – следственное действие, в процессе которого производится изъятие объектов, имеющих значение для правомерного решения задач уголовного судопроизводства, в тех случаях, когда их местонахождение точно известно следователю и изъятие прямо или косвенно не нарушает прав личности[1].

Носители информации, имеющие отношение к расследуемому преступлению, изымаются, упаковываются соответствующим образом, исследуются, оцениваются, признаются вещественными доказательствами и приобщаются к материалам уголовного дела[2] с соблюдением установленного Уголовно-процессуального кодекса Российской Федерации.[3]

Для участия в обыске и выемке целесообразно приглашать специалиста[4] в области телекоммуникаций и компьютерной информации.

При осуществлении таких следственных действий, как осмотр, обыск, выемка, сопряженных с изъятием компьютерной техники и компьютерной информации, возникает ряд специфических вопросов, связанных с некоторыми особенностями изымаемых объектов, относящихся к расследуемому преступному событию.

В данной ситуации необходимо предвидеть предпринимаемые злоумышленниками возможные способы противодействия, целью которых является уничтожение вещественных доказательств. Например, они могут **использовать специальное оборудование, уничтожающее следы совершенного или подготавливаемого преступления.**

Злоумышленник, зная о том, что неблагоприятная ситуация может возникнуть в любое время, заранее подготавливается путем внедрения в программное обеспечение «манипуляции», которая периодически запрашивает пароль, и, если в определенное время данный пароль не введен, вся информация будет искажена или уничтожена.

Злоумышленник, зная о том, что неблагоприятная ситуация может возникнуть в любое время, заранее программирует свое оборудование для иден-

---

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 01.09.2017). Ст. 176, 182,183.
[2] УПК РФ. Ст. 81-82.
[3] Далее УПК РФ.
[4] УПК РФ. Ст. 58.

тификации «себя» с использованием **тайминга** и если через определенный период времени не будет подтверждения «себя», то в этом случае вся информация будет искажена или уничтожена, а также бывают случаи воздействия на само оборудование, влекущее за собой повреждение, деформацию и уничтожение. Время отклика при введении авторизированных данных зависит от компьютерного оборудования.

Во избежание неблагоприятных последствий для здоровья участников проводимых следственных действий желательно иметь с собой и использовать при обыске и осмотре устройство для определения наличия и измерения магнитных полей.

Изъятые в процессе производства выше упомянутых следственных действий объекты (компьютеры, их составные части, различные носители информации), которые могут быть признаны в последующем вещественными доказательствами, требуют особой аккуратности при транспортировке и последующем хранении. Им противопоказаны удары, перепады температуры и повышенная влажность, так как данные внешние факторы могут отрицательно повлиять на функциональные свойства аппаратуры и повлечь за собой потерю информации.

Не следует забывать при осмотрах и обысках о возможностях сбора традиционных доказательств (скрытых отпечатков пальцев на клавиатуре, выключателях и других устройствах компьютерной системы, шифрованных рукописных записей и пр.). **Осмотру подлежат все устройства конкретной телекоммуникационной сети и компьютерной системы.**

Фактически оптимальный вариант изъятия компьютеров и носителей информации – это их фиксация на месте обнаружения и упаковка. Данные действия должны производиться таким образом, чтобы аппаратуру можно было бы успешно, правильно и точно так же, как на месте обнаружения, собрать в лабораторных условиях или на месте производства экспертиз с участием специалистов.

По прибытии на место осмотра или обыска **следует принять меры к обеспечению сохранности всей информации** на находящихся в проверяемом помещении компьютерах и электронных носителях. Для этого необходимо:

1) не разрешать кому бы то ни было из лиц, присутствующих на объекте проведения обыска, прикасаться к работающим компьютерам, носителям информации, включать и выключать компьютеры;

2) самому не производить никаких манипуляций с компьютерной техникой, если результат этих манипуляций заранее не известен;

3) при наличии в помещении, где находятся средства компьютерной техники и носители информации, взрывчатых, легковоспламеняющихся, токсичных и едких веществ или материалов как можно скорее удалить эти вещества в другое помещение.

Исходя из создавшейся ситуации, всегда необходимо соблюдать определенные особенности при производстве оперативно-розыскных мероприятий и вышеупомянутых следственных действий.

Если компьютер работает, ситуация для следователя (оперативного сотрудника), производящего следственное действие без помощи специалиста, существенно осложняется, однако и в этом случае не следует отказываться от оперативного изъятия интересующих данных[1].

В этой ситуации необходимо:

а) *определить, какая программа выполняется*. Для этого необходимо изучить изображение на экране дисплея и, по возможности, детально описать его.

Используя «Диспетчер задач» (одновременное нажатие клавиш Ctrl-Alt-Del), можно посмотреть, какие процессы на данном компьютере запущены (за исключением скрытых). **Необходимо помнить**, что программы, имеющие функцию экстренного уничтожения информации, могут работать и в **скрытом** режиме.

После остановки программы и выхода в операционную систему иногда при нажатии функциональной клавиши «F3» **можно восстановить** наименование вызывавшейся последний раз программы.

Можно осуществить фотографирование или видеозапись изображения.

б) *остановить исполнение программы*. Остановку можно осуществить также с использованием «Диспетчера задач», либо одновременным нажатием клавиш Ctrl-C или Ctrl-Break;

в) *зафиксировать (отразить в протоколе) результаты своих действий и реакции компьютера на них*;

г) *определить наличие у компьютера внешних устройств, накопителей информации на жестких магнитных дисках и картах памяти, виртуального диска;*

д) *определить наличие у компьютера внешних устройств удаленного доступа к системе и определить их состояние (отразить в протоколе), после чего разъединить сетевые кабели так, чтобы никто не мог изменить или уничтожить информацию в ходе обыска (например, отключить телефонный шнур из модема);*

е) *скопировать программы и файлы данных. Копирование осуществляется стандартными средствами операционной системы;*

ж) *выключить подачу энергии в компьютер и далее действовать по схеме «компьютер не работает»*[2].

Если компьютер не работает, следует:

а) точно отразить в протоколе следственного действия и на прилагаемой к нему схеме местонахождение компьютера и его периферийных устройств;

---

[1] Криминалистика. Полный курс: учебник для вузов / под общ. ред. А.Г. Филиппова. 5-е изд., перераб. и доп. М.: Юрайт, 2020. 855 с. Серия: Бакалавр. Углубленный курс.

[2] Там же.

б) точно описать порядок соединения между собой этих устройств с указанием особенностей (цвет, количество соединительных разъемов, их спецификация) соединительных проводов и кабелей; перед разъединением полезно осуществить видеозапись или фотографирование мест соединения;

в) с соблюдением всех мер предосторожности разъединить устройства компьютера, предварительно обесточив его;

г) упаковать раздельно носители (диски, карты памяти и др.) и поместить их в оболочки, не несущие заряда статического электричества;

д) упаковать каждое устройство и соединительные кабели, провода;

е) особой осторожности требует транспортировка жесткого диска.

Отдельного внимания заслуживают особенности поиска и изъятия информации, следов воздействия на нее в компьютере и его устройствах.

В компьютере информация может находиться непосредственно в **оперативном запоминающем устройстве** (ОЗУ) при выполнении программы, в ОЗУ периферийных устройств и на **внешних запоминающих устройствах** (ВЗУ)[1].

Наиболее эффективным и простым способом фиксации данных из ОЗУ является распечатка на бумагу информации, появляющейся на мониторе. Так же можно использовать специализированное программное обеспечение для сохранения и последующей визуализации дампа памяти.

Дамп памяти – это копия содержимого оперативной памяти, находящаяся на жёстком диске или другом энергонезависимом устройстве памяти[2]. Естественно, дампом может быть не вся оперативная память, а только какая-то определённая её часть, которая, так сказать, интересует в данный момент ту программу, которая делает этот дамп.

Рассмотрим **один из способов** получения дампа памяти:

1. Правой кнопкой мышки щелкнуть по значку «Мой компьютер». Выбрать пункт меню «Свойства», появится окно «Система», далее пункт «Защита системы» (рис. 7).

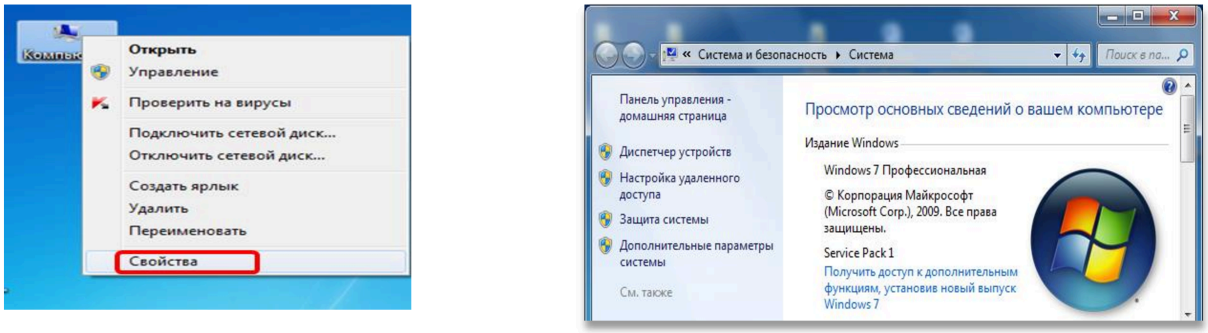


Рис. 7. Всплывающее меню на элементе «Мой компьютер»

[1] Криминалистика. Полный курс: учебник для вузов / под общ. ред. А.Г. Филиппова. С. 417.
[2] Юдин М., Куприянова А., Матвеев М. Windows XP. Полное руководство 2010 // Наука и Техника. 2010. Ст. 65.

2. Появится окно «Свойства системы». Перейти на вкладку «Дополнительно», выбрать «Параметры» (рис. 8).

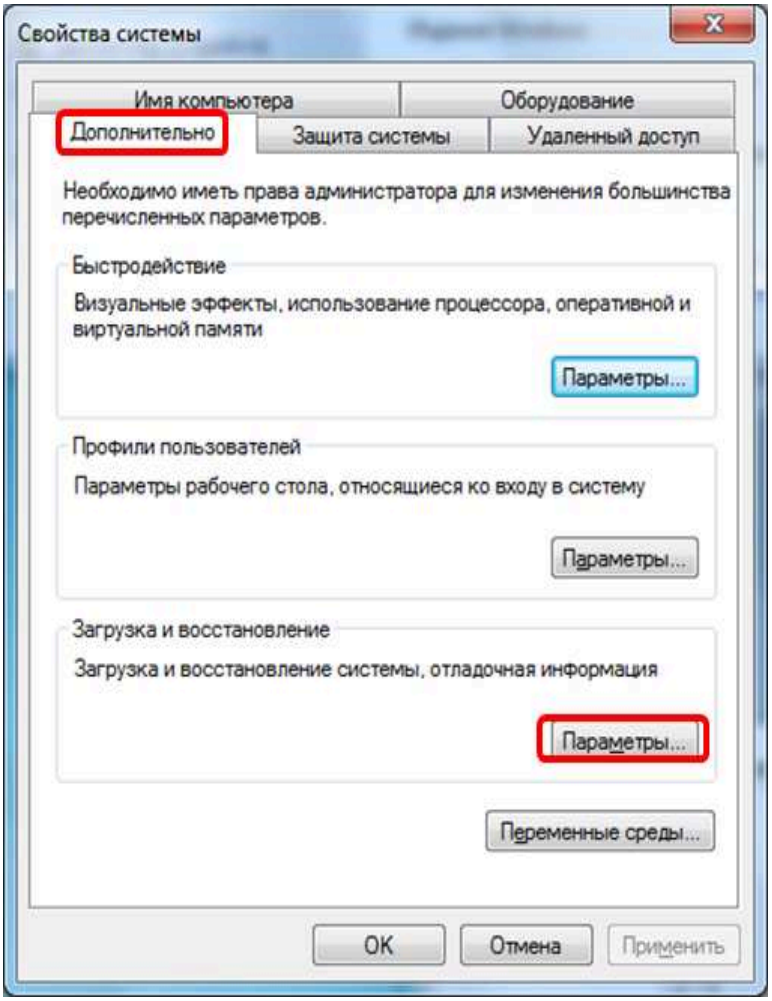


Рис. 8. Свойства системы

3. Снять галочку с «Выполнить автоматическую перезагрузку» (на рис. 9 обозначено 1).

4. Указать путь, по которому будет создан дамп – 3.

5. В секции «Запись отладочной информации» (см. рис. 9) выбрать «Дамп памяти ядра». Для этого необходимо щелкнуть по выпадающему списку (см. рис. 10).

6. Нажать кнопку ОК. По указанному адресу будет записан дамп памяти.

Если в процессе работы система упадет в BSOD (до того, как Вы ее настроили, как указано выше), найдите в каталоге windir\minidump\ (где windir – каталог, куда установлена операционная система, обычно «Windows») файл вида MiniMMDDYY-NN.dmp, где DD, MM и YY – сегодняшний день, месяц и год соответственно, NN – порядковый номер файла дампа. Скорее всего, он там будет не один.

Если Вы указали дамп памяти ядра, то дамп будет находиться в каталоге Windows с именем Memory.dmp.

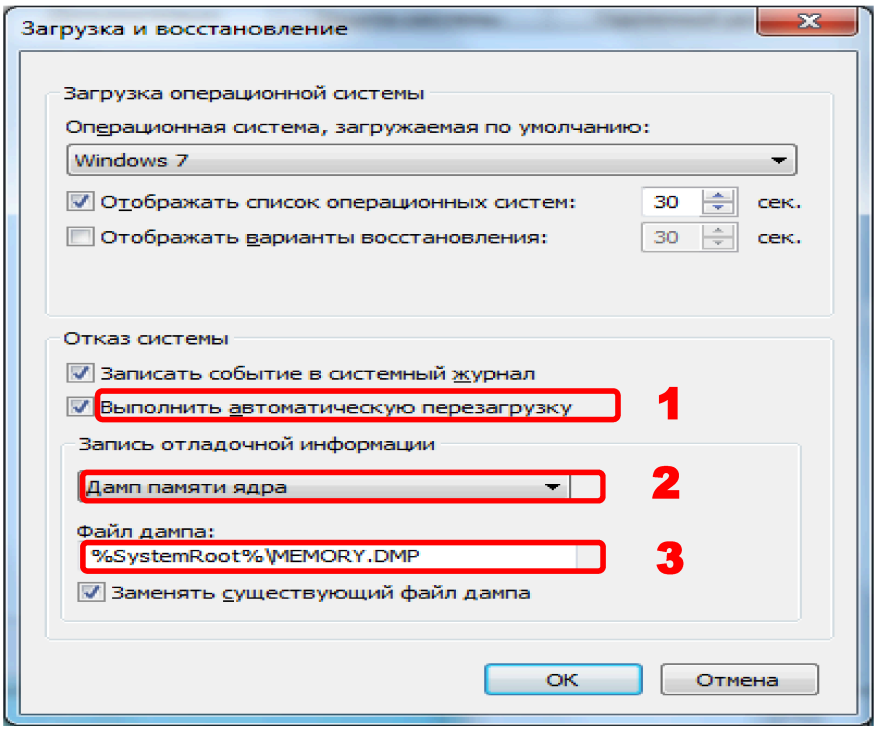


Рис. 9. Загрузка и восстановление

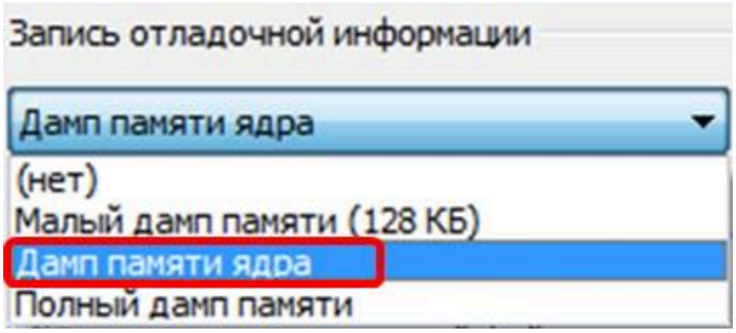


Рис. 10. Запись отладочной информации

Если компьютер не работает, информация может находиться в ВЗУ и других компьютерах информационной системы или в «почтовых ящиках» электронной почты или сети ЭВМ.

Необходимо произвести детальный осмотр файлов и структур их расположения, лучше это осуществить с участием специалиста в лабораторных условиях или на рабочем месте следователя.

Следует обращать внимание на поиск так называемых «скрытых» файлов и архивов, где может храниться важная информация.

Периферийные устройства ввода-вывода могут также некоторое время сохранять фрагменты программного обеспечения и информации, однако для вывода этой информации необходимы глубокие специальные познания.

Осмотр компьютеров и **изъятие компьютерной техники** производится в присутствии понятых, которые расписываются на распечатках информации, изготовленных в ходе осмотра.

В ходе осмотров по делам данной категории могут быть обнаружены и изъяты следующие виды важных документов, которые могут стать вещественными доказательствами по делу:

а) документы, носящие следы совершенного преступления, – телефонные счета, пароли и коды доступа, дневники связи и пр.;

б) документы со следами действия аппаратуры. Всегда следует искать в устройствах вывода (например, в принтерах) бумажные носители информации, которые могли остаться внутри их в результате сбоя в работе устройства;

в) документы, описывающие аппаратуру и программное обеспечение;

г) документы, устанавливающие правила работы с ЭВМ, нормативные акты, регламентирующие правила работы с данной ЭВМ, системой, сетью, доказывающие, что злоумышленник их знал и умышленно нарушал;

д) личные документы подозреваемого или обвиняемого[1].

Комплекс неотложных следственных действий обязательных для первоначального этапа расследования также включает:

1. Проведение обыска в служебном помещении, на рабочем месте подозреваемого с целью обнаружения и изъятия физических носителей компьютерной информации и других документов, имеющих или возможно имеющих отношение к несанкционированному использованию программного обеспечения или носящих иные следы подготовки к преступлению.

2. Назначение и производство **компьютерно-технических** экспертиз, которые, в свою очередь, подразделяются на следующие виды:

– *аппаратно-компьютерные*, где предметом исследования являются факты и обстоятельства, устанавливаемые на основе исследования закономерностей эксплуатации аппаратных средств компьютерной системы – материальных носителей информации о факте или событии гражданского либо уголовного дела;

– *программно-компьютерные*, где предметом исследования являются закономерности разработки и применения программного обеспечения компьютерной системы;

– *информационно-компьютерная* (экспертиза данных), она **является ключевым видом** судебных компьютерно-технических экспертиз, которая позволяет осуществить поиск, обнаружение, анализ и оценку информации, подготовленной пользователем или созданной программами для организации информационных процессов в компьютерной системе;

– *компьютерно-сетевая* экспертиза. Она позволяет исследовать функциональное предназначение компьютерных средств, реализующих какую-либо сетевую информационную технологию[2].

---

[1] Криминалистика. Полный курс: учебник для вузов / под общ. ред. А.Г. Филиппова. С. 417.

[2] Россинская Е.Р. Судебная экспертиза в гражданском, административном и уголовном процессе. М.: Норма, 2005. С. 458-467.

Вышеперечисленные виды экспертиз целесообразно производить с привлечением специалистов правоохранительных органов, специалистов в области средств компьютерной техники, специалистов по обеспечению безопасности информации в сфере телекоммуникаций и компьютерных системах[1].

Результаты компьютерно-технической экспертизы **должны быть оформлены в виде заключения эксперта**, которые в дальнейшем можно использовать в виде доказательств в ходе предварительного расследования и судебного исследования, и разрешения уголовных дел по существу[2]. В настоящее время с помощью таких экспертиз **могут решаться задачи идентификационного и диагностического характера**, например:

1. Относится ли изъятое устройство к аппаратным компьютерным средствам.
2. Восстановление информации, ранее содержавшейся на физических носителях и впоследствии стертой или измененной по различным причинам.
3. Установление времени ввода, изменения, уничтожения либо копирования той или иной информации.
4. Расшифровка закодированной информации, подбор паролей и раскрытие систем защиты.
5. Установление авторства, места, средств подготовки и способа изготовления документов (файлов, программ).
6. Выяснение возможных каналов утечки информации из компьютерной сети и помещений.
7. Установление уровня профессиональной подготовки отдельных лиц, проходящих по делу в области программирования и в качестве пользователя.
8. Наличие какой-либо информации о проведении электронных платежей и использовании кодов кредитных карт.
9. Воспроизведение и распечатка всей или части информации, содержащейся на физических носителях. В том числе, находящейся в нетекстовой форме[3].

Таким образом, рассматривая типичные следственные ситуации, встречающиеся в ходе расследования преступлений в сфере телекоммуникаций и компьютерной информации, наиболее часто приходится проводить следующие **следственные** действия:

– контроль и запись переговоров
– следственный осмотр;
– допрос (свидетеля, потерпевшего, обвиняемого, подозреваемого, эксперта, специалиста);
– обыск;
– выемка;
– назначение и производство судебных информационно-технических экспертиз;
– следственный эксперимент.

---

[1] Криминалистика. Полный курс: учебник для вузов / под общ. ред. А.Г. Филиппова. С. 417.
[2] УПК РФ. Ст. 85-89.
[3] Криминалистика. Полный курс: учебник для вузов / под общ. ред. А.Г. Филиппова. С. 417.

Для выявления противоправности действий преступника и поиска следов преступлений, совершаемых в сфере телекоммуникаций и компьютерной информации требуется эксперт, обладающий опытом и знаниями в области электронной техники и информационных технологий никак не меньшими, чем сам преступник. **Без грамотного экспертного заключения привлечение лица к уголовной ответственности, даже при наличии признаков состава преступления, становится проблематичным.**

2.4. ОСОБЕННОСТИ ВЗАИМОДЕЙСТВИЯ СОТРУДНИКОВ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОВД С ПОДРАЗДЕЛЕНИЯМИ СТМ ОВД ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ В ХОДЕ ПРОИЗВОДСТВА ОРМ И СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

Прерогативой каждого сотрудника правоохранительных органов является то, что, не взирая на занимаемую должность, он ежедневно должен вносить свой вклад в недопущение противоправных действий лиц, которые склонны к совершению преступлений. Если преступление будет совершено или допущено, то в таком случае его необходимо своевременно раскрыть, расследовать, выяснить обстоятельства расследуемого преступления, установить лиц, причастных к его совершению, определить роль каждого участника. В предусмотренные законом сроки должны быть установлены все обстоятельства совершенного преступления, собраны доказательства виновности или невиновности лица и обеспечено своевременное назначение ему наказания или освобождение от него.

Специфика уголовно-правовых отношений, возникающих в связи с совершением общественно-опасных деяний, обусловливает особенности механизма осуществления как оперативно-розыскных, в том числе и специальных технических мероприятий, так и параллельное сопровождение их во время производства следственных действий и до окончания уголовного судопроизводства, а в исключительных случаях и на некоторое время, и после него[1]. В таких случаях, когда ведется уголовное преследование лица, предполагаемо виновного в совершении средней тяжести, тяжкого и особо тяжкого преступления, его привлечение к уго-

[1] Алескеров В.И. Применение мер безопасности к участникам уголовного судопроизводства // Вестник Российской Правовой Академии Министерства Юстиции. 2007. № 4. С. 70 – 73.

ловной ответственности и возложение на него мер уголовно-правового воздействия принимает на себя государство в лице специально уполномоченных органов, а потерпевший же при этом выступает в качестве одного из участников уголовного судопроизводства на стороне обвинения.

Так, до недавнего времени такое мероприятие, как прослушивание телефонных и иных переговоров, проводилось только в рамках оперативно-розыскной деятельности, которую регламентировал Федеральный закон «Об оперативно-розыскной деятельности» от 1995 года, тогда как в настоящее время, в связи с выходом ныне действующего Уголовно-процессуального кодекса Российской Федерации, данное мероприятие включено в разряд следственного действия и заложено в нормы ст.186 УПК Российской Федерации [1] (см. схему 1).

Схема 1

Контроль и запись переговоров (ст. 186 УПК РФ)[2]

Контроль телефонных и иных переговоров – это следственное действие, предполагающее прослушивание и запись переговоров путем использования любых средств коммуникации, осмотр и прослушивание фонограмм

↓

При наличии достаточных оснований полагать, что телефонные и иные переговоры подозреваемого, обвиняемого и других лиц могут содержать сведения, имеющие значение для уголовного дела, их контроль и запись допускаются при производстве по уголовным делам о преступлениях средней тяжести, тяжких и особо тяжких преступлениях

↓

В ходатайстве следователя (дознавателя) о производстве контроля и записи телефонных и иных переговоров указываются:

уголовное дело, при производстве которого необходимо применение данной меры;

основания, по которым производится данное следственное действие;

фамилия, имя и отчество лица, чьи телефонные и иные переговоры подлежат контролю и записи;

срок осуществления контроля и записи;

наименование органа, которому поручается техническое осуществление контроля и записи

↓

Основанием является судебное решение, принятое в порядке ст. 165 УПК РФ.
При наличии угрозы совершения насилия, вымогательства и других преступных действий в отношении потерпевшего, свидетеля или их близких родственников, родственников, близких лиц контроль и запись телефонных и иных переговоров допускаются по письменному заявлению указанных лиц, а при отсутствии такого заявления – на основании судебного решения. Постановление о производстве контроля и записи телефонных и иных переговоров **направляется следователем для исполнения в соответствующий орган**

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 01.09.2017).

[2] Шаталов А.С. Уголовно-процессуальный кодекс Российской Федерации в схемах: учебное пособие. М.; Проспект, 2021. 816 с.

Хотя некоторыми специалистами задолго до появления указанной статьи в российском уголовно-процессуальном законодательстве приводились не столько убедительные, сколько эмоциональные доводы против введения этого следственного действия[1]. Однако возникшие требования правительства к компетентным органам по вопросу улучшения эффективности борьбы с преступностью оказались более высоким аргументом, чем мифическая угроза нарушения прав и законных интересов граждан. Более того, в настоящее время ведется дискуссия и о том, что в необозримом будущем данное следственное действие будет проводиться при возникновении необходимости по всем уголовным делам вне зависимости от степени их общественной опасности.

В Российской Федерации охране прав и свобод личности при производстве по уголовным делам, вообще, и на предварительном следствии, в частности, придается весьма важное значение[2]. В связи с чем в целях обеспечения соблюдения конституционного права граждан на тайну телефонных и иных переговоров в УПК Российской Федерации была включена специальная статья[3]. Данная статья является единственным следственным действием, производство которого допускается по возбужденному уголовному делу при наличии достаточных оснований полагать, что телефонные и иные переговоры могут содержать сведения, имеющие значение по уголовному делу. Данное следственное действие является настолько специфичным, что его производство требует помимо тщательной подготовки еще и задействование (подключение) соответствующих оперативных служб[4]. В соответствии с п. 11 ч. 2 ст. 29 УПК Российской Федерации разрешение на производство данного следственного действия уполномочен давать суд в порядке, предусмотренном статьей 165 УПК Российской Федерации. Однако необходимо отметить, что при наличии угрозы совершения насилия, вымогательства и других преступных действий в отношении свидетеля[5], потерпевшего[6] или их близких родственников[7], близких лиц[8], контроль и запись переговоров допускаются по их

---

[1] Савицкий В.М. Правосудие и личность // Советское государство и право. 1983. № 5. С 58.

[2] Шаталов А.С. Контроль и запись переговоров на предварительном следствии: правовые основания, тактические условия, технология проведения // Журнал Высшей школы экономики «Право». 2009. № 3. С. 57-84.

[3] УПК РФ. Ст. 186.

[4] См.: УПК РФ. СТ. 38. п. 4.

[5] В соответствии с частью первой ст. 56 УПК РФ свидетелем является лицо, которому могут быть известны какие-либо обстоятельства, имеющие значение для расследования и разрешения уголовного дела, и которое вызвано для дачи показаний.

[6] В соответствии с частью первой ст. 42 УПК РФ потерпевшим является физическое лицо, которому преступлением причинен физический, имущественный, моральный вред, а также юридическое лицо в случае причинения преступлением вреда его имуществу и деловой репутации.

[7] Близкие родственники – супруг, супруга, родители, дети, усыновители, усыновленные, родные сестра и братья, дедушка, бабушка, внуки. См.: УПК РФ. Ст. 5. п. 4.

[8] Близкие лица – иные, за исключением близких родственников и родственников, лица, состоявшие в свойстве с потерпевшим, свидетелем, а также лица, жизнь, здоровье и благополучие которых дороги потерпевшему, свидетелю в силу сложившихся личных отношений. См.: УПК РФ. Ст. 5. п. 3.

письменному заявлению, а при его отсутствии – на основании судебного решения, вынесенного по ходатайству следователя[1]. Согласно нормам статьи 186 УПК Российской Федерации данное следственное действие не может осуществляться свыше шести месяцев и должно быть прекращено по постановлению следователя, но не позднее окончания предварительного расследования по уголовному делу (см. схема 2).

Схема 2

Общие правила контроля и записи переговоров (ст. 186 УПК РФ)[2]

Срок производства контроля и записи телефонных и иных переговоров не должен превышать шести месяцев

↓

В течение всего срока производства контроля и записи телефонных и иных переговоров следователь вправе в любое время истребовать от органа их осуществляющего, фонограмму для осмотра и прослушивания. Она передается ему в опечатанном виде с сопроводительным письмом, в котором должны быть указаны даты и время начала и окончания записи указанных переговоров и краткие характеристики использованных при этом технических средств

↓

О результатах осмотра и прослушивания фонограммы следователь с участием специалиста (при необходимости), а также лиц, чьи телефонные и иные переговоры записаны, **составляет протокол,** в котором должна быть дословно изложена та часть фонограммы, которая, по мнению следователя, имеет отношение к данному уголовному делу

↓

Фонограмма в полном объеме **приобщается к материалам уголовного дела** на основании постановления следователя **как вещественное доказательство** и хранится в опечатанном виде в условиях, исключающих возможность прослушивания и тиражирования фонограммы посторонними лицами и обеспечивающих ее сохранность и техническую пригодность для повторного прослушивания, в том числе в судебном заседании

---

[1] По законодательству США, например, прослушивание должно быть прекращено не только по окончании срока, но и сразу после того, как были получены искомые доказательства. См.: Махов В.Н., Пешков М.А. Уголовный процесс США (досудебные стадии): учебное пособие. М: ЗАО «Бизнес-школа»; Интел-Синтез», 1998. С. 111. Подобный порядок существует во многих других странах мира. Например, вплоть до 2001 года, в США ордер на прослушивание выдавался как на федеральном уровне, так и на уровне штатов, но только строго определенным кругом судей и лишь по тем обращениям полиции, которые завизированы высшими должностными лицами атторнейской службы. См., напр.: Пешков М. Прослушивание и электронное наблюдение в уголовном процессе США.// Российская юстиция. 1997. № 4. С 56. После беспрецедентных по жесткости и масштабам терактов 11 сентября 2001 г. спецслужбы этой страны получили упрощенный доступ к телефонам граждан благодаря специальному закону – Патриотическому акту. Этот упрощенный доступ имел конкретный срок и должен был завершить свое действие не раз. Однако спецслужбы США снова и снова утверждали в Конгрессе его обновленную версию.

[2] Шаталов А.С. Уголовно-процессуальный кодекс Российской Федерации в схемах: учебное пособие. М.; Проспект, 2021. 816 с.

При производстве такого действия, как контроль и запись телефонных и иных переговоров, следователь имеет право в любое время истребовать от органа, их осуществляющего, фонограмму для просмотра и прослушивания. Фонограмма передается следователю в опечатанном виде с сопроводительным письмом, в котором должны быть указаны даты, время начала и окончания записи переговоров лица, интересующего следствие, а также краткие характеристики использованных при этом технических средств. О результатах осмотра и прослушивания фонограммы следователь с участием понятых и, при необходимости специалиста, а также лиц, чьи телефонные и иные переговоры записаны, составляет протокол, где должна быть дословно изложена та часть фонограммы, которая, по мнению следователя, имеет отношение к данному уголовному делу. Фонограмма в полном объеме приобщается к материалам уголовного дела на основании постановления следователя в виде вещественного доказательства. Ее хранение должно осуществляться в опечатанном виде в условиях, исключающих возможность ее прослушивания и тиражирования посторонними лицами и обеспечивающих, кроме того, сохранность и техническую пригодность фонограммы для необходимого последующего прослушивания[1]. Такова законодательная рекомендация порядка производства контроля и записи переговоров.

Состязательный характер действующего российского уголовного судопроизводства, жесткие требования законодателя к ходу и результатам предварительного расследования, а также к решениям, которые могут быть приняты судом по его итогам порождают для современной отечественной криминалистики необходимость разработки новых научных положений и основанных на них теоретических рекомендаций, относящихся к особенностям проведения этого следственного действия и соответствующего оперативно-розыскного мероприятия, к определению наиболее целесообразной линии поведения осуществляющих его лиц[2].

В настоящее время методы и познавательные технологии, используемые сотрудниками оперативных подразделений, во многих случаях не позволяют сохранять процессуальную безупречность криминалистически значимой информации, полученной при производстве оперативно-розыскных мероприятий с использованием даже современных технико-криминалистических возможностей.

Иными словами, при производстве одноименного специального технического мероприятия не всегда удается добиться соблюдения всех требований, предъявляемых уголовно-процессуальным законом к доказательствам. В результате чего, собранные оперативными сотрудниками сведения о переговорах и других, в широком понимании этого значения, задокументированных действиях лиц могут признаваться судом недопустимыми в доказывании их преступной деятельности в ходе судебного рассмотрения и окончательного

---

[1] УПК РФ. Ст.186. Ч. 5-8.

[2] Шаталов А.С. Контроль и запись переговоров на предварительном следствии: правовые основания, тактические условия, технология проведения … С. 57-84.

разрешения по уголовным делам. В целях улучшения получения качества необходимой информации при ее документировании на протяжении всех последних лет ведется дискуссия с участием научных и практических сотрудников, результаты которых доводятся до соответствующих служб правоохранительной системы Российской Федерации. В связи с чем, наряду с необходимой правовой базой, правоохранительные органы Российской Федерации получают в свое распоряжение технические средства, специально созданные для обнаружения, фиксации, изъятия и проверки криминалистически значимой информации путем производства специальных технических мероприятий, а также право на использование в этих целях любых средств коммуникации[1].

Следователь и сотрудники оперативно-розыскных подразделений заинтересованы в своевременном раскрытии подготавливаемых или уже совершенных преступлений и успешном расследовании уголовных дел, для чего им необходимо установить причастность разрабатываемого, подозреваемого, обвиняемого, а в ряде случаев и подсудимого лица (фигуранта) к совершенному преступлению. В тех случаях, когда возникает ситуация для проведения оперативно-розыскных мероприятий, указанным должностным лицам необходимо поэтапно совершить следующие действия, а именно:

1) принятие решения о производстве необходимого мероприятия (действия) и согласование своего решения с руководителем органа;

2) получение разрешения на осуществление данного мероприятия;

3) поручение технического осуществления органу, уполномоченному на производство конкретного специального технического мероприятия;

4) истребование полученных результатов;

5) осмотр полученных в ходе проведения ОРМ результатов;

6) оценка полученных результатов;

7) подготовка и приведение полученных результатов к соответствующей форме для их последующего приобщения к материалам уголовного дела в качестве вещественного доказательства;

8) приобщение полученных результатов к материалам уголовного дела в качестве вещественного доказательства.

После совершения всех вышеперечисленных действий у оперативного сотрудника появляется ***основание для использования*** полученных результатов в процессе доказывания по уголовному делу. Таким образом, анализ правовых оснований и тактических условий рассматриваемых (проводимых) специальных технических мероприятий позволяет убедиться в том, что их суть заклю-

---

[1] Действующими нормативными актами предусматривается обязательная установка и эксплуатация оборудования в учреждениях связи для проведения следственных действий и оперативно-розыскных мероприятий. См.: Об упорядочении организации и проведения следственных действий и оперативно-розыскных мероприятий с использованием технических средств: Указ Президента Российской Федерации от 1 сентября 1998 г. № 891; Об утверждении требований к сетям электросвязи для проведения оперативно-розыскных мероприятий. Приказ Мининформсвязи РФ от 16.01.2008 № 6.

чается в организации практического осуществления контроля, как в целях оперативно-розыскных мероприятий, так и в процессуальном плане. Иными словами, при расследовании уголовных дел специально уполномоченными участниками уголовного судопроизводства создаются необходимые условия для целенаправленного собирания интересующей следствие криминалистически значимой информации. Необходимость ее получения, целесообразность и последующая результативность использования в доказывании по уголовному делу предопределены не только строгим соблюдением законодательных предписаний, имеющих прямое отношение к проведению специальных технических мероприятий, но и применением криминалистической технологии, учитывающей самые разнообразные закономерные связи[1]. Полученная криминалистически значимая информация имеет универсальный характер и, в принципе, может применяться для познания каждого из обстоятельств, входящих в предмет доказывания по уголовному делу[2]. Мы не будем останавливаться на каждом виде специальных технических мероприятий, но при производстве любого из них всегда присутствует компонент негласности, дефицит протяженности во времени, за исключением контроля и записи переговоров. Оно выгодно отличается от любого вида СТМ, и, естественно, обуславливает вполне определенную последовательность действий следователя и оперативного сотрудника для легализации средства доказывания. Технологическая последовательность специальных технических мероприятий начинается с принятия решения об их проведении. Каждое возникающее в зависимости от оперативно-розыскной и следственной ситуации проводимое специальное техническое мероприятие имеет свою технологию, ранее апробированную и основанную на теоретических научных рекомендациях, что дает оперативным сотрудникам ОВД и следователям вырабатывать оптимальную линию поведения по вопросам взаимодействия. Такое взаимодействие положительно сказывается на получении **относимых, допустимых, достаточных и достоверных доказательств,** что в последующем играет неоценимую роль в окончательно раскрытии преступлений.

Вместе с тем принятие решения о проведении одного из видов специальных технических мероприятий неминуемо влечет за собой определенные ограничения конституционных прав и свобод граждан, в связи с чем ***должны быть соблюдены все условия о недопустимости разглашения любых (полученных) данных***, необходимых в дальнейшем с их практической реализацией в процессе доказывания преступной деятельности разрабатываемых лиц, подозреваемых в совершении преступления.

---

[1] В криминалистике под технологией следственного действия принято понимать систему раскрывающих его механизм операций, каждая из которых основывается на требованиях уголовно-процессуального закона и рекомендациях криминалистики. См., напр.: Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика: учебник для вузов / под ред. Р.С. Белкина. М., 1999. С. 549-678; Юрина Л.Г., Юрин В.М. Указ. соч. С. 69 и др.

[2] Шаталов А.С. Контроль и запись переговоров на предварительном следствии: правовые основания, тактические условия, технология проведения … С. 57-84.

Для наглядности приведем один из примеров, взятый из практических наработок ПСТМ:

Сотрудниками Управления «К» УМВД России по Н-ской обл. была получена оперативная информация о том, что некоторые врачи отделения гинекологии при оказании медицинских услуг различного характера систематически получали от своих пациентов взятки. В результате проведения проверочных действий несколько врачей-гинекологов и медицинская сестра-акушерка были взяты на оперативный учет по окраске «взяточничество».

В ходе отработки первичной информации было принято решение о взятии данной категории врачей под проведение конкретных мероприятий на основании судебного решения. В процессе осуществления последовательных оперативно-розыскных мероприятий оперативными сотрудниками была получена информация, что врач-гинеколог совместно с медсестрой-акушеркой, принимая роды, допустили серьезную врачебную ошибку. Таким образом, указанные лица совершили преступление в виде халатности, злоупотребления должностными полномочиями и др. В целях уклонения от уголовной ответственности и сокрытия следов совершения преступления, посоветовавшись друг с другом, медработники приняли решение утопить младенца-новорожденного в ведре с водой. Их преступный сговор был направлен на совершение убийства и нашел свое отражение: новорожденный ребенок был убит путем утопления. В результате своевременно полученной и задокументированной информации в отношении разрабатываемых лиц, изобличающей их преступную деятельность, данное преступление было раскрыто благодаря тесному взаимодействию сотрудников оперативных и следственных подразделений органов внутренних дел.

Данный пример красноречиво говорит о следующем:

1. Поступила первичная информация о совершении преступной деятельности на группу лиц, которая при осуществлении медицинских услуг систематически получали взятки.

2. Своевременно группа фигурантов была взята на оперативный учет по окраске «взяточничество».

3. В ходе разработки и изобличении данной преступной группы путем документирования было принято решение о проведении необходимых СТМ.

4. В результате проведения одного из намеченных СТМ была получена информация как о взяточничестве разрабатываемых лиц, так и о совершении одного из видов тяжкого преступления – убийство новорожденного ребенка, путем утопления его в ведре с водой.

5. Данная информация была своевременно передана в структурное оперативное подразделение органов внутренних дел.

6. В результате полученной оперативной информации была проведена оперативная комбинация, в ходе которой разрабатываемые лица были задержаны и изобличены в содеянных преступлениях.

7. Вина их полностью доказана, и виновные лица понесли наказание в соответствии с нормами действующего уголовно-процессуального законодательства.

В разных регионах страны подходы к своевременному получению необходимой криминалистически значимой информации значительно отлича-

ются. В связи с этим взаимодействие между оперативными подразделениями необходимо упорядочить и привести к единой алгоритмизации согласно действующим нормативным правовым документам, а также в соответствии с возникающей ситуацией в ходе раскрытия и расследования преступлений. В данном случае необходимы оперативность, конкретика, наличие унифицированных алгоритмов взаимодействия.

Как известно, оперативно-розыскная или следственная ситуация являются величинами переменными, поэтому при принятии решения о проведении того или иного оперативно-розыскного мероприятия сотрудники, наделенные такими полномочиями, обязаны учитывать сведения и иного рода, обладающие признаками постоянства, которые содержат в себе:

1. Нормы УК РФ, позволяющие отнести расследуемые преступления к категории средней тяжести, тяжким и особо тяжким.

2. Нормы УПК Российской Федерации, определяющие полномочия участников контроля и записи переговоров, предмет и пределы доказывания, общие условия и порядок производства этого следственного действия.

3. Научные положения криминалистической тактики и основанные на них рекомендации, предназначенные для применения в условиях типичной оперативно-розыскной и следственной ситуации[1].

4. Собственный опыт оперативных сотрудников и следователей в принятии решений о проведении оперативно-розыскных мероприятий.

5. Оценивание полученной криминалистически значимой информации, последующая ее легализация и использование в процессе доказывания.

Как бы ни складывалась та или иная оперативно-следственная ситуация, в любом случае сотрудники, наделенные правами документирования фактов, имеющих отношение к преступной деятельности разрабатываемых лиц, и последующего эффективного расследования уголовного дела, всегда должны знать о предпочтительной последовательности и нюансах практической реализации полученных следов. Задокументированная информация признается вещественным доказательством и в дальнейшем приобщается к материалам уголовного дела. В ходе взаимодействия оперативных сотрудников органов внутренних дел со следователями при проведении оперативно-розыскных мероприятий иногда возникают и типичные ситуации, которые поддаются алгоритмизации и программированию. Однако все принимаемые решения должны носить законную правовую основу[2] и содержать в себе обоснованность, мотивированность, своевременность и реальность их исполнения. Законность предполагает, что принимаемое решение предусмотрено действующим законодательством и полностью ему соответствует. Обоснованность выражает необходимость проведения конкретного оперативно-розыскного мероприятия, подтверждается совокупностью фактических данных, имеющихся в распоряжении, как оперативных сотрудников, так и следователей. Мотивированность свидетельствует, что решение опирается на доводы, обеспечивающие его обоснованность, а своевременность заключается в принятии данного решения в наиболее подходящий момент. Естественно, со-

---

[1] Шаталов А.С. Контроль и запись переговоров на предварительном следствии: правовые основания, тактические условия, технология проведения … С. 57-84.

[2] См.: УПК РФ. Ст. 7. Ч. 4.

здание всех вышеперечисленных условий – задача очень непростая. Однако ее решение должно быть осуществлено в рамках подготовки к проведению как оперативно-розыскного мероприятия, так и при производстве следственного действия (контроль и запись телефонных и иных переговоров), что является одним из основных звеньев в технологической цепочке по взаимодействию оперативных сотрудников и следователей в ходе раскрытия и расследования преступлений.

Как показывает анализ деятельности сотрудников соответствующих структурных подразделений органов внутренних дел Российской Федерации, в 2016-2020 гг. можно отметить высокую эффективность по тесному взаимодействию следственных действий и оперативно-розыскных мероприятий (далее ОРМ), проводимых в отношении лиц, скрывающихся от правосудия. Эти выводы подтверждаются полученными сведениями, содержащимися в оперативно-справочных учетах ГИАЦ МВД России.

Вместе с тем нельзя забывать и о том, что в настоящее время в связи с быстро развивающимися информационными технологиями разработаны и активно используются новые возможности (Wi-Fi сети общего доступа), *позволяющие пользователям обмениваться сообщениями без выхода и подключения в сеть сотовой связи*. Данное обстоятельство создает благоприятные условия лицам, замышляющим или уже совершившим преступление, избежать ответственности и своевременно быть разоблаченными и наоборот создает значительные трудности сотрудникам при проведении оперативно-розыскных мероприятий и в ходе документирования следов совершения преступлений.

2.5. НЕКОТОРЫЕ ВИДЫ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

В настоящее время основными видами преступлений, совершаемых в телекоммуникационных сетях, являются:

1. Преступления в проводных телекоммуникационных сетях:

а) преступления в отношении операторов фиксированной (проводной) связи:

- воздействие на технические средства операторов.

Данный вид правонарушений трудно поддаётся уголовно-правовой квалификации, так как зачастую находится на границе уголовного и гражданского права.

Правонарушение совершается по следующей схеме: злоумышленники предоставляют гражданам и организациям услуги связи (традиционной телефонии, IP-телефонии) по ценам значительно ниже рыночных, не создавая при этом альтернативной инженерной инфраструктуры (линейно-кабельных сооружений, линий связи и т.п.), а используя оборудование того или иного оператора проводной связи (см. рис. 11).

Такое правонарушение, как правило, причиняет ущерб охраняемым законом интересам операторов, занимающих существенное положение в сети связи общего пользования, является длящимся и совершается группой лиц (либо лицами), имеющих необходимую техническую подготовку.

- аренда номеров и каналов с последующей неоплатой.

Суть данного правонарушения заключается в его определении. Лица (физические и юридические) арендуют у оператора связи абонентские номера, при этом оплату аренды в соответствии с заключенным договором не осуществляют. Данный вид правонарушений также может рассматриваться как в рамках уголовного, так и гражданского законодательства. В данном случае ущерб наносится операторам связи, так как они не получают от клиента оплату за предоставленные услуги;

б) преступления с использованием ресурсов фиксированной связи:

- неправомерный доступ к учрежденческим автоматическим телефонным станциям (далее – УАТС) с последующей генерацией трафика (несанкционированный доступ к оборудованию УАТС с целью генерации трафика на абонентские номера с услугой звонка за дополнительную плату (платные номера) международных операторов). Несанкционированный доступ к УАТС (взлом УАТС, PBX[1], IP-PBX[2]) путем использования изъянов (уязвимостей) в настройках УАТС (функции DISA, командного интерфейса, стека протоколов TCP/IP) со стороны злоумышленников реализуется следующими способами.

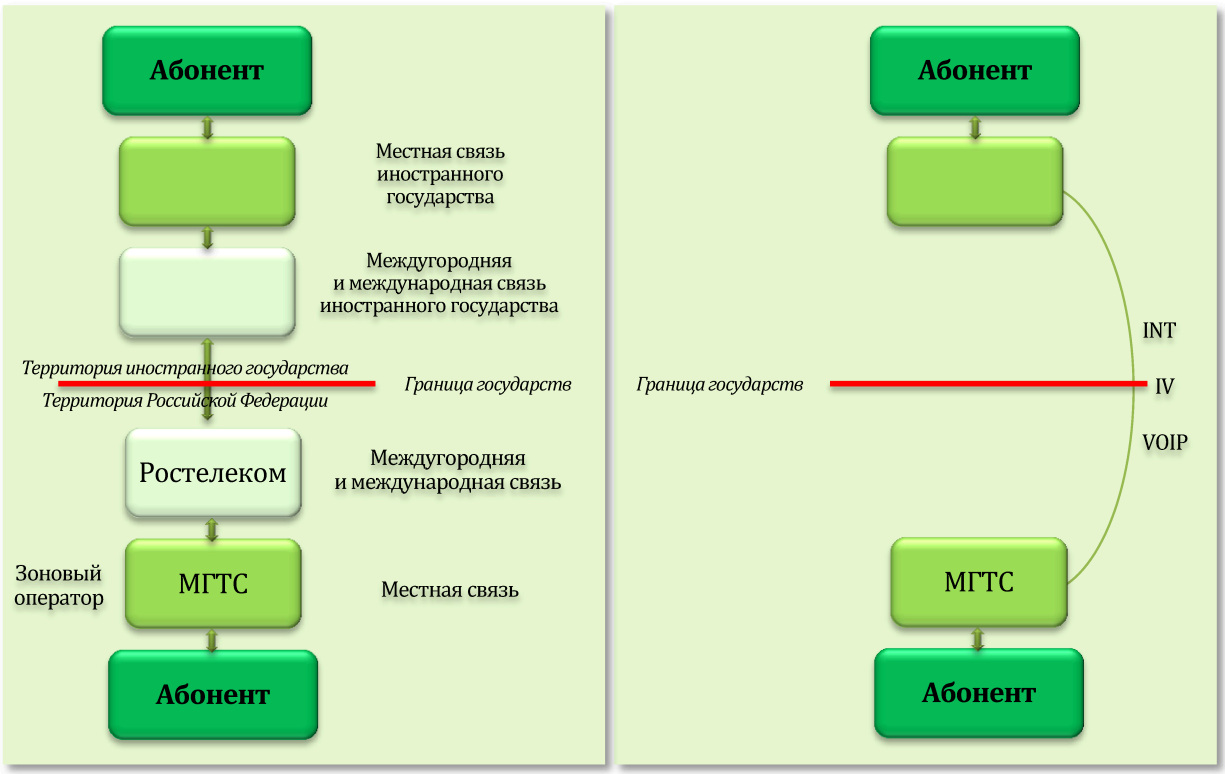


Рис. 11. Работа операторов фиксированной (проводной) связи

---

[1] Английский термин, обозначающий офисную телефонную станцию, обеспечивающую установление, поддержание и разрыв соединений между аппаратами, т.е. коммутацию. Система PBX необходима любой организации, так как позволяет организовать телефонную связь на предприятии.

[2] Учрежденческая телефонная станция на основе межсетевого протокола IP. Как и обычная УАТС, IP-PBX призвана выполнять те же и другие функции; так как почти все функции реализованы через программное обеспечение, то в IP-PBX легко наращивать функционал, модернизировать его, исправлять ошибки.

Способ 1. Паразитная генерация трафика (соединения с большой длительностью, отличающейся от средней длительности коммерческого вызова) на конкретные зарубежные В-номера (или диапазоны В-номеров) с целью извлечения финансовой выгоды при получении оплаты трафика за указанные вызовы со стороны оператора связи, предоставляющего указанные В-номера в продажу.

Противоправные действия совершаются по такой схеме (рис. 12): злоумышленники, используя средства мобильной связи или сеть Интернет, осуществляют несанкционированный доступ к УАТС клиента и направляют трафик на В-номера, которые арендуются сообщниками злоумышленников у операторов местной связи неразвитых стран (Африка, Южная Америка, Океания, Зимбабве, Лихтенштейн, Сьерра Леоне и т.п.), поскольку указанные операторы предлагают тарифы, предусматривающие выплату денежного вознаграждения злоумышленнику за определенный объем входящего трафика, сгенерированного на такие В-номера (например, это такие услуги с добавленной стоимостью, как секс по телефону, развлекательные диалоги, реклама, онлайн игры, викторины и т.п.).

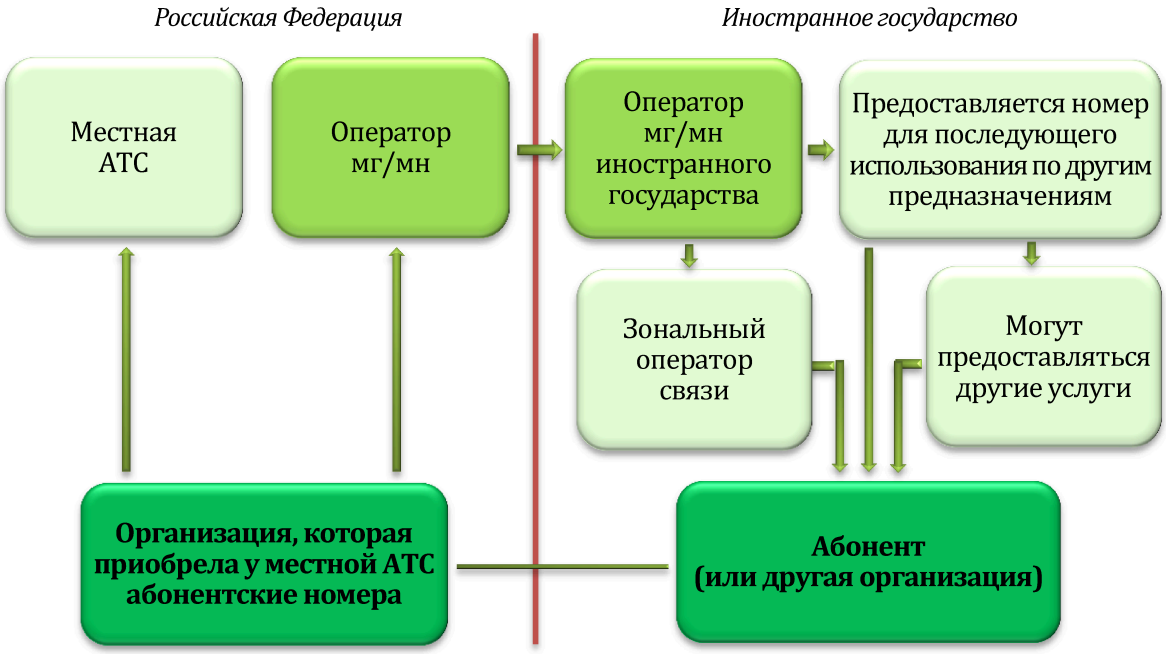


Рис. 12. Схема работы несанкционированного доступа к УАТС с целью генерации трафика на абонентские номера с услугой звонка за дополнительную плату (платные номера) международных операторов

Размещение таких номеров в неразвитых странах связано с наличием свободных экономических зон, ***не предусматривающих ответственности за взаиморасчеты с зарубежными операторами, а также за отсутствие***

законодательства в сфере пресечения киберпреступности в области средств и сетей связи.

В результате данных деяний реальные расходы за пропуск и терминацию трафика оплачивают «взломанный» клиент (УАТС) и оператор связи, осуществляющий транзит указанного трафика на сеть другого мн-оператора. Как правило, ***клиент отказывается*** от оплаты за такой трафик в связи с большим объемом и дорогостоящим тарифом, ***убытки же терпит оператор***.

Способ 2. Использование УАТС для транзита коммерческого трафика с целью извлечения финансовой выгоды мошенниками при перепродаже данного трафика через VoIP-биржи трафика.

Противоправные действия совершаются по следующей схеме: злоумышленники, используя сеть Интернет, осуществляют несанкционированный доступ к УАТС клиента, далее этими лицами осуществляется настройка приема трафика на УАТС с источника, указываемого в настройках злоумышленниками. Затем злоумышленники направляют коммерческий трафик, который они покупают на VoIP-бирже трафика, на эту УАТС, получая денежное вознаграждение за пропуск и терминацию трафика, при этом реальные расходы за пропуск и терминацию трафика оплачивают взломанный клиент (УАТС) и мг/мн-оператор, осуществляющий транзит указанного трафика на сеть другого мн-оператора.

Как правило, **клиент отказывается** от оплаты за такой трафик в связи с большим объемом и дорогостоящим тарифом, **убытки же терпит оператор**.

Так, например, в сетях операторов Московского региона еженедельно происходят случаи несанкционированного доступа к УАТС клиентов, выявляются случаи взлома оборудования, тем самым наносится значительный ущерб.

Еще одним видом преступлений в проводных сетях является организация ISUP-шлюзов на сетях операторов связи для нелегальной терминации междугороднего и международного трафика, в том числе с подменой вызывающего номера.

Предпосылками для совершения данных деяний являются:

- во-первых, большое различие в тарифах за терминацию трафика на международном и зоновом уровнях и очень низких тарифах за терминацию VOIP-трафика;

- во-вторых, существование бирж по продаже VOIP-трафика (например, voipexchange.com), и, наконец, ***отсутствие нормативной базы по вопросам регулирования терминации VOIP трафика на телефонные сети общего пользования***.

Данные противоправные деяния совершаются по следующей схеме: злоумышленник подает заявку на подключение к оператору и выполняет организацию присоединения к узлам связи на локальном или зоновом уровне с использованием потоков E1 (цифровой поток передачи данных, аналогичный 30 телефонным линиям) или IP-канала. С другой стороны, указанное лицо

подключается к интернет-провайдеру, затем ***устанавливает VOIP-шлюз***[1], предназначенный для приема и преобразования VOIP-голосового трафика в формат TDM-канала, **реализуя стык** между указанными сетями. Далее злоумышленник регистрируется на бирже трафика и объявляет о возможности терминации трафика на сеть оператора связи, к которому присоединен, по определенному тарифу. Биржа продает заявленные им услуги по терминации трафика на рынке ***«серого»*** трафика.

Данная схема терминации трафика приводит к таким проблемам для оператора, как претензии абонентов, принявших звонки с измененными АОН, в связи с подменой оригинального номера вызывающего абонента, арендуемого злоумышленником у оператора связи; претензии абонентов, связанные с низким качеством услуг связи; загрузка соединительных линий, арендуемых у оператора.

Подмена оригинального номера вызывающего абонента недопустима согласно действующим нормативным правовым актам:

- приказу Минкомсвязи Российской Федерации от 16 января 2008 г. № 6 «Об утверждении требований к сетям электросвязи для проведения оперативно-разыскных мероприятий» в части сокрытия (или модификации) А-номера при передаче его на пункт управления;

- приказу Минкомсвязи Российской Федерации от 8 августа 2005 г. № 98 «Об утверждении требований к порядку пропуска трафика в телефонной сети связи общего пользования»;

- приказу Минсвязи и массовых коммуникаций Российской Федерации от 16 апреля 2014 г. № 83 «Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий»;

- условиям лицензий операторов местной связи при приеме и шлюзовании международного трафика от зарубежных операторов на своем оконечном оборудовании связи через сети передачи данных (IP-сети, Интернет) и его терминации на телефонные сети общего пользования.

Кроме того, в действиях злоумышленников усматриваются признаки состава преступления, предусмотренного ст. 171 УК РФ «Незаконное предпринимательство» – осуществление незаконной предпринимательской деятельности клиентами – юридическими лицами, подключенными к услугам сети связи, путем перепродажи трафика и оказания услуг связи третьим лицам).

---

[1] Устройство, имеющее подключение к нескольким сетям с различными видами технологий доступа, таких как IP-сети (Интернет, IP-PBX-предприятия, VoIP-оператор и т.д.), аналоговым линиям сетей фиксированной связи, E1 TDM-потокам, с одной стороны, и к сети радиодоступа (RAN) GSM/CDMA/UMTS-оператора - с другой.

2. Преступления в беспроводных телекоммуникационных сетях:

а) преступления в отношении операторов мобильной связи:

- незаконное использование GSM-шлюзов.

Остановимся подробнее на определении шлюзов и принципах его работы.

Модель получения выгоды от применения GSM-шлюза основана на разнице тарифов для вызовов внутри сети оператора сотовой связи и тарифов для межсетевого, междугородного и международного трафиков. В основе этой распространенной схемы получения дохода от нелегальной схемы терминации трафика лежат использование льготных пакетов услуг или безлимитных тарифов, и очень низкая стоимость передачи трафика через Интернет с применением VoIP-технологий.

Злоумышленник приобретает GSM/CDMA/UMTS-шлюз, устанавливает в него sim-карты оператора (-ов), на сеть которого планируется выполнять терминацию трафика. С другой стороны, он подключается к интернет-провайдеру, реализуя связь между сетями (рис. 13). Далее злоумышленник регистрируется на бирже трафика и объявляет о возможности терминации трафика на сеть оператора связи, sim-карты которого используются в шлюзе, по определенному тарифу. Биржа продает заявленные им услуги по терминации трафика на рынке «серого» трафика. Данный вид правонарушений является широко распространённым: так, например, на сети московских операторов мобильной связи факты работы GSM-шлюзов выявляются еженедельно.

Рис. 13. Осуществление злоумышленником связи между сетями

- нанесение ущерба путем инициализации трафика на «короткие номера».

Данный вид правонарушений появился относительно недавно, вскоре после внедрения операторами мобильной связи такого сервиса, как короткие номера, которые позволяют совершать операции с денежными средствами при помощи электронных платежных систем.

Рис. 14. Варианты схем современного телефонного мошенничества

Правонарушители действуют следующим образом: участниками группы по поддельным документам приобретаются ***постоплатные (кредитные) sim-карты компаний – сотовых операторов***. С помощью специального оборудования участники группы отправляют с данных sim-карт на заранее арендованные короткие номера платные sms-сообщения, что образует отрицательный баланс и причиняет оператору ущерб в особо крупном размере. Полученные денежные средства впоследствии **выводятся через электронные платежные системы** и распределяются среди участников группы.

- заключение фиктивных контрактов на предоставление услуг связи.

Правонарушения совершаются следующим образом: группа лиц с целью получения вознаграждения за привлечение большого количества абонентов заключает фиктивные контракты на предоставление услуг сотовой связи, активирует их, а затем обращается к оператору за выплатой дилерского вознаграждения.

Данный вид правонарушений основан на отсутствии законодательно закрепленной ответственности за осуществление действий по подключению пользователей к сети подвижной радиотелефонной связи лицами, не имеющими на это надлежащих полномочий от оператора связи и (или) без заключения договора об оказании услуг связи; за предоставление недостоверных или заведомо ложных персональных данных оператору персональных данных при заключении договора; а также ответственности операторов мобильной связи, не контролирующих соблюдение дилерами, распространяющими sim-карты, установленного порядка подключения пользователей к сети подвижной связи.

Приведем пример противоправного деяния.

МВД России проводило проверку по факту фиктивного заключения контрактов сотовой связи ОАО «МТС», совершенного с одной из коммерческих структур с целью получения вознаграждения за привлечение большого количества абонентов.

В результате проведенной проверки было установлено, что сотрудники коммерческой организации заключили более 38 тысяч контрактов, при этом их активация осуществлялась с 208 телефонов через базовые станции, расположенные в непосредственной близости с офисом указанной компании. В процессе проведения проверочных действий были установлены и опрошены граждане, на чьи данные были зарегистрированы контракты, они пояснили, что никогда не являлись абонентами ОАО «МТС», указанных контрактов не заключали. Паспортные данные, на которые были оформлены около 7000 абонентских номеров, являлись недействительными. Впоследствии руководство проверяемой коммерческой организации обратилось в ОАО «МТС» за выплатой дилерской премии.

По данному факту было возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 3 ст.30 ч. 4 ст. 159 УК РФ. Виновные лица были осуждены к различным срокам наказания.

б) преступления с использованием средств мобильной связи:

- телефонное мошенничество.

Данный вид правонарушений возник вскоре после массового распространения мобильных телефонов.

Преступники действуют в соответствии с несколькими устоявшимися схемами, при этом варьируются лишь некоторые детали.

Схема телефонного мошенничества «Случай с родственником».

Мошенник звонит на мобильные или городские абонентские номера в порядке возрастания или убывания последней цифры номера. При ответе абонента он представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции за совершение того или иного преступления (это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений).

Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что может решить вопрос о не возбуждении уголовного дела

за вознаграждение в сумме от 10 до 500 тысяч рублей и что уже не раз помогал людям таким образом.

В настоящее время участились случаи фактов мошенничеств, совершаемых организованными преступными группами, участниками которых в большинстве случаев являются заключенные, отбывающие наказания в различных учреждениях ФСИН России.

В связи с чем была проведена совместная проверка сотрудниками Следственного комитета Российской Федерации, директором ФСИН России, прокуратурой города Москвы, заместителем председателя правления Сбербанка России и журналистами общероссийского государственного информационного телеканала «РОССИЯ – 24». По результатам проверки подготовлен документальный материал, который 28 ноября 2020 года был представлен в рубрике «Расследование Э. Петрова «Звонок из СИЗО».

В данной передаче было указано, что на основании проведенного расследования в различных учреждениях ФСИН России были выявлены следующие факты мошенничеств, совершаемых при использовании мобильных средств связи, и некоторые нарушения своих должностных обязанностей сотрудниками учреждений ФСИН России:

1. «Более 40% телефонных мошенничеств совершается из наших колоний (тюрем)», – указал Станислав Кузнецов, заместитель председателя правления Сбербанка России.

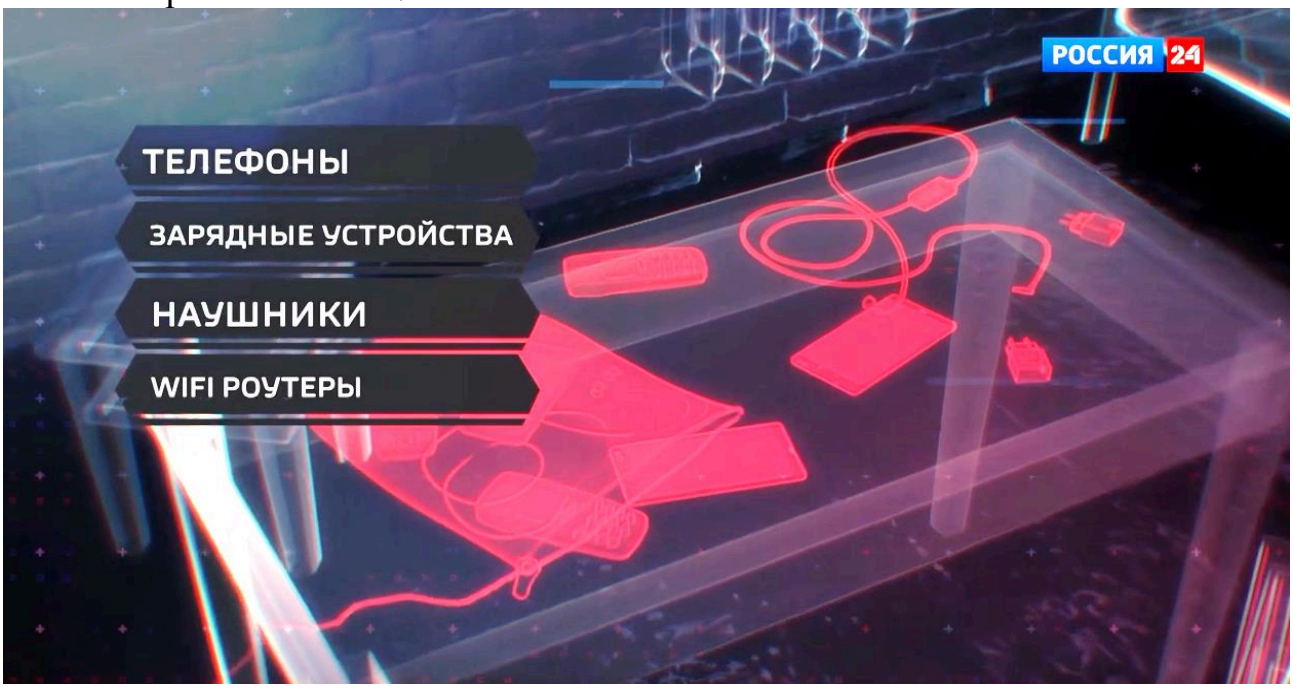


Рис. 15. Информационный телеканал «РОССИЯ – 24»

2. «Стоимость проноса смартфона составляла 20 000 руб., сим-карты – 1000 руб., алкоголь – 3000 руб./литр», – отметила Людмила Нефедова, начальник отдела взаимодействия со СМИ прокуратуры г. Москвы.

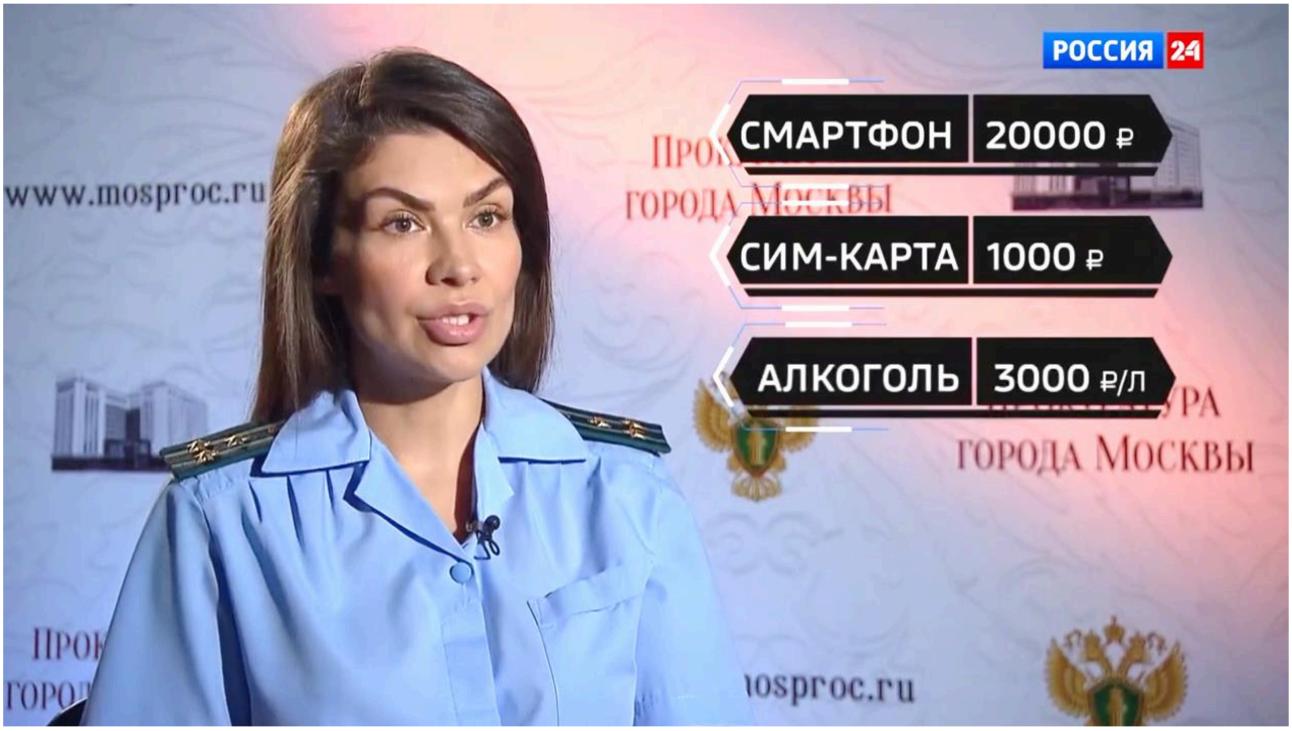


Рис. 16. Интервью информационному телеканалу «РОССИЯ – 24»

3. «Всего с января по июнь 2019 года двумя сотрудниками СИЗО незаконно передано заключенным от 80 до 100 смартфонов», – дополнила Людмила Нефедова, начальник отдела взаимодействия со СМИ прокуратуры г. Москвы.

4. «В 2020 году было возбуждено около 99 уголовных дел в отношении 56 сотрудников, а 170 сотрудников по этой причине уволены из рядов уголовно-исполнительной системы», – проинформировал Александр Калашников, директор ФСИН России.

5. Директор ФСИН России Александр Калашников в своем интервью указал, что в учреждения ФСИН России мобильные телефоны попадают следующими способами:

пронос адвокатами, близкими родственниками;

поступление телефонов через посылки;

провоз в автотранспорте;

с использованием беспилотных дронов;

самый неприятный и злободневный способ, когда сотрудники предают интересы службы и за определенную плату проносят запрещенные предметы и средства мобильной связи лицам, которые находятся в учреждениях ФСИН России.

В продолжение сказанного Александр Калашников добавил, что за десять месяцев 2020 года в учреждениях ФСИН в результате внезапно проведенных проверок было изъято более 50 000 единиц средств мобильной связи, из которых половину удалось отобрать на входе в СИЗО и колонии.

Рис. 17. Интервью информационному телеканалу «РОССИЯ – 24»

Рис. 18. Интервью информационному телеканалу «РОССИЯ – 24»

6. В этой же передаче Василий Пискарев, председатель Комитета по безопасности и противодействию коррупции Государственной Думы Российской Федерации, привел следующую статистику: «За первое полугодие 2020 года задержано на режимной территории учреждений за передачу или попытку передачи средств мобильной связи 1719 чел., за 2019 год – 5212 чел., за 2018 год – 5064 чел.»

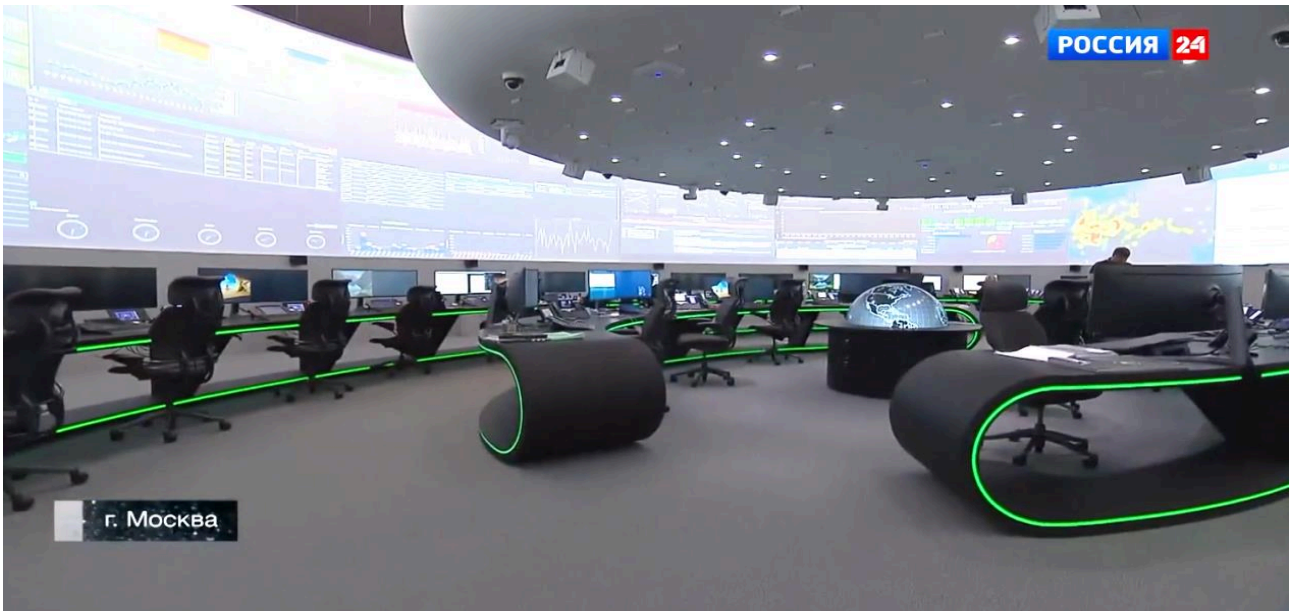


Рис. 19. Студия информационного телеканала «РОССИЯ – 24»

7. «Мы зафиксировали большое количество мошеннических операций, которые проходили именно из колоний, о чем мы регулярно информировали правоохранительные органы, в том числе Федеральную службу исполнения наказаний. Однако, к моему сожалению и по непонятным для меня причинам, наша информация ни разу не была реализована», – констатировал Станислав Кузнецов, заместитель председателя правления Сбербанка России.

В настоящее время депутаты Государственной Думы предлагают решить проблему кардинально и принять закон, обязывающий операторов сотовой связи блокировать мобильные телефонные номера, которые работают в колониях и следственных изоляторах, так как на законодательном уровне пользоваться телефонными аппаратами на режимной территории не имеют права не только лица, отбывающие наказание, но и сотрудники исправительного учреждения.

Далее Станислав Кузнецов, заместитель председателя правления Сбербанка России, проинформировал граждан и клиентов банков о том, что сотрудники банков и других кредитных организаций никогда не спрашивают номера банковских карт и другие персональные данные. «Как только задаются вопросы подобного рода вопросы, знайте, что это точно преступник, это точно мошенник», – добавил Станислав Кузнецов.

В результате проведенного анализа материалов, представленных в телевизионной программе, можно сделать следующие выводы.

В организации данной схемы может участвовать как один, так и несколько преступников. Звонящий может находиться как в исправительно-трудовом учреждении, так и на свободе.

Если жертва преступления поддалась на обман и согласилась привезти указанную сумму, звонящий называет адрес, куда нужно приехать, или узнаёт адрес потерпевшего.

Часто мошенники предлагают снять недостающую сумму в банке и сопровождают жертву лично. Мошенники стараются запугать жертву, не дать ей опомниться, поэтому ведут непрерывный разговор с ней вплоть до получения денег.

Для передачи им денежных средств преступники могут придумать и иные, более оригинальные мотивы.

Предлагаем рассмотреть пример из новостного интернет-портала (издательство «КОММЕРСАНТ» от 16.07.2020) о подделке документов путем копирования и перевыпуска сим-карт с целью похищения денежных средств с банковских счетов клиентов.

Рис. 20. Студия информационного телеканала «РОССИЯ – 24»

Оперативные сотрудники МУРа в декабре 2020 года обезвредили преступную группу, похитившую десятки миллионов рублей с банковских счетов граждан путем незаконного перевыпуска их телефонных сим-карт. Таким способом они получали коды доступа в «Мобильные банки» жертв, что создавало благоприятные условия для последующего списания с них денежных средств. Один из злоумышленников был ранее судим за подобные преступления. Имея криминальный опыт, данное лицо, вступив в преступный сговор с мошенниками, продолжил свою преступную деятельность, обкрадывая находящихся в заключение «товарищей по несчастью».

По данным источников «Ъ» в силовых структурах, в недалеком прошлом оперативным сотрудникам МУРа поступила информация о группе лиц, промышляющих мошенничествами с помощью перевыпуска телефонных сим-карт. В основном, жертвами злоумышленников становились частные лица – крупные клиенты различных российских банков. Для сбора информации о по-

тенциальных жертвах они использовали специальные сервисы «пробивки» людей в соцсетях или на подпольных хакерских форумах. Как правило, у владельцев подобных сервисов были налажены контакты с сотрудниками банков с высоким уровнем доступа.

Мошенников интересовала одна цель: возможность получения в режиме реального времени не только персональных данных клиентов, но и состояние их банковских счетов.

Получив необходимые данные, мошенники задействовали свою сообщницу, которая изготавливала поддельную доверенность от имени клиента банка на возможность проведения операций с телефонной сим-картой клиента. С поддельной доверенностью девушка приходила в салон сотовой связи в Москве или Подмосковье с просьбой о перевыпуске сим-карты. Ее просьбу легко удовлетворяли. Мошенница предъявляла в качестве удостоверения личности поддельные водительские права. Как правило, никаких вопросов у представителей операторов сотовой связи не возникало, однако трудности возникали у настоящего владельца сим-карты. После активации сим-карты-клона мошенниками у жертвы пропадала сотовая связь.

Пока абонент пытался восстановить прерванную сотовую связь, мошенница успевала отправлять в банк жертвы запросы на получение одноразовых кодов доступа.

В ряде случаев сообщница мошенников даже не утруждала себя пересылкой сим-карты – она просто отправляла или диктовала полученные коды по телефону. Соучастники преступной группы сразу же переводили со счетов жертв деньги на третьих лиц, а потом через целую цепочку транзакций обналичивали их в других городах, в частности, в Самаре. Суммы похищенных средств варьировались, но чаще всего составляли 50-100 тыс. руб.

Как указывают источники «Ъ», если в 2017-2018 гг. преступники выводили крупные суммы практически моментально, то, начиная с 2019 года, ситуация несколько изменилась. Учитывая скорость похищения денежных средств мошенниками, банки приняли решение о том, что после перевыпуска сим-карты и осуществления транзакции должны пройти сутки.

Введенное новшество заставило мошенников изыскивать новые схемы обмана: выбирать жертв из числа довольно состоятельных людей, которые находились в СИЗО по обвинению в совершении преступлений либо уже отбывали сроки в исправительных колониях. Обязательным условием было наличие у заключенного денег на счету и мобильного телефона.

Исходя из создавшейся криминогенной обстановки, оперативные сотрудники МУРа обобщили данные о случаях списания денежных средств с банковских счетов граждан, а столичные следователи возбудили уголовное дело о мошенничестве в особо крупном размере, совершенном группой лиц (ч. 4 ст. 159 УК РФ). Согласно действующим нормам УПК Российской Федерации, которые предусматривают для получения необходимой информации привлечение к расследованию специалистов, обладающих специальными знаниями в области банковской деятельности. В связи с чем к расследованию и

установлению личностей участников организованной преступной группы были привлечены и специалисты компании Group-IB. В результате проведенной оперативной комбинации была получена криминалистически значимая информация, были установлены все участники организованной преступной группы, двое организаторов группы были задержаны в Солцево и Коммунарке. Девушка из «сервиса по восстановлению сим-карт» была задержана в Подмосковье, а их сообщник, занимавшийся обналичиванием денежных средств, был задержан в г. Самаре. Характерно то, что один из участников преступной группы был ранее судим за аналогичные преступления в 2014-2015 гг. После отбытия срока наказания ранее осужденный не встал на путь исправления. Он продолжил свою преступную деятельность, совершая преступления в отношении оставшихся в местах лишения свободы лиц, с кем ранее отбывал наказание.

При проведении обысков у задержанных оперативные сотрудники обнаружили многочисленные сим-карты, ноутбуки, смартфоны и кнопочные телефоны, поддельные документы (паспорта и водительские удостоверения), а также банковские карты и привязанные к ним сим-карты, на которые поступали похищенные деньги.

Для хранения конфиденциальной информации мошенники использовали флеш-криптоконтейнеры. Все фигуранты уголовного дела полностью признали свою вину, в настоящее время им предъявлены официальные обвинения. По приблизительным оценкам, общий ущерб от действий мошенников составляет несколько десятков миллионов рублей.

После тщательно проведенного анализа серии аналогичных преступлений эксперты в области киберпреступлений из компании Group-IB, оказавшие помощь полицейским в поимке мошенников, предупреждают о необходимости тщательно следить за личными данными и перевыпуск сим-карт разрешать только в своем присутствии.

Ниже рассмотрим схему возможных вариантов мошенничества (см. рис. 21).

Рассмотрим пример раскрытия мошенничества, совершенного с использованием средств мобильной связи.

В МВД России поступила оперативная информация о том, что в Московской области организована преступная группа, которая совершает мошеннические действия, используя средства мобильной связи.

Проведенными оперативно-розыскными мероприятиями установлено, что указанная группа организована по принципу преступного сообщества с четким распределением ролей, с наличием «общака» и внешних криминальных связей.

Преступники действовали по следующей схеме:

- один из участников группы осуществлял звонки на прямые мобильные телефоны граждан, непродолжительное время беседовал с ними на общие темы до тех пор, пока они не признавали в нем кого-то из своих знакомых;

Рис.21. Схема возможных вариантов мошенничества

- затем на правах старого знакомого фигурант просил одолжить ему денежные средства в размере 200 тыс. рублей для решения проблем с полицией и обещал вернуть эти деньги в максимально короткие сроки (через неделю). Поскольку в настоящее время он был занят либо находился в отъезде, денежные средства потерпевшими переводились посредством платежной системы «Вестерн Юнион» в один из банков г. Раменское Московской области. Впоследствии данные денежные средства получали другие члены преступной группы, а затем передавали сестре лидера этой преступной группы. Родственница лидера преступной группы, в свою очередь, переводила деньги на сберегательную книжку, оформленную на ее имя, и периодически переводила некоторые суммы в одну из исправительных колоний для нужд содержащихся там заключенных.

В ходе комплексного использования сил, форм и методов оперативно-розыскной деятельности Управлением «К» БСТМ МВД России были установлены все участники преступной группы и собраны исчерпывающие доказательства причастности указанных лиц к совершению данных преступлений.

По данному факту возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 4 ст. 159 УК РФ.

Впоследствии все пятеро членов преступной группы задержаны и допрошены в качестве подозреваемых по вышеуказанному уголовному делу, в том числе организатор С., отбывающий наказание в одной из ИК Минюста России, осуществлявший звонки потерпевшим и дававший сообщникам указания о получении и хранении денежных средств; изъято 580 тыс. рублей. В ходе допросов подозреваемые признали свою вину полностью и сообщили информацию о лицах, причастных к совершению данных преступлений. Установлены более 50 потерпевших, проведены необходимые следственные действия. Лица, виновные в совершении указанных преступлений, в зависимости от степени содеянного и причиненного ими вреда, привлечены к уголовной ответственности к различным срокам наказания.

Рассмотрим пример раскрытия мошенничества, совершенного с использованием утерянных сим-карт:

В БСТМ Северной Осетии поступила информация о том, что у гр-на Сидорова всю ночь снимались с его лицевого счета денежные суммы, о которых автоматически передавалась информация путем смс-сообщений на его телефон.

Гражданин Сидоров обратился в письменном виде в Сбербанк, где ему было сказано, что в недалеком прошлом к Вашему текущему счету были привязаны через «мобильный банк» два абонентских телефонных номера. Один из этих ранее привязанных номеров принадлежит ему самому, а другой телефонный номер принадлежал его бывшей супруге Н.В. Ивановой.

После этого Сидоров обращается в полицию с заявлением о том, что с его лицевого банковского счета похищены деньги в размере 50 000 рублей. В ходе проведения проверочных действий по факту хищения денежных средств с лицевого банковского счета заявителя был установлен номер сотового телефона, ранее принадлежащий его бывшей супруге Ивановой Наталье Владимировне. В процессе беседы с ней было выяснено, что она данным телефонным номером уже давно не пользуется, так как она потеряла сим-карту и приобрела новую с другим телефонным номером. Об этом она нигде ранее не сообщала.

При отработке был установлен ранее принадлежащий бывшей супруги Ивановой телефонный номер. В ходе проведения соответствующих мероприятий был установлен IMEI – код телефона, а так же были установлены лица, у которых таким же способом систематически снимались с лицевых банковских счетов денежные суммы.

В процессе проведенного глубокого анализа поступающей информации о совершаемых преступлениях путем снятия денежных сумм с лицевых банковских счетов клиентов в поле зрения попали большое количество сим-карт

и мобильные сотовые телефоны, которые использовались при совершении преступлений.

Далее в ходе отработки лиц, причастных к совершению преступлений был установлен факт активной работы мобильного телефона. По данному мобильному телефону было проведено соответствующее оперативно-розыскное мероприятие, в ходе которого была получена доказательственная информация о причастности лиц, ведущих с этих телефонов постоянные переговоры.

В последующем в результате проведения всесторонней аналитической работы были установлены места их дислокации, и разрабатываемые лица, причастные к содеянным преступлениям, были задержаны.

В результате совершения указанных преступлений пострадало около 20 человек, и ущерб от совершения хищений денежных средств превысил 3 млн. рублей.

По данному факту было возбуждено уголовное дело по ч. 4 ст. 159 УК РФ, и виновные лица осуждены к 10 годам лишения свободы.

Далее предлагаем продолжить рассмотрение способов мошенничества, имеющих место в практической деятельности раскрытия преступлений сотрудниками Управления «К» БСТМ МВД России. Следующий способ такой, как:

- выигрыш в лотерее.

В связи с проведением всевозможных рекламных акций, лотерей и розыгрышей мошенники часто используют их для прикрытия своей деятельности и обмана людей. Злоумышленники действуют следующим образом: рассылают на мобильные телефоны граждан смс-сообщения о выигрыше ценного приза, например, ценными призами могут быть телефон, ноутбук, автомобиль. Чтобы получить приз, необходимо в ближайшее время перезвонить по указанному контактному номеру. Перезвонившему абоненту отвечает «сотрудник «призового отдела» и подробно объясняет условия акции, грамотно убеждает в ее честности и сообщает алгоритм дальнейших действий. В данном случае выигрыш приза выступает не только в роли приманки, но является поводом затребовать перечисления крупных денежных средств.

Для уточнения всех деталей потенциальному потерпевшему могут предложить посетить определенный сайт и ознакомиться с условиями акции, а также позвонить по одному из указанных телефонных номеров.

Во время разговора мошенники сообщают о том, что надо выполнить необходимые формальности: получить восьмизначный код, дающий право на приобретение приза, уплатить госпошлину, для чего необходимо посредством платежных терминалов перечислить на счет мобильного телефона гражданина сумму, составляющую 1 % от стоимости выигрыша, а затем под руководством «специалиста информационно-справочной службы» набрать определенную комбинацию цифр и символов якобы для проверки получения «кода регистрации». При этом злоумышленники уверяют, что денежные средства, потраченные на прохождение стандартной процедуры регистрации, остаются на счете абонента и могут быть использованы по его усмотрению. Возможно также перечисление денежных средств на указанный злоумышленниками

электронный кошелек. В первом случае, оплачивая абонентский номер под руководством злоумышленника, жертва сама этого не подозревая, переводит деньги на его счет, во втором – изначально переводит денежные средства в карман злоумышленника.

- смс-сообщения из банка.

Данный вид преступлений стал широко распространен относительно недавно. В последнее десятилетие подавляющее большинство граждан Российской Федерации стали владельцами банковских карт того или иного банка (иногда нескольких) и активно их используют при оплате услуг, покупок, в путешествиях. Для удобства граждан банки подключают пользователям карт услугу так называемого «мобильного банка», позволяющую контролировать все операции, совершаемые посредством банковской карты в режиме реального времени, привязывая банковскую карту к абонентскому номеру ее владельца. Злоумышленники рассылают на мобильные телефоны граждан смс-сообщения о том, что банковские карты граждан заблокированы либо приостановлены, либо о том, что успешно осуществлен перевод, которого на самом деле не было. Для уточнения информации потенциальному потерпевшему предлагается перезвонить по указанному телефону службы безопасности банка.

В случае если гражданин перезванивает по телефонному номеру, указанному в сообщении, мнимый сотрудник службы безопасности банка выяснит, в каком банке была оформлена карта, данные гражданина, а затем предложит последнему подойти к ближайшему банкомату и с помощью нехитрых манипуляций, продиктованных мнимым сотрудником службы безопасности банка, разблокировать карту путем набора комбинации цифр, что является не чем иным, как кодом мобильного перевода со счета жертвы на счет злоумышленника или его сообщников.

- смс-просьба о помощи.

Смс-сообщения позволяют упростить схему обмана по телефону. Дополнительную опасность представляют упростившиеся схемы перевода денежных средств с одного телефона на другой.

Преступники действуют следующим образом: отправляют абонентам на мобильный телефон сообщение примерно такого содержания: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «папа», «друг» или т.п.

В случае согласия оказать помощь родственнику или знакомому жертва преступления пополняет счет мобильного телефона, указанного преступником. Данный вид преступлений характеризуется высоким уровнем латентности ввиду малозначительности ущерба и психологических особенностей потерпевших, не желающих афишировать то, что они поддались на достаточно примитивный обман.

- платный код от оператора связи.

На мобильный телефон граждан поступают звонки либо приходят смс-сообщения якобы от сотрудника службы технической поддержки оператора мобильной связи.

Обоснованием этого звонка или смс-сообщения могут являться:

- предложение подключить новую эксклюзивную услугу;

- перерегистрация во избежание отключения связи из-за технического сбоя;

- улучшение качества связи;

- защита от СПАМ-рассылки;

- предложение принять участие в акции от сотового оператора. Потенциальной жертве предлагается набрать под диктовку код или смс-сообщение, при помощи чего подключат новую услугу, улучшится качество связи и т.п. Код, который гражданину предложат отправить, является средством для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников.

- ошибочный перевод средств.

На мобильный телефон граждан приходят смс-сообщения о поступлении на счет денежных средств, переведенных с помощью услуги «Мобильный перевод» либо с терминала оплаты услуг, после чего сразу поступает звонок или смс, и потенциальному потерпевшему сообщают, что на его счет ошибочно переведены деньги, поэтому их просят вернуть обратно тем же «Мобильным переводом».

- роумерское мошенничество.

Данный вид правонарушений был очень распространен в период 2004–2009 гг. и был связан с задержкой получения операторами мобильной связи биллинговой информации о своих sim-картах, находящихся в роуминге. Выше указанный вид нарушения осуществляются и в настоящее время.

Приведем пример преступления данного вида.

В результате проведенных Управлением «К» БСТМ МВД России оперативно-розыскных мероприятий был установлен факт хищения денежных средств ОАО «МСС» в размере 44 953 594,65 рублей, совершенного гражданином К. в составе организованной преступной группы путем обмана.

В ходе ОРМ установлено, что в офисе ОАО «Московская сотовая связь» гражданин К. приобрел для ООО «Юнивест» двадцать три RUIM-карты с услугой «пластиковый роуминг», позволяющей осуществлять звонки за пределами России. При этом гражданин К. предъявил сфальсифицированные доверенности от имени генерального директора ООО «Юнивест» гражданина П.

В течение двух дней с территории Республики Бангладеш с указанных RUIM-карт в круглосуточном режиме было осуществлено аномально большое количество исходящих вызовов на платные номера зарубежных операторов на общую сумму 44 953 594,75 руб., однако данные услуги ООО «Юнивест» оплачены не были, чем ОАО «Московская сотовая связь» причинен ущерб в особо крупном размере.

По данному факту возбуждено уголовное дело по п. «б» ч. 3 ст. 165 УК РФ

- распространение вредоносных программ.

Данные преступления совершаются по следующей схеме: на Интернет-ресурсах пользователям предлагаются различные услуги и сервисы, которые не всегда соответствуют заявленным: приложения для мобильных телефонов, не являющиеся таковыми (например, программное обеспечение якобы для общения в сети Интернет через мобильные устройства), различные игровые приложения, вводящие пользователей в заблуждение, такие как «мобильный шпион», «конструктор диет», «GSM-локатор» и др.).

Для получения желаемого контента гражданам предлагается отправить смс-сообщение на указанный злоумышленниками короткий номер либо ввести свой номер мобильного телефона на сайте.

В ходе проведения Управлением «К» БСТМ МВД России оперативно-розыскных мероприятий установлено, что члены организованной преступной группы путем распространения вредоносного программного обеспечения в сети Интернет и мошеннических действий с использованием сервисов «коротких» номеров завладели денежными средствами граждан в размере свыше 15 миллионов рублей.

Преступные лица зарегистрировали сайт www.all4se.mobi на виртуальном сервере ЗАО «МастерХост», после чего в период с 20 января 2010 г. по 22 февраля 2010 г. распространяли с вышеназванного сайта через веб-сайт www.icq2mobile.ru программное обеспечение, якобы предназначенное для общения в сети Интернет через мобильные устройства, фактически представлявшее собой вредоносную программу J2ME/ TrojansSMS.Espaw.NAB, нацеленную на хищение денежных средств с мобильных телефонов путем отправки sms-сообщений на «короткие» номера.

По материалам Управления «К» БСТМ МВД России возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 1 ст. 273 УК РФ.

3. Преступления в сети Интернет:

а) распространение вредоносных программ для ЭВМ;

б) мошеннические действия с использованием сети Интернет (интернет-магазины, проведение различных акций).

Данные виды правонарушений характеризуются большим разнообразием способов и схем совершения, зачастую тесно связаны с ранее рассматриваемыми видами телефонного мошенничества.

Обратимся к конкретным примерам.

Пример 1.

В БСТМ МВД России поступила информация о том, что неустановленная группа лиц совершает мошеннические действия в отношении граждан России.

Данное преступление совершалось по следующей схеме.

Преступники размещали в Интернете и региональных СМИ объявления об оказании помощи в получении потребительских кредитов в различных коммерческих банках. Потенциальный клиент обращается по указанному в объявлении телефону, и оператор объясняет клиенту условия получения кредита.

Одним из условий является выезд представителя организации к клиенту для проверки документов клиента и заключения с ним договора за счёт клиента. Под этим предлогом потенциальному клиенту предлагается оплатить командировочные расходы представителя в сумме 700 долларов и перевести данную сумму по электронной платежной системе «Western Union» на счёт одного из членов преступной группы, находящегося на территории России или Украины. После этого клиент переводит на счёт указанного лица денежные средства и в течение 3 дней ожидает приезда представителя, который не приезжает, ссылаясь на различные причины. Далее клиенту предлагается оформить получение кредита без выезда представителя и под различными поводами, такими, как «согласование выдачи кредита», «согласование со службой безопасности банка», «выдача кредита» и другие – таким образом, у клиента снова вымогаются различные суммы. В итоге клиент оплачивает все возможные командировочные расходы и согласования в общей сумме от пяти до десяти тысяч долларов США, но никаких потребительских кредитов так и не получает. Данная преступная группа осуществляла свою деятельность около 2 лет, и уже нанесла крупный материальный ущерб сотням граждан по всей территории Российской Федерации. В ходе проведения оперативно-розыскных мероприятий были установлены лидер, организатор и члены данной преступной группы. Лидер преступной группы принимал непосредственное участие в совершении мошеннических действий путем введения в заблуждение граждан, желающих получить кредит, подбирал участников группы, руководил операторами по приему звонков от граждан, получателями денежных средств, курьерами, а также распределял денежные средства между участниками преступной группы.

Установлены более 500 потерпевших в 52 регионах Российской Федерации, в отношении которых вышеуказанная преступная группа совершила мошеннические действия, причиненный ущерб составил более 11 млн. рублей. По данному факту возбуждено уголовное дело по признакам состава преступления, предусмотренного ч.4 ст. 159 УК РФ.

Пример 2.

По данным средств массовой информации от 25 февраля 2021 года, в Москве 24 февраля 2021 года задержали мужчину, который занимался аферами в сети Интернет. Он предлагал людям мобильные телефоны известного бренда, электронику «Премиум-класса». Товар выставлял по очень привлекательной цене, заметно ниже, чем в среднем по рынку. Клиенты вносили предоплату, после чего продавец переставал выходить на связь. Следствие полагает, что злоумышленнику удалось таким способом обмануть более полусотни человек и похитить у них, в общей сложности, 6,5 млн. рублей.

В ходе обысков изъята компьютерная техника, мобильные телефоны, печати различных государственных учреждений, документы с признаками подделки, бланки и удостоверения, а также другие электронные носители информации.

Пример 3.

Путем мошенничества в сети Интернет похищаются у граждан крупные денежные суммы. Так, в феврале 2021 года несколько граждан через «зеркальный сайт» под названием «Северный ветер» приобрели в Московской области авиабилеты рейсом Ереван – Москва.

Как только деньги были перечислены представителю фиктивно обозначенной компании, указанный в Интернете сайт перестал существовать.

в) незаконная организация и проведение азартных игр в сети Интернет и с ее использованием.

МВД России проводятся мероприятия по пресечению противоправной деятельности группы лиц, занимающихся организацией и проведением азартных игр в сети Интернет в нарушение Федерального закона Российской Федерации «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» от 29 декабря 2006 г. № 244-ФЗ.

В ходе анализа поступающей информации установлено, что члены преступной группы организовали в сети Интернет ряд web-сайтов с расположенным на них программным обеспечением в виде интернет-казино, на которых осуществлялись азартные игры (более 470 видов).

Для осуществления своей корыстной преступной деятельности фигуранты создали основной интернет-ресурс – сайт www.goldfishka.com.

В целях монополизации присутствия в российском сегменте сети Интернет участниками группы был создан ряд внешних оболочек игровой направленности, отсылающих игроков на основной сайт. Все указанные интернет-ресурсы были ориентированы на жителей Российской Федерации.

С целью придания вида легализованной деятельности и обеспечения безопасности от попыток взлома и несанкционированного доступа серверы с программным обеспечением интернет-казино находились за пределами Российской Федерации: в ЮАР, Канаде, Малайзии и других государствах.

Денежные средства за игру перечислялись игроками на счета, зарегистрированные участниками преступной группы в различных платежных системах на подставных лиц посредством смс-сервисов, перечислением денежных средств с электронных кошельков, пластиковых карт и иных платежных систем. Вывод денежных средств, полученных в результате противоправной деятельности, осуществлялся через специализированную площадку за границу Российской Федерации, для последующего их обналичивания и распределения между участниками группы.

В ходе проведения оперативно-розыскных мероприятий было установлено, что преступная группа состояла из 12 человек, в основном граждан Российской Федерации. Все участники имели четко распределенные следующие обязанности:

– общее руководство и управление;

– администрирование и техническая поддержка;

– продвижение сайта;

– управление электронными кошельками и распределение выигрышей;

– вывод и обналичивание денежных средств.

По данному факту возбуждено уголовное дело по признакам состава преступления, предусмотренного ч.2 ст.171 УК РФ.

г) незаконный доступ к услугам кабельного и спутникового телевидения.

Злоумышленники устанавливают, т.е. распространяют комплекты спутникового телевидения с модифицированным программным обеспечением, предназначенным для нейтрализации средств защиты компьютерной информации, используемых операторами спутникового телевидения, с целью возможности получения незаконного доступа к каналам операторов спутникового телевидения, например, каналам ОАО «НТВ-плюс», причиняя тем самым ущерб правообладателю.

2.6. ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С БЛОКЧЕЙНОМ

Современное общество невозможно представить без сотовой связи: покупки, запись к врачам, оплата коммунальных услуг и обзор новостей; мы начинаем и заканчиваем свой день с сотовым телефоном в руках. Все это задает определенный ритм и темп нашей жизни. Развитие систем сотовой связи, сравнимо лишь с ростом производства персональных компьютеров и эволюции Интернета, не замедляется уже четверть века и включает в себя несколько поколений. Компьютерная сеть Интернет привела к большому числу положительных изменений, но возможности коммерческой и экономической деятельности в сети, по-прежнему, значительно ограничены и небезопасны. В сети мы не имеем возможности безошибочно установить личность другого человека и полностью довериться друг другу. Чтобы производить финансовые операции, переводить или обменивать деньги, приходится пользоваться услугами банков. Банк в финансовых вопросах является посредником и гарантом выполнения сделки, не забывая о собственной выгоде в виде комиссии с операции. Рост сетевого общения и онлайн-торговли создает новые возможности для киберпреступности. Считается, что каждый год увеличивается развитие Интернет активности и возможности фальсификаторов и кибермошенников в финансовой сфере, спамеров, фишеров, вымогателей, которые требуют выкуп за нераспространение персональных данных.

В связи с этим, разработчики разных стран пытались решить проблемы Интернета, связанные с защитой персональных данных и финансовых операций с помощью шифрования. Но, как не менялась конструкция процесса, возможность утечек всегда оставалась, поскольку в нем участвовали третьи стороны. Оплата карточкой через Интернет была ненадежной: пользователям приходилось предоставлять слишком много личной информации, а стоимость транзакций была слишком высока для небольших платежей.

В 2008 году некто под псевдонимом «Сатоси Накамото» описал новый протокол для системы прямых электронных расчетов с помощью криптовалюты под названием «биткойн». Криптовалюта (или цифровая валюта) отличается от традиционных валют, поскольку не создается и не контролируется ни одним государством. Этот протокол установил ряд правил – в виде распределенных вычислений, – которые обеспечивали целостность информации, передаваемой между миллиардами устройств напрямую, без обращения к надежной третьей стороне. Это незначительное на первый взгляд нововведение стало искрой, взбудоражившей и перепугавшей весь мир информационных технологий и покорившей его воображение. Из этой искры разгорелся пожар в коммерческом секторе и госуправлении: повсюду о ней заспорили защитники частной жизни, активисты социального развития, теоретики медиа, журналисты и многие другие. Именно технология Blockchein и криптовалюта Биткоин позволила достаточно четко определить новые подходы к обеспечению целостности информации, передаваемой между абонентами, не имеющими оснований доверять друг другу.

Рис. 22. Соотношение децентрализованных распределенных систем

Биткоин (от англ. Bit Coin – цифровая монета) – криптовалюта, которая в отличие от фиатных денег не создается и не контролируется на государственном уровне, а также является дефляционной по своей природе, благодаря строго ограниченной эмиссии. По сути, сеть Биткоин представляет одноранговую платежную систему (отсутствуют какие-либо управляющие или процессинговые центры). Для учета операций используется одноименная единица – BTC. Минимальная составная часть BTC – сатоши (Satoshi, 1 сатоши = 10^{-8} BTC). Все сделки в сети Биткоин абсолютно прозрачны и необратимы, т.е. сделка подтверждена и записана в реестр операция (транзакция) и не может быть отменена. При работе непосредственно в сети Биткоин обеспечивается анонимность пользователей. Необходимым и достаточным усло-

вием для работы с платежной системой является наличие установленного клиента. Протокол платформы Биткоин и программный код базового клиента (Bitcoin Core) полностью открыты. Технологически доверие между участниками системы поддерживается с помощью децентрализованного консенсуса. Консенсус достигается на конкурентной основе, для его реализации используется механизм доказательства используемой работы (Proof of Work).

Блокчейн (от англ. Block Chain – цепочка блоков) – структура данных, в которой информация о совершенных взаимодействиях (транзакциях) унифицирована и хранится в виде цепочки (связанной последовательности) блоков. Представляет собой децентрализованное хранилище транзакций, не требующее для совершения операций участия каких-либо посредников. Использование технологии блокчейн впервые позволило обеспечить децентрализованный консенсус. Объем цепочки блоков перманентно увеличивается по мере добавления новых блоков, содержащих самые последние записи. Блоки добавляются в блокчейн в линейном последовательно хронологическом порядке. После добавления блоки становятся навсегда неизменяемыми. Это касается также их содержания. Управление блокчейном, построенным на принципе децентрализации, в целом и в частности осуществляется сетью.

Децентрализованные приложения (от англ. Distributed Application, DApps) – приложения, построенные согласно парадигме, являющиеся архитектурным антиподом централизованной (клиент-серверной) модели. В децентрализованной системе отсутствуют узлы, управляющие функционалом иных узлов.

Таким образом, протокол Биткоин – частный случай категории систем, основанных на технологии блокчейн, являющихся, в свою очередь, подклассом децентрализованных приложений.

Характерные признаки успешной децентрализованной модели:

Максимальна децентрализация. Прежде всего, идеальное решение должно обеспечить децентрализацию данных (данные хранятся децентрализовано, максимально надежно, без какого-либо участия арбитра или центрального узла). Каждый пользователь обладает полностью функциональной копией всей совокупности данных. Кроме того, осуществляется децентрализация ценности, идентичности, вычислений.

Синхронизация данных всех пользователей осуществляется в автоматическом режиме на основе механизма достижения распределенного консенсуса, а не за счет "контроля сверху" (управляющего узла).

Открытость кода. Все технологические аспекты доступны любому желающему. Абсолютная прозрачность и несомненная безопасность данных лучше всех остальных доводов вызывают доверие к приложению.

Монетизация приложения осуществляется через внутреннюю криптовалюту. Схема получения прибыли разработчиком может походить на механизм, опробованной в сети Биткоин. Рост ценности платформы дал возможность хорошо заработать всем, кто стоял у ее истоков и немало способствовал ее развитию. Поэтому разработчику достаточно предусмотреть в системе де-

фицитные, полезные для пользователей ресурсы. Оплата доступа к ресурсам осуществляется посредством специальных токенов (коинов). Пользователи будут конкурировать за токены, чтобы получить возможность работать с системой. Владельцы дефицитных ресурсов получают плату в токенах. Перманентный рост сети при ограниченном количестве токенов, вызывает неизбежный рост ценности внутренних коинов. Токенами может поощряться любая полезная работа в рамках приложения, например, майнинг.

Отсутствие единой точки отказа. Работоспособность приложения (доступность данных) не должна нарушаться при выходе из строя или блокировке какого-то оборудования или инфраструктуры.

Эффективность работы приложения не должна зависеть от количества устройств, на которых оно активировано. Такую же природу имеет требование, согласно которому ни одно лицо или организация не может владеть "контрольным пакетом" его токенов.

Не все децентрализованные приложения удовлетворяют всей совокупности представленных признаков. Например, криптовалюта Ripple последнему критерию не соответствует.

Существует несколько видов транзакций, самая распространенная из них – простой платеж с одного адреса на другой, включающая второй выход с целью начисления сдачи отправителю (один вход и два выхода). Другим распространенным видом платежа является транзакция, объединяющая несколько входов в один выход (аналог обмена множества мелких монет на одну крупную купюру в реальной жизни). Довольно часто выполняется по сути обратная по смыслу финансовая операция – распределение средств одного входа по нескольким выходам, содержащим адреса нескольких разных получателей. Таким образом, удобно расплачиваться с группой сотрудников, выполнивших определенный объем работы. Каждая транзакция в сети Биткоин должна быть подписана подлинной электронной подписью, которая может быть получена только при наличии валидных цифровых криптографических ключей. Следовательно, любой, получивший копии данных ключей, имеет точно такой же контроль над средствами, ассоциированными с этой учетной записью, как и ее истинный владелец.

Право владения токенами, в том числе, биткоинами устанавливается через криптографические (цифровые) ключи, Биткоин-адреса и цифровые подписи. Закрытые криптографические ключи не перемещаются по сети. Они генерируются и хранятся пользователями в специализированном клиенте (кошельке). Цифровые ключи в кошельке пользователя являются абсолютно независимыми от протокола Биткоин, генерируются и управляются с помощью программного обеспечения кошелька пользователя без обращений к блокчейну или к сети Интернет. Благодаря такой стратегии управления ключами становятся возможными многие из важнейших свойств сети Биткоин, в том числе децентрализованные консенсус и контроль, подтверждение владения, и модель безопасности, основанная на математическом (криптографическом) доказательстве.

Ассиметричная схема шифрования подразумевает наличие криптопары: частного (закрытого) и публичного (открытого) ключей. Публичный ключ можно сравнить с номером банковского счета, тогда приватный ключ выполняет функцию PIN-кода или подписи на банковском чеке, обеспечивая полный доступ к учетной записи. Эти цифровые ключи почти никогда не попадаются на глаза пользователям сети Биткоин. В основном, они хранятся в файлах бумажника, а манипуляции ключами выполняет программное обеспечение кошелька – разумеется по инициативе владельца.

Таким образом, в рамках сети Биткоин адреса обеспечивают анонимность пользователей. Не существует способа ассоциировать биткоин-адрес с конкретным физическим или юридическим лицом. Но эта анонимность поддерживается только в рамках сети Биткоин. Использование токенов на криптобиржах или магазинах, принимающих криптовалюту, в большинстве случае потребует стандартной идентификации владельца криптосредств. Из выше сказанного следует, что в отличие от стандартной схемы цифровой подписи даже публичный ключ не распространяется по сети и не передается другим пользователям. Вместо него для решения задач авторизации используются биткоин-адреса.

Выбор кошелька для криптовалюты давно перестал быть вопросом исключительно безопасности или простоты. Использование разных кошельков для разных целей становится обычным делом, как и использование разных счетов при работе с фиатными деньгами. Разработчики программного обеспечения активно эксплуатируют эту концепцию и непрерывно предлагают новые программные средства, в том числе и вполне работоспособные. В отличие от традиционных банковских счетов, работающих с фиатными деньгами, криптокошельки не хранят наличность в буквальном смысле. Они содержат открытые и секретные цифровые ключи, предоставляющие доступ к биткоин-адресам, и позволяют подписывать транзакции. При совершении платежных операций в блокчейне появляется запись о переходе прав на определенную сумму криптовалюты к новому владельцу, фактической передачи ценностей при этом не происходит. По способу хранения наиболее критичной информации, речь идет о ключах, кошельки принято делить на "горячие" и "холодные". К первым относятся кошельки с постоянным доступом к интернету: онлайн-кошельки, мобильные приложения, программы для персональных компьютеров, имеющих постоянное подключение к сети Интернет. Безусловно, они очень удобны в использовании, обеспечивают синхронизацию блокчейна и готовы мгновенно обрабатывать транзакции. При этом они подвержены хакерским атакам и вирусам. И уж тем более не стоит серьезно относиться к кошелькам, предлагаемым криптовалютными биржами. Нельзя доверять секретные ключи посреднику.

В системах, реализующих принцип холодного хранения, критичные данные хранятся в оффлайн-режиме на физическом носителе, не имеющим прямого соединения с Интернетом. Разумеется, такой способ обеспечивают гораздо более высокую степень защиты криптовалютной наличности. При

этом в плане проведения транзакций они не столь удобны. Другой угрозой является отличная от нуля вероятность поломки специальной техники или ее потери. Но здесь есть традиционный и достаточно простой способ защиты – своевременное создание резервных копий критичных данных. Холодный способ хранения реализуется в бумажных кошельках (имеются даже зашифрованные бумажные кошельки), системах с дополнительным физическим носителем и специальных аппаратных кошельках (например: Trezor, Keepkey или Ledger Nano S).

Классификация криптовалютных кошельков, учитывающий технологию изготовления:

Веб-кошельки (или онлайн кошельки). Идеально подходят для новичков, не желающих самостоятельно администрировать собственное программное обеспечение, или обладателей "маломощной" вычислительной техники. Популярные онлайн (браузерные) кошельки: Матби, Coinbase, Blockchain.info, Cryptopay, Xapo, Bitpay и др.

Достоинства веб-кошельков:

- отсутствует необходимость в скачивании, хранении и последующей синхронизации блокчейна (очень серьезно экономит время и место на постоянных носителях);
- управлять Веб-кошельком можно с самых разных устройств. Единственное условие наличие свободного доступа к Интернету.
- дополнительные сервисы и профессиональная поддержка.

Недостатки веб-кошельков – низкий уровень защиты (секретный ключ хранится на стороне).

Мобильные кошельки (устанавливаются на смартфоны и т.п.). Мобильные клиенты позволяют совершать платежи по схеме «scan-and-pay». Нет необходимости прокатывать карту, набирать PIN-код или вносить данные вручную. Единственное, что нужно для приема платежа, это открыть QR-код в своем мобильном кошельке и показать его контрагенту, чтобы он просканировал код своим мобильным телефоном, или просто поднести телефоны друг к другу (если они поддерживают технологию NFC). Мобильные кошельки, чтобы не скачивать весь блокчейн, хранят только его облегченную версию. А при транзакциях обращаются к доверенным блокчейн-сетям (нодам). Делается это, чтобы сэкономить значимые для телефона ресурсы как память и трафик. Популярные кошельки для мобильных устройств: Blockchain Mobile; Bitcoin Wallet; Electrum; Mycelium; Coin Pocket; Xapo и др. Очевидное достоинство – удобство использования при оплате и постоянный доступ к кошельку. В качестве недостатка можно выделить высокую вероятность кражи самого телефона или потери. Дискредитации ключей в этом случае может помешать высокая степень безопасности (двухуровневая аутентификация, смс-оповещения), которую обеспечивают мобильные криптовалютные кошельки.

Локальные кошельки (установленные на персональный компьютер или ноутбук). Подразделятся на два вида, «Толстые» или «тяжелые» – такие кошельки загружают на компьютер весь блокчейн, возводя пользователя в ранг полноценного участника сети Биткоин и занимая при этом большой объем памяти на постоянном носителе (на начало февраля 2019 года – уже более 236 GB). В отличие от тяжелых криптокошельков «тонкие» или «легкие» не скачивают весь блокчейн на персональный компьютер, а обращаются к нему через API сторонних агрегаторов. Занимают значительно меньше места по сравнению с «толстыми», несколько быстрее проводят транзакции, но из-за обращений к стороннему ресурсу уступают «толстым» в безопасности. Хотя приватные ключи в обоих случаях хранятся у пользователя. Популярные локальные кошельки: Bitcoin Core, Electrum, Jaxx, Exodus и др. Локальные кошельки обеспечивают достаточно высокий уровень надежности кошелька и защищенности средств. Но при этом могут занимать очень много места на жестком диске и долго синхронизируются с блокчейном.

Аппаратные кошельки (в виде отдельного устройства). При инициализации таких устройств вводится код, ограничивающий доступ к аппаратному кошельку в случае его потери или кражи. Взломать данное устройство невозможно. Все транзакции совершаются в защищенной среде прибора. Даже, если подключить аппаратный кошелек к взломанному персональному компьютеру, злоумышленникам не удастся получить контроль над кошельком. Единственным недостатком является довольно высокая цена (порядка $100).

Бумажные кошельки. Это обычный листок бумаги, на которой распечатаны приватные и открытые ключи в виде QR-кода. Для практического использования этих ключей их следует отсканировать. Безусловно, в плане удобства уступают аппаратным кошелькам, но тем не менее обеспечивают сравнимый с ними высокий уровень безопасности.

Часть узлов сети Биткоин оснащено специализированным оборудованием для майнинга. Майнинг (от англ. mining — добыча полезных ископаемых) – деятельность специализированных узлов сети по поддержанию распределенного реестра, обеспечению безопасности, нахождению консенсуса и созданию новых блоков, предусматривающая возможность получения вознаграждения в форме новых монет (эмиссия) за создание нового блока и комиссионных сборов за проверку и подтверждение транзакций. Майнинг характерен для большого числа криптовалют, в том числе, для платформы Биткоин. Сложная система вычислений, сопровождающая майнинг, требуется для обеспечения консенсуса и защиты от двойных трат, а вознаграждение стимулирует участников сети использовать свои вычислительные мощности в целях поддержания работы платформы. Кроме майнинга имеются и другие технологии создания новых блоков, например, форжинг (минтинг). Большинство платежных систем придерживается только одной технологии, но некоторые используют сразу несколько (например, EmerCoin, YaCoin, NovaCoin, PeerCoin и Reddcoin). Как полные ноды, майнинговые узлы получают и ретранслируют неподтвержденные транзакции в сети Биткоин (при этом они не

обязательно поддерживают полноценный локальный блокчейн). Но в отличие от полных нод майнеры способны агрегировать транзакции в новые блоки. Каждый майнинговый узел инспектирует сеть Биткоин в поиске новых блоков. Хотя, такое поведение характерно и для остальных нод, для майнера обнаружение вновь сгенерированного блока имеет особое значение. Это сигнал для начала нового цикла конкурентной борьбы за право представить новый блок сообществу. Т.е., состязание за текущий блок проиграно, следовательно, не теряя времени, нужно включаться в процесс создания нового.

Мошенничество с криптовалютой появилось практически с самого зарождения индустрии. Мошенники быстро поняли, как можно обманывать людей, которые не разбираются в тематике, но хотят стать обладателями популярных цифровых активов. Некоторые продавали сувенирные монетки, выдавая их за биткоин, другие проворачивали более хитрые сделки.

Виды мошенничества:

Поддельные кошельки. Мошенники не пропустили высокий спрос на мобильные кошельки и начали создавать поддельные приложения. Фейковые кошельки для биткоинов обычно имеют имя, очень похожее на официальные и проверенные кошельки, такие как Coinbase или Mycelium, а в некоторых случаях подделки размещают тот же логотип. Мошенничество с криптовалютой по этой тактике запутывает неопытного пользователя, который думает, что устанавливает официальный кошелек, который все рекомендуют. Некоторые поддельные кошельки просачивались в магазины приложений Apple и Android, маскируясь под настоящие. Еще один способ, которым фейковые кошельки привлекают клиентов, – это обещание большей анонимности транзакций.

Предполагаемая мошенническая схема может быть следующей:

- пользователь загружает кошелек;
- пользуется им;
- когда сумма достигаем определенного порога, она выводится с кошелька.

Способ борьбы весьма прост: загружайте кошельки с прямых ссылок на сайте криптовалюты или производителя проверенного кошелька.

Мошенничество при облачном майнинге. Компании, занимающиеся облачным майнингом, берут с пользователей комиссию в обмен на мощности для майнинга биткоинов (или других криптовалют) от имени пользователя. Это позволяет людям получать вознаграждения за добычу, не приобретая и не обслуживая дорогостоящее оборудование. Тем не менее, эта область буквально окупирована мошенниками. Фейковый облачный майнинг — это вебсайты, на которых предлагается купить мощности, но фактически майнинга не будет. Как правило, эти сайты сами платят пользователям в течение определенного периода после оформления поддельного контракта. Затем, спустя какое-то время, компания перестает платить, а средства пользователей исчезают. В этом случае облачный майнинг — просто мошенническая схема, другими словами, финансовая пирамида, потому что средства выплачиваются,

пока пользователи привлекаются к сервису знакомых. Как только количество новых пользователей иссякает, мошенники прекращают кампанию. Примерами скама в облачном майнинге являются Hashinvest, Hashpoke, Cointellect, GAW Miners и HashOcean. Последние два, возможно, были самыми крупными мошенниками с криптовалютами в этой области в последнее время. Владелец GAW Miners заработал предположительно более чем 10 миллионов долларов от инвесторов. Он убедил всех в том, что в его распоряжении много вычислительных мощностей, что привело к крупным продажам его поддельных контрактов на облачный майнинг. Чтобы не стать жертвой мошенников на облачном майнинге, проводите тщательные исследования компаний, которые предлагают эти услуги и убедитесь, что они ведут бизнес прозрачно. Комментарии и отзывы не могут служить доказательством хорошей работы какого-либо облачного майнинга, так как это может быть частью скрытого маркетинга и людей, заинтересованных в заработке на пирамиде.

Инвестиционные схемы. Вложения в биткоин — еще один распространенный тип мошенничества с криптовалютой. Эти схемы несколько схожи с облачным майнингом, так как тоже обещают доходность и ежедневно производят небольшие выплаты, пока вдруг не прекратятся все платежи и мошенник не пропадет с инвестированными средствами. Это тоже работает на принципе пирамиды. Сначала эти «инвестиции» кажутся очень прибыльными, так как есть ежедневные выплаты. Многие пользователи повторно инвестируют туда же, ожидая большую прибыль. Однако, когда пользователь пытается вывести свой доход, возникает проблема, и, прежде чем вы ее обнаружите, компания перестает платить, а пользователи теряют вложенные средства. Если вы решите вложить средства в какой-либо фонд, убедитесь, что компанией управляют профессионалы отрасли. Кроме того, убедитесь, что предлагаемая инвестиционная стратегия полностью описана и имеет здравый смысл, а также приводятся риски и выход. Прежде всего стоит помнить, что любой, кто гарантирует высокую доходность в инвестициях, врет, поскольку никогда нет уверенности в мире инвестиций.

Одним из самых ярких примеров мошенничества с криптовалютой через инвестиционную схему является случай, произошедший в Южной Африке, когда исчезли два основателя криптовалютной инвестиционной платформы, а вместе с ними — 69 000 биткоинов стоимостью $3,6 млрд. Это одно из крупнейших мошенничеств с криптовалютами в мире. Два брата-основателя из Южной Африки Амир и Раис Каджи запустили криптовалютную инвестиционную компанию Africrypt в 2019 году, а в июне 2021 года исчезли вместе с деньгами пользователей платформы — 69 000 биткоинов, стоимость которых составила $3,6 млрд. Еще в апреле 2021 года гендиректор компании Амир Каджи, старший из братьев, заявил клиентам, что компания подверглась взлому. Каджи попросил инвесторов не обращаться к юристам и властям: заявил, что это замедлит процесс возврата утраченных денег. Но некоторые из инвесторов были настроены скептически и наняли юридическую компанию Hanekom Attorneys, которая в ходе расследования заявила, что сра-

зу с подозрением отнеслась к просьбе гендиректора Africrypt, так как сотрудники Africrypt потеряли доступ к программно-аппаратной платформе (back-end) за семь дней до предполагаемой атаки.

Hanekom Attorneys не смогла установить местонахождение братьев, но выяснила, что биткоины со счетов платформы Africrypt вывели и провели через крупные майнинг-пулы, после чего криптовалюту стало невозможно отследить.

Случай Africrypt изучает финансовый регулятор Южной Африки, но официальное расследование он начать не может, поскольку криптовалюта в стране не считается официальным финансовым инструментом.

Еще один похожий случай случился в Турции, когда в апреле 2021 года без вести пропал основатель турецкой криптобиржи Thodex Фарук Фатих Озер. Как сообщало турецкое агентство DHA, топ-менеджер выехал из Турции с $2 млрд денег инвесторов в криптовалюте. Thodex внезапно приостановила торги тоже в апреле, 22 апреля она объявила, что ей не хватает финансового обеспечения для продолжения операций.

Фальшивые обменники и биржи. Биткоин-обменники позволяют обменять одну монету на другую, а также вывести или ввести фиатные деньги. На криптовалютной бирже можно спекулировать валютой и покупать альткоины по более выгодной цене в ходе торгов. В истории были случаи мошеннических обменников и бирж. Такие биржи просят внести платеж, который идет на покупку биткоина. Однако обратно ничего не передается. Эти компании обычно привлекают клиентов за счет снижения комиссий, прием большего количество платежных систем и прочего.

Фишинг с биткоинами. Одна из схем – отправка электронных писем с намерением украсть личную информацию. Жертве отправляют письмо, где говорится, что она выиграла биткоины. Чтобы забрать монеты, нужно войти в свой кошелек (форма располагается сразу в теле письма). Пользователь просто сливает свои данные мошенникам и теряет доступ к своему кошельку, так как данные уже украдены. Фишинг-мошенничества очень распространены, а недавно начали набирать популярность в сообществе держателей криптовалют. Всегда будьте осторожны при нажатии на любые ссылки в сообщениях электронной почты, которые кажутся недостоверными, особенно когда вы проверяете электронную почту на телефоне. Эта же схема применяется при создании копии сайтов.

Пожертвование криптовалюты. Были случаи, когда мошенники создавали поддельные страницы для пожертвований. Например, после террористической атаки в Орландо была создана поддельная страница пожертвований, которая побуждала пользователей отправлять криптовалюту, чтобы помочь выжившим.

Существующая методология деанонимизации транзакций криптовалюты предполагает отслеживание всей цепочки их совершения от момента проведения изучаемого платежа и до предполагаемого обмена криптовалюты на «фиатные деньги» через криптовалютные биржи, в обменнике или банкомате.

Для сбора данных о криптокошельках и отслеживания их транзакций можно использовать штатные обозреватели блокчейна:

btc.com;
etherscan.io;
xrpcharts.ripple.com/#/graph;
explorer.bitcoin.com/bch;
litecoinblockexplorer.net;
steexp.com.

А также универсальные обозреватели:

blockchair.com;
tokenview.com;
blockchain.com;
bitaps.com;
live.blockcypher.com.

Последние дают возможность проводить более тщательный анализ и изучать несколько криптовалют в одном сервисе. В обозревателях хранится следующая информация о совершенных транзакциях:

дата и время совершения транзакции;
адреса криптовалютных кошельков отправителя и получателя;
количество переводимой криптовалюты;
гонорар за осуществление транзакции и хэш (служащий доказательством транзакции и используется для её проверки).

К недостаткам таких обозревателей относятся: отсутствие встроенных систем визуального представления и анализа транзакций, невозможность постановки криптокошелька на контроль (отслеживание), а также невозможность автоматического отнесения изучаемых криптокошельков к известным сущностям (лицам, проектам, биржам, миксерам и т.п.).

Частично эти недостатки можно нивелировать за счет использование бесплатного программного обеспечения. Так визуальное представление криптовалютных транзакций можно организовать при помощи сервисов:

sicp.ueba.su;
graphsense.info;
blockpath.com;
c-hound.ai;
oxt.me;
репозиторий github.com/s0md3v/Orbit.

7. Еще один вид мошенничества, это заражение оборудования предназначенного для добычи криптовалюты. Самую популярную в мире криптовалюту – Биткоин добывают на специальном оборудование – ASIC-майнеры.

В недалёком прошлом крипто монеты можно было добыть при помощи обычного компьютера. Но с ростом популярности криптовалют сложность их добычи увеличилась. Людям «добывающим» криптовалюту – майнерам, было

необходимо устройство, которое позволяло бы добыть большое количество монет за меньший срок. Так и появились айсики.

До появления айсиков Биткоины добывались при помощи видеокарт и компьютерных процессоров. Большинство крипотовалют и по сей день добываются при мощи видеокарт и процессоров, но при добычи Биткоина это стало не выгодно, так как счета за электричество превышали доход от «добычи» криптомонеты.

Эти проблемы были решены при помощи создания ASIC-майнеров. ASIC расшифровывается как «интегральная схема специального назначения» (англ.: «Application Specific Integrated Circuit»). ASIC-майнинг – это добыча крипловалюты при помощи специального оборудования. Айсики создают специально для майнинга определенной монеты и другого применения у них нет. Принципы майнинга на айсике такие же, как и у видеокарты – асики занимаются расшифровкой блокчейна и созданием новых блоков. Он отличается тем, что вычисления осуществляются при помощи специальных чипов, а его мощности – выше. Таким образом, при помощи айсиков можно добыть больше монет.

Но как и все компьютеры, айсики подвержены заражению вирусными программами. Если айсик заряжён вредоносной программой, то все Биткоины которые он «добыл» будут уходить на чужой крипто-кошелек. Вернуть добытые монеты конечно же не получится.

Для предотвращения подобного рода мошенничеств, следует приобретать асики у надежного поставщика и проверять его на отсутствие вредоностных программ. Также следует постоянно мониторить свой крипто-кошелек на количество «добытых» крипто монет, иначе вся заработанная криптовалюта может уйти к злоумышленникам, а счета за электричество останутся у хозяина айсика.

8. Многие люди которые не хотят платить комиссию за обмен криптовалюты, делают это через группы в мессенджерах (например Telegram), а не на специализированных обменниках в сети Интернет. Обычно в таких Telegram-группах тысячи и даже десятки тысяч пользователей, который обменивают криптовалюту на фиатные деньги между собой без привлечения посредников. Но найти добросовестного продавца или покупателя не так то просто. Мошенники пользуются неопытностью новичков – получают от них криптомонеты на свои крипто-кошельки, а затем теряются и не выходят на связь. После чего вернуть криптовалюту не представляется возможным.

Чтобы избежать такого рода мошенничества, следует выбирать проверенного покупателя криптомонет, советуясь с другими пользователями Telegram-группы и опытными людьми, профессионально занимающимися инвестициями в крипто монеты.

Рис.23. Схема распределения криптовалюты на примере биткоина

2.7. ПРЕСТУПЛЕНИЯ ТЕРРОРИСТИЧЕСКОГО ХАРАКТЕРА И ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ СФЕРЫ ТЕЛЕКОММУНИКАЦИЙ И КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Все мировое сообщество бросает огромные силы, разрабатывает новые способы и средства борьбы с такими особо тяжкими преступлениями, как терроризм и экстремизм, приносящие весьма жестокие и порой непоправимые последствия (рис. 24).

В настоящее время террористы и экстремисты все чаще стали использовать для осуществления своих преступных целей сферу телекоммуникаций и компьютерной информации. Об этом свидетельствуют последние факты совершения данного вида преступлений.

Преступления **террористического характера и экстремистской направленности, совершаемые с использованием сферы телекоммуникаций и компьютерной информации, несут глобальные угрозы и являются весьма опасными** как для нашего общества и государства, так и для всего мирового сообщества в целом. Ущерб, наносимый этими видами преступлений, в настоящее время имеет рост в геометрической прогрессии.

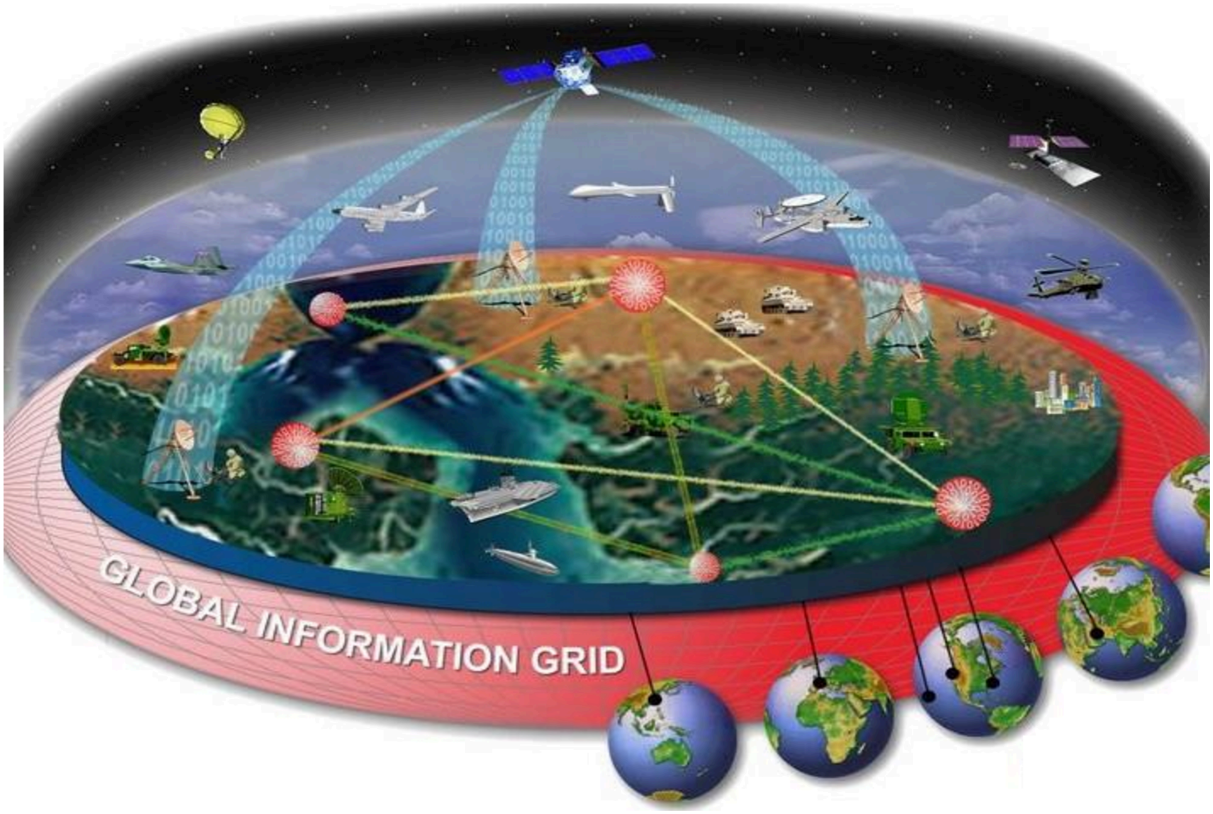


Рис. 24. Сетецентрические войны

Проведенный анализ рассматриваемых видов преступлений показывает, что практически каждое крупное преступление террористического характера

и экстремистской направленности совершается с применением телекоммуникационных систем и компьютерной информации (рис. 25).

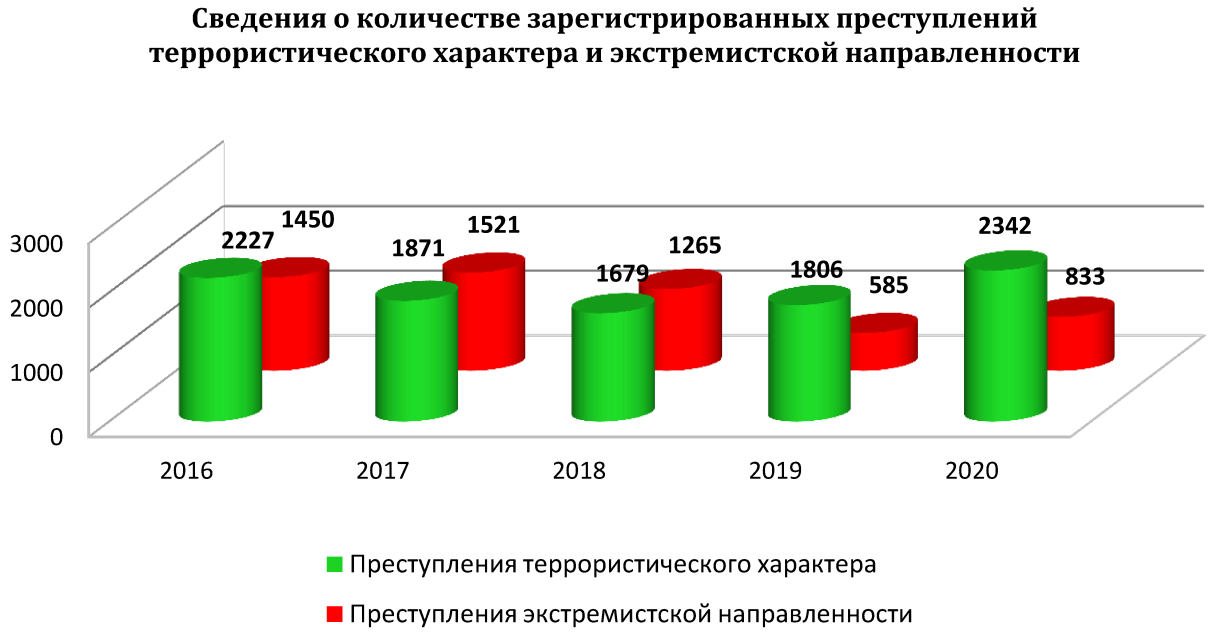


Диаграмма 5. Сведения о количестве зарегистрированных преступлений террористического характера и экстремисткой направленности

Так как в настоящее время участились случаи незаконного использования сферы телекоммуникаций и компьютерной информации, возникла потребность установления нововведения в уголовное законодательство и пересмотр в сторону усиления ответственности в связи с несанкционированным использованием информации террористического характера и экстремистской направленности, хранящейся на различных электронных носителях.

Рис. 25. Использование коммуникаций и компьютерной информации в преступлениях террористического характера и экстремистской направленности

В целях своевременного документирования преступной деятельности данного вида преступлений и получения необходимой доказательной базы в отношении лиц, их совершивших, 6 сентября 2008 г. было создано ГУПЭ[1] МВД России.

Основными направлениями оперативно-служебной деятельности ГУПЭ МВД России являются:

1. Противодействие экстремистской деятельности терроризму.

2. Организация и участие в формировании основных направлений государственной политики по вопросам своей деятельности.

3. Организация взаимодействия подразделений Министерства с федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации по вопросам своей компетенции.

4. Координация в установленном порядке деятельности территориальных органов МВД России и подразделений центрального аппарата МВД России по вопросам деятельности ГУПЭ МВД России.

5. Организационно-методическое обеспечение и оказание практической помощи территориальным органам МВД России и их структурным подразделениям по вопросам своей деятельности.

Как уже было сказано выше, важное значение в раскрытии любого вида рассматриваемых преступлений играет *своевременно полученная информация,* раскрывающая характерологическую особенность психологии личности преступника (рис. 26).

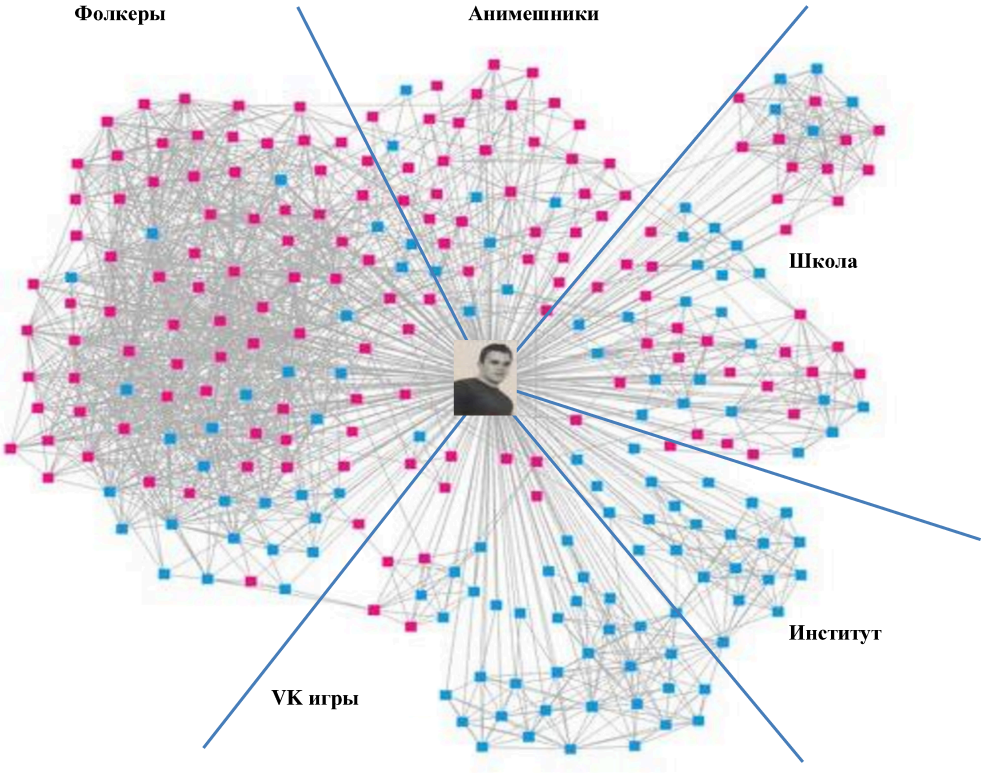


Рис. 26. Пример визуализации связей в социальной сети

[1] ГУПЭ - Главное управление по борьбе с экстремизмом и терроризмом.

Рассмотрим следующие примеры из положительного опыта работы по своевременно полученной информации о субъективной характерологической особенности личности подозреваемого лица.

Пример 1. В городе Энске оперативными сотрудниками ГУПЭ МВД России была получена своевременная информация о том, что некий гр-н Иванов С.Т, являющийся активным участником фанатской группировки, постоянно размещал информацию, направленную на разжигание межнациональной розни, возбуждение ненависти и вражды, а также унижение человеческого достоинства по признаку национальности, происхождения, отношения к религии, в частности, евреев и лиц кавказской национальности, пропагандируя идеологию нацизма, с публичной демонстрацией нацистской атрибутики. В целях получения более точной информации и тщательной ее проверки был намечен план по противодействию и документированию преступной деятельности гр-на Иванова С.Т. В ходе реализации намеченных пунктов плана по его разоблачению активный фигурант был изобличен, а его преступная деятельность документирована. Как результат, в отношении фигуранта было возбуждено уголовное дело, где в ходе судебного слушания преступная деятельность была доказана полностью, и Иванов был осужден по признакам состава преступления, предусмотренного ч.1 ст. 282 УК РФ.

Пример 2. В суд г. Энска с обвинительным заключением направлено уголовное дело, возбужденное Ленинским МСО по г. Энску СУ СК Российской Федерации в отношении активного участника фанатской группировки «Партизаны» гр. Петрова А.В., 12.03.1988 г/р по признакам состава преступления, предусмотренного ч.1 ст. 282 УК РФ. Установлено, что указанный гражданин в социальной сети «Вконтакте» под ником «Александр Йцукерман» на своей странице по адресу: http://vk.com/id176270805 опубликовал видеоролик «obe I kanobe – hip hop ist krieng – Warwarreich», направленный на разжигание межнациональной розни, возбуждение ненависти и вражды, а также унижение человеческого достоинства по признаку национальности, происхождения, отношения к религии, в частности евреев и лиц кавказской национальности, пропагандируя идеологию нацизма, с публичной демонстрацией нацистской атрибутики.

Из приведенных примеров мы видим, что своевременно полученная информация позволяет при более глубоком анализе определить правильную линию поведения оперативных сотрудников подразделений «К» БСТМ МВД России и ГУПЭ МВД России, сузить круг подозреваемых лиц, установить мотив преступления, способ его совершения, а также выдвинуть конкретные версии, отработка которых точно сориентирует и приблизит оперативных сотрудников и следователей к проведению оперативно-розыскных, специальных технических мероприятий и следственных действий, способствующих раскрытию данного вида подготавливаемых и (или) совершаемых преступлений. Это позволит с наименьшей затратой времени выйти на более точное оперативное сопровождение по установлению конкретных лиц, причастных к совершенному или подготавливаемому преступлению, и как положительный

результат приведет к изобличению фигурантов с ***закреплением полученных в ходе документирования доказательств.***

Приведем яркий пример, связанный со своевременным получением информации от спецслужб.

В недавнем прошлом члены террористической группировки, используя возможности современных информационных технологий, склонили студентку Московского Государственного Университета имени М.В. Ломоносова В.П. Караулову (после смены имени и фамилии – А.П. Иванова) перейти на сторону террористической группировки. Затем путем агитационно-пропагандистской деятельности члены указанной группировки осуществили классическую вербовку с намерением дальнейшего использования студентки в проведении террористических актов.

В результате своевременно полученной оперативной информации и слаженных действий специальных служб силовых структур Российской Федерации В.П. Караулова была задержана на территории зарубежного государства и экстрадирована в Российскую Федерацию. Данное задержание положительно сказалось на дальнейшей судьбе В.П. Карауловой, которое не позволило членам запрещенного в России «Исламского государства» ИГИЛ внедрить В.П. Караулову в террористическую организацию и довести их преступный замысел до совершения особо тяжкого преступления.

Преступления террористического характера и экстремистской направленности, совершаемые с использованием **сферы телекоммуникаций и компьютерной информации**, как уже было сказано, являются одними из разновидностей преступлений, входящих в настоящее время в Главу 28 УК РФ «**Преступления в сфере компьютерной информации»,** а рассматриваемые виды преступлений могут входить в Главу 24 «Преступления против общественной безопасности», Глава 29. Преступления против основ Конституционного строя и безопасности государства. Рассмотрим некоторые примеры:

<u>Пример 1.</u> В феврале 2018 г. в ходе регулярно проводимого мониторинга информационных ресурсов сети Интернет выявлена 41 страница социальной сети «В контакте» с призывами к участию в шествии и митинге националистов 12 марта 2018 г., которое на тот момент не было согласовано с органами власти. Принятыми во взаимодействии с прокуратурой Волгоградской области мерами доступ к указанным страницам был заблокирован. В дальнейшем, при взаимодействии Управлений МВД России и ФСБ России по г. Волгограду и иных заинтересованных служб были осуществлены оперативно-профилактические мероприятия в отношении участников радикальных групп, в том числе фанатов и политизированных объединений и групп, пытающихся использовать публичные акции для пропаганды деструктивной идеологии и склонных к совершению правонарушений. Принятыми мерами количество участников акции минимизировано, экстремистских проявлений и иных правонарушений в период проведения митинга не допущено.

<u>Пример 2.</u> Сотрудниками Центров по противодействию экстремизму[1] регионального уровня в рамках постоянно проводимого мониторинга инфор-

[1] Далее – ЦПЭ.

мационных ресурсов сети Интернет, направленного на сбор информации о лицах и группах, причастных к организации и осуществлению экстремистской деятельности на территории региона, выявлены и привлечены к административной ответственности 3 активных участника фанатского движения: по ст. 20.3 КоАП РФ – 1 (публичная демонстрация нацистской символики); ст. 20.29 КоАП РФ – 2 (распространение экстремистских материалов). Обеспечение контроля за активностью объединений футбольных болельщиков осуществлялось путем реализации комплекса оперативно-розыскных и оперативно-профилактических мероприятий, организованных в рамках имеющихся в производстве материалов. При получении оперативно значимой информации о готовящихся акциях незамедлительно ориентируются соответствующие территориальные отделы МВД России, УФСБ России, планируются и проводятся оперативно-профилактические мероприятия (рис. 27).

Рис. 27. Сбор информации о лицах и группах лиц, причастных к организации и осуществлению экстремистской деятельности

В настоящее время возможности глобальной сети Интернета активно используются для организации «цветных революций» во многих странах мира, целью которых является дестабилизация как внутренней обстановки государства, так и состояния современного общества в целом. Например, обнаруженный в 2010 г. червь Worm.Win32.Stuxnet был создан по инициативе спецслужб США и Израиля для проведения кибератак, направленных на разрушение цен-

трифуг, обогащающих уран в Иранском ядерном центре в Бушере. В ходе проведения такой атаки значительная часть центрифуг была выведена из строя. Информация, подтверждающая причастность США и Израиля к атаке с использованием червя Stuxnet, а также согласование ее проведения с руководством США, появилась сравнительно недавно[1].

Рис. 28. Факторы, влияющие на распространение идей терроризма и экстремизма

Также помимо «цветных революций» преступники используют возможности мобильной связи, направленные на дестабилизацию обстановки в обществе. Попытки подобного рода в последнее время значительно участились. Так, например, по данным СМИ, в г. Москве, начиная с сентября 2017 года по настоящее время, злоумышленники через отдаленные серверы, расположенные за пределами Российской Федерации, осуществляют кибератаки путем производства телефонных звонков, через которые периодически отправляются сведения о заложенных взрывных устройствах и взрывчатых веществах в крупных гипермаркетах, кинотеатрах, музеях и других местах массового скопления людей, что наносит помимо некоторого замешательства в обществе еще и значительный экономический урон, превышающий миллиарды рублей.

В настоящее время все чаще стали использовать возможности Интернета террористы, которые осуществляют пропагандистскую деятельность посредством показа материалов с помощью мультимедийных коммуникаций, содержащих идеологические или практические наставления, разъяснения, оправдания или рекламу террористической деятельности (см. рис. 28). К ним могут от-

[1] Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2012. №1. С. 11.

носиться виртуальные сообщения, презентации, журналы, теоретические работы, аудио- и видеофайлы, а также электронные игры, разрабатываемые террористическими организациями или их сторонниками.

Одним из способов своевременного получения информации и раскрытия преступлений террористического характера и экстремистской направленности становится интенсивно развивающийся метод использования многофункциональных комплексов (рис. 29) на основе беспилотного воздушного судна (БВС), которые предназначены для оперативного и достоверного получения информации об объектах различного происхождения, проведения инженерной разведки, выявления электронных компонентов мино-взрывных устройств в грунте, а также для оценки результатов деятельности при осуществлении воздушной разведки протяженных участков местности. Такие многофункциональные комплексы позволяют решать следующие задачи:

1. Ведение фотографической, телевизионной, инфракрасной, радиотехнической, радиолокационной, радиационной, химической разведки с воздуха.

2. Проведение аэрофотосъемки высокого качества с использованием профессиональной фотоаппаратуры, создание 3 «D» моделей местности и объектов.

Рис. 29. Использование новых информационных технологий и радиотехнических методов в борьбе с преступностью

3. Осуществления наблюдения и охраны районов сосредоточения экстремистских и террористических группировок при проведении специальных мероприятий.

В начале января 2018 года международными террористами были использованы так называемые летательные самодельные беспилотники (рис. 30). Данные беспилотные воздушные судна начинялись боекомплектами с современным процессорным оборудованием, которые получали свое управление на отдаленном расстоянии посредством возможностей радиолокационных и телекоммуникационных сетей с целью совершения серии террористических актов на территории Сирии.

Согласно данным, полученным из средств массовой информации, благодаря проведению миротворческой миссии по ликвидации террористической организации в Сирии со стороны военно-космических сил и органов внутренних дел Российской Федерации была проведена контртеррористическая операция по уничтожению данных беспилотников.

В этот же период была сформирована военная полиция по противодействию террористам, которая и в настоящее время осуществляет свою деятельность по своевременному выявлению бандформирований террористического характера и экстремистской направленности. Подобные беспилотные судна использовались и в ходе военных столкновений в Нагорном Карабахе, возникших в сентябре-октябре 2020 года.

Рис. 30. Беспилотный летательный аппарат

О необходимости получения своевременной оперативной криминалистически значимой информации и ее роли в последующем планировании конкретных мероприятий, направленных на раскрытие подготавливаемых и совершаемых преступлений, красноречиво говорят следующие примеры.

В ходе оперативно-розыскной деятельности, направленной на своевременное предотвращение, выявление и раскрытие преступлений террористического характера и экстремистской направленности, сотрудниками ФСБ России был обнаружен сайт под завуалированным названием, в котором находилась переписка членов международной террористической организации «Катиба Таухид валь-Джихад» (запрещена в России). Данная переписка указывала на подготовку террористического акта в г. Волгограде и его окрестностях.

Так после намеченных конкретных оперативно-розыскных мероприятий в октябре 2020 года сотрудниками ФСБ России были нейтрализованы два участника ячейки международной террористической организации «Катиба Таухид валь-Джихад». Все действия террористов координировались посредством завуалированных сайтов и через социальные сети.

Согласно сведениям Центра общественных связей ФСБ России, деятельность террористов координировалась с территории Сирии. Злоумышленники собирались совершить террористические атаки на здания органов власти, места проживания военнослужащих и взрыво-пожароопасные предприятия.

Далее была получена информация, что главарь и его сообщник, пытавшиеся извлечь средства террора из заранее оборудованного в Волгограде тайника, при задержании оказали вооруженное сопротивление сотрудникам ФСБ России и в результате были нейтрализованы.

В ФСБ уточнили, что члены террористической ячейки были выходцами одной из стран Центрально-Азиатского региона. Следователи обнаружили на месте происшествия и в квартирах, где проживали радикальные исламисты, огнестрельное оружие, боеприпасы, химические компоненты и поражающие элементы к СВУ. Кроме того, там была найдена религиозная литература.

Помимо этого, сотрудники спецслужб нашли карту Волгограда, на которой были обозначены планируемые места совершения террористических атак. В частности, одной из планируемых атак боевики собирались совершить теракт возле монумента «Родина-мать». Была изъята карта, на которой монумент «Родина-мать» обведен черным цветом. При допросе задержанных установлено, что указанный объект был основной целью совершения преступления террористического характера.

Оперативно-розыскные мероприятия, направленные на своевременное выявление и предотвращение подготавливаемых преступлений террористического характера и установление их участников, сотрудниками ФСБ России проводились одновременно в Москве, Санкт-Петербурге, Уфе, Майкопе и Волгограде, в результате которых были задержаны другие участники меж-

региональной ячейки, в отношении которых приняты различного рода процессуальные решения.

В конце лета 2020 года ФСБ России задержала шестерых «финансистов», собиравших деньги для террористической организации «Исламское государство», запрещенное в России. Как отметили в службе, задержанные россияне участвовали в деятельности преступной группы. Данные участники – террористы ранее уже были осуждены за финансирование действовавших в Сирии террористических структур. По сведениям спецслужб, у задержанных участников террористической группы, отвечающих за сбор денежных средств для финансирования террористических актов, в ходе проведения обысков было изъято до 500 тыс. руб.

В июле 2020 года сотрудниками ФСБ России в Санкт-Петербурге были задержаны несколько членов террористической организации «Исламское государство». Согласно имеющейся оперативной информации, указанные лица планировали совершить убийства военнослужащих и сотрудников правоохранительных органов Российской Федерации, после чего намеревались выехать на территорию ближневосточного региона для участия в МТО (Международная террористическая организация).

По сведениям Центра общественных связей ФСБ России, спецоперацию, направленную на задержание сторонников террористической ячейки, проводили сотрудники ФСБ России совместно с оперативными подразделениями МВД России в рамках уголовного дела, возбужденного по ч. 1.1 ст. 205.1 УК РФ «Содействие террористической деятельности».

В ходе производства дальнейших оперативно-розыскных мероприятий и необходимых следственных действий по месту жительства фигурантов уголовного дела были обнаружены и изъяты средства связи, банковские карты, имеющие отношение к расследуемым преступным событиям.

В начале лета 2020 года уроженцем одной из стран Центральной Азии подготавливался террористический акт в г. Москве. В его преступный замысел входило проведение массового расстрела. Указанный террорист скрывался в заброшенном гаражном кооперативе, расположенном в г. Химки Московской области. Однако его преступный замысел не был осуществлен, так как благодаря слаженным действиям оперативных сотрудников ФСБ России преступник был своевременно обезврежен и в ходе перестрелки ликвидирован.

Далее в ходе проведения дальнейших оперативно-розыскных мероприятий и следственных действий были обнаружены и изъяты в сети Интернет следы, оставленные в виде электронной переписки с эмиссарами международной террористической организации в Сирии. При осуществлении обыска в арендованной преступником квартире обнаружены вещественные доказательства того, что уничтоженный бандит готовил массовый расстрел граждан.

Сотрудники спецслужб обнародовали кадры с места операции. На них запечатлен убитый и стоящая рядом с ним сумка. В ней правоохранители обнаружили оружие и вещи мужчины. В телефоне подозреваемого в террори-

стической деятельности мужчины оперативники нашли материалы, подтверждающие его связь с преступным сообществом.

Преступления террористического характера и экстремистской направленности содержат в своей основе огромную подготовительную работу. Зная о том, что в настоящее время существует некоторая зависимость подрастающего поколения от Интернета, злоумышленники через различные сайты социальных сетей активно подбирают среди молодежи и несовершеннолетних кандидатов на последующее вовлечение этих лиц в преступную деятельность. Для осуществления своего преступного замысла террористы или экстремисты активно используют сферу телекоммуникаций и компьютерной информации, демонстрируя материалы с порнографическими изображениями несовершеннолетних, а также материалы, относящиеся к преступлениям против здоровья населения, общественной безопасности и нравственности, против основ конституционного строя и безопасности государства. Молодые лица, которые откликаются на демонстрацию перечисленных материалов, попадают в список будущих кандидатов. С этого момента начинается следующий этап вербовочной работы над кандидатами для проведения с ними психологического и агитационного воздействия, конечной целью которого является их реальная вербовка к совершению будущих тяжких и особо тяжких преступлений.

В связи с чем мы считаем, что преступления, совершаемые в сфере телекоммуникаций и компьютерной информации, являются одними из разновидностей преступлений, входящими в гл. 28 Уголовного кодекса Российской Федерации (далее УК РФ) «Преступления в сфере компьютерной информации», а некоторые из них могут тесно взаимодействовать и с другими видами преступлений, входящими в другие главы. Например, ст. 242.1 УК РФ «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних» и ст. 242.2 УК РФ «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов», которые входят в гл. 25 УК РФ «Преступления против здоровья населения и общественной нравственности», а рассматриваемые виды преступлений входят в гл. 24 УК РФ «Преступления против общественной безопасности», гл. 29 УК РФ «Преступления против основ Конституционного строя и безопасности государства».

Для наглядности рассмотрим некоторые примеры, взятые из практической деятельности.

Пример 1.

Осенью 2020 года во Владимирской области похитили ребенка. Задержание лица, совершившего данное преступление, произошло 19 ноября 2020 года сотрудниками Интерпола.

По данным средств массовой информации (РИА Новости), 7-летний мальчик из села Горки во Владимирской области пропал в конце сентября. Он вышел на остановке из школьного автобуса, но дома не появился. Его искали

несколько тысяч людей: полиция, местные жители, пешие и водолазные поисковые отряды. Однако поиски результата не принесли.

В ходе проведения необходимых оперативно-розыскных мероприятий и следственных действий был установлен 26-летний мужчина, у которого, по словам соседей, были проблемы с психикой. Он удерживал ребенка полтора месяца в подвале соседней деревни.

Было установлено, что похититель, увидев около пруда мальчика, остановился и начал с ним беседу. После чего насильно посадил в автомобиль и отвез в деревню Макариха.

Похищенного нашли благодаря Интерполу – от зарубежных коллег сотрудники полиции узнали о публикациях в теневом сегменте интернета DarkNet, где сообщалось о человеке, удерживающем в доме ребенка. Похититель переписывался с кем-то из лиц, проживающих на территории Болгарии. Данные сведения были получены сотрудниками Интерпола, которые в рамках стран «Большой восьмерки» своевременно передали информацию оперативным сотрудникам органов внутренних дел Российской Федерации.

Помимо этого в поисковом отряде «Лиза Алерт» искали ребенка при помощи специальной нейросети, в которую загрузили более 44 тысяч снимков, чтобы опознать исчезнувшего мальчика. Уполномоченный по правам ребенка во Владимирской области Геннадий Прохорычев назвал этот случай уникальным.

Штурм дома похитителя начался 19 ноября 2020 года в 21.30. В одной из неопрятных комнат нашли похитителя с ребенком. В момент задержания преступник держал мальчика на коленях.

Благодаря нейросети и работе Интерпола в теневом сегменте DarkNet ребенка вернули живым.

Пример 2.

Ст. 242.1 УК РФ «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних».

Игнатьев Д.В. приобрел и хранение в целях распространения, а также распространение материалов с порнографическими изображениями несовершеннолетних, в отношении лица, не достигшего четырнадцатилетнего возраста, с использованием информационно-телекоммуникационных сетей (включая сеть Интернет).

Игнатьев Д.В. с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) совершил распространение порнографических материалов. Указанное преступление подсудимый совершил при следующих обстоятельствах.

Игнатьев Д.В., находясь в своем жилище, действуя умышленно с целью приобретения, хранения и последующего распространения порнографических материалов, в том числе с изображением несовершеннолетних, установил на свой персональный компьютер программу «Shareaza», версии 2.7.9.0. Данная прогармма представляла собой файлообменную сеть, то есть одноранговую компьютерную сеть для совместного использования файлов. Программа бы-

ла основана на равноправии участвующих в обмене файлами пользователей, где каждый участник (пользователь) одновременно являлся и клиентом, и сервером. Программа давала возможность копирования и просмотра файлов ее пользователями при условии предоставления общего доступа к папкам и файлам, хранящимся на жестких магнитных дисках.

Далее, Игнатьев Д.В. умышленно копировал на жесткий диск своего персонального компьютера у неустановленных лиц из некоторых источников информационно-телекоммуникационной сети Интернет материалы с порнографическими изображениями несовершеннолетних, в том числе лиц, не достигших четырнадцатилетнего возраста.

В судебном заседании подсудимый Игнатьев Д.В. свою вину в предъявленных ему по п.п. «а», «г» ч.2 ст.242.1, п. «б» ч.3 ст.242 УК РФ обвинениях не признал.

Руководствуясь ст.ст.296-300, 302-304, 307-313 Уголовно-процессуального кодекса Российской Федерации, суд приговорил Игнатьева Д.В. признать виновным в совершении преступлений, предусмотренных п.п. «а», «г» ч.2 ст.242.1, п. «б» ч.3 ст.242 Уголовного кодекса Российской Федерации и назначить наказания:- по п.п. «а», «г» ч.2 ст.242.1 Уголовного кодекса Российской Федерации – лишение свободы на срок 3 (три) года,- по п. «б» ч.3 ст.242 Уголовного кодекса Российской Федерации – лишение свободы на срок 2 (два) года. В соответствии с ч.3 ст.69 Уголовного кодекса Российской Федерации по совокупности преступлений путем частичного сложения назначенных наказаний, назначить Игнатьеву Денису Вячеславичу окончательное наказание – лишение свободы на срок 3 (три) года 6 (шесть) месяцев с отбыванием наказания в исправительной колонии общего режима.

Пример 3.

Ст. 242.1 УК РФ «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних».

Гражданин Дутов М.В., достигший 18-летнего возраста, во время обучения на геологическом факультете Воронежского государственного университета для личного пользования приобрел персональный компьютер – ноутбук.

У Дутова М.В. возник преступный умысел, направленный на приобретение, хранение в целях дальнейшего распространения порнографических материалов с изображениями несовершеннолетних, в том числе лиц, не достигших 14-летнего возраста, с использованием информационно-телекоммуникационной сети Интернет. Реализуя свой преступный умысел, Дутов М.В., обладающий достаточными знаниями в области информационных технологий и навыками пользования компьютерной техникой, установил файлообменную программу посредством пиринговой сети, дающей возможность обмена файлами между ее абонентами, на накопитель на жестких магнитных дисках, находящихся в его персональном компьютере. После чего Дутов М.В., осознавая общественную опасность своих действий, посягающих на психическое здоровье населения и общественную нравственность,

предвидя наступление общественно-опасных последствий и желая этого, находясь у себя в комнате, преследуя цель, направленную на дальнейшее хранение и распространение порнографических материалов с изображениями несовершеннолетних, в том числе лиц, не достигших 14-летнего возраста, с использованием информационно-телекоммуникационной сети Интернет, путем скачивания незаконно приобрел видео-файл, содержащий материалы порнографического характера с участием несовершеннолетних, в том числе с участием лиц, не достигших 14-летнего возраста, и стал незаконно хранить его. Файлы, находящиеся в этой директории, являются общедоступными для пользователей файлообменной сети.

Продолжая свои преступные действия, Дутов М.В., находясь у себя в комнате, используя файлообменной сети, незаконно распространил через сеть Интернет материалы с порнографическими изображениями несовершеннолетних.

Оперуполномоченными отдела «К» БСТМ ГУ МВД России по Н-ской области были произведены поиск и фиксация пользователей, осуществляющих на территории России, в том числе на территории Воронежской области, раздачу видеофайла с порнографическими изображениями несовершеннолетних. В результате вышеуказанных мероприятий был получен файл, содержащий материалы порнографического характера.

Согласно заключению эксперта, файл являлся демонстрацией действий сексуального характера с детальным изображением половых органов несовершеннолетних, направленной на получение патологического возбуждения, что позволяет отнести эти материалы к порнографическим материалам. Согласно признакам, характеризующим изображение несовершеннолетних лиц в фильме либо с использованием детей для создания фильма, в видеозаписи присутствует изображение лица, не достигшего 14-летнего возраста.

Подсудимый Дутов М.В. предъявленное обвинение признал в полном объеме.

Действия Дутова М.В. суд квалифицировал по п.п. «а», «г» ч. 2 ст.242.1 УК РФ, как приобретение, хранение в целях распространения, распространение материалов с порнографическими изображениями несовершеннолетних, совершенное в отношении лица, не достигшего четырнадцатилетнего возраста, с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей, включая сеть Интернет.

Согласно заключению стационарной комплексной судебной психолого-психиатрической комиссии Дутов М.В. в период, относящийся к инкриминируемому ему деянию, каким–либо психическим расстройством не страдал и не страдает в настоящее время, грубых нарушений психической деятельности не выявлено. В применении принудительных мер медицинского характера Дутов М.В. не нуждался.

На основании изложенного и руководствуясь ст.ст.307-309, 316 УПК РФ, суд приговорил признать Дутова М. В. виновным в совершении преступления, предусмотренного п.п. «а», «г» ч. 2 ст.242.1 УК РФ, и назначил ему

наказание в виде 1 года 6 месяцев лишения свободы с отбыванием наказания в исправительной колонии общего режима.

Пример 4.

Ст. 242.2 УК РФ «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов».

Благовещенский городской суд Амурской области рассмотрел в закрытом судебном заседании материалы уголовного дела в отношении Ж., ранее судимого, обвиняемого в совершении преступлений, предусмотренных ч. 1 ст. 137, ч. 1 ст. 137, ч. 1 ст. 137, ч. 1 ст. 137, п.п. «а,в» ч. 2 ст. 242.2, п. «в» ч. 2 ст. 242.2, ч. 1 ст. 137, п. «в» ч. 2 ст. 242.2 УК РФ (совершил незаконное собирание сведений о частной жизни лица, составляющих его личную тайну, без его согласия (видеосъёмка в отношении Д. и несовершеннолетней А.); кроме того, совершил незаконное собирание сведений о частной жизни лица, составляющих его личную тайну, без его согласия (фотосъемка в отношении несовершеннолетних А. и Е.); кроме того, совершил фотосъемку несовершеннолетнего в целях изготовления порнографических материалов, совершенную лицом, достигшим восемнадцатилетнего возраста, в отношении двух лиц, не достигших четырнадцатилетнего возраста (в отношении несовершеннолетних А. и Е.); кроме того, совершил видеосъемку несовершеннолетнего в целях изготовления порнографических материалов, совершенную лицом, достигшим восемнадцатилетнего возраста, в отношении лица, не достигшего четырнадцатилетнего возраста (в отношении несовершеннолетней Ф.).

В квартире дома г. Благовещенска Амурской области Ж. произвел видеозапись на принадлежащий ему мобильный телефон, сделав 2 видеозаписи, тем самым совершил незаконное собирание сведений о частной жизни Д. и несовершеннолетней А., составляющих их личную тайну, без их согласия.

Кроме того Ж. произвел фотосъемку на принадлежащий ему мобильный телефон, сделав 110 фотоснимков, тем самым совершил незаконное собирание сведений о частной жизни несовершеннолетних А. и Е. составляющие их личную тайну, без их согласия.

Кроме того, Ж. произвел фотосъемку на принадлежащий ему мобильный телефон, сделав 17 и 29 фотоснимков порнографического характера. Он тем самым изготовил порнографические материалы, которые в последующем перенес путем их копирования в электронном виде на цифровой носитель – накопитель жесткого магнитного диска принадлежащего ему персонального компьютера, где хранил их до момента обнаружения и изъятия в ходе обыска.

Кроме того, Ж. сделал видеозапись и изготовил порнографические материалы, использовав в целях их изготовления спящую несовершеннолетнюю Ф., которые в последующем хранил в своем мобильном телефоне до момента их обнаружения и изъятия.

В судебном заседании подсудимый Ж. свою вину по предъявленному обвинению признал полностью, от дачи показаний отказался.

Руководствуясь ст.ст. 307, 308, 309 УПК РФ, суд приговорил Ж. виновным в совершении преступлений, предусмотренных ч. 1 ст. 137, ч. 1 ст. 137, п.п. «а», «в» ч. 2 ст. 242.2, п. «в» ч. 2 ст. 242.2 Уголовного кодекса Российской Федерации и назначил ему наказание в виде 9 лет лишения свободы с отбыванием наказания в исправительной колонии особого режима.

Пример 5.

Гаврилова, стала пользователем социальной сети «В», создав личную страницу, зарегистрировавшись под именем «Т», при этом получила возможность в соответствии с правилами данного интернет-ресурса указывать свои личные данные, личную и контактную информацию, размещать иные сведения, доступные иным пользователям социальной сети «В» и обновлять указанную информацию. Гаврилова, имея религиозные убеждения, связанные с пропагандой идеологии терроризма, при помощи ноутбука и модема осуществила выход в сеть И., где на неустановленном информационном ресурсе ознакомилась со статьей «Ответ «алимам-антиэкремизма»», содержащей информацию, призывающую к осуществлению террористической деятельности, обосновывающую и оправдывающую необходимость осуществления террористической деятельности. Преследуя цель ознакомления с текстом статьи «Ответ «алимам-антиэкстремизма»» неопределенного круга лиц, желая распространить идеологию терроризма, имея умысел на публичные призывы к осуществлению террористической деятельности и публичное оправдание терроризма, Гаврилова целенаправленно, сознавая противоправность своих действий, разместила путем копирования с неустановленного следствием ресурса текст статьи.

«Ответ «алимам-антиэкстремизма»» на своей личной странице социальной сети «В», пользователь «Т» представил его неопределенному кругу лиц, из числа зарегистрированных пользователей социальной сети «В». Согласно заключению комплексной психолого-лингвистической экспертизы в тексте статьи «Ответ «алимам-антиэкстремизмама»» содержались публичные призывы к осуществлению террористической деятельности, трансляция установки автора на осуществление такой деятельности, а также высказывания, оправдывающие террористическую деятельность.

На основании изложенного, руководствуясь ст. 316 УПК РФ, суд приговорил признать Гаврилову Т.В. виновной в совершении преступления, предусмотренного ч. 1 ст. 205-2 УК РФ и назначил ей наказание в виде 2 лет лишения свободы.

Пример 6.

Калиниченко М.С., неоднократно входил в открытую информационно-телекоммуникационную сеть Интернет на общедоступный ресурс социальной сети, используя регистрационное имя «Х», при помощи принадлежащего ему персонального компьютера, расположенного в жилище с подведенной к нему линией связи, принадлежащей компании Интернет-провайдеру ООО, «Х» умышленно, с целью привлечения к экстремисткой деятельности неограниченного круга лиц, размещал на общедоступном ресурсе – группе «Х»

по сетевому адресу X, то есть публично, изображения с текстом «X». Указанные высказывания были направлены на организацию, подготовку и подстрекательство к воспрепятствованию законной деятельности государственных органов и органов местного самоуправления, соединенные с насилием либо угрозой его применения, то есть содержали в себе публичные призывы к осуществлению экстремисткой деятельности.

Таким образом, Калиниченко М.С. умышленно, осознавая общественную опасность своих действий, желая наступления общественно опасных последствий в виде воспрепятствования деятельности государственных органов и органов местного самоуправления, соединенного с угрозой применения насилия, совершал публичные призывы к осуществлению экстремистской деятельности, то есть совершил преступление, предусмотренное ч.1 ст.280 УК РФ.

На основании изложенного, руководствуясь ст.ст.314-316 УПК РФ, суд приговорил признать Калиниченко М.С. виновным в совершении преступления, предусмотренного ч.1 ст.280 УК РФ, в соответствии с которой назначить ему наказание в виде 2 лет 7 месяцев лишения свободы с отбыванием наказания в исправительной колонии строгого режима, с лишением права занимать должности на государственной службе и в органах местного самоуправления на срок 1 год 1 месяц.

Одновременно считаем необходимым затронуть **проблему**, возникающую по вопросу использования **возможностей** сферы телекоммуникаций и компьютерной информации для осуществления **преступлений террористического характера и экстремисткой направленности в целях манипулирования** общественным мнением и **дестабилизации** социально-политической обстановки не только на территории **нашего государства**, но и **на международной арене**.

Так на территории Российской Федерации в ходе регулярно проводимого мониторинга информационных ресурсов сети Интернет выявляются страницы социальной сети «В контакте» с призывами к участию в шествии и митингах националистов, которые на момент их проведения не согласовываются с органами власти. Принимаемыми мерами в тесном взаимодействии с органами прокуратуры в регионах Российской Федерации доступ к указанным страницам постоянно блокируется. В этих целях регулярно проводятся при взаимодействии Управлений МВД России и ФСБ России и иных заинтересованных служб оперативно-профилактические мероприятия в отношении участников радикальных групп, в том числе фанатов и политизированных объединений и групп, пытающихся использовать публичные акции для пропаганды деструктивной идеологии и склонных к совершению правонарушений. Осуществляемые профилактические меры минимизируют количество участников акций, а экстремистские проявления и иные правонарушения в период проведения митингов не допускаются.

Об этом красноречиво говорят **примеры из отечественного и зарубежного опыта** деятельности сотрудников правоохранительных органов начала **2021 года** (январь-февраль).

В январе 2021 года при проведении протестных акций в поддержку блогера А. Навального своевременное противодействие сотрудников органов внутренних дел и ФСБ России преступлениям против общественной безопасности и основ конституционного строя и безопасности государства положительно сказалось на предотвращении тяжких и особо тяжких преступлений.

В начале февраля 2021 года сотрудниками полиции МВД Сербии при проведении оперативно-розыскных мероприятий путем мониторинга социальных сетей была своевременно получена информация о готовящемся покушении на президента Сербии Александра Вучича. Данное преступление экстремистской направленности планировалось осуществить во время открытия памятника основателю Сербского государства Стефану Немане, работы российского академика Александра Руковишникова. В результате слаженной работы Управления уголовной полиции МВД Сербии покушение на президента Сербии Александра Вучича было предотвращено. По данному факту были задержаны 17 членов крупной преступной экстремисткой организации, которая предположительно связана с черногорскими мафиозными кланами. Радикалы маскировались под футбольных фанатов. При обыске у них было обнаружено и изъято оружие. Следствие считает, что их наняли главари преступных группировок. Устранив Вучича руками экстремистов, мафия хотела остановить масштабную борьбу с криминалом в Сербии. На главу государства планировали напасть 27 января, когда он открывал памятник на площади в Белграде. В ходе проведения оперативно-розыскных мероприятий и следственных действий было установлено, что в президента Сербии Александра Вучича должны были стрелять два снайпера. Остальным боевикам поручалось вызвать панику в толпе и обеспечить отход соучастников. Ранее глава МВД пояснил, что президент Сербии «объявил войну организованной преступности», которая, в свою очередь, приняло решение о ликвидации Александра Вучича. В связи с появлением **в соцсетях** постоянных угроз в адрес А. Вучича и членов его семьи сотрудниками правоохранительных органов Сербии были задержаны несколько человек. Проправительственные СМИ регулярно заявляют о «травле» сербского президента, близких ему людей и политиков со стороны оппозиции и преступного сообщества.[1]

Прогноз развития ситуации, начиная с 2017 года по 2019 год, подтверждает тенденцию уменьшения количества преступлений террористического характера и экстремистской направленности, а сведения, представленные ФКУ «Главный информационно-аналитический центр МВД России» о состоянии преступности в России за 2020 год, указывают на резкий скачок данных преступлений с 2391 зарегистрированных преступлений в 2019 году до 3175 пре-

[1] Белград, 8 февраля - РИА Новости.

ступлений, зарегистрированных в 2020 году, что составляет 32,78% роста (см. диаграмму 6).

Диаграмма 6. Динамика зарегистрированных преступлений террористического характера и экстремистской направленности

Ежедневная практическая деятельность, направленная на эффективную работу по вопросу раскрытия рассматриваемых видов преступлений, осуществляется путем тесного взаимодействия сотрудников ПСТМ, ГУПЭ и следственных подразделений, что положительно сказывается на результате раскрываемости подготавливаемых или уже совершенных преступлений. Одновременно в образовательных организациях системы МВД России в настоящее время активизирована работа по эффективной и более качественной подготовке сотрудников органов внутренних дел, которые по своим функциональным обязанностям призваны раскрывать преступления террористического характера и экстремистской направленности. Данный путь целевой профессиональной подготовки специалистов по своевременному раскрытию преступлений рассматриваемой направленности дает свои результаты, подтвержденные статистическими сведениями, приведенными ФКУ «Главный информационно-аналитический центр МВД России» (см. диаграмму 7).

Диаграмма 7. Динамика раскрываемости преступлений террористического характера и экстремистской направленности

Согласно приведенным сведениям о состоянии преступности в России[1] за 1 полугодие 2020 года было выявлено 1183 преступления террористического характера, за аналогичный период 2019 года их было выявлено 972. Данное количество преступлений указывает на то, что за 1 полугодие 2020 года их было выявлено на 211 преступлений больше, что составляет 21,71% роста.

Преступлений экстремисткой направленности за 1 полугодие 2019 года было выявлено 314 фактов, тогда как за аналогичный период 2020 года их было выявлено 442, что на 128 случаев больше и в процентном соотношении составляет рост на 40,76% (см. диаграмму 8).

Согласно приведенным сведениям о состоянии преступности в России[2] за 2020 год было выявлено 2342 преступления террористического характера, за 2019 год их было выявлено 1806. Данное количество преступлений указывает на то, что за 2020 год их было выявлено на 536 преступлений больше, что составляет 29,68% роста.

---

[1] Состояние преступности в России ФКУ «Главный информационно-аналитический центр МВД России» за 1 полугодие 2020 года, Москва.

[2] Состояние преступности в России ФКУ «Главный информационно-аналитический центр МВД России» за 2020 год, Москва.

Диаграмма 8. Динамика преступлений террористического характера и экстремистской направленности за 1 полугодие 2020 года по отношению к 1 полугодию 2019 года

Преступлений экстремисткой направленности за 2019 год было выявлено 585 фактов, тогда как за 2020 год их было выявлено 833, что на 248 случаев больше и в процентном соотношении составляет рост на 42,39% (см. диаграмму 9).

Данные сведения заставляют нас задуматься о том, что необходимо активизировать работу по эффективному противодействию рассматриваемым видам преступлений, совершаемых с использованием современных информационно-телекоммуникационных сетей. Необходимо тщательно анализировать складывающуюся криминогенную обстановку, делать соответствующие выводы и расширять источники информации, способствующие своевременному предупреждению и не допущению совершения преступлений террористического характера и экстремистской направленности, так как рассматриваемые виды преступлений, совершаемые в сфере телекоммуникаций и компьютерной информации, составляют высокую степень опасности нашему современному обществу и национальной безопасности любого государства.

Диаграмма 9. Динамика преступлений террористического характера и экстремистской направленности за 2020 год по отношению к 2019 год.

Подводя итоги вышесказанному можно сделать следующий вывод, что свобода проявлений себя в информационном пространстве позволяет преступным элементам действовать дерзко и безбоязненно, в связи с чем возможно утверждать, что информатизация общества, обладая, несомненно, множеством позитивных качеств, привела и к информатизации криминальной среды, придала ей ярко выраженный интернациональный и высокотехнологичный характер. Лица, склонные к совершению вышеуказанных преступлений, используют возможности информационно-телекоммуникационных систем, что способствует расширению транснационального масштаба, и, как результат, в конечном итоге определяют и создают угрозу национальной безопасности.[1]

[1] Алескеров В.И., Баранов В.В. Телекоммуникация и киберпространство как средство преступлений экстремистской и террористической направленности // Труды Академии управления МВД России. 2020, №1 (53). С. 104-113.

Контрольные вопросы

1. Где и когда был зарегистрирован факт убийства при помощи использования компьютерных технологий?
2. Назовите типичные ситуации, наиболее часто встречающиеся при расследовании преступлений в сфере телекоммуникаций и компьютерной информации.
3. Определите ход и тактику проведения оперативно-розыскных и следственных действий при каждой складывающейся типичной ситуации.
4. Что включает в себя технология (требования) работы с вещественными доказательствами?
5. Что такое дамп памяти?
6. Что включает в себя комплекс неотложных оперативных и следственных действий при раскрытии преступлений данной категории?
7. Во что преобразуются результаты компьютерно-технической экспертизы? Какие задачи решаются в ходе производства компьютерно-технической экспертизы?
8. Перечислите порядок производства контроля и записи переговоров на предварительном следствии, а также правовые основания, тактические условия, технология проведения.
9. Перечислите этапы взаимодействия оперативных служб со следственными органами в ходе раскрытия преступлений, совершаемых в сфере телекоммуникация и компьютерной информации.
10. Что Вы понимаете под технологией производства следственного действия и оперативно-розыскного мероприятия? Какими величинами являются оперативно-розыскная и следственная ситуация?
11. Что должны знать и на что должны быть нацелены сотрудники, наделенные правами документирования фактов, имеющих отношение к преступной деятельности разрабатываемых лиц, и последующего эффективного расследования уголовного дела?
12. Что должны носить и содержать в себе принимаемые решения должностными лицами при раскрытии преступлений данной категории?
13. Что отрицательно влияет на ДБО (дистанционное банковское обслуживание)?
14. Что такое «клиентский риск и банковский риск»?
15. Что такое DoS-атака и DDoS-атаки? В чем их принципиальное отличие?
16. Кого принято считать «отцом» компьютера и какое изобретение он сделал являющееся предметом множества споров в области информационного права?
17. В каком году появился вирус, который не причинял вреда, а лишь выводил сообщение на экран?
18. С какого времени проблема вирусов начинает принимать глобальный характер?

19. Кто является автором «Маленькая чёрная книжка о компьютерных вирусах»?

20. Какой может причиняться вред при запуске вредоносной программы в ПО отдельного пользователя? Перечислите некоторые из них.

21. Какие нарушаются права человека в результате запуска вредоносной программы в ПО пользователя?

22. Что является побуждающим фактором и степенью общественной опасности к совершению неправомерного доступа к охраняемой законом компьютерной информации?

23. Как и на какие группы были разделены хакеры на 1-й Международной конференции Интерпола по компьютерной преступности?

24. Как Вы считаете, возможно ли в настоящее время на 100% обезопасить компьютерную информацию от преступных посягательств?

25. Назовите мотивы, перечислите предупредительные меры и группы вероятных преступников, совершающих преступления в сфере телекоммуникаций и компьютерной информации.

26. Перечислите основные задачи, возникающие в ходе расследования преступлений, связанных с созданием и использованием вредоносных программ.

27. Перечислите некоторые виды преступлений, совершаемых в телекоммуникационных сетях.

28. Можете ли Вы нарисовать схему работы операторов фиксированной (проводной) связи?

29. Можете ли Вы нарисовать схему работы несанкционированного доступа к УАТС с целью генерации трафика на абонентские номера с услугой звонка за дополнительную плату (платные номера) международных операторов?

30. Можете ли Вы привести пример преступления совершенного в проводных телекоммуникационных сетях?

31. Можете ли Вы привести пример преступления, совершенного в беспроводных телекоммуникационных сетях?

32. Можете ли Вы нарисовать преступную схему осуществления злоумышленником связи между сетями (нанесение ущерба путем инициализации трафика на «короткие номера)?

33. Что такое телефонное мошенничество? Можете ли Вы привести пример с телефонным мошенничеством?

34. Какие особенности характеризуют преступления, связанные с «sms-сообщениями из банка», «sms – просьба о помощи», «платный код от оператора связи»?

35. Можете ли Вы привести пример преступления совершенного в сети Интернет?

36. Классифицируйте преступление, связанное с незаконным доступом к услугам кабельного и спутникового телевидения.

ГЛАВА III
РАСКРЫТИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

В настоящее время в мире происходят экономические преобразования динамического характера, которые влияют не только на политический сегмент, но и на быстро развивающуюся сферу информационных-телекоммуникационных и компьютерных технологий. Информационные потоки, вливающиеся во все сферы жизнедеятельности современного общества, придают возможности бурного развития социального обеспечения, финансов, экономики, медицины, образования, всевозможных научных исследований на всех направлениях. Несмотря на эту положительную сторону, как всякое новое веяние, преобразования, кроме масштабных революционных изменений, неизбежно влекут за собой и некоторые нежелательные последствия. К таким последствиям мы можем отнести преступления, совершаемые в сфере телекоммуникаций и компьютерной информации. Одним из разновидностей таких преступлений являются преступления, совершаемые в системе дистанционного банковского обслуживания, статистика которых из года в год показывает геометрическую прогрессию, а ущерб от данного вида преступлений, к нашему сожалению, велик (см. диаграмму 10).

Диаграмма 10. Количества преступлений, совершаемых в системе ДБО[1]

[1] *Данные взяты из статистических данных ФКУ «Главный информационно-аналитический центр МВД России».*

За последние годы проводится целый ряд глубоких исследований преступлений данной направленности, на основе чего подготовлены доклады, отчеты, статьи и рекомендации, но во всех перечисленных документах прослеживается четкое высказывание, что преступления, совершаемые в системе дистанционного банковского обслуживания, являются преступлениями, относящимися к разновидностям киберпреступлений. А если выражаться еще точнее, то данный вид преступлений можно отнести и к **компьютерно-экономическим** преступлениям. Повсеместное использование технологических возможностей информационно-телекоммуникационных сетей и компьютерной информации в глобальной сети Интернет порождает благоприятные условия, способствующие осуществлению преступного замысла среди лиц, совершающих преступления в системе дистанционного банковского обслуживания. Данное обстоятельство не может не вызывать тревогу у сотрудников оперативных подразделений, призванных вести активную и целенаправленную работу по противодействию данному виду преступлений, так как в большинстве случаев лица, совершающие этот вид преступлений, остаются без соответствующего наказания.

Киберпреступность, ее рост являются следствием продолжающейся глобализации внедрения информационно-телекоммуникационных технологий и появления международных компьютерных сетей. С масштабным ростом информационных систем в различных областях деятельности возрастает и их применение в целях совершения преступлений. В этой связи можно утверждать, что электронная революция дала толчок преступности, использующей возможности информационно-телекоммуникационных сетей для извлечения прибыли. Появились новые формы и виды преступлений, представляющие угрозу для граждан, предприятий, организаций, государств.

Алексей Лунин, автор статьи *«Как не стать жертвой мошенников?»,* не зря упоминает о том, что воры-психологи все чаще крадут деньги с банковских карт пенсионеров. Так по оценкам аналитиков, в 2017 году мошенники с помощью социальной инженерии похитили с банковских карт жителей нашей страны почти 750 млн. руб., причем большая часть пострадавших – пенсионеры. Он же в своей статье *«Реально ли победить киберпреступность?»* приводит следующую информацию: «Сумму ущерба мировой экономике от действий киберпреступников в 2017 году аналитики экономического форума в Давосе оценили в 1 трлн. долл. США».[1] В России потери тоже ощутимы. «Статистика говорит о 150-200 млн. руб. в 2017 г. но, видимо, это только официально зафиксированные и как-то расследованные инциденты. Оценка аналитиков, касающаяся всей страны, – 550-600 млрд. руб. Что касается прогноза возможных потерь на 2018 год, то они могут составить 1 трлн. руб.», – приводит красноречивые цифры заместитель председателя правления Сбербанка России Станислав Кузнецов.

[1] «Аргументы и факты» № 26, 2018 (www/aif/ru).

В начале июля 2018 г. Сбербанк провел в Москве Международный конгресс по безопасности в сфере информационных технологий. Это один из первых шагов России к созданию всемирной системы обмена информацией о преступлениях в сфере информационных технологий и борьбы с лицами, их совершающих. Разработчики антивирусных программ, руководители банков, представители Интерпола и правоохранительных органов обменивались опытом и обсуждали общие правила противодействия угрозам в сфере информационных технологий. Как организатор конгресса Сбербанк решил открыто показать свои методы работы. Защищая своих клиентов, он действует по **четырем направлениям**:

Первое – безопасность центральных банковских систем, где хранятся все сведения о счетах. Второе – разработка новых финансовых продуктов, в программный код которых уже на старте проекта зашиваются базовые принципы безопасности. Третье – анализ нестандартных действий и ошибок клиентов. Для этого используется специальная система антифрода с искусственным интеллектом, которая способна выявить и не допустить до 97 % мошеннических операций. Четвертое – тщательное расследование каждой кибератаки, нацеленное на выявление мошенников.[1]

В целях консолидации усилий в противодействии электронной преступности Советом Европы была разработана Конвенция о киберпреступности, ставшая первым международно-правовым документом в этой области. На заседании в Будапеште 23 ноября 2001 года министрами иностранных дел Европейского Сообщества принята Европейская Конвенция по борьбе с компьютерной преступностью, а сегодня к этой конвенции присоединилось более 40 стран.[2]

Мошенничество является одним из самых распространенных криминальных проявлений на территории Российской Федерации. Прежде всего, это связано с тем, что российское законодательство придает особое значение проблемам усиления ответственности за различные виды мошеннических действий. В период с 2003 по 2011 гг. в ст. 159 Уголовного кодекса Российской Федерации внесены значительные изменения и дополнения, усиливающие уголовную ответственность за данный вид хищения. В 2012 году на основании Федерального закона от 29 ноября № 207-ФЗ в Уголовный кодекс введены шесть новых видов мошеннических действий, в том числе:

- ст. 159.1 – мошенничество в сфере кредитования;
- ст. 159.2 – мошенничество при получении выплат;
- ст. 159.3 – мошенничество с использованием платежных карт;
- ст. 159.4 – мошенничество в сфере предпринимательской деятельности;
- ст. 159.5 – мошенничество в сфере страхования;
- ст. 159.6 – мошенничество в сфере компьютерной информации.

---

[1] «Аргументы и факты» № 26, 2018 (www/aif/ru).

[2] Тарасов А.М. Электронное правительство и информационная безопасность: учебное пособие. – СПб: ГАЛАРТ, 2011. - 648 с.

В соответствии со ст. 159 Уголовного кодекса Российской Федерации, мошенничеством признается хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

При мошенничестве обман, или злоупотребление доверием, является способом завладения чужим имуществом. Особенностью такого вида хищения, как мошенничество, является то, что в результате обмана потерпевший сам передает преступнику имущество, при этом добровольность передачи имущества является мнимой, поскольку обусловлена совершенным в отношении потерпевшего обманом, введением его в заблуждение. Любая форма обмана и злоупотребления доверием, в целом, сводится к тому, что виновный при осуществлении своих действий создает у потерпевшего уверенность в правомерности или выгодности для него передачи имущества или права на него. С развитием современного общества, появлением прогрессивных технических возможностей, научными открытиями и изобретениями, к сожалению, все чаще выявляются новые виды мошеннических действий, которые в последнее время активно совершенствуются.

Мошенничество – это общественно опасное деяние, которое причиняет не только имущественный вред гражданам, но и подрывает доверие между людьми, разрушает нравственные устои общества в целом. Как показывает практика, за последнее время нашел активное распространение такой вид преступления, как мошенничество с использованием средств сотовой телефонной связи и дистанционного банковского обслуживания. С 2008 года данные виды мошенничества начали активно совершенствоваться и получили достаточно широкое распространение на территории Российской Федерации. Среди большого многообразия видов мошенничества данные виды получили название «телефонное» мошенничество и мошенничество в сфере ДБО (дистанционного банковского обслуживания), поразив практически все регионы России.

«Телефонное» мошенничество можно охарактеризовать как мошенничество, при котором деньги похищаются у потерпевшего под различными предлогами: путем обмана или введения в заблуждение последнего, с помощью средств сотовой телефонной связи. По данным ФКУ «ГИАЦ МВД России», в структуре преступности за период 2008 – 2018 гг. мошенничество занимает – 10,8%, что составляет пятую часть от всего объема хищений. Особо следует отметить, что в 2018 году, несмотря на предпринимаемые меры противодействия, происходит рост рассматриваемых видов преступлений на 9,8%. В настоящее время количество рассматриваемых видов преступлений продолжает расти.

3.1. УГОЛОВНО-ПРАВОВАЯ И КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Статистика свидетельствует, что хищения денежных средств, совершенных с использованием вредоносных программ, составляют незначительную часть в структуре преступности. Однако ущерб, причиненный ими, по мнению ведущих специалистов в этой области, настолько велик, что сразу не поддается конкретной оценке. Используемые злоумышленниками замаскированные способы преступных действий и осуществление адекватного противодействия расследованию существенно затрудняет ведение борьбы с преступлениями рассматриваемого вида. Каждая вновь возникшая ситуация, требуют индивидуального подхода и актуализации возрождающих вопросов, необходимых в ходе решения раскрытия хищений денежных средств, совершаемых в системе дистанционного банковского обслуживания (ДБО). ДБО – технологии предоставления банковских услуг на основании распоряжений, передаваемых клиентом без его визита в банк, чаще всего с использованием компьютерных и телефонных сетей (рис. 31). В каждой конкретной ситуации рассматриваемого вида преступлений присутствует **корысть** и как результат происходит безвозмездное противоправное изъятие денежных средств и оборот их в пользу участника преступления.

Рис. 31. Дистанционное банковское обслуживание (ДБО)

В связи с вопросами, возникшими в судебной практике при рассмотрении уголовных дел о хищениях, Пленум Верховного Суда Российской Федерации дал некоторые разъяснения[1], но данные разъяснения лишь фрагментарно затронули вопросы квалификации хищения денежных средств в системе

[1] О судебной практике по делам о краже, грабеже и разбое: постановление Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29 // Бюллетень Верховного Суда Российской Федерации. 2003. № 2; О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 // Бюллетень Верховного Суда Российской Федерации. 2008. № 2.

ДБО (с использованием электронных средств платежа). Кроме того, данные разъяснения были даны до изменений действующего уголовного законодательства и законодательства в сфере банковской деятельности, связанных с регламентацией безналичных расчётов. В связи с чем, в практической деятельности судов, а также следственных органов остаются множество неразрешенных вопросов.[1]

Одним из распространенных способов хищений денежных средств с лицевых счетов клиентов банка может быть преступный сговор сотрудников кредитных организаций, уполномоченных осуществлять различного вида услуги в системе дистанционного банковского обслуживания, или иных лиц, наделенных правами и возможностями доступа к компьютеру, подключенному к системе ДБО (рис. 32).

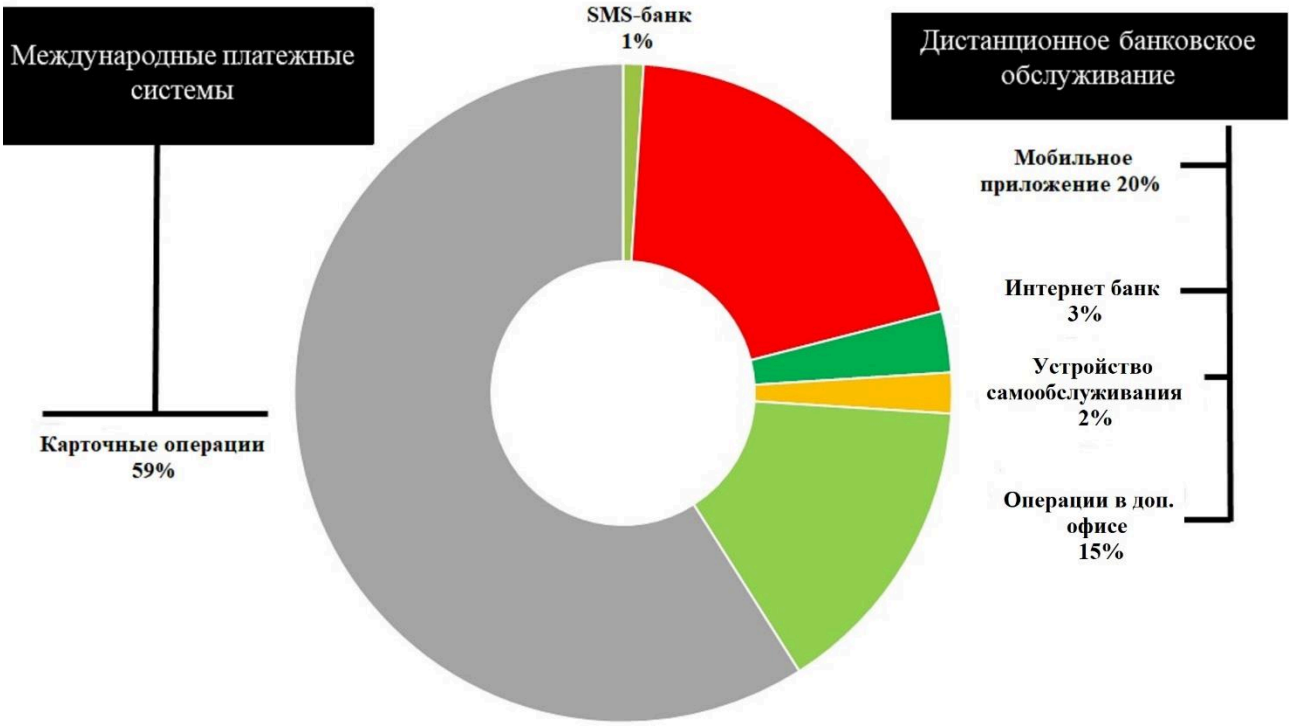


Рис. 32. Удаленные каналы обслуживания как объект преступного посягательства

В зависимости от складывающейся обстановки, а также способа совершения хищений денежных средств в системе дистанционного банковского обслуживания, согласно нормам ст. 158, 159.6 УК РФ, преступления могут совершаться в виде краж и мошенничества в сфере телекоммуникационных систем.

[1] Шмонин А.В., Баранов В.В. Организация выявления, раскрытия и расследования хищений денежных средств в системе дистанционного банковского обслуживания: учебно-практическое пособие / под науч. ред. доктора юридических наук, профессора А.В. Шмонина. – М.: Академия управления МВД России, 20014. – 312 с.

Исходя из криминогенной обстановки, авторы работы считают необходимым рассмотрение ст. 160 УК РФ, так как преступления в системе дистанционного банковского обслуживания при определенных ситуациях можно рассматривать в виде присвоения либо растраты.

Предлагаем рассмотреть вышеуказанные виды преступлений.

Ст. 158 УК РФ. Кража.

Предметом хищения в анализируемой статье является чужое имущество в виде денежных средств. При краже денежные средства изымаются безвозмездно, то есть без соответствующего возмещения.

Родовым **объектом** кражи денежных средств в системе дистанционного банковского обслуживания являются общественные отношения в сфере экономики. Видовой и непосредственный объект: общественные отношения по охране собственности.

Характеризуя **объективные признаки** кражи денежных средств в системе дистанционного банковского обслуживания, мы можем выделить общественно опасные действия и наступившие в их результате общественно опасные последствия. Общественно опасные действия в данном случае выражены активной формой поведения – действиями, направленными на тайное хищение чужого имущества в виде денежных средств. Общественно опасные последствия выражаются в нанесении материального ущерба потерпевшему.

Субъектом кражи является физическое вменяемое лицо, достигшее 14-летнего возраста, способное нести уголовную ответственность.

Субъективная сторона преступления в виде кражи денежных средств в системе дистанционного банковского обслуживания характеризуется умышленной формой вины, прямым умыслом, корыстным мотивом.

Цель совершения преступления – материальное обогащение.

Согласно п.6 Постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. «О судебной практике по делам о краже, грабеже и разбое», кража считается оконченным преступлением с того момента, когда виновный изъял чужое имущество и получил реальную возможность использовать его или иным образом распорядиться им по своему усмотрению.[1]

К **квалифицированным признакам** кражи денежных средств в системе дистанционного банковского обслуживания следует отнести кражу, совершенную группой лиц по предварительному сговору (п. «а» ч. 2 ст. 158 УК РФ), с причинением значительного ущерба гражданину (п. «в» ч. 2 ст. 158 УК РФ).

Кража признается совершенной группой лиц по предварительному сговору, если в ней принимали непосредственное участие два или более лица, заранее договорившиеся о совместном совершении кражи до начала преступления. При этом каждый из исполнителей либо полностью, либо частично выполнял объективную сторону преступления.

---

[1] Постановление Пленума Верховного Суда РФ от 27 декабря 2002 г. «О судебной практике по делам о краже, грабеже и разбое».

Кражу с причинением значительного ущерба гражданину следует квалифицировать в случае, если похищенные в системе дистанционного банковского обслуживания денежные средства, принадлежавшие физическому лицу, существенно ухудшили его материальное положение. При этом ущерб не может признаваться значительным, если он составляет менее 5000 рублей, согласно примечанию 2 к ст. 158 УК РФ.

Особо квалифицированные виды кражи денежных средств в системе дистанционного банковского обслуживания предусмотрены п. «в» ч. 3 ст. 158 УК РФ – кража, совершенная в крупном размере; п. «г» ч. 3 ст. 158 УК РФ – с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст.159.3 УК РФ).

Крупный размер кражи в данном случае означает, что похищены денежные средства в размере, превышающем 250 тысяч рублей (примечание 4 к ст. 158 УК РФ).

Наиболее опасные виды кражи предусмотрены ч. 4 ст.158 УК РФ: кража, совершенная организованной группой (п. «а») и в особо крупном размере (п. «б»). **Особо крупный размер** кражи означает хищение денежных средств в размере, превышающем 1 млн. рублей (примечание 4 к ст. 158 УК РФ).

Ст. 159.6 УК РФ. Мошенничество в сфере компьютерной информации.

Предметом в анализируемой статье является чужое имущество в виде денежных средств, похищенное путем обмана или злоупотребления доверием.

Родовым **объектом** в данном случае являются общественные отношения в сфере экономики. Видовой и непосредственный объект – общественные отношения по охране собственности.

Характеризуя **объективные признаки** хищения денежных средств в системе дистанционного банковского обслуживания, совершенные путем обмана или злоупотребления доверием, мы можем выделить общественно опасные действия и наступившие в их результате общественно опасные последствия.

Общественно опасные действия в данном случае могут быть выражены активным обманом владельца денежных средств посредством сообщения ему заведомо ложных сведений, создающих у него ошибочное представление о совершаемых действиях. Такой обман может состоять в том, что преступник выдает себя, например, за сотрудника банка, тем самым создает иллюзию наличия законных оснований для сообщения ему конфиденциальных сведений, необходимых для получения доступа к его денежным средствам.

Общественно опасные последствия выражаются в нанесении материального ущерба потерпевшему.

Субъектом мошенничества является физическое вменяемое лицо, достигшее 16-летнего возраста, способное нести уголовную ответственность.

Субъективная сторона преступления в виде хищения денежных средств в системе дистанционного банковского обслуживания, совершенного

путем обмана или злоупотребления доверием, характеризуется умышленной формой вины, прямым умыслом, корыстным мотивом.

Цель совершения преступления – материальное обогащение.

Специфика мошенничества состоит в том, что собственник имущества, введенный в заблуждение, может сам передавать преступнику свое имущество либо сообщать ему информацию, дающую право доступа к нему. При этом потерпевший ошибочно полагает, что действует в своих интересах.

Согласно п.8 Постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», мошенничество, то есть хищение чужого имущества, совершенное путем обмана или злоупотребления доверием, признается оконченным с момента, когда указанное имущество поступило в незаконное владение виновного или других лиц, и они получили реальную возможность (в зависимости от потребительских свойств этого имущества) пользоваться или распорядиться им по своему усмотрению.

Если предметом преступления при мошенничестве являются безналичные денежные средства, в том числе электронные денежные средства, то по смыслу положений п. 1 примечаний к ст. 158 УК РФ и ст. 128 Гражданского кодекса Российской Федерации содеянное должно рассматриваться как хищение чужого имущества. Такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб.[1]

На основании п. 20 вышеуказанного Постановления Пленума Верховного суда, по смыслу ст. 159.6 УК РФ вмешательством в функционирование средств обработки, хранения, систематизации и передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, систематизации и передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 272, 273 ил 274.1 УК РФ[2].

---

[1] Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

[2] Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

К **квалифицированным признакам** преступления в виде хищения денежных средств в системе дистанционного банковского обслуживания, совершенного путем обмана или злоупотребления доверием, следует отнести мошенничество, совершенное группой лиц по предварительному сговору, а также с причинением значительного ущерба гражданину (ч. 2 ст. 159.6 УК РФ).

Особо квалифицированные признаки анализируемого преступления предусмотрены ч. 3 ст. 159.6 УК РФ: деяния, совершенные лицом с использованием своего служебного положения (п. «а»); в крупном размере (п. «б»); с банковского счета, а равно в отношении электронных денежных средств (п. «в»).

Наиболее опасные виды мошенничества предусмотрены п. 4 ст.159.6 УК РФ: деяния, совершенные организованной группой либо в особо крупном размере.

В целях квалификации преступлений по данной статье признаки понятия крупного и особо крупного размера похищенных денежных средств совпадают с признаками, используемыми при квалификации преступлений по ст. 158 УК РФ (см. примечание 4 к ст. 158 УК РФ).

Итак, выше нами были проанализированы элементы составов преступлений в системе ДБО, предусмотренных ст. 158 и ст. 159.6 УК РФ, выявлены квалифицирующие и особо квалифицирующие признаки по данным составам, приведены понятия оконченного преступления, крупного и особо крупного размера, применяемых в целях квалификации по вышеуказанным статьям.

С целью проведения анализа криминалистической информации, характеризующей особенности преступлений в системе ДБО, необходимо установить **место, время, способ, обстоятельства** совершения преступления, используемые **технические средства**, выявить **следы** приготовления, совершения преступления, а также их возможное сокрытие.

Временем совершения преступления в системе ДБО следует признавать момент нажатия управляющей клавиши компьютера (или другого устройства), запускающей конечную целевую команду. При этом, в зависимости от способа совершения преступления общественно опасные последствия могут наступить сразу после его совершения либо через длительное время, которое может потребоваться для действия используемой вредоносной программы.

Что касается определения места совершения преступлений, то в большинстве случаев – это компьютерные и (или) телекоммуникационные сети. Местом преступления может признаваться как место совершения общественно опасного деяния, так и место наступления общественно опасных последствий, при этом они могут быть отделены друг от друга многими километрами и даже континентами.

К способам преступлений, совершаемых в системе ДБО, относятся: использование вредоносных программ скрытого управления, использование программ считывания пароля, применение программ удаленного доступа, создание «зеркального сайта» и другие.

Анализу подлежат также все обстоятельства, сложившиеся в момент совершения преступления. Они влияют на выбор способа, механизма совер-

шения преступления, позволяют определить причины и особенности поведения участников общественно опасного деяния.

К используемым техническим средствам относятся банкоматы, терминалы, компьютеры, планшеты, телефоны, платежные карты (финансовые инструменты), специальные устройства считывания и копирования информации с платежной карты, терминала или банкомата, другие технические средства и оконечные устройства.

Следами, позволяющими установить лицо, совершившее преступление, являются: сведения об IP-адресах, сведения о запросах к интернет-сайтам, следы подбора паролей, программы для удаленного администрирования, вредоносные программы, сведения о загрузке и выгрузке файлов, переписка, звонки, геолокационные данные мобильных устройств, информация из социальных сетей и др.

Проанализировав элементы, составляющие криминалистическую характеристику преступлений, совершенных в системе ДБО, мы можем сделать вывод о том, что в ходе расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий, наибольшей спецификой обладают электронные следы преступлений. Они представляют собой результаты создания, преобразования компьютерной информации в форме копирования, изменения, модификации, блокирования, уничтожения, непосредственно связанной с совершением преступления. Именно такие электронные следы подлежат тщательному всестороннему исследованию.

Предположим, что если со счета клиента банка были похищены денежные средства без ведома его владельца, то данное преступное деяние, согласно нормам ст. 158 УК РФ, можно квалифицировать, как **кражу**. Что же касается совершенного преступления в виде **мошенничества**, совершаемого в сфере компьютерной информации и телекоммуникационной сети, то в данном случае должны присутствовать: корыстная цель со стороны участника преступления или же соучастника, обман и злоупотребление доверием клиента, сопряженные с вводом, последующим удалением, блокированием, модификацией имеющейся и хранящейся в технических средствах информации. В этом случае такое противоправное деяние будет квалифицироваться как **мошенничество** по ст. 159.6 УК РФ.

Согласно нормам ст. 160 УК РФ **«Присвоение или растрата»** в действиях злоумышленника должно присутствовать противоправное безвозмездное обращение денежных средств в свою пользу или пользу других лиц с использованием дистанционного банковского обслуживания сотрудником (работником), которому доверено в силу его должностного или иного служебного положения иметь доступ к лицевому счету клиента.

В п. 12 Постановления № 51 Пленума Верховного Суда Российской Федерации от 2008 года дается разъяснение, что основываясь на положения ст. 140 ГК Российской Федерации, мошенничество считается оконченным с того момента, когда лицо перечислило денежные средства на банковский счет виновного либо на счета других лиц.

Ст. 160 УК РФ. Растрата и присвоение.

Присвоение и растрата – два вида противоправных деяний, имеющих один и тот же объединяющий признак: **похищение материальных ценностей**, которые обвиняемый или подозреваемый получил во временное распоряжение.

Обращение преступником материальных ценностей, принадлежащих иному лицу или государству, в личную собственность квалифицируется как присвоение. Лицо, владеющее ими, передает материальные ценности преступнику не навсегда, а во временное пользование. Это выражается в отсутствии действий по их отчуждению.

Растрату и присвоение денежных средств возможно рассматривать применимо и к сфере дистанционного банковского облуживания. По мнению авторского коллектива, преступления в сфере дистанционного банковского облуживания подразумевают хищение денежных средств с банковских счетов клиентов сотрудниками банков, которые в силу своих должностных обязанностей имеют возможность доступа к денежным средствам клиентов, последующего присвоения и их растраты.

Преступное деяние, совершаемое в личных целях, квалифицируется как растрата. Ее сутью является передача чужих материальных ценностей в расходование, пользование или потребление иным лицам с нарушением действующих правовых норм. Материальные ценности, а именно денежные средства в данном случае вверяются лицу, совершившему противоправное деяние в соответствии с договором на оказание банковских услуг.

Присвоение и растрата в сфере дистанционного банковского облуживания может совершаться только в виде незаконных действий, направленных на хищение денежных средств в виртуальном пространстве.

Основополагающим признаком растраты и присвоения считается то, что собственник денежных средств не давал своего согласия на их отчуждение.

Для данного вида преступных деяний предусмотрен специальный субъект – дееспособное, 18-летнее лицо, сотрудник (работник) банка, имеющий в силу своих должностных полномочий доступ к лицевому счету клиента банка.

Если в присвоении и растрате участвовало несколько человек, их следует считать **пособниками, подстрекателями или организаторами**.

В ходе судебного разбирательства должно быть установлено, что лицо, совершившее противоправные деяния, имело корысть и умысел. Основным признаком корысти является желание преступника использовать чужие имущественные ценности в личных интересах.

Считаем необходимым рассмотреть о**сновные различия между растратой и присвоением.** Эти два вида квалифицируются по одной статье Уголовного кодекса Российской Федерации, но имеют **ряд различий**.

Под присвоением принято понимать противоправный переход права собственности к лицу, ранее не являющегося его собственником. Ценность

похищенного не уменьшается и его без ущерба можно возвратить законному собственнику.

При растрате нередки случаи, когда возврат похищенного невозможен. Поэтому у лица, совершившего растрату, возникает ответственность по возмещению нанесенного ущерба.

Присвоение считается завершенным, когда **начались действия по переходу права собственности к лицу, совершающему это противоправное деяние**. Завершением растраты считается момент, когда произошло **отчуждение ценностей,** вверенных лицу, совершающему противоправное деяние.

Нормы ст. 160 УК РФ имеют отличия от иных статей Уголовного кодекса, сходных ей по составу.

Схожими по составу с этой статьей, в **Уголовном кодексе Российской Федерации** являются ст. 158 «Кража» и ст. 159 «Мошенничество». Однако для правильной квалификации именно растраты или присвоения необходимо знать основные признаки схожих между собой преступлений.

Основным признаком, характеризующим кражу, является тайность осуществляемого деяния, которое совершается без очевидцев или в том случае, когда вор уверен в этом. **Основным отличием** кражи от растраты или присвоения является то, что преступник до совершения преступления **не владел похищенными ценностями**.

Основным признаком мошенничества является перевод материальных ценностей, принадлежащих жертве, в пользу иного лица **при помощи психологического воздействия на нее.**

Если при растрате или присвоении собственник материальных ценностей на добровольной основе передает их на хранение или в пользование, то при мошенничестве или краже этот признак отсутствует.

Квалифицирующие признаки присвоения и растраты сформулированы в чч. 2, 3 и 4 ст. 160 УК РФ. Квалифицированным видом вышеупомянутых преступных деяний является осуществление присвоения или растраты группой лиц по предварительному сговору (**ч. 2 ст. 160 УК РФ**). Категория **«группа лиц по предварительному сговору»** определяется в ч. 2 ст. 35 УК РФ. Сравнительный анализ ч. 2 и ч. 1 ст. 135 УК РФ позволяет сформулировать вывод о том, что этот признак предполагает существование двух или более соучастников, которые заранее договорились о реализации преступного деяния, установленного ч. 2 ст. 160 УК РФ. Ввиду того, что группа лиц по предварительному сговору признается отдельной формой соучастия, осуществление хищения только одним гражданином при участии иных граждан, не соответствующих критериям субъекта преступления, не повлечет за собой возникновение рассматриваемого квалифицирующего признака ст. 160 УК РФ.

Присвоение или растрата, совершенные **с причинением значительного ущерба гражданину**, установлены в ч. 2 ст. 160 УК РФ. Согласно ч. 2 ст. 19 Конституции Российской Федерации в России гарантируется соблюдение принципа равенства прав и свобод человека и гражданина, причем независи-

мо от того, какое имущественное положение занимает конкретный гражданин, в связи с чем при определении значительности ущерба стоит опираться на фактическую сумму присвоенных или растраченных средств со счета клиента банка.

Присвоение или растрата, реализованные гражданином с использованием своего служебного положения, раскрываются в ч. 3 ст. 160 УК РФ.

Следует отметить, что в случае присвоения и растраты, совершенных посредством дистанционного банковского обслуживания, под данным лицом подразумевается сотрудник банка, имеющий доступ к персональным данным и счетам клиентов банка. Может быть ситуация, при которой денежные средства на счетах предоставляются не непосредственно виновному гражданину, а другим гражданам. При этом ввиду занимаемого должностного положения гражданин обладает компетенцией по управлению и распоряжению через других граждан. Данные компетенции применяются виновным гражданином вопреки интересам службы для неправомерного завладения денежных средств или передачи их с корыстной целью другим гражданам. Безусловно, служебное положение преступника характеризуется тем видом деятельности и набором компетенций, которые им реализуются. Соответственно, гражданин, реализующий служебную деятельность, бесспорно, занимает конкретное служебное положение. Значит, такое положение может им применяться при реализации преступного деяния, установленного ч. 3 ст. 160 УК РФ. Стоит отметить, что в правоприменительной практике реализация служебной деятельности трактуется как действия гражданина, включенные в перечень его профессиональных обязанностей, установленных конкретным трудовым договором или служебным контрактом, заключенным с организацией, государственным или муниципальным учреждением, а также предпринимателями, осуществление деятельности которых согласуется с действующими законодательными требованиями. **Крупным размером присвоения или растраты** (ч. 3 ст. 160 УК РФ) признается стоимость имущества, превышающая 250 тыс. руб. Данное положение указано в примечании 4 к ст. 158 УК РФ. Присвоение или растрата, реализованные организованной группой, раскрывается в ч. 4 ст. 160 УК РФ. **Главной особенностью**, позволяющей отграничивать организованную группу от группы лиц по предварительному сговору, следует считать **устойчивый характер**. Высокий уровень опасности преступного деяния, реализованного организованной группой, характеризуется и иными факторами. Однако данные признаки не имеют свойства перманентности, или их невозможно формализовать. В случае признания хищений реализованными организованной группой поведение всех соучастников должно быть квалифицировано как соисполнительство без указания ст. 33 УК РФ. При этом личный вклад в совершение преступного деяния, установленного ст. 160 УК РФ, никакого юридического значения не имеет. В правоприменительной деятельности судебные органы, как правило, констатируют устойчивый характер группы в том случае, если доказана продолжительность реализации противоправной деятельности. Руководители организованных групп привлекаются к уго-

ловной ответственности за все реализованные такой группой преступные деяния, установленные ст. 160 УК РФ, если они охватывались их умыслом. Особо крупным размером присвоения или растраты (ч. 4 ст. 160 УК РФ) признается стоимость имущества, превышающая 1 млн. руб. Это следует из содержания примечания 4 к ст. 158 УК РФ.

Для того, чтобы определить **криминалистическую характеристику** данного преступления необходимо верно определить его вид и группу. Присвоение и растрата является преступлением в сфере экономики и направлено против собственности, совершается дистанционно с использованием вверенных личных данных клиента банка. **Механизм** данного преступления заключается в безвозмездном обращении денежных средств в свою пользу или в пользу других лиц с использованием дистанционного банковского облуживания. Личность преступника соответствует вышеупомянутому специальному субъекту. **Предметом доказывания** в случае присвоения и растраты посредством дистанционного банковского обслуживания будет:

наличие информации о проделанном виртуальном пути похищенных денежных средств со счета клиента банка на счет преступника;

данные, подтверждающие проведение определенных банковских операций конкретным виновным лицом.

Необходимым условием для начала уголовного преследования по ст. 160 УК РФ «Присвоение и растрата» необходимо наличие следующих факторов:

объект преступных деяний;

имущественные ценности;

мотив;

умысел;

состав преступных деяний в виде материальных ценностей.

При отсутствии любого из перечисленных признаков начать уголовное преследование по ст.160 УК РФ невозможно.

Квалификация тяжести преступления производится на основании установления стоимости растраченных или присвоенных материальных ценностей. Для этого при необходимости назначается дополнительная экспертиза. При определении статьи, по которой квалифицируются эти преступные деяния, судом учитывается состояние жертвы и значимость материальных ценностей для нее, таких как источники дохода и стоимость присвоенных или растраченных ценностей; наличие несовершеннолетних детей, родителей пожилого возраста и иных иждивенцев; общий размер получаемых всеми членами семьи доходов; мнение жертвы о значимости нанесенного ущерба.

Согласно Постановлению Пленума Верховного Суда Российской Федерации от 30.11.2017 года № 48 «О судебной практике по делам о мошенничестве присвоении и растрате» указано, что такие преступные деяния, как растрата и присвоение относятся к категории преступлений, имеющих экономический характер. Конечной целью таких преступных деяний является присво-

ение и использование чужих материальных ценностей для получения личной выгоды.

Правовые нормы действующего Уголовного Кодекса Российской Федерации за растрату или присвоение указывают, что, исходя из ситуации, могут назначаться как штрафы соответствующего размера, так и принудительная изоляция на различные сроки.

Подводя итог проведенной уголовно-правовой и криминалистической характеристики ст.ст. 158, 159.4 и 160 УК РФ в сфере дистанционного банковского обслуживания можно сделать вывод о том, что данный вид преступлений является последствием развития банковских технологий. Реализация информационных, документационных, компьютерных технологических инноваций обеспечивает оптимизацию рабочего процесса в сфере обслуживания клиентов банками. Однако такие возможности могут являться благоприятным условием для совершения противоправных деяний в отношении граждан, предоставляющих банкам свои персональные данные и денежные средства на хранение.

В связи с вышеизложенным сотрудникам правоохранительных органов требуется постоянное повышение профессиональной квалификации в области современных технологий банковского обслуживания, в том числе и международного уровня. Кроме того необходимо разработать методику своевременного предупреждения, выявления, раскрытия и расследования данного вида преступлений и внедрить их в практическую деятельность сотрудников органов внутренних дел.

Анализируя практический опыт раскрытия преступлений в системе дистанционного банковского обслуживания сотрудников органов внутренних дел, необходимо отметить, что одним из основных элементов криминалистической характеристики преступлений является способ совершения преступления.

3.2. НЕКОТОРЫЕ СПОСОБЫ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ В СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Предлагаем рассмотреть некоторые способы преступлений, совершаемых в системе ДБО[1]:

- *использование вредоносных программ скрытого управления;*
- *использование программ считывания пароля;*
- *применение программ удаленного доступа;*
- *создание «зеркального сайта»*;
- *перечисление денежных средств преступниками на «электронные кошельки»;*
- *ложная информация «проблема у родственника»;*
- *получение звонков, SMS– сообщений «Ваша карта заблокирована»;*

[1] Данный перечень не является исчерпывающим, так как возможно появление новых способов хищений денежных средств, а также в какой-то части измененных.

- размещение объявления на сайте «Авито» и иных ресурсах сети Интернет;

- «Мобильный банк»;

- заражение вредоносным программным обеспечением телефонных аппаратов и других технических устройств на операционной системе «Android».

Использование вредоносных программ скрытого управления

В данном случае преступниками используется вредоносная программа, которая проникает и устанавливается в мобильный телефон потерпевшего. Далее она *самостоятельно* (без непосредственных команд преступников) рассылает с него SMS-сообщения, управляя его банковским счетом через услугу «Мобильный банк».

Данная программа проникает и устанавливается на телефон при открытии в сети Интернет страниц различных сайтов, адреса которых потерпевшие чаще всего получают в SMS или MMS-сообщениях. Кроме того, потерпевшие сами неосознанно могут устанавливать на мобильные устройства вредоносные программы, замаскированные под игры и другие программные продукты.

Одним из признаков (необязательным) наличия вредоносной программы на мобильном телефоне является направление «пустых» SMS или MMS-сообщений на телефоны, имеющиеся в контактах устройства. При открытии адресатом такого SMS или MMS происходит дальнейшее заражение вирусом телефонов, получивших данное сообщение.

Возможно получение потерпевшим в виде SMS с номера 900 или других сервисных номеров различной информации, которую он не запрашивал. Это связано с тем, что направление информации с сервисных номеров вызвано действиями вредоносных программ.

Одним из способов первичного средства выявления вредоносных программ на телефоне является использование антивирусных программ, получение детализации телефонных звонков и SMS. При наличии вредоносной программы в разделе детализации «исходящие SMS» будут сообщения, которые владелец телефона не направлял на сервисный номер 900 либо номера, используемые преступниками для списания средств потерпевшего через поступившие SMS.

Пример 1. *Сотрудниками Управления «К» в рамках оперативного сопровождения уголовного дела, возбужденного СЧ ГУ МВД России по СКФО по ч. 2 ст. 273 УК РФ, установлены и задержаны участники организованной преступной группы, действовавшей под руководством жителя г. Владикавказа, который разработал уникальное вредоносное программное обеспечение для хищения конфиденциальной информации и скрытой генерации криптовалюты на «зараженных» технических устройствах.*

Следственные действия в отношении участников группы по множеству фактов противоправной деятельности производились одновременно на территории 9 субъектов Российской Федерации.

Данный пример красноречиво говорит о причиненном вреде клиентам банков в особо крупном размере и его территориальной масштабности.

Пример 2. *В результате сопровождения уголовного дела, возбужденного по ч. 4 ст. 159 УК РФ, сотрудниками Управления «К» на территории г. Москвы установлен и задержан злоумышленник, которым разработано уникальное программное обеспечение, позволяющее эксплуатировать уязвимости терминалов системы «UPOS» и получать одобрение платежных операций без подтверждения банком. Указанной уязвимости на текущий момент времени оказалось подвержено более 1,7 млн. платежных терминалов ПАО «Сбербанк России».*

Пример 3. *В ходе раскрытия преступления было установлено, что мошенники расклеивали QR- коды на прокат автомобилей и велосипедов где не было продавцов. Клиент, ничего не подозревая, сканировал QR-код, после чего оплачивал услуги по прокату. Но денежные средства поступали на прямую мошенникам на их лицевые счета, и клиент оставался без денежных средств и услуг проката (рис. 33).*

Рис. 33. Мошенничество с использованием QR – кода

Использование программ считывания пароля

В этом случае в индивидуальное электронное устройство потерпевшего проникает и устанавливается вредоносная программа, которая фиксирует вводимый пользователем логин и пароль в момент доступа к удаленному банковскому сервису (например, «Сбербанк Онлайн»). Преступники позже, используя этот логин и пароль, входят в личный кабинет пользователя с другого компьютера и совершают хищение.

Применение программ удаленного доступа

Преступниками используется программа, которая предварительно устанавливается на электронное устройство потерпевшего лица. Она позволяет в режиме реального времени отправлять на него команды управления через сеть Интернет (действие аналогично программе «Android» и др.). Отличие от способа, рассмотренного выше, заключается в непосредственном управлении преступниками перечислением похищаемых денежных средств путем удаленного направления команд мобильному устройству (данный способ встречается сравнительно реже иных).

Рассмотрим пример, взятый из практической деятельности БСТМ МВД России, носящий межрегиональный характер.

В ходе оперативного сопровождения уголовного дела, возбужденного СО СУ УМВД по ВАО ГУ МВД России по г. Москве по ч. 4 ст. 159.6 УК РФ, установлены и задержаны уроженцы Саратовской области и их соучастники, которые совершали хищения денежных средств посредством несанкционированного подключения к банкоматам различных кредитно-финансовых учреждений. Общий ущерб от противоправной деятельности фигурантов на территории более 15-ти субъектов Российской Федерации превысил 30 млн. рублей.

Благодаря отлаженным действиям Управления «К» БСТМ МВД России по организации межрегионального взаимодействия в ходе проведения оперативно-розыскных и иных необходимых мероприятий важную роль сыграло своевременное получение криминалистически оперативно значимой информации. Тактически грамотное планирование оперативного сопровождения уголовного дела способствовало своевременному обнаружению и анализу информации обо всех совершенных преступлениях рассматриваемого вида и установлению лиц, причастных к ним.

Создание «зеркального» сайта

Данный способ возможен, когда потерпевший пользуется «личным кабинетом» на сайте банка. Преступниками создается и используется фейковый (поддельный) сайт, адрес которого и внешнее оформление страниц трудноотличимы от официального сайта банка, интернет-магазинов, страницы в социальных сетях. Если потерпевший при входе на сайт банка не использует сохраненную ссылку, а просто набирает название банка в поисковой системе, то ему обычно предлагается несколько вариантов. Если потерпевшим будет осуществлен вход на «зеркальный» сайт, то вводимыми данными для входа в кабинет банка (логин и пароль) могут воспользоваться злоумышленники и войти на настоящем сайте от имени потерпевшего в его личный кабинет. Далее возможен перевод денег со счета потерпевшего из личного кабинета или подключение к его счету услуги «мобильный банк» на любом абонентском номере.

Основным признаком посещения клиентом «зеркального» сайта банка является то, что после ввода логина и пароля на странице пользователя появляется надпись о техническом обслуживании сайта или любая иная информация. В данном случае **информационное SMS-сообщение** от банка о входе в

личный кабинет **может отсутствовать** или поступит информация, в которой будет указано: **«Обратиться на сайт позднее»**. Данное обстоятельство создает благоприятные условия и временной период злоумышленнику для хищения денежных средств со счета лица, которое само предоставило все сведения о наличии денежных средств.

Одним из главных признаков преступлений в сфере информационных технологий является то, что совершать преступления могут лица вне зависимости от возраста и полученного образования.

Преступления в сфере компьютерной информации совершаются **преимущественно молодыми людьми**, ранее не привлекавшимися к уголовной ответственности. Наибольшую криминальную активность проявляют лица от 14 до 35 лет. Значительная их часть имеет специальное образование, связанное со сферой компьютерных технологий, но встречаются и те, кто получил знания и навыки, способствующие совершению преступлений, самостоятельно.

Их положение в обществе может варьироваться от школьника и студента до ответственного сотрудника учреждения, компании (фирмы). Вместе с тем данный вид преступлений могут совершать и высококвалифицированные специалисты, владеющие полной информацией и способные создавать вредоносные программы и знать их принцип работы.

Отдельные члены преступной группы в некоторых случаях могут проживать в различных регионах и до момента задержания и доставления в органы внутренних дел лично не встречаться с другими соучастниками. Для знакомства и координации своих действий они используют сайты и специальные сетевые ресурсы, где обсуждают способы совершения преступлений и маскировки следов.

Перечисление денежных средств преступниками на «электронные кошельки»

Преступники при совершении преступлений в сфере информационных технологий часто используют «электронные кошельки» платежных систем Yota, RBK-money, Yandex-деньги и подобные им. Предпочтение злоумышленников использованию «электронных кошельков» объясняется тем, что последние выполняют функции банковского счета, не требуя ни указания персональных данных его владельца (как правило, указываются вымышленные данные), ни его непосредственной идентификации при проведении финансовых операций. Зарегистрировать «электронный кошелек» можно через сеть Интернет, при этом указав вымышленное имя, либо вообще вместо имени ввести случайное сочетание букв и цифр. Преступниками «электронные кошельки» в основном используются как «промежуточное звено» в цепи перемещения похищенных денежных средств. После поступления на используемые злоумышленниками «электронные кошельки» денежные средства далее переводятся на другие «электронные кошельки», счета номеров сотовой связи или банковские счета.

Для выявления лиц, совершивших хищения, сотрудникам органов внутренних дел в этом случае необходимо устанавливать «IP-адреса» технических

устройств, с которых регистрировался «электронный кошелёк» и осуществлялся выход в сеть при совершении платежной операции, а также **отслеживать путь** перечисления денежных средств с «электронного кошелька» (на какие другие «электронные кошельки» или счета) **путем запроса в администрацию электронной платежной системы.** При этом целесообразно ставить вопрос не только о счетах, на которые перечислялись средства, но и об иных счетах, с которых совершалось перечисление на выявленный «электронный кошелек» (для установления других потерпевших и «электронных кошельков», используемых преступниками).

Ложная информация «проблема у родственника»

Преступник осуществляет звонок на телефон (мобильный, стационарный) потерпевшего и сообщает о том, что у его родственника (знакомого) возникла проблема (попал в ДТП, совершил преступление, иное) и предлагает ему разрешить эту проблему, но при этом необходимо заплатить определенную денежную сумму. Потерпевший соглашается и ждет человека, которому необходимо передать деньги.

Преступник звонит в такси и через оператора узнает номер таксиста. Таксисту преступник сообщает, что ему необходимо подъехать к условленному адресу, где ему передадут деньги. Прибыв по указанному адресу, таксист получает определенную денежную сумму и информирует об этом преступника.

Злоумышленник сообщает таксисту номера телефонов, на которые необходимо перевести денежные средства, полученные от потерпевшего. С помощью банкомата (терминала) таксист осуществляет перевод денежных средств на номера телефонов, указанные ему преступником (телефонных номеров может быть несколько).

При поступлении денежных средств на различные номера телефонов осуществляется их перевод на единый расчетный счет банка (пластиковой карты). Соучастник преступления, осуществивший снятие денежных средств с расчетного счета, используя банкомат (терминал или интернет), переводит денежные средства преступнику.

Для данной схемы часто случается упрощенная вариация, при которой исключаются действия с таксистом, при этом платежные операции производятся потерпевшим самостоятельно (схема аналогична случаю с сообщениями о блокировке банковских карт):

- преступник осуществляет звонок на телефон (мобильный, стационарный) потерпевшего и сообщает о том, что у его родственника (знакомого) возникла проблема (попал в ДТП, совершил преступление, иное) и предлагает ему разрешить данную проблему, но при этом необходимо заплатить определенную денежную сумму. Потерпевший соглашается, и преступник указывает ему номера телефонов, банковских карт и т.п., на которые необходимо зачислить денежную сумму;

- потерпевший с помощью банкомата (терминала) осуществляет перевод денежных средств на номера телефонов, указанные ему преступником. При этом возможно будет указано несколько телефонных номеров.

При поступлении денежных средств на различные номера телефонов, осуществляется их перевод на указанный расчетный счет банка (пластиковой карты). Далее соучастник преступления, осуществивший снятие денежных средств с расчетного счета, используя банкомат (терминал или интернет) переводит денежные средства преступнику (рис. 34).

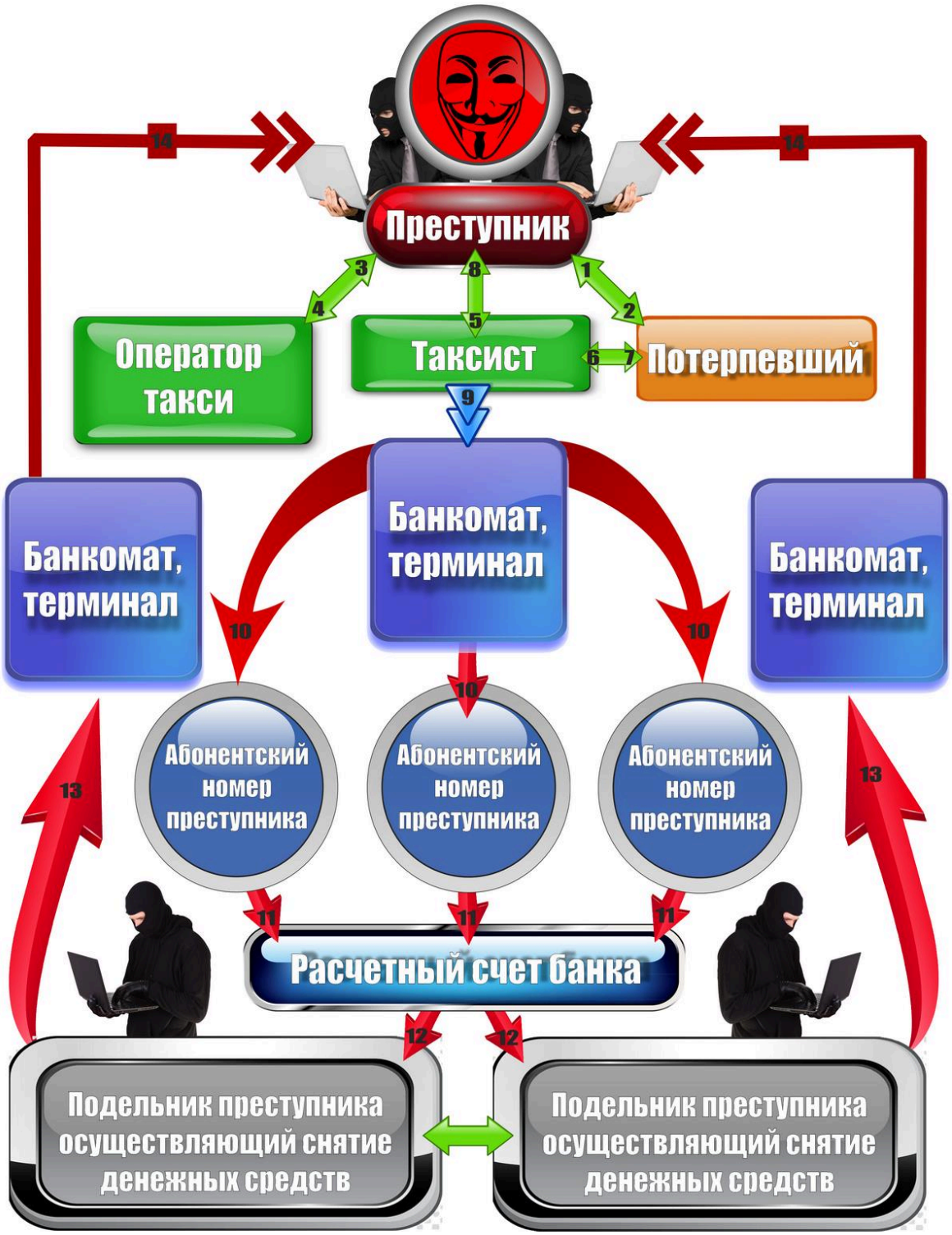


Рис. 34. Общая схема преступной деятельности «проблема у родственника»

Рис. 35. Пример успешного взаимодействия

Предлагаем рассмотреть следующий пример.

Мошенники приобретали базы данных с персональными сведениями граждан Московского региона и осуществляли звонки на сотовые и стационарные телефоны жителей Московского региона, представляясь сотрудниками службы социального обеспечения (Собес) и предлагали получить компенсацию за неиспользованные путевки в г. Геленджике.

Благодаря тесному взаимодействию службы кибербезопасности ПАО «Сбербанк» и сотрудников органов внутренних дел Российской Федерации все члены организованной преступной группы были изобличены и понесли соответствующие наказания (см. рис. 35).

В случаях совершения хищений денежных средств со счетов клиентов банков и получения информации о подготавливаемом или совершенном преступлении необходимо применять предлагаемый алгоритм действий:

1. Подробно опросить потерпевшего об обстоятельствах происшествия. С целью установления абонентского номера злоумышленника необходимо от потерпевшего получить заявление на предоставление сведений о соединениях в момент совершения преступления.

2. Прибыть на место происшествия, где потерпевший передавал денежные средства. Определить границы осмотра, произвести качественный осмотр места происшествия с привлечением эксперта (специалиста) для своевременного обнаружения и последующего изъятия возможных характерных следов данного вида преступления с целью дальнейшей идентификации лица, получившего от потерпевшего деньги.

3. Установить очевидцев и свидетелей. С этой целью произвести поквартирный (подомовой) опрос граждан для получения информации о лице, которому были переданы денежные средства, и наличии автотранспорта. Составить словесный (композиционный) портрет подозреваемого лица.

4. Установить наличие видеокамер (видеодомофонов), видеорегистраторов, фиксирующих различного рода действия в зоне совершения преступления.

5. Осуществить выборку автомобилей по полученной информации о части буквенной или цифровой серии госномерного знака автотранспортного средства, на котором передвигался злоумышленник (подозреваемое лицо), и проверить их собственников на осуществление ими частного извоза в составе таксомоторной компании.

6. Направить запросы в таксомоторные компании о выезде таксистов, работающих у них в компании, на адрес, где осуществлялась передача денежных средств;

8. При определении госномерных знаков, принадлежащих автомобилю, установить лицо, которому потерпевший передал денежные средства. При установлении лица, которому потерпевший передал денежные средства (водитель такси), опросить его. В ходе опроса необходимо установить следующее:

- кому и каким способом передавались денежные средства, полученные от потерпевшего;
- каким способом осуществлялась связь с лицом, которое сообщило ему, куда и как перевести денежные средства, полученные от потерпевшего;
- подробное описание голоса лица, звонившего таксисту;
- установить номер телефона, с которого звонили таксисту;

- истребовать с таксиста и таксомоторной компании, в которой он работает, детализацию по используемому абонентскому номеру (входящие и исходящие соединения) за период поступления звонка преступника для последующего анализа;

9. В случае если таксист, по указанию злоумышленника, перевел денежные средства через терминал (банкомат) на абонентские номера, то необходимо установить номера, на которые были переведены денежные средства потерпевшего, и местонахождение терминала (банкомата);

10. Опросить оператора такси;

11. После проведения необходимых оперативно-розыскных мероприятий по выявлению обстоятельств и лиц, причастных к совершению преступления, принять неотложные меры для решения вопроса о возбуждении уголовного дела;

12. Направить запросы (судебные решения) операторам сотовой связи с целью установления:

- владельцев абонентских номеров, использованных для совершения преступления, и их местоположения в момент совершения преступления;

- IMEI телефонов, с которых звонил преступник;

- детализации с указанием информации об абонентах;

- движения денежных средств по счетам абонентских номеров, на которые были зачислены денежные средства потерпевшего, и абонентских номеров, с которых звонил преступник;

13. При получении ответов от операторов сотовых компаний необходимо осуществить анализ данной информации:

- установить наличие учреждения ФСИН России, находящегося рядом с местом указанном в географическом положении абонентского номера, с которого звонил преступник в момент совершения преступления;

- проанализировать детализацию с целью установления лица, совершившего преступление;

- установить номер счета, на который были перечислены денежные средства, и установить дальнейшее движение денежных средств с этого номера. Если деньги обналичивались, то установить место (банкомат, отделение связи, интернет-ресурсы), где была совершена данная денежная операция, и осуществить направление необходимых запросов в организации, осуществляющие денежные переводы для установления лица, осуществившего снятие денежных средств;

- при определении места расположения исправительного учреждения, откуда был осуществлен звонок, направить запрос с целью обнаружения и последующего изъятия сотрудниками ФСИН России телефонных аппаратов с указанными идентификационными номерами и SIM-карт.

14. Сотрудники, ответственные за формирование информационно-поисковой системы (ИПС), осуществляют ввод информации в базу данных и ее корректировку при получении новых сведений.

Получение звонков, SMS– сообщений «Ваша карта заблокирована»

Преступник осуществляет звонок на телефон (мобильный, стационарный) потерпевшего или отправляет ему SMS-сообщение о том, что «Ваша карта заблокирована» (или об иной проблеме со счетом, пластиковой картой). В процессе беседы злоумышленник предлагает потерпевшему для решения внезапно возникшей неблагоприятной ситуации осуществить в кратчайший срок ряд операций через ближайший банкомат. По прибытию к банкомату потерпевшее лицо созванивается с преступником и выполняет все его указания.

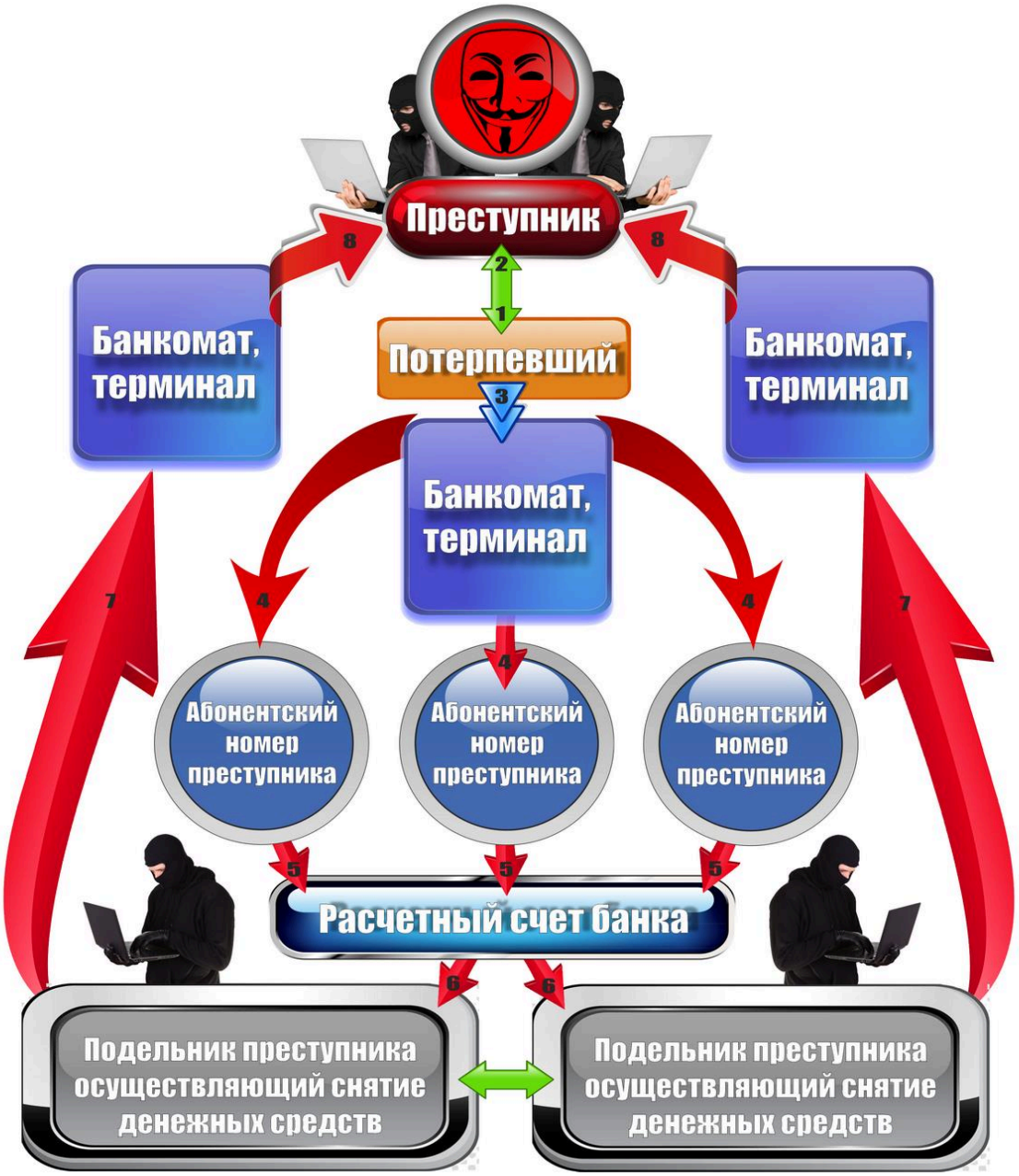


Рис. 36. Общая схема преступной деятельности «Ваша карта заблокирована»

Преступник сообщает потерпевшему набор цифр для устранения проблем с картой (счетом). При поступлении денежных средств на различные

номера телефонов осуществляется их перевод на единый расчетный счет банка (пластиковой карты).

Сообщник преступления, осуществивший снятие денежных средств с расчетного счета, используя банкомат (терминал или интернет), осуществляет перевод денежных средств преступнику (см. рис. 36).

В случаях осуществления преступной деятельности «Ваша карта заблокирована» необходимо применять следующий алгоритм действий:

1. Опросить потерпевшего и очевидцев.

2. Истребовать распечатку детализации соединений потерпевшего.

3. Установить, на какие номера (расчетные счета) потерпевший перевел денежные средства.

4. В случае если денежные средства были переведены на телефонные номера, необходимо направить запросы (судебные решения) операторам сотовой связи с целью установления:

- владельцев сим-карт;

- IMEI используемых злоумышленниками телефонов;

- географического местоположения, детализации с указанием информации об абонентах;

- движения денежных средств по счетам абонентских номеров, на которые было осуществлено зачисление денежных средств потерпевшего и по абонентскому номеру, с которого звонил злоумышленник.

5. В случае если денежные средства были переведены на расчетные счета банковских карт, другие банковские счета, необходимо направить запрос в банк, в котором обслуживается клиент-потерпевший, с целью получения информации о расчетных счетах, использованных злоумышленником.

7. Принять решение о возбуждении уголовного дела.

8. Сотрудники, ответственные за формированием ИПС, осуществляют ввод информации в банк данных и ее корректировку при получении новых сведений.

9. В рамках возбужденного уголовного дела необходимо:

- проанализировать детализацию с целью установления лица, совершившего преступление;

- установить номер счета (абонентский номер), на который были перечислены денежные средства, и определить дальнейшее направление денежных средств с этого номера. В случае, если деньги обналичивались, то установить место (банкомат, отделение связи, интернет-ресурсы), где была совершена данная денежная операция, и направить необходимые запросы в организации, осуществляющие денежные переводы, для установления лица, снимавшего денежные средства;

- провести иные необходимые оперативные мероприятия и следственные действия, направленные на выяснение всех обстоятельств, причинно-

связанных с расследованием преступления, а также на установление лиц, причастных к совершению преступления.

Действия в ситуациях, когда предлогом мошенничества является выигрыш приза потерпевшим, оказание медицинских услуг и т.п., аналогичны вышеизложенным.

Размещение объявления на сайте «Авито» и иных ресурсах сети Интернет (потерпевший/преступник)

В среднем каждый день на сайте «Avito.ru» размещается около 2500 объявлений.

В целях профилактики совершения мошенничеств с использованием Интернет-ресурса «Avito.ru» сотрудниками отдела «К» ежедневно обзванивается в среднем 100 человек, что составляет 0,02% от общего числа объявлений и 2% – от поданных в текущий день.

Для повышения эффективности принимаемых мер и снижения числа мошенничеств, совершаемых в отношении пользователей сайта «Avito.ru», целесообразно привлекать к профилактической работе сотрудников следственно-оперативных групп территориальных органов внутренних дел.

Предлагаем рассмотреть пример, взятый из практической деятельности.

В отдел УМВД России по Кузнецкому району Пензенской области обратились граждане с заявлением о мошенничестве. Сотрудниками уголовного розыска отдела УМВД России по Кузнецкому району совместно с сотрудниками Управления «К» было выяснено, что потерпевший разместил на сайте «Avito.ru» объявление о продаже крупного рогатого скота. Злоумышленник воспользовался этим объявлением, чтобы создать свое «зеркальное» объявление на этом же сайте с указанием своего номера телефона.

Покупатели увидели «зеркальное» объявление и совершили звонок мошеннику. Мошенник позвонил настоящему продавцу и в процессе разговора, представившись потенциальным покупателем, выяснил необходимые подробности такие, как место нахождения товара, его окрас, вес, породу и размер, а также, где и когда можно посмотреть животных. Позже злоумышленник перезвонил настоящим покупателям и рассказал подробности про животный товар и его место расположения. Далее мошенник в разговоре сделал акцент на возможную скидку, если покупатели ускорят приобретение крупного рогатого скота. Покупатели были заинтересованы в покупке животных и намеревались приехать по обозначенному месту нахождения товара. Мошенник предупредил покупателей, что в момент просмотра животных он будет отсутствовать на ферме. Их встретит его управляющий. При этом мошенник объяснил покупателям, что договариваться о стоимости с управляющим не нужно. В свою очередь, преступник настоящего продавца скота поставил в известность, что во время осмотра товара он будет находиться в Москве по причине своей занятости, и поэтому не сможет присутствовать на встрече. К продавцу приедут работники «реального покупателя», и разговоры о стоимости животных с ними вести нет необходимости.

Согласно намеченному договору было проведено знакомство с товаром. Стороны договорились о конкретном времени предстоящей сделки купли-продажи. Мошенник, предвидя конечный результат, заранее подготовил настоящего продавца и настоящих покупателей о том, что им необходимо осуществить денежный перевод на указанный номер банковской карты.

В назначенное время настоящие покупатели совместно с настоящим продавцом отправились в ближайшее отделение «Сбербанка» и осуществили перевод денежных средств мошеннику на номер его банковской карты в размере 235 тыс. рублей.

После того, как транзакция состоялась, абонентский номер мошенника был выключен. Сотрудниками уголовного розыска отдела УМВД России по Кузнецкому району Пензенской области совместно с сотрудниками Управления «К» было установлено, что абонентский номер мошенника оформлен на гражданина ближнего зарубежья. Банковская карта, на номер которой осуществлялся перевод денежных средств, не имеет привязки к данным конкретного лица.

В настоящее время проводятся оперативно-розыскные мероприятия по установлению преступника.

Размещение объявления на сайте «Авито» и иных ресурсах сети Интернет (объявление разместил преступник)

Преступник размещает на сайте электронных объявлений («Авито» или иных сайтов) информацию о продаже каких-либо товаров, для связи указывает телефон. Потерпевший обнаруживает объявление и, решив приобрести заявленные в нем товары, созванивается с преступником по указанному в объявлении абонентскому номеру сотовой связи. Преступник сообщает лицу, что товар имеется в наличии, и злоумышленник готов его продать по низкой цене. В данном случае под разными предлогами преступник всегда отказывается показать товар, при этом сообщает, что интересующий товар находится в другом городе (субъекте Российской Федерации). Злоумышленник предлагает будущей жертве внести предоплату. Преступник и потерпевший еще некоторое время ведут телефонные переговоры, в ходе которых оговариваются цена товара, способ оплаты и сроки поставки.

Потерпевший перечисляет денежные средства на указанный злоумышленником банковский счет (карту, электронный кошелек, абонентский номер). После осуществления всех намеченных операций преступник собирает денежные средства с промежуточных платежных средств на какой-либо банковский счет, карту и т.п. и затем обналичивает собранные денежные средства либо сам, либо через своих сообщников.

Размещение объявления на сайте «Авито» и иных ресурсах сети Интернет (объявление разместил потерпевший)

Потерпевший размещает на сайте электронных объявлений («Авито» или иных сайтов) информацию о продаже каких-либо товаров и для связи указывает номер телефона. Преступник обнаруживает объявление и созвани-

вается с потерпевшим по указанному в объявлении абонентскому номеру сотовой связи, сообщает, что он готов приобрести товар, но в настоящее время находится в другом регионе и предлагает внести предоплату.

Потерпевший в ходе телефонного разговора сообщает преступнику реквизиты банковской карты (полный номер карты, срок действия и имя держателя, указанные на лицевой стороне), а также одноразовый пароль, подтверждающий операции по перечислению денежных средств со счета банковской карты, поступивший ему в SMS-сообщении с сервисного номера «900».

Путем перевыпуска сим-карты настоящего владельца преступник посредством услуги дистанционного банковского обслуживания «Сбербанк – онлайн» получает доступ ко всем счетам, открытым на имя потерпевшего и осуществляет списание с них денежных средств на используемые карты, счета. Далее преступник либо его сообщники обналичивают собранные денежные средства.

В случаях осуществления преступной деятельности путем размещения объявлений на сайте «Авито» и иных ресурсах сети Интернет необходимо применять следующий алгоритм действий:

1. Принять от потерпевшего подробное объяснение, в котором необходимо отразить:

- дату и время обнаружения объявления, по возможности найти само объявление в сети Интернет и зафиксировать его номер, сделать снимок экрана либо попросить потерпевшего предоставить указанные сведения;

- если объявление уже отсутствует, то как можно более подробно описать его (текст, средства связи с продавцом, цена товара, дата размещения объявления);

- способы связи потерпевшего с преступником, порядок взаимодействия (связь по телефону), отразить номера телефонов;

- дату и время звонков, период разговоров;

- способ перечисления преступнику денежных средств, реквизиты банковского счета, карты; название платежной системы (КИВИ, Яндекс.Деньги и т.п.); дату и время перевода денежных средств.

2. Направить оператору электронных объявлений («Авито» или иных сайтов) запрос с целью установления:

- даты и времени размещения объявления;

- контактных данных, указанных и использованных автором объявления;

- IP-адресов, даты и времени доступа автора объявления к сайту при размещении объявления и иных сеансах доступа.

3. Если потерпевший общался с преступником по телефону, истребовать у него детализацию звонков за данный период, в которой должен быть отражен номер телефона преступника.

4. Провести ОРМ – «наведение справок» по абонентским номерам, на которые осуществлен перевод денежных средств. При необходимости в целях установления региона, к емкости которого относятся абонентские номера, а

также персональных данных владельца можно использовать возможности справочных программ в сети Интернет.

5. Принять решение о возбуждении уголовного дела.

6. После того, как потерпевший укажет номер счета (оператора связи, платежную систему), на который им осуществлялись перечисления денежных средств, направить запрос в банк с целью установления:

- сведений о владельце банковской карты, счета (клиента электронной платежной системы, оператора связи);
- сведений о дальнейшем движении поступивших средств до момента обналичивания либо вывода их из системы;
- IP-адресов, даты и времени доступа пользователя к системе (для электронных платежных систем).

7. При получении запрашиваемых сведений от операторов электронных объявлений, платежных систем, банков, операторов сотовой связи проанализировать поступившие сведения:

- установлено ли место обналичивания средств потерпевшего;
- установлен ли оператор связи, посредством которого размещено объявление в сети Интернет, велась ли электронная переписка;
- установлено ли географическое положение абонентских номеров, посредством которых преступник взаимодействовал с потерпевшим;

8. Сотрудники, ответственные за формирование информационно-поисковой системы, осуществляют ввод информации в базу данных и ее корректировку при получении новых сведений.

«Мобильный банк». «Двойной Мобильный банк»

Потерпевшим при заключении договора указывается абонентский номер, который и подключается к «мобильному банку». По различным причинам, многие владельцы пластиковых карт банков перестают в дальнейшем пользоваться абонентскими номерами (потерял, переехал, сменил оператора и т.д.), в связи с чем оператор сотовой связи через 6 месяцев перевыпускает SIM-карту с данным абонентским номером и выставляет ее на продажу. Также возможна утеря SIM-карты и неотключение ее «мобильного банка».

Новый абонент, приобретая данную SIM-карту, начинает получать SMS о движении денежных средств по счёту потерпевшего (бывшего владельца SIM-карты). Вследствие чего образуется «двойной мобильный банк». Все транзакции, проводимые бывшим владельцем SIM-карты, становятся известными как потерпевшему, так и новому владельцу. Кроме того новый владелец SIM-карты получает возможность управлять денежными средствами лицевого счета, к которому она подключена.

Заражение вредоносным программным обеспечением телефонных аппаратов и других технических устройств на операционной системе «Android»

Потерпевший получает SMS или MMS-сообщение от контент-провайдера либо от неизвестного посредством сети Интернет со ссылкой на

информационный ресурс, перейдя по которой, абонент закачивает на телефон вредоносное программное обеспечение (далее ВПО).

Потерпевший получает SMS-сообщение от своего «знакомого», телефон которого уже заражен ВПО, при этом ВПО само направляет данное сообщение на номера, которые имеются в адресной книге потерпевшего. В данном сообщении также находится ссылка на информационный ресурс, перейдя по которой, абонент закачивает на телефон ВПО.

Потерпевшее лицо, находясь в сети Интернет, с помощью телефона получает по электронной почте либо через социальные сети ICQ сообщение, в котором находится ссылка на информационный ресурс, перейдя по которой абонент закачивает на телефон ВПО.

Также потерпевшее лицо, находясь в сети Интернет, может с помощью телефона, скачивать, например, программные продукты, музыку, фотографии, в которых находится ссылка на конкретный информационный ресурс, перейдя по которой, абонент закачивает на телефон ВПО.

Рис.37. Общая схема преступной деятельности «хищения денежных средств с помощью мобильного вируса»

После заражения телефона «вирус» проверяет наличие подключенной услуги «Мобильный банк». Если услуга подключена, то вирус с помощью нее осуществляет перевод денежных средств с банковской карты потерпевшего на различные абонентские телефонные номера, электронные платежные системы (Киви-кошелек и др.), либо на лицевой счет абонентского телефонного номера потерпевшего и далее на электронные платежные системы, либо бан-

ковские карты преступника. При этом вирус блокирует (не выводит на дисплей телефона, а также удаляет их из телефона потерпевшего) информационные SMS-сообщения о произведенных транзакциях, которые поступают от банка (см. рис. 37).

В случаях осуществления преступной деятельности «заражение вредоносным программным обеспечением телефонных аппаратов и других технических устройств на операционной системе «Android» необходимо применять следующий алгоритм действий:

В ходе опроса заявителя в обязательном порядке выяснить, подключена ли услуга «Мобильный банк», а также установить модель телефона, используемого потерпевшим. Кроме того, выяснить, имеется ли у потерпевшего аккаунт системы Киви-кошелек, «привязанный» к абонентскому номеру, приходили ли потерпевшему подозрительные сообщения на телефон с различными ссылками. Далее у потерпевшего необходимо выяснить:

- обращался ли он в банк, если да, то каким образом;
- какой был получен ответ от сотрудника банка (в устном или письменном виде).

Часто при получении SMS о снятии денежных средств со счета, потерпевшие обращаются по телефону в банк. В процессе телефонного разговора оператор сообщает, куда были перечислены денежные средства, с какого номера телефона было отправлено SMS, и иногда сообщается абонентский номер, на счет которого перечислены денежные средства. В случае, если у потерпевшего имеется детализация звонков и SMS от оператора сотовой связи, а также выписка из лицевого счета, то необходимо данные документы (или копии) приобщить к материалам проверки, если вышеперечисленных документов при обращении в полицию у потерпевшего нет, то после принятия заявления необходимо незамедлительно вместе с потерпевшим выехать в отделение ПАО «Сбербанк России» и получить следующую расширенную выписку о движении денежных средств по счету:

1. У потерпевшего истребовать детализацию телефонных соединений с целью установления способа и направления перевода денежных средств.

2. Установить принадлежность абонентских номеров, используемых злоумышленниками в противоправных целях (запросить информацию в соответствующем оперативном подразделении органов внутренних дел или у оператора связи).

3. В случае создания учетной записи мобильного кошелька с использованием номера потерпевшего, в целях получения детализации транзакций осуществить вход в личный кабинет, SMS-сообщение с паролем поступит на телефон потерпевшего.

4. Согласно собранным документам, при наличии основания, указывающего на признаки соответствующей статьи УК РФ, принять решение о возбуждении уголовного дела.

5. В тех случаях, когда денежные средства поступают на счет абонентского номера, преступники производят их обналичивание через различные

кредитные организации (платежные системы). В связи с этим необходимо направить запросы в финансовые организации для получения информации о владельцах счетов, на которые были переведены денежные средства.

6. Направить запрос в платежную систему для получения информации об ip-адресе администрирования и движении денежных средств. Запрос должен быть утвержден руководителем следственного органа и заверен гербовой печатью.

7. Изъять телефон у потерпевшего. Изъятие производится без SIM-карты потерпевшего, но с находящейся flash-картой или другим накопителем в телефоне. Изъятый телефон направить в экспертно-криминалистическое подразделение для производства дальнейшего исследования и получения необходимых ответов на интересующие органы дознания вопросы.

8. С учетом возникшей ситуации необходимо перед экспертом поставить следующие вопросы:

- имеются ли в памяти мобильного устройства и на flash-памяти программные продукты, детектируемые антивирусным программным обеспечением как вредоносные;

- если да, произвести копирование обнаруженных программных продуктов на неизменяемый оптический носитель информации.

Обязательно вносить после представленных вопросов следующие рекомендации: «*Разрешаю внесение изменений в первоначальное состояние вещественного доказательства, в объеме, необходимом для проведения исследования».*

9. При получении информации о принадлежности абонентских номеров, а также о владельцах счетов (электронных платежных систем, банковских) необходимо подготовить ходатайство перед судом на получение технической информации:

- о соединениях интересующих абонентских номеров;

- о месте положения терминала сотовой связи в зоне действия конкретной базовой станции с привязкой к местности с целью установления фактического местонахождения злоумышленника в момент совершения противоправных действий;

- о движениях денежных средств по счетам с указанием суммы, реквизитов получателей и мест администрирования во время выполнения операций.

10. Получив судебные решения, истребовать необходимую информацию. В случае отсутствия филиала организации, владеющей информацией, запрос и судебное решение необходимо направить в структурное подразделение полиции по месту нахождения головного офиса.

11. Сотрудники, ответственные за формирование информационно-поисковой системы, осуществляют ввод информации в банк данных и ее корректировку при получении новых сведений.

По установлению конечного места завладения денежными средствами провести необходимые оперативно-розыскные мероприятия, направленные на отождествление личности злоумышленника.

Более сложные схемы хищения денежных средств

Далее представлены более сложные схемы совершения преступлений в системе дистанционного банковского обслуживания.

Рис. 38. Разработка сложных схем хищения денежных средств «Хакерами»

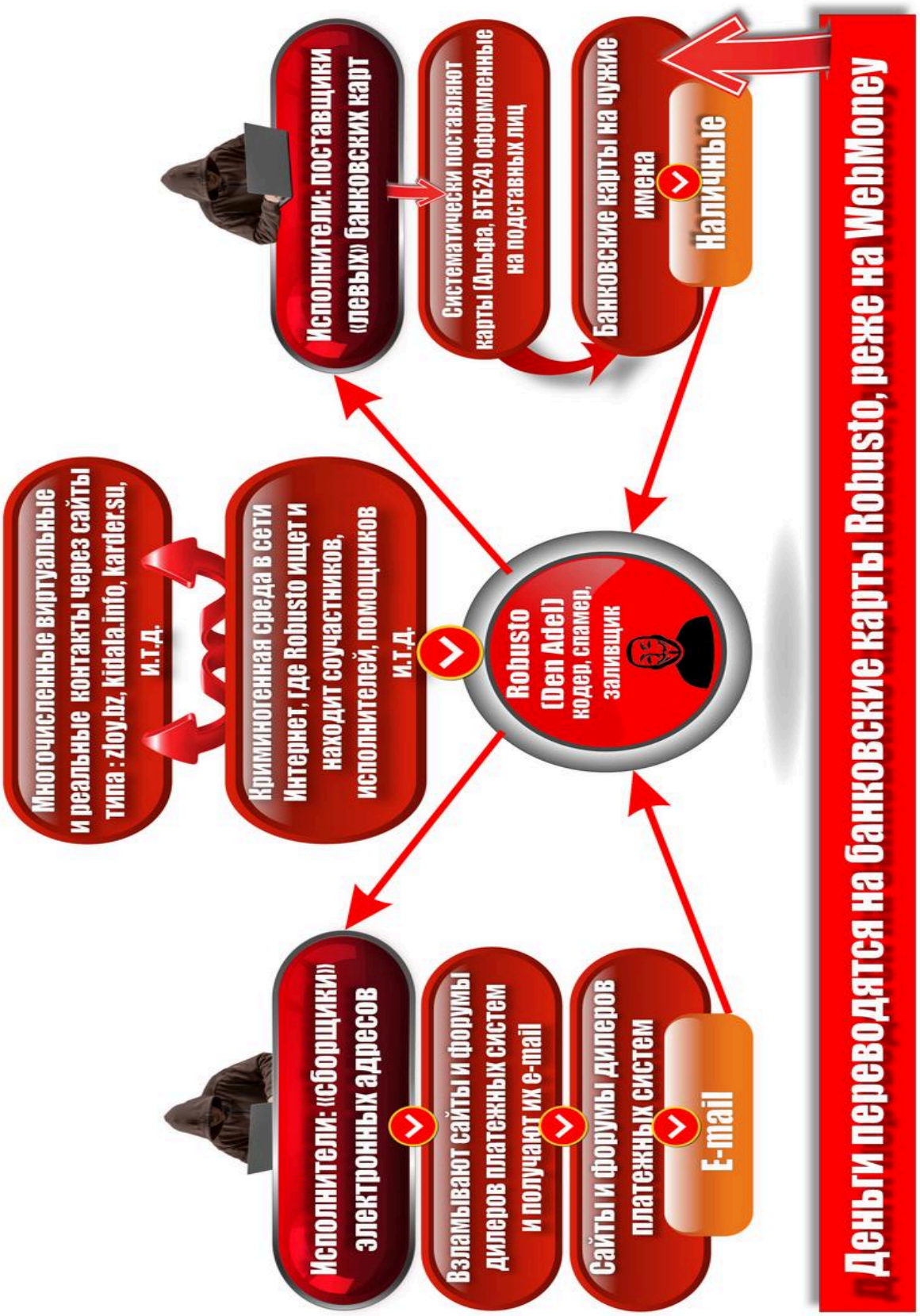


Рис. 39. Тактика хищения денежных средств

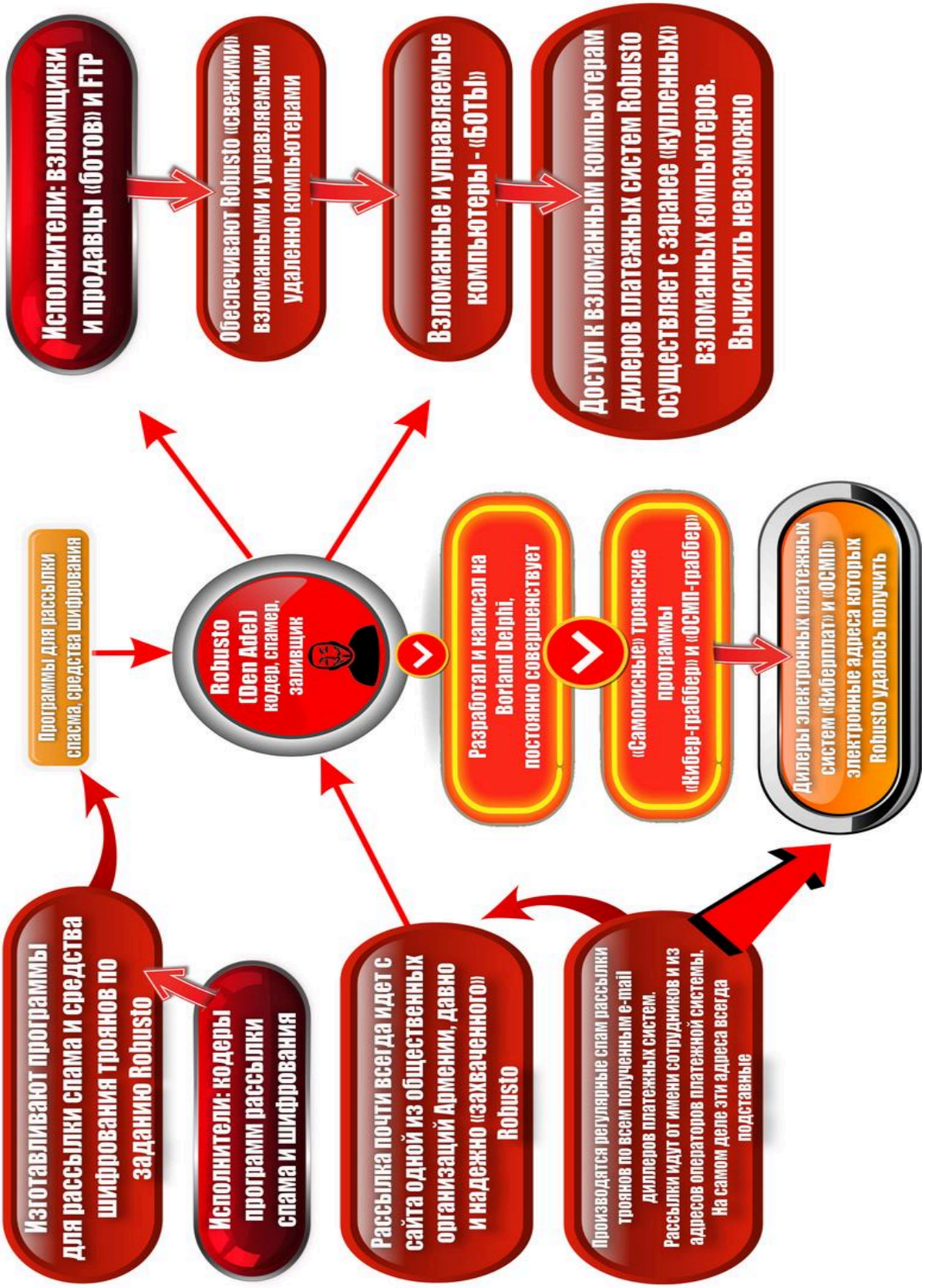


Рис. 39 (продолжение). Тактика хищения денежных средств

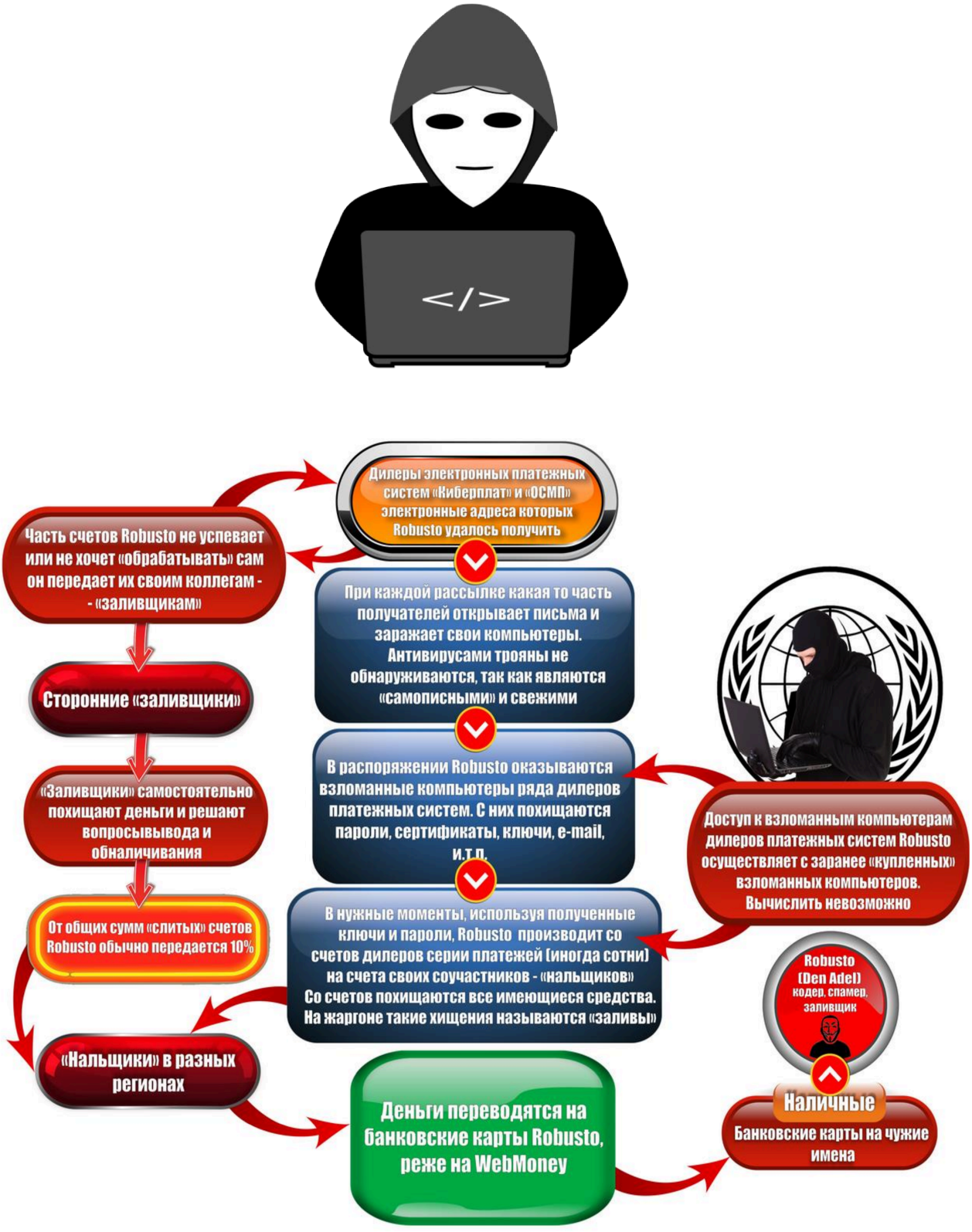


Рис. 39 (продолжение). Тактика хищения денежных средств

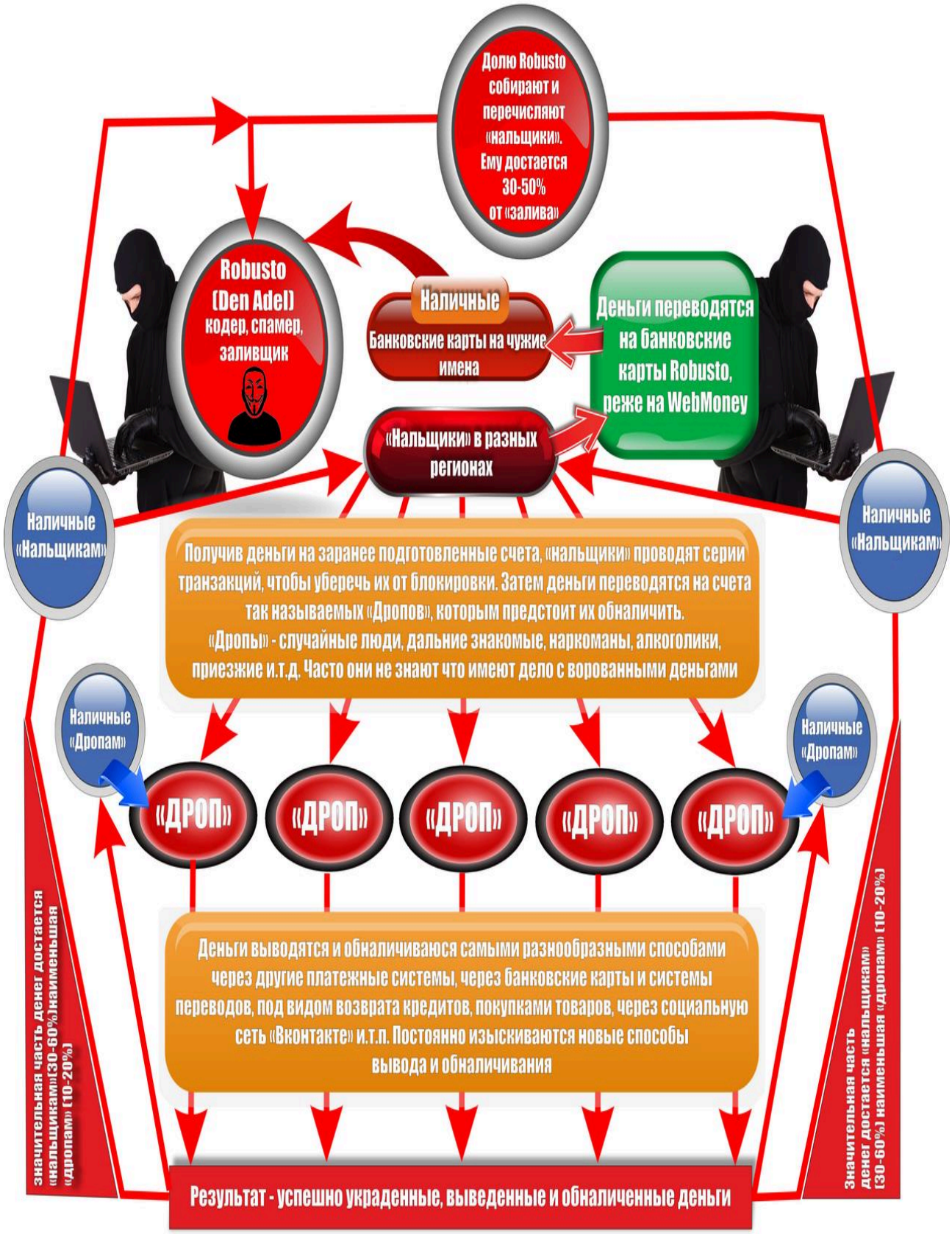


Рис. 39 (продолжение). Тактика хищения денежных средств

В одном из блоков схемы мы видим, что злоумышленники используют управляемые сети из зараженных компьютеров – так называемые «ботнеты» (сеть компьютеров, зараженных вредоносной программой, позволяющей киберпреступникам удаленно управлять зараженными машинами: каждой в отдельности, частью компьютеров, входящих в сеть, или всей сетью целиком без ведома пользователя). На диаграмме 11 показано распределение зараженных компьютеров по категориям их деятельности в международной сети Интернет.

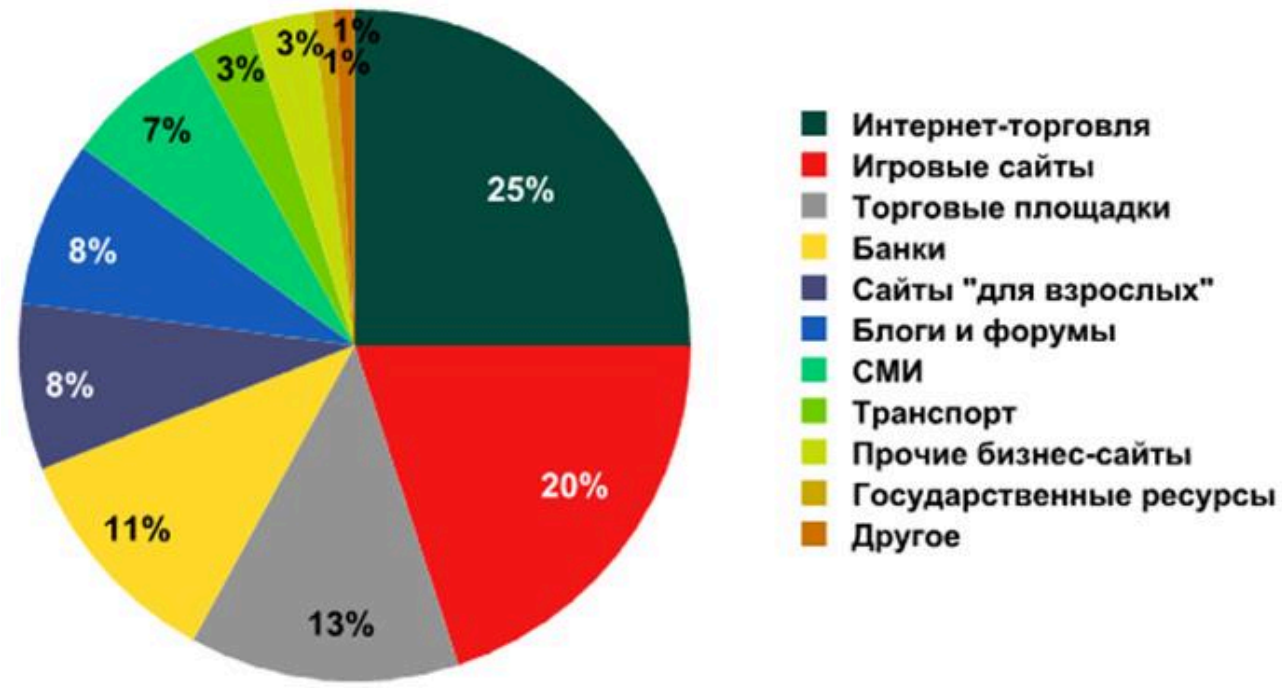


Диаграмма 11. Распределение атакованных ресурсов по категориям Интернет-деятельности при хищении денежных средств

Таким образом, понятно, что наибольшему риску заражения для участия в управляемой злоумышленником сети подвержены сайты Интернет-торговли и игровые сайты.

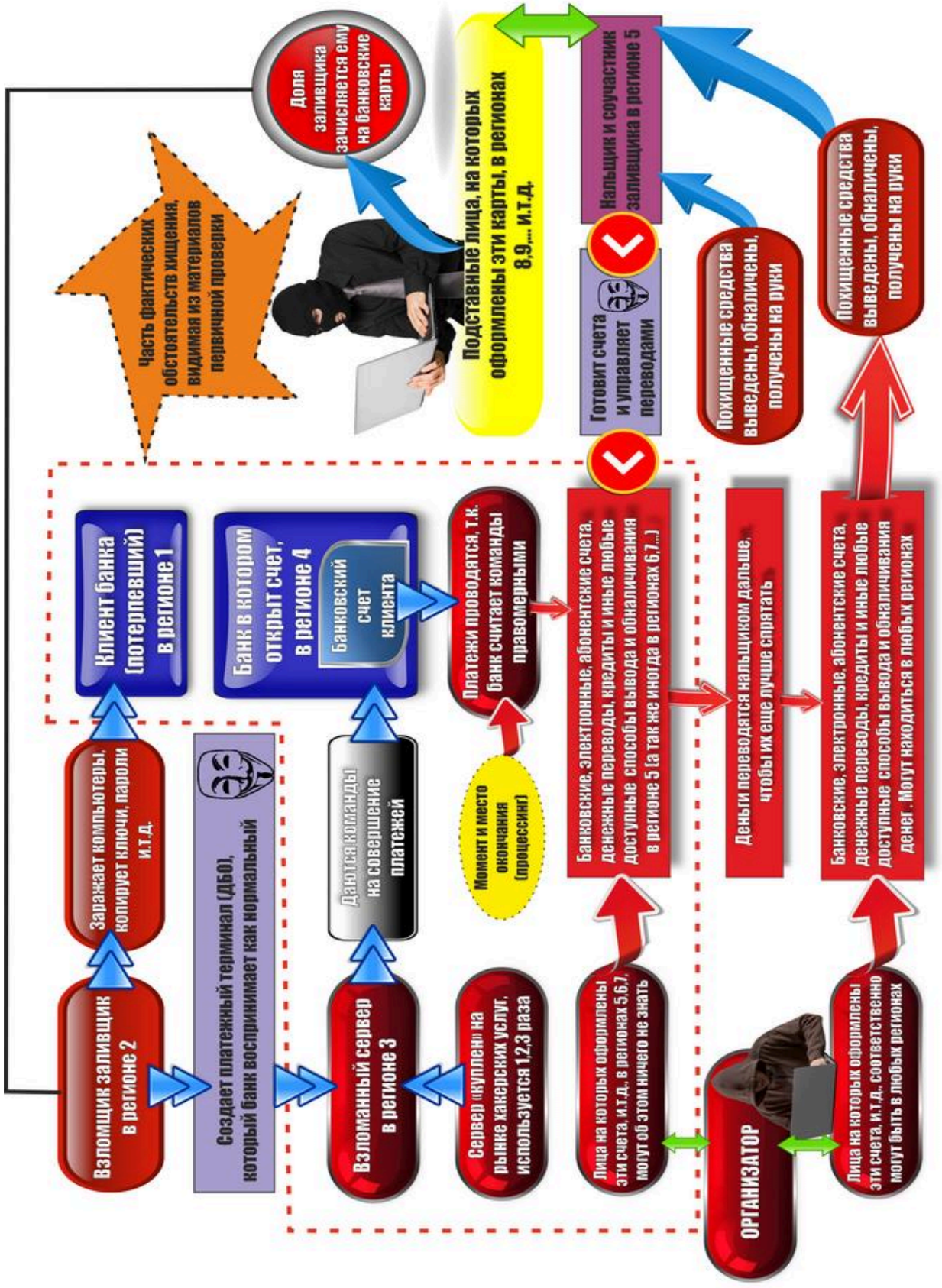


Рис. 40. Территориальная схема типового хищения

3.3. ОСОБЕННОСТИ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ХИЩЕНИЕМ ДЕНЕЖНЫХ СРЕДСТВ В СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Тактика раскрытия хищений денежных средств в системе дистанционного банковского обслуживания.

В случае поступления информации о совершенном хищении денежных средств со счета клиента банка в органы внутренних дел уполномоченным сотрудникам необходимо установить способ совершения хищения, а именно: выехать на место дислокации организации (компании или лица) для осуществления **осмотра** электронного устройства, на котором установлено ДБО.

В ходе проведения осмотра электронного устройства необходимо:

1. Выяснить, каким образом осуществляется подключение данного электронного устройства к сети Интернет.
2. Определить, какой вид ДБО установлен (у каждого банка свой вид ДБО).
3. Зафиксировать факт наличия подключенных и находящихся на месте «ключей» электронной цифровой подписи (ЭЦП). «Ключи» ЭЦП необходимы для проведения финансовых операций с использованием ДБО. Их количество может варьироваться от двух и более.

В ходе проведения первоначальных проверочных мероприятий установить или опровергнуть причастность к хищению денежных средств сотрудников данной организации (компании).

После чего необходимо опросить директора, главного бухгалтера, а также, при наличии в штате, администратора сети организации (компании). В ходе проведения опроса выше указанных лиц необходимо акцентировать внимание на получении следующей информации:

- кто имел и имеет доступ к электронному устройству, на котором установлено ДБО;
- не было ли замечено ими в период похищения денежных средств подозрительной активности на данном электронном устройстве (самостоятельное включение и выключение компьютера, непонятная активность курсора мыши на мониторе компьютера, зависание компьютера либо еще какие-либо события, ранее не происходившие);
- о точном времени составления и отправления платежного поручения, в результате чего были похищены денежные средства;
- в период хищения денежных средств подробно установить, чем занимались опрашиваемые лица, а также все те, кто имел или имеет доступ в обследуемое помещение, где находится компьютер;
- установить, каким способом компьютер подключается в сеть, а именно, возможно ли с него получение доступа в локальную сеть, либо он напрямую подключен в сеть Интернет;

- установить, ведется ли логирование доступа в сеть Интернет рабочих компьютеров организации, что обязательно необходимо для установления возможного неправомерного доступа в сеть организации из вне.

4. После вышеперечисленных действий в обязательном порядке данное электронное устройство, подвергшееся атаке, необходимо изъять для последующего проведения компьютерно-технической экспертизы.

5. По возможности до приезда следственно-оперативной группы связаться с пострадавшей организацией (компанией) и сообщить о необходимости отключения данного электронного устройства от локальной сети и сети Интернет, а также полного отключения электропитания.

6. Одновременно с целью получения информации о движении похищенных денежных средств связаться с банком, клиентом которого является пострадавшая организация (компания), заявившая, что с ее счета были похищены денежные средства.

7. Получить лог-файлы (информация об IP-адресе, дате и времени) доступа к системе «Клиент-Банк».

8. По завершении всех необходимых проверочных мероприятий и получения оперативно значимой и другой информации следует осуществить ее тщательный анализ.

9. Запросить у провайдера, оказывающего пострадавшей организации (компании) услуги доступа в сеть Интернет, детализированную статистику доступа в сеть Интернет (при необходимости получить судебное разрешение на получение этой информации); период получения запрашиваемой информации должен составлять около 7 дней.

10. Провести анализ полученной детализированной статистики. В ходе просмотра информации необходимо установить, какие IP-адреса обращались к IP-адресу организации (компании) в момент хищения, а также проверить информацию с целью получения сведений о совпадении IP-адресов за проверяемый период. При установлении «подозрительного» IP-адреса проанализировать объем переданной и полученной им информации, а также используемый порт, при его доступе к IP-адресу организации.

11. Необходимо получить информацию о принадлежности «подозрительного» IP-адреса. Если IP-адрес российский, направить запрос в организацию, которой он принадлежит, либо в РНЦБ Интерпола.

12. Отработать информацию о движении денежных средств: куда и на какой счет были переведены похищенные денежные средства; был ли установлен факт их обналичивания; в случае подтверждения интересующего события осуществить его документирование и сохранить видеозапись с банкоматов и камер видеонаблюдения.

Предлагаем рассмотреть понятия основных способов идентификации лиц, подозреваемых в совершении преступлений, в сети Интернет.

Основные способы идентификации преступника в сети Интернет (сведения об «IP-адресе» и «MAC-адресе»).

Сотрудники оперативных подразделений, в чьи должностные обязанности входит раскрытие преступлений, связанных с хищением денежных средств в системе ДБО, **обязаны знать** часто встречающиеся ключевые понятия, имеющие отношение к данной сфере. Предлагаем их рассмотреть.

Анонимизация **–** совокупность действий, направленных на сокрытие личности пользователя путем маскировки или подмены характеристик пользователя и его устройств**.**

Деанонимизация **–** совокупность действий, совершаемых лицом или автоматизированной системой, направленных на раскрытие реальной личности пользователя и характеристик его устройств.

Виртуальная личность **–** совокупность данных, характеризующих пользователя и представляющих его в интернете: логин, аватар, почтовый адрес, подпись на форуме.

Анонимизированная личность **–** замаскированная виртуальная сущность, используемая для создания анонимности.

Субъект деанонимизации **–** тот, кто осуществляет деанонимизацию.

Объект деанонимизации **–** тот, деанонимизацию кого осуществляют.

VPN «виртуальная частная сеть» — это обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

TOR – это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания.

Виртуальная машина – программа, которая эмулирует реальный (физический) компьютер со всеми его компонентами (жесткий диск, привод, BIOS, сетевые адаптеры и т.д.).

Виртуальный сервер – услуга предоставления в аренду так называемого виртуального выделенного сервера. В плане управления операционной системой по большей части она соответствует физическому выделенному серверу.

Веб–сервер – сервер, принимающий HTTP-запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными.

IP-адрес (ай-пи адрес, сокращение от англ. Internet Protocol Address) – сетевой адрес узла в компьютерной сети, построенной по протоколу IP. При связи через сеть Интернет требуется глобальная уникальность адреса, в случае работы в локальной сети требуется уникальность адреса в пределах сети.

MAC-адрес компьютера (электронного устройства) (от англ. Media Access Control – управление доступом к среде) – уникальный идентификатор, присваиваемый каждой единице активного оборудования (устройства) или некоторым их интерфейсам в компьютерных сетях Ethernet.

«IP-адрес» может быть статическим (постоянным) или динамическим (временным). В любом случае «IP-адрес» «привязан» к месту расположения устрой-

ства, выходящего в сеть, либо персональным данным лица, на чье имя заключался договор (при использовании мобильного Интернета). Сведения о том, кому был присвоен «IP-адрес», хранятся у поставщика услуг Интернета (например, компании «Ростелеком» и др.) и содержат данные о том, по какому адресу находится компьютер, с которого был осуществлен выход в сеть, информацию о лице, с которым был заключен договор о предоставлении услуг Интернета.

Таким образом, можно выделить две технологические основы, одна из них – инфраструктура пользователя (рис.41), то есть какой тип ЭВМ используется и как осуществляется доступ в сеть. Вторая технологическая основа – организация защиты, т.е. безопасность пользователя в процессе соединений (см. рис. 42).

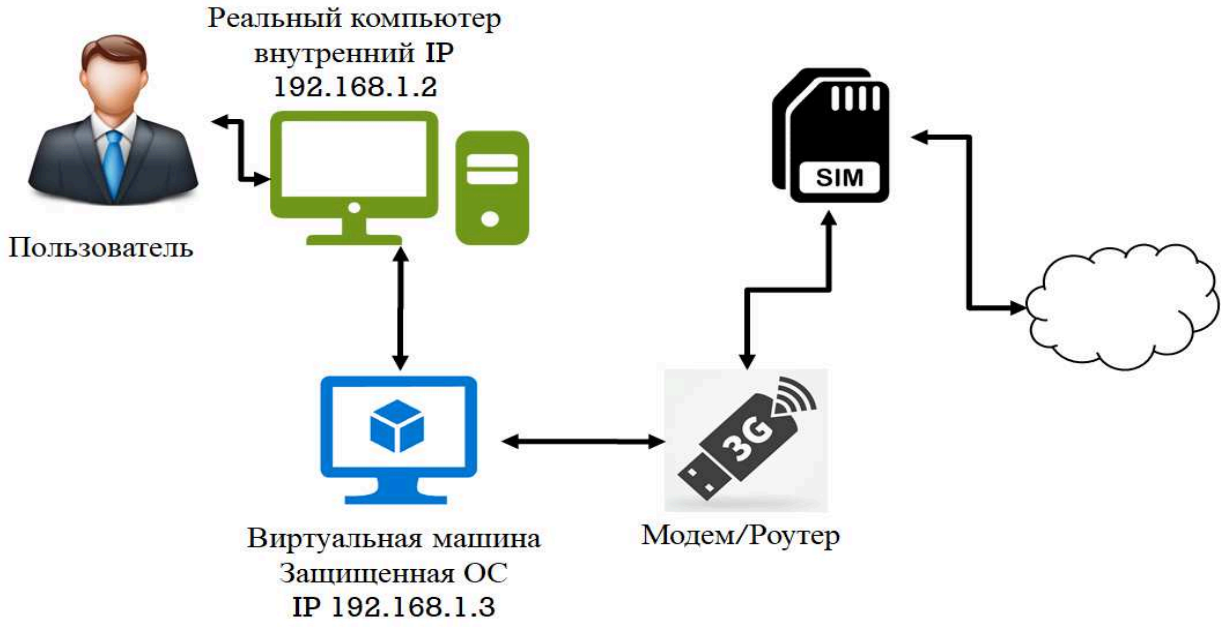


Рис. 41. Технические основы. Инфраструктура пользователя

Отсюда следует, что в случае установления «IP-адреса», с которого преступники выходили в сеть через проводной Интернет, компания-провайдер может предоставить сведения, как о месте расположения компьютера, так и о персональных данных лица, на чье имя заключался договор. Однако необходимо помнить, что подобные сведения хранятся непродолжительное время. **Период хранения зависит от технических возможностей провайдеров и может составлять от 1 месяца до нескольких лет. Поэтому промедление может привести к утрате важной информации**[1]**.**

[1] В соответствии с п.12 Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность, утвержденными Постановлением Правительства Российской Федерации от 27 августа 2005 № 538, сведения об оказанных услугах связи должны храниться оператором в течение 3 лет. Однако, в ряде случаев операторы связи не соблюдают указанное требование, ссылаясь на отсутствие технических возможностей для хранения значительного объема информации.

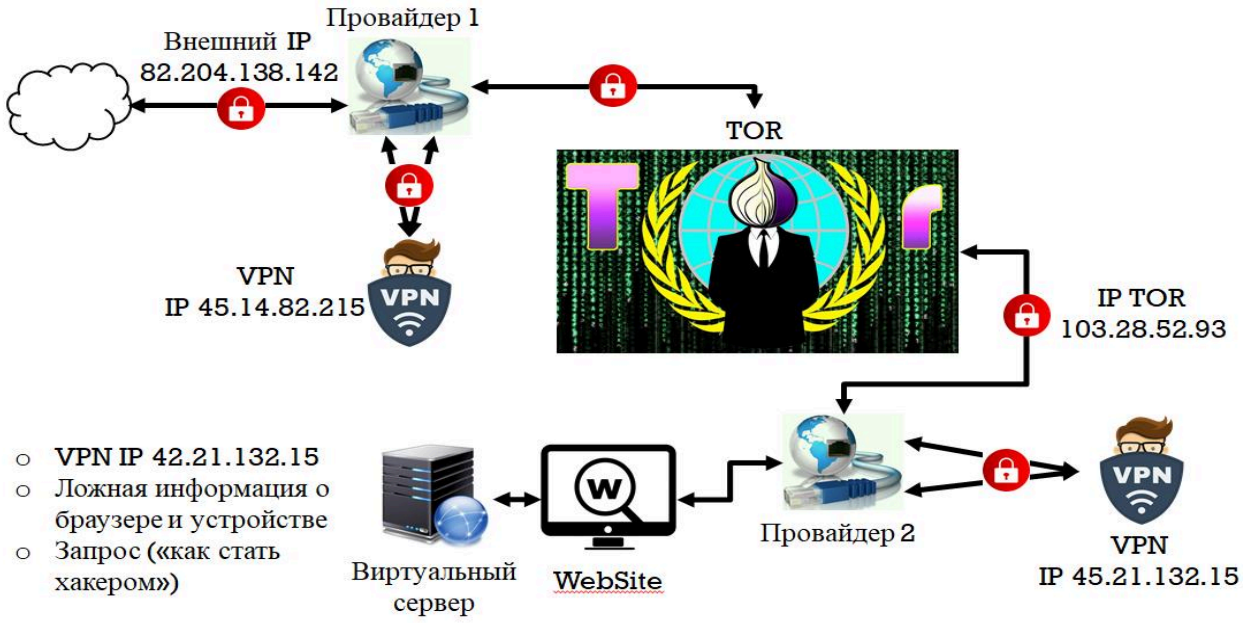


Рис. 42. Технические основы. Организация защиты

При использовании преступниками мобильного Интернета (через USB-модем или сотовый телефон) по известному сотрудникам органов внутренних дел «IP-адресу» компания-провайдер может предоставить сведения лишь о персональных данных лица, на чье имя заключался договор о предоставлении услуг связи при оформлении (приобретении) SIM-карты (см. рис. 43).

Определенные затруднения может вызвать ситуация, когда выход в сеть преступниками был осуществлен из так называемой «зоны свободного Wi-Fi»-участка. В нем Интернет предоставляется всем желающим бесплатно: территории крупных торговых центров, некоторые кафе, вагоны метрополитена и др., где каждый может воспользоваться услугами Интернета с любого портативного устройства (ноутбук, телефон). В этом случае по «IP-адресу» будут представлены лишь сведения о том, что доступ был осуществлен из зоны «Wi-Fi» по определенному адресу населенного пункта.

В качестве **способа выявления лиц**, осуществляющих выход в Интернет в преступных целях из «Wi-Fi»-зон, **необходимо**:

1. Анализировать видеозаписи с прилегающей территории (если таковая ведется) и осуществлять последующую проверку выявленных лиц, используемого автотранспорта.

2. Сопоставлять «MAC-адрес» изъятых у подозреваемых электронных коммуникационных устройств с теми, которые были зафиксированы при совершении рассматриваемых видов преступлений.

Несмотря на то, что «MAC-адрес» может быть незаконно изменен пользователем в попытке уйти от контроля, существует вероятность выхода компьютера преступника в сеть в нескольких точках доступа с одним и тем же

«MAC-адресом». Например, используется ноутбук, который периодически **приносят в одну или различные зоны «Wi-Fi», либо с него выходят в сеть, используя проводной Интернет в различных стационарных точках доступа (квартиры, офисы).**

В целях получения информации, представляющей оперативный интерес, необходимо запросить компании, ранее предоставляющие доступ в сеть Интернет по установлению «IP-адресов» (место, территория), у которых был зарегистрирован выход компьютера в сеть с «MAC-адресом» (серийный номер устройства).

Также еще одним из способов разоблачения преступника является установление все учетных данных в сети Интернет, но часто это осложняется нахождением виртуальной личности, а также личности, которая может быть анонимизированной (схема 8).

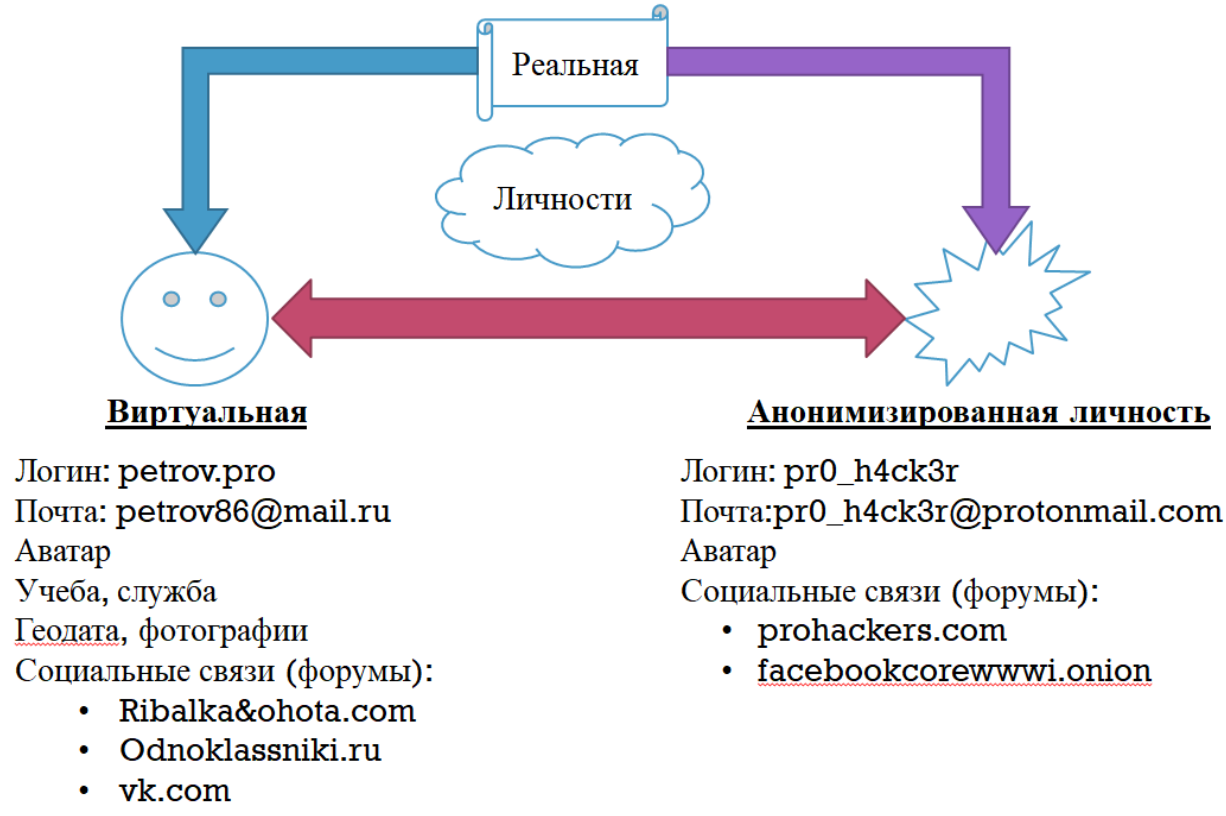


Рис. 43. Пример виртуальной личности

Особенности предоставления услуг «хостинга» в сети Интернет при создании сайтов преступниками.

В случае создания вымышленных «сайтов», например, «зеркальных» сайтов, рассмотренных выше, преступники могут пользоваться ячейками. Данные ячейки выделяются администрацией крупных сайтов для размещения на них своих небольших по объему страниц – **мини-сайтов** (услуги *«хостинга»*). Услуги «хостинга» в большинстве случаев оплачиваются, что позволяет установить, с каких счетов преступниками перечислялись денежные средства. Кроме того, создателю страницы сайта предоставляется право выхода и ад-

министрирования, что позволяет установить «IP-адреса», с которых преступники управляли сайтом. Помимо IP-данных, зафиксированных при создании и последующем управлении сайтом, **злоумышленники могут регистрироваться в администрации хостинга**, указывая почтовый ящик (E-mail). Данный E-mail они могут использовать несколько раз при создании сайтов, а также для ведения собственной переписки. Вся информация технического и организационного характера от организации (компании), предоставляющей услуги хостинга, будет направляться на данный почтовый ящик E-mail. Полученную информацию в дальнейшем следует учитывать при доказывании вины преступников. Злоумышленники вынуждены периодически проверять почту, а также отвечать организатору хостинга по вопросам функционирования страницы своего сайта.

В связи с этим необходимо направлять запросы в компании, предоставляющие ресурсы, на которых преступники размещали данные сайты. Целью направляемых запросов является: установление «IP-адресов» и «MAC-адресов» регистрации сайта, управление сайтом, сведений об оплате услуг, адреса использовавшейся электронной почты. Вся полученная информация подвергается глубокому анализу для последующего общего сбора оперативной и доказательственной информации, а также посредством проведения оперативно-розыскного мероприятия «снятие информации с технических каналов связи».

Особенности предоставления операторами сотовой связи дополнительных услуг абонентам.

Зачастую, при совершении хищений денежных средств, преступниками в качестве своеобразной платежной системы используются счета абонентских номеров сотовой связи. Их выбор объясняется относительной простотой перевода денежных средств, а также легкой возможностью управления счетом телефонного номера через «личный кабинет» в сети Интернет для дальнейшего перечисления похищенных денежных средств. В случае перечисления преступниками похищенных денежных средств на телефонные номера сотовой связи необходимо через соответствующие структурные подразделения органов внутренних дел направить запрос в компании, предоставляющие услуги связи. Целью запроса является: установление телефонных номеров или иных счетов, на которые были перечислены денежные средства со счета данного телефонного номера, кем и где данные средства были обналичены.

Таким образом, своевременность и качество выявления и раскрытия хищений денежных средств, совершенных с использованием вредоносных программ, напрямую **зависит** от учета **специфики способов** совершения преступлений, предоставления операторами сотовой связи дополнительных услуг абонентам и средств идентификации преступника в сети Интернет. По выполнению всех первоначальных мероприятий и получении необходимой информации оперативный сотрудник избирает тактически грамотную линию

своего поведения и акцентирует работу на дальнейшую организацию и планирование хода раскрытия преступлений.

Особенности опроса потерпевшего.

Заявление (сообщение), поступившее в орган внутренних дел о факте хищения денежных средств с банковской карты (расчетного счета), подлежит регистрации в установленном порядке[1]. После этого необходимо составить план проведения первоначальных оперативно-розыскных мероприятий и следственных действий.

В ходе опроса заявителя (потерпевшего) ***в объяснении необходимо отразить***:

– каким образом, где и при каких обстоятельствах стало известно о хищении денежных средств с банковской карты (расчетного счета);

– время обнаружения пропажи денежных средств и в какой сумме;

– номер банковской карты и (или) банковского счета, с которого были похищены денежные средства, наименование банка;

– адресат, куда переведены денежные средства (абонентский номер сотового телефона или банковский счет, используемая платежная система и т.д.);

– название и модель используемого сотового телефона, где и когда приобретался, имеются ли соответствующие документы (кассовый, товарный чек);

– каким образом, где и при каких обстоятельствах была подключена услуга «Мобильный банк», «Сбербанк Онлайн»: дата подключения, «привязка» к абонентскому номеру;

– факт поступления SMS-сообщений на сотовый телефон от имени каких-либо банковских учреждений, если да, то когда и при каких обстоятельствах;

– факты поступления SMS-сообщений со ссылками на интернет-страницу, если да, то когда и какого содержания;

– используемые на сотовом телефоне интернет-ресурсы: «Одноклассники», «Вконтакте», «Play Маркет» и т.д.

При принятии заявления и отборе объяснения у потерпевшего необходимо установить все обстоятельства и определить, каким способом произошло хищение денежных средств. Кроме того, необходимо выяснить:

1. Обращался ли потерпевший по факту данного хищения денежных средств в банк?

2. Если да, то каким образом он обращался и в какой форме представители банка ему ответили?

---

[1] Приказ МВД России от 29.08.2014 № 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях».

3. Были ли предприняты какие-либо меры со стороны представителей банка после обращения потерпевшего? Если да, то как быстро произошло реагирование на информацию заявителя?

Часто при получении SMS о снятии денежных средств со счета потерпевшие обращаются по телефону в банк, где операторы обратившемуся клиенту сообщают, куда были перечислены денежные средства, с какого номера телефона было отправлено SMS, и иногда сообщают абонентский номер, на счет которого перечислены денежные средства.

Для принятия соответствующих мер по возврату похищенных денежных средств, а также ускорения получения информации об обстоятельствах преступления потерпевшему необходимо в кратчайшие сроки связаться с представителями банка. Далее потерпевшему оперативные сотрудники рекомендуют подготовить и направить сотрудникам банка заявление об отмене платежа и получить справку по факту инцидента[1]. В случае, если у потерпевшего имеется детализация звонков и SMS от оператора сотовой связи, а также выписка из лицевого счета, необходимо данные документы (или копии) приобщить к имеющимся проверочным материалам. **Обязательным условием** при первичном опросе потерпевшего является **получение и приобщение вышеуказанных документов** к материалам проверки. По окончании опроса потерпевшему разъясняется право имеющейся возможности обращения в суд с исковым заявлением о взыскании похищенных денежных средств с обслуживающего его банка[2].

Виды запросов подразделений МВД России в Сбербанк России

При получении от потерпевших информации о банковских счетах или банковских картах, а также другой информации, касающейся банковских услуг, сотрудники органов внутренних дел отправляют в банки, в частности в Сбербанк России, соответствующие запросы. Чаще всего оперативные сотрудники осуществляют тесное взаимодействие со Сбербанком России.

В процессе сотрудничества соответствующих подразделений МВД России может направить в Сбербанк России **три вида запросов** (см. рис. 44).

Первый вид запроса – это получение информации оперативными сотрудниками органов внутренних дел о банковской карте (банковском счете) потерпевшего или злоумышленника.

Если в дальнейшем от Сбербанка России поступает ответ, что данная карта (или счет) принадлежит банку, необходимо установить следующую информацию:

об отправителе средств:

- установочные данные;

---

[1] Методические рекомендации о порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента. Утверждены Рабочей группой ассоциации Российских банков (2012). Доступ из СПС «КонсультантПлюс».

[2] Ст. 845, 849, 854 ГК РФ.

- дату/время, сумму операции /выписка/;
- через какой сервис (Яндекс, Qiwi и прочие) была совершена операция.

Если от Сбербанка России поступает отрицательный ответ, то в этом случае запросы осуществляются в другие банки.

Второй вид запроса – это получение информации оперативными сотрудниками органов внутренних дел о сервисе Сбербанка России.

В том случае, когда от Сбербанка России поступает на указанный запрос положительный ответ, необходимо выяснить информацию о принадлежности сервиса:

- СБОЛ (Сбербанк онлайн – IP-адрес);
- СБОЛ МП (мобильное приложение «Сбербанк онлайн» – IP-адрес);
- МБК (Мобильный банк);
- УС (установочные данные – номер, место установки, фото-, видео – при наличии).

В случае отсутствия данных Сбербанк России может предоставить информацию об организации, владельце сервиса.

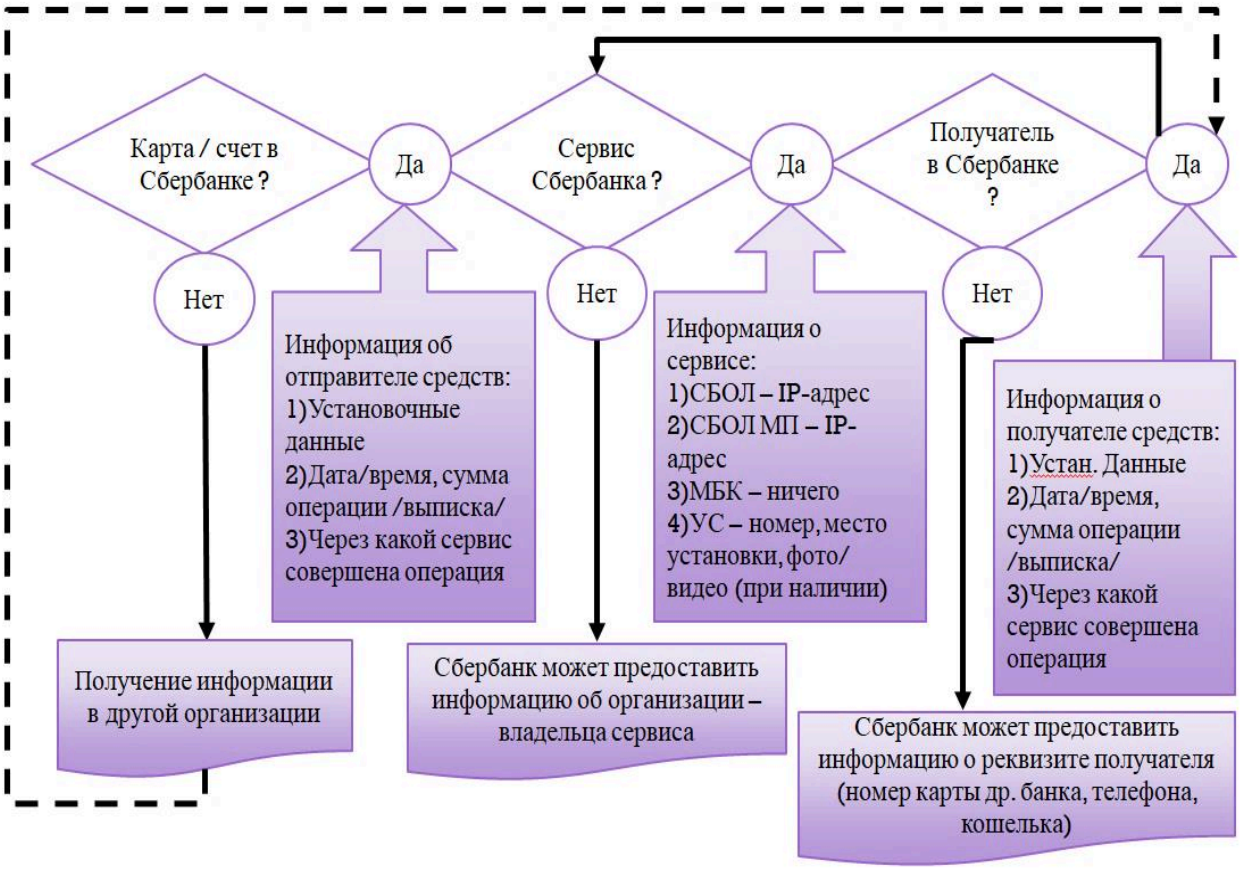


Рис. 44. Виды запросов подразделений МВД России в Сбербанк России

Третий вид запроса проводится, когда у оперативных сотрудников органов внутренних дел имеется информация о получателе Сбербанка России.

При поступлении положительного ответа необходимо установить следующую информацию о получателе средств:

- установочные данные;
- дату/время, сумму операции /выписка;
- через какой сервис совершена операция.

Если отсутствуют интересующие оперативных сотрудников конкретные данные, то в этом случае Сбербанк России может предоставить информацию о реквизите получателя (номер карты другого банка, номер телефона, кошелька).

Изъятие сотового телефона и flash-карты

После опроса потерпевшего необходимо изъять сотовый телефон и flash-карту[1].

Изъятие мобильного телефона чаще всего производится без SIM-карты потерпевшего, поскольку она в ряде случаев не несет информации, требующей исследования. Находящуюся в телефоне flash-карту или другой накопитель информации необходимо изъять, так как они могут содержать внедренные преступниками вирусы или следы их действия.

Изъятый телефон направляется в экспертно-криминалистическое подразделение для проведения компьютерного исследования и установления наличия в памяти устройства вредоносных программ, определения задач, механизма и особенностей действия.

В случае получения от эксперта неполного ответа на все указанные вопросы (например, если было установлено лишь наличие следов вредоносной программы, которая самостоятельно удалилась из памяти устройства; программа обнаружена, но не выявлен механизм ее действия), возможно проведение дополнительных исследований в сторонних организациях или иных экспертно-криминалистических подразделениях. Независимо от фактической полноты проведенного исследования, его результаты имеют значение для квалификации деяния, и полученные результаты подлежат обязательному приобщению к материалам предварительной проверки, содержащим признаки состава преступления.[2] Данные материалы в ходе предварительного расследования могут быть признаны вещественными доказательствами, что положительно скажется на раскрытии преступления.

---

[1] Изъятие телефона у потерпевшего для последующего исследования, исходя из содержания действий сотрудников полиции, должно оформляться протоколом изъятия (ч.1 ст.15 Федерального закона «Об ОРД»).

[2] По результатам проведения предварительной проверки в порядке ст.144 УПК РФ и установления признаков состава преступления, предусмотренного ч.1 или ч.2 ст.158 УК РФ, материалы могут направляться по подследственности для возбуждения уголовного дела. После получения результатов компьютерного исследования и соответствующих экспертиз деяние может быть дополнительно квалифицировано по ст.272, 273 УК РФ.

Оперативно-розыскные мероприятия, проводимые при установлении факта перечисления денежных средств на абонентский номер сотового оператора

При установлении факта перечисления денежных средств на абонентский номер сотового оператора проводятся следующие оперативно-розыскные мероприятия (далее – ОРМ):

– ОРМ «Наведение справок» по абонентским номерам, на которые осуществлен перевод денежных средств, путем обращения к базам данных и использования справочных программ в сети Интернет в целях установления региона, к которому они относятся, а также персональных данных владельца. Данные мероприятия необходимы для определения региона, в котором зарегистрирован абонентский номер. После проведенного анализа собранных материалов полученная информация направляется в территориальный орган внутренних дел того региона, к которому относится абонентский номер, и производится запрос в сотовую компанию с целью получения имеющейся информации.

При этом необходимо учитывать, что полученные в ходе ***предварительной проверки сообщения о преступлении,*** сведения о фамилии, имени, отчестве абонента-гражданина, наименовании (наименовании фирмы) абонента – юридического лица, фамилии, имени, отчестве руководителя и работниках этого юридического лица, а также об адресе абонента, абонентских номерах) не ограничивают право лица на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; установление данной информации осуществляется без судебного решения путем проведения гласного оперативно-розыскного мероприятия «Наведение справок».

– ОРМ «Наведение справок» о владельце абонентского номера по учетам «ИБД-Р», «ИБД-Ф», «ПТК Розыск-Магистраль», в социальных сетях Интернета, для подтверждения факта существования такого лица, его регистрации по месту жительства на территории региона, получения фотографии указанного лица.

– ОРМ «Снятие информации с технических каналов связи». В данном случае необходимо подготовить и направить в суд ходатайство на получение судебного решения на проведение мероприятия «Снятие информации с технических каналов связи» об абонентских номерах, на которые были переведены денежные средства.

В случае получения информации о нахождении абонента сотовой сети в другом регионе, необходимо подготовить и направить в установленном порядке весь собранный материал по территориальности.

В подготовленном материале, представляющем оперативный интерес и требующем дополнительной проверки, рекомендовать уточнить анкетные данные установленных лиц по учетам, выявить их местонахождение с последующим проведением опроса и обязательным выяснением следующих обстоятельств:

– когда, где и при каких обстоятельствах была приобретена SIM-карта;

– какими сведениями располагает опрашиваемый о лице, использующем SIM-карту;

– где находился опрашиваемый в момент совершения преступления.

В результате проведенных оперативно-розыскных мероприятий и полученной информации:

– о местонахождении абонентских номеров, на которые происходило зачисление денежных средств в момент совершения преступления, а также в последующий период;

– о базовых станциях, через которые происходило соединение, и их местоположении;

– об азимуте направления;

– о сведениях, содержащих входящие и исходящие соединения;

– об IMEI – коде мобильного устройства, регистрировавшегося с абонентским номером, IMSI (идентификационный номер SIM-карты);

– о входящих и исходящих SMS-сообщениях, – *должностное лицо в праве самостоятельно расширять круг устанавливаемых обстоятельств, имеющих отношение к преступной деятельности.*

С целью установления всех обстоятельств совершенного преступления необходимо направить в различные кредитные организации (платежные системы ЗАО «МОБИ Деньги», ЗАО «Национальная сервисная компания», ЗАО «КИВИ Банк», банк «Юнистрим» и другие) запросы о маршруте перечисления похищенных денежных средств, способе их обналичивания, а также о получателе платежа.

Перечень рассмотренных оперативно-розыскных мероприятий может быть расширен в зависимости от возникшей на конкретный промежуток времени ситуации.

Получение оперативно значимых сведений оперативным сотрудником по учетным записям «электронного кошелька»

Необходимо установить следующие сведения о движении средств по учетной записи «электронного кошелька»:

– откуда поступали деньги, в каком объеме и в какой период времени;

– с какого «электронного кошелька» и кем осуществлялась операция;

– какие при этом использовались терминалы;

– с помощью какой платежной системы или банка осуществлялась операция.

Движение средств по учетной записи «электронного кошелька» также позволяет установить:

– куда и когда переведены деньги;

– за какие услуги и товары переведены денежные средства;

– в какую платежную систему (банк) они были переведены.

Сведения об IP-адресе компьютера, с которого управляли «электронным кошельком», **позволяют установить адрес объекта** (через провайдера), выяснить, какими еще «кошельками» управляли с этого IP-адреса.

Информация об UDID[1]-коде телефона, создающемся для устройств компании Apple на основе Apple-ID[2], дает возможность узнать, какие еще электронные кошельки» управлялись с данного устройства.

Сведения о MAC-адресе, данных зоны Wi-Fi **позволяют установить** место (места), **откуда пользователь «выходил»** в Интернет для управления «электронным кошельком», а также *идентифицировать* электронное устройство в случае его изъятия.

В данной ситуации мы считаем необходимым уточнить понятие идентификации, так как этот вопрос вызывает затруднение и носит спорный характер.

С этой целью нами предпринята попытка сформулировать свое видение на данное понятие: **криминалистическая идентификация – криминалистический способ познания, в основе которого лежит процесс сравнительного исследования как минимум двух объектов, причинно связанных с расследуемым преступным событием, с целью использования поученных результатов в ходе расследования и успешного раскрытия преступлений.**

Данные о **«привязке»** банковских карт (их банковских счетов) к **«электронному кошельку»** дают *возможность установить, счета* каких пластиковых карт и каких банков «привязаны» к «электронному кошельку».

По этим данным можно установить, какие именно платежи проводились, когда и в каком объеме, по каким реквизитам.

Установление регистрационных данных владельца «электронного кошелька» позволяет использовать сведения, которые указал пользователь при регистрации электронного счета («кошелька»):

– персональные данные – фамилию, имя отчество;

– основные и дополнительные телефоны;

– адреса электронной почты и т.д.;

– IP-адреса, с которых осуществлялась регистрация.

Получение оперативно значимых сведений оперативным сотрудником по платежам в терминалах

При получении информации, содержащей сведения, указывающие, где, когда, кем и на какую сумму пополнялся счет, «привязанный» к мобильному телефону абонента, можно установить историю (периодичность) пополнения данного счета, а именно: в каком терминале, когда (с точностью до секунд) и на какую сумму производилось пополнение счета, «привязанного» к конкретному мобильному телефону. Это позволит определить место, в котором находился объект в конкретный момент.

---

[1] UDID – уникальный идентификатор устройства, состоящий из 40 символов. Он есть у каждого мобильного устройства категории iPad, iPhone или iPod Touch.

[2] Apple-ID – персональный идентификатор в системе Apple iTunes и AppStore/ Он имеет вид почтового ящика E-mail, который пользователь самостоятельно регистрирует в специальной программе iTunes, где указывает действующий E-mail и некоторые персональные данные.

Сведения об иных платежах объекта дают возможность выявить его «вторые» телефоны, либо телефоны его связей, что создает необходимость проведения такого оперативно-розыскного мероприятия, как «Прослушивание телефонных переговоров».

Данные о том, где объект совершает платежи (по регулярному использованию одного терминала или рядом расположенных терминалов) **позволяют сделать предположение** о местонахождении объекта: по платежам в позднее и раннее время – о примерном месте жительства; по платежам в дневное время – о примерном месте работы (учебы) или ориентировочной территории нахождения объекта в то или иное время.

В целях предупреждения хищений терминалы устанавливают в местах, оборудованных камерами видеонаблюдения. По записям с камер видеонаблюдения (супермаркеты, магазины, стоянки, торговые центры) можно установить время и место платежа в терминале, определить лицо, осуществляющее платеж, автотранспортное средство и лиц, находящихся поблизости.

Работа по запросам продолжается до тех пор, пока не будет получен ответ о фактическом снятии денежных средств подозреваемыми лицами через банкомат или в филиале банка.

При необходимости продления срока проверки по имеющимся материалам, содержащим сообщение о преступлении, возникает необходимость проведения соответствующих оперативно-розыскных мероприятий и получения их результатов; в соответствии с ч. 3 ст. 144 УПК РФ выносится мотивированное постановление с ходатайством перед руководителем органа дознания о продлении срока проверки до 10 суток. В дальнейшем при развитии оперативно-розыскной ситуации и постоянно поступающей информации, представляющей оперативный интерес, выносится мотивированное постановление с ходатайством перед прокурором о продлении срока проверки до 30 суток.

Постановление о продлении срока должно быть мотивированным. В нем необходимо указать **вид** проводимого оперативно-розыскного мероприятия, а также **цель** и **основания** проведения ОРМ.

В случае, если потерпевший по каким-либо причинам не может предоставить детализацию о движении похищенных денежных средств, необходимо подготовить и направить в районный суд ходатайство о получении судебного решения на предоставление исчерпывающей информации по движению денежных средств со счета.

Действия оперативного сотрудника в случае установления факта перечисления денежных средств на банковские счета

Установив номер банковского счета (банковской карты), необходимо в кредитной организации запросить следующую информацию:

– о персональных данных лица (организации), на чье имя выпущена банковская карта (открыт счет); при возможности запросить копии документов, предоставленных лицом при оформлении договора;

– о транзакциях, осуществленных по карте (счету) за анализируемый период, с указанием мест снятия денежных средств;

– о месте открытия и обслуживания карты, а также данные расчетного счета (с указанием номера офиса банка и адреса его местонахождения);

– о подключении услуги оповещения или услуги «Мобильный банк» к банковской карте и расчетному счету, с указанием всех абонентских номеров и адресов электронной почты.

При получении ответа из банка и установлении мест снятия денежных средств, необходимо незамедлительно направить запрос на получение видео- и фотоизображений из банкоматов и помещений, где установлены банкоматы, так как сроки их хранения ограничены.

В случае неполучения своевременного ответа от организации на направленный запрос о предоставлении информации существует возможность привлечения к административной ответственности виновных лиц по ст.19.7 КоАП РФ «Непредставление сведений (информации)».

Таким образом, основными оперативно-розыскными мероприятиями, проводимыми для выявления и раскрытия хищений денежных средств со счетов клиентов банков, совершенных при помощи вредоносных программ, являются опрос потерпевшего, исследование изъятого сотового телефона и flash-карты, наведение справок и снятие информации с технических каналов связи.

3.4. ОСОБЕННОСТИ ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ НА НАЧАЛЬНОМ ЭТАПЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Некоторые следственные действия, проводимые в ходе расследования хищений денежных средств, совершаемых в системе дистанционного банковского обслуживания

В ходе раскрытия преступлений, совершаемых в системе дистанционного банковского обслуживания, необходимо проводить, наряду с оперативно-розыскными мероприятиями, следующие, наиболее часто осуществляемые, следственные действия, такие как:

1. Осмотр места происшествия.

Данное следственное действие является одним из самых значимых и распространенных. В ходе его производства следует обращать внимание на источники информации, которыми могут быть:

- компьютеры, ноутбуки, моноблоки;
- носители информации (накопители на flash-памяти), карты памяти и т.д.;
- смартфоны, мобильные устройства, планшеты и т.д.;
- всевозможные журналы регистрации событий от интернет-провайдера;

- журналы регистрации событий от кредитной организации, предоставляющей систему ДБО.[1]

Рассматривая данные объекты, можно уточнить и получить разъяснения на следующие вопросы:

- с кем осуществлялась переписка в социальных сетях, на интернет-ресурсах, в программах для мгновенного обмена сообщениями;
- какие посещались интернет-сайты, в том числе в период совершения хищений;
- какие производились поисковые запросы;
- установлено ли на изъятых объектах вредоносные программы;
- можно ли получить сведения о подключаемых пользователях;
- можно ли получить информацию о сетевых соединениях и запущенных процессах;
- можно ли получить сведения об организации и фактическом лице, на имя которого был осуществлен платеж.

Предлагаем рассмотреть схему «Основания и порядок производства осмотра» согласно нормам ст. 176, 177 УПК РФ[2] (схема 3).

Схема 3

Основания и порядок производства осмотра
(ст. 176, 177 УПК РФ)

Осмотр места происшествия,
местности, жилища, иного помещения, предметов и документов
производится в целях обнаружения следов преступления,
выяснения других обстоятельств, имеющих значение
для уголовного дела

↓

Особенности производства осмотра:

осмотр места происшествия, документов и предметов может быть произведен до возбуждения уголовного дела;

осмотр жилища производится только с согласия проживающих в нем лиц или на основании судебного решения;

осмотр помещения организации производится в присутствии представителя администрации этой организации

↓

В ходе осмотра изъятию подлежат
только те предметы, которые могут иметь отношение к уголовному делу.
В протоколе осмотра по возможности указываются индивидуальные признаки и особенности изымаемых предметов. Все обнаруженное и изъятое при осмотре должно быть предъявлено участникам осмотра

---

[1] Шмонин А.В., Баранов В.В. Организация выявления, раскрытия и расследование хищений денежных средств в системе дистанционного банковского обслуживания: учебно-практическое пособие / под науч. ред. доктора юридических наук, профессора А.В. Шмонина. М.: Академия управления МВД России, 2014. 312 с.

[2] Шаталов А.С. Уголовно-процессуальный кодекс Российской Федерации в схемах: учебное пособие. М.: Проспект, 2021. С. 304.

2. Обыск и выемка.

Данное следственное действие, именуемое обыском, при расследовании рассматриваемого вида преступлений носит весьма специфичный характер и является чуть ли не основным средством доказывания, который заключается в обследовании помещений (жилища). Его целью является отыскание и изъятие объектов, причинно связанных с расследуемым преступлением. Таковыми могут быть предметы электронных носителей информации, компьютерная информация, различного рода документы, например, поддельные учредительные, регистрационные, банковские карты, похищенные денежные средства.

Все вышеперечисленные обнаруженные и в последующем изъятые объекты могут быть признаны в виде источников доказательств и использованы в процессе доказывания, а также приобщения к материалам уголовного дела, что может послужить в дальнейшем его раскрытию. В ряде случаев при производстве данного следственного действия, носящего принудительный характер, могут быть обнаружены и задержаны лица, скрывающиеся от правосудия.

Отличительной особенностью обыска от выемки является то, что при производстве (осуществлении) выемки категорически запрещается ведение поисковых действий.

В ходе производства обыска и выемки все значимые объекты, которые по внутреннему убеждению сотрудников органов внутренних дел, входящих в оперативно-следственную группу, могут иметь доказательственное значение, подлежат изъятию при непосредственном участии понятых и в присутствии специалиста.

В случае поступления ходатайства от законного владельца обнаруженных и изымаемых объектов – электронных носителей информации – возможно удовлетворение его ходатайства и проведение копирования информации, но лишь в тех случаях, когда это действие не приведет к воспрепятствованию расследования преступления и не повлечет утрату или не изменит информацию. Затем сделанные копии передаются законному владельцу, а в протоколе обыска или выемки согласно ч .1 ст. 182, ч.3.1 ст. 183 УПК делается соответствующая запись.

Предлагаем рассмотреть схемы «Основания и порядок производства обыска» согласно нормам ст. 182 УПК РФ[1] (схема 4) и «Основания и порядок производства выемки» согласно нормам ст. 183 УПК[2] РФ (схема 5).

[1] Шаталов А.С. Указ. раб. С. 312.
[2] Там же. С. 315.

Схема 4

Основания и порядок производства обыска (ст. 182 УПК РФ)

Обыск производится при наличии достаточных данных полагать, что в каком-либо месте или у какого-либо лица могут находиться орудия, оборудование или иные средства совершения преступления, предметы, документы и ценности, которые могут иметь значение для дела. Обыск может производиться и в целях обнаружения разыскиваемых

↓

Обыск производится на основании постановления следователя, в жилище - на основании судебного решения

↓

До начала обыска:

Следователь предъявляет постановление или судебное решение о его производстве;

предлагает добровольно выдать подлежащие изъятию предметы, документы и ценности, которые могут иметь значение для уголовного дела;

если они выданы добровольно и нет оснований опасаться их сокрытия, то следователь **вправе не производить обыск**

↓

При производстве обыска:

могут вскрываться любые помещения, если владелец отказывается добровольно их открыть (при этом не должно допускаться не вызываемое необходимостью повреждение имущества);

следователь вправе запретить лицам, присутствующим в месте, где производится обыск, покидать его, а также общаться друг с другом или иными лицами до окончания обыска;

при производстве обыска, во всяком случае, изымаются предметы и документы, изъятые из оборота;

изъятые предметы, документы и ценности предъявляются понятым и другим лицам, присутствующим при обыске (в случае необходимости они упаковываются и опечатываются

Схема 5

Основания и порядок производства выемки
(ст.183 УПК РФ)

При необходимости изъятия определенных предметов и документов, имеющих значение для уголовного дела, и если точно известно, где и у кого они находятся, производится их выемка

↓

Порядок выемки соответствует порядку производства обыска, предусмотренному ст. 182 УПК РФ. Вместе с тем выемка предметов и документов, содержащих государственную или иную охраняемую федеральным законом тайну, предметов и документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях, а также вещей, заложенных или сданных на хранение в ломбард производится на основании судебного решения, принимаемого в порядке, установленном ст. 165 УПК РФ. На основании судебного решения, также производится выемка медицинских документов, содержащих сведения о наличии у гражданина психического расстройства, о фактах обращения за психиатрической помощью и лечении в учреждении, оказывающем такую помощь, а также иные сведения о состоянии психического здоровья, являющиеся врачебной тайной

↓

До начала выемки следователь предлагает выдать предметы и документы, подлежащие изъятию, а в случае отказа производит выемку принудительно

↓

О производстве выемки составляется протокол, форма и содержание которого идентичны с протоколом обыска.
Лицо, получившее копию протокола, дает об этом расписку.
В случае выемки заложенной или сданной на хранение в ломбард вещи в трехдневный срок производится уведомление об этом заемщика или поклажедателя

3. Назначение и производство предварительных исследований или судебных экспертиз.

В ходе раскрытия и расследования хищений денежных средств в системе дистанционного банковского обслуживания в зависимости от возникшей оперативно-розыскной и следственной ситуации могут проводиться различные виды предварительных исследований и судебных экспертиз. Они могут быть разными, но в научной литературе их называют судебными компьютерно-техническими экспертизами, которые подразделяют на:

– аппаратно-компьютерные;
– программно-компьютерные;
– информационно-компьютерные;
– компьютерно-сетевые.

Схема 6

Порядок назначения судебной экспертизы (ст. 195 УПК РФ)

Однако во всех случаях при производстве перечисленных видов исследований или экспертиз объектом исследования будет являться компьютерная информация. Она может быть в виде дампа памяти, дампа сетевого трафика, журналов регистрации событий от интернет-провайдера, журналов регистрации событий кредитной организации, предоставляющей систему ДБО, операционной системы, программного обеспечения комплектующих и периферийных устройств, прикладных программ, а также различной вспомогательной компьютерной информации, необходимой для их функционирования, различных баз данных, представленных в форматах, обеспечивающих автоматизированное хранение, поиск, обработку и передачу и т.д.

В ходе производства исследования или судебной экспертизы по хищениям денежных средств, совершаемых в системе ДБО, ключевыми вопросами, подлежащими выяснению, являются:

– установление способа хищения и определения способа доступа к компьютеру потерпевшего;

– установление сведений о лице (-ах), причастном (-ых) к хищению денежных средств, а также определение роли каждого участника;

– каким способом осуществлялось списывание денежных средств со счета потерпевшего в системе ДБО.

Предлагаем рассмотреть схему «Порядок назначения судебной экспертизы» согласно нормам ст. 195 УПК РФ[1] (схема 6).

4. Допрос.

Как нам известно, в природе раскрытия и расследования подготавливаемых или уже совершенных преступлений не существует ни одного уголовного дела, в расследовании которого не было проведено хотя бы одного допроса.

Предлагаем ознакомиться с классической схемой допроса обвиняемого. Протокол допроса обвиняемого согласно нормам ст. 174 УПК РФ должен быть оформлен следующим образом2:

1. При каждом допросе обвиняемого следователь составляет протокол с соблюдением требований ст. 190 УПК РФ.

2. В протоколе первого допроса указываются данные о личности обвиняемого:

1) фамилия, имя и отчество;

2) дата и место рождения;

3) гражданство;

4) образование;

5) семейное положение, состав его семьи;

6) место работы или учебы, род занятий или должность;

7) место жительства;

8) наличие судимости;

9) иные сведения, имеющие значение для уголовного дела.

---

[1] Шаталов А.С. Указ. Раб. С. 340.

[2] Шаталов А.С. Уголовно-процессуальный кодекс Российской Федерации в схемах: учебное пособие. М.: Проспект, 2021. С. 301.

Схема 7

Допрос обвиняемого (ст. 173 УПК РФ)[1]

Следователь допрашивает обвиняемого немедленно после предъявления ему обвинения

↓

Вначале допроса он выясняет у обвиняемого, признает ли он себя виновным, желает ли дать показания по существу предъявленного обвинения и на каком языке.
В случае отказа обвиняемого от дачи показаний следователь делает соответствующую запись в протоколе его допроса. **Повторный допрос** обвиняемого по тому же обвинению в случае его отказа от дачи показаний на первом допросе может проводиться только по просьбе самого обвиняемого

↓

Следователь свободен в выборе тактики допроса, но с условием непременного соблюдения следующих правил:

при допросе обвиняемого **недопустимо** применение насилия, угроз и иных незаконных мер, а равно создание опасности для жизни и здоровья, участвующих в нем лиц;

по инициативе следователя или по ходатайству допрашиваемого лица в ходе допроса **могут быть проведены** фотографирование, аудио- и(или) видеозапись, киносъемка, материалы которых хранятся при уголовном деле, по окончании предварительного следствия опечатываются;

обвиняемый **вправе** пользоваться документами и записями;

задавать наводящие вопросы **запрещается**

↓

До первого допроса обвиняемый вправе иметь свидания с защитником наедине и конфиденциально, без ограничения их числа и продолжительности. В случае неявки приглашенного защитника в течение 5 суток со дня заявления ходатайства о приглашении защитника дознаватель, следователь, прокурор или суд вправе предложить подозреваемому, обвиняемому пригласить другого защитника, а в случае его отказа принять меры по назначению защитника

3. В протоколах следующих допросов данные о личности обвиняемого, если они не изменились, можно ограничить указанием его фамилии, имени и отчества.

---

[1] Шаталов А.С. Уголовно-процессуальный кодекс Российской Федерации в схемах: учебное пособие. М.: Проспект, 2021. С. 300.

После ознакомления с необходимыми следственными действиями и представленными схемами полагаем перейти к тактике осуществления допроса применимо к расследованию уголовных дел по факту хищения денежных средств, совершаемых в системе ДБО.

Все виды допросов (потерпевшего, свидетеля, подозреваемого, обвиняемого) согласно существующим разработанным положениям науки криминалистики осуществляются с использованием тактических рекомендаций.[1]

Каждый из них нацелен на получение полных и правдивых показаний относительно событий, имеющих отношение к расследуемому уголовному делу. Они связаны с получением вербальной (то есть словесной) информации, интересующей следствие.

При их производстве следователь познает события, получая доказательства опосредствованно – путем передачи ему сведений другими лицами, ранее воспринимавшими те или иные факты, явления, действия.[2]

Основание и его производство урегулированы ст. 187-191 УПК РФ. Данное следственное действие по праву считается наиболее распространенным. Довольно редко возникает острая потребность в проведении следственных экспериментов. Что касается допроса, то можно безошибочно предположить, что в истории уголовного судопроизводства, пожалуй, не было ни одного расследованного уголовного дела, по которому он вообще не производился.

Допрос осуществляется по месту производства предварительного следствия.

В зависимости от складывающейся ситуации следователь вправе, если считает это необходимым, провести допрос в месте нахождения допрашиваемого (например, в жилище, по месту работы, в следственном изоляторе).

Допрос не может длиться более 4 часов. Его продолжение законом допускается после перерыва для отдыха и принятия пищи. Длительность такого перерыва составляет не менее одного часа, а общая продолжительность допроса в течение дня не должна превышать 8 часов. **Наводящие вопросы допрашиваемому лицу задавать запрещается.**

В остальном следователь свободен в выборе тактики допроса. Допрос проводится без понятых. Ход и результаты данного следственного действия отражаются в протоколе, составленном в соответствии со ст. 166 и 167 УПК РФ.

Как известно, в ходе расследования уголовных дел по факту хищений денежных средств, совершенных в системе дистанционного банковского обслуживания, возникают различные следственные ситуации.

В зависимости от возникшей обстановки для выяснения спорных и возникающих вопросов в процессе производства допросов потерпевшего и лиц, имеющих возможность доступа к компьютеру, на котором установлена система ДБО, необходимо уточнить следующее:

---

[1] Криминалистика. Полный курс: учебник для вузов / под общ. ред. А.Г. Филиппова. С. 417.

[2] Шаталов А.С., Крымов А.А. Уголовно-процессуальное право Российской Федерации: академический курс по направлению «Юриспруденция». М.: Проспект, 2018. 864 с.

– кто интересовался программным обеспечением, установленным на компьютер потерпевшего;

– в помещении, где расположен компьютер, были ли когда-либо посторонние лица;

– были ли в данном помещении посторонние лица, работающие на проверяемом компьютере и не имеющие доступа к нему;

– не зафиксированы ли случаи работы кого-либо из лиц, имеющих доступ к компьютеру, с информацией, не относящейся к их компетенции;

– как часто проверялись установленные программы на наличие вирусов и каковы были их результаты, в частности последних проверок;

– каким путем и где приобретаются проверочные программы на наличие и устранение вирусов;

– были ли зафиксированы сбои в работе компьютерного оборудования, электронных сетей и средств защиты компьютерной информации;

– имели ли место случаи неправомерного доступа к компьютерной информации ранее, если да, то как часто;

– кто еще подключен к компьютерной сети и является ее абонентом;

– каким образом осуществляется защита компьютерной информации, какие при этом средства и методы защиты применяются;

– как Вы считаете, могло ли случайно произойти списание денежных средств с банковского счета (результат Вашего неосторожного действия или неисправности работы компьютерной системы или сбоев программного обеспечения);

– были ли такие факты, как отстранение от работы лиц, имевших доступ к компьютеру потерпевшего и в том числе в результате увольнения в течение интересующего периода времени, и по каким мотивам.

Таблица 11

Оперативно-розыскные мероприятия
и первоначальные следственные действия

Номер пункта	***Первоначальные следственные действия и мероприятия***	***Подразделения ОВД, ответственные за проведение указанных действий и мероприятий***
1	Незамедлительное информирование дежурной части УМВД России по г. Энску о зарегистрированных фактах хищения денежных средств, совершенных с использованием средств мобильной (стационарной связи). Организация своевременного выезда следственно-оперативной группы (СОГ) на место происшествия.	*Дежурная часть территориального ОВД*

2	*Мероприятия, осуществляемые сотрудниками отдела уголовного розыска (ОУР):* 1) Опрос заявителя (получение информации об абонентских номерах, номерах банковских карт, интернет-страницах, используемых преступниками, с указанием точного времени поступления звонка, если звонок потерпевшим поступил на стационарный телефон, необходимо отобрать у владельца заявление с исчерпывающей информацией; 2) Полученную информацию передать дежурному сотруднику Управления уголовного розыска (УУР), отдела «К», Управления экономической безопасности и противодействия коррупции (УЭБиПК) УМВД России по Энской области; 3) Принять меры к получению детализации по абонентскому номеру потерпевшего, на который поступил звонок (через Интернет, отделение операторов связи совместно с потерпевшим), получению выписки по карте (через отделения банков по заявлению потерпевшего), сведений об интернет-страницах (приобщению копий страниц к материалу проверки), чеков денежных перечислений. 4) При получении новых сведений сотрудники, ответственные за формирование информационно-поисковой системы (ИПС), осуществляют ввод информации в базу данных (БД) и ее корректировку.	*СОГ территор. ОВД*
3	*Мероприятия, осуществляемые сотрудниками следственного отдела (СО) и отдела дознания (ОД):* 1) Осмотр места происшествия, аппарата сотовой связи, компьютерной техники, банкоматов, терминалов оплаты; изъятие документов, подтверждающих информацию о переводах денежных средств; 2) Принятие решения по обращению заявителя в порядке статей 144-145 УПК РФ; 3) Допрос заявителей, свидетелей; 4) При установлении факта незаконного списания денежных средств неустановленным способом изъять сотовый телефон (без SIM -карты) потерпевшего для направления в ЭКЦ УМВД России по Энской области для проведения компьютерной экспертизы; В рамках возбужденного уголовного дела в течение суток следователю необходимо: 1) Вынести ходатайства перед судом: - о получении информации о соединениях между абонентами и (или) абонентскими устройствами;	*СО, ОД*

	- о получении информации о движении денежных средств по расчетному банковскому счету потерпевшего, балансу абонентского номера телефона, месте фактического нахождения сотовых телефонов злоумышленников; - о наложении арестов на расчетные счета/виртуальные счета SIM-карт злоумышленников; - на проведение соответствующих ОРМ по абонентским и IMEI-номерам преступников (при необходимости); 2) Запросить информацию в кредитных организациях (банках) операторов сотовой связи, электронных платежных системах: - сведения о движении денежных средств по счетам (банковским картам) потерпевшего и преступника; - сведения о принадлежности абонентских номеров, используемых преступником; - сведения о виртуальных счетах (регистрационные данные, электронное администрирование, движение денежных средств); 3) При установлении места нахождения собственников SIM-карт и банковских карт направить поручение в соответствующие органы для полноты установления фактических обстоятельств совершенного преступления. 4) При получении новых сведений сотрудники, ответственные за формирование ИПС, осуществляют ввод информации в БД и ее корректировку. 5) Своевременное внесение необходимой информации в базу Информационного центра (ИЦ) УМВД «Дистанционные Преступления» (по примеру Энской области).	
4	*Мероприятия, осуществляемые сотрудниками отдела «К»:* 1) принять неотложные меры для оперативного получения информации об имеющихся абонентских номерах, принадлежности банковских карт (счетов), используемых злоумышленниками; движении по ним денежных средств и местах их обналичивания (номера и адреса банкоматов); при возможности использования сервисов дистанционного банковского обслуживания карты потерпевшего; детализации телефонных соединений по стационарному номеру потерпевшего, во взаимодействии с ПАО «Ростелеком»; 2) подготовить постановление о приостановлении услуг связи по установленным абонентским номерам; 3) подготовить информационное письмо в Роскомнадзор, если абонентский номер реализован без внесения сведений	*Отдел «К»*

	об абоненте или реализован с внесением недостоверных данных об абоненте; 4) передать полученную информацию дежурному сотруднику УУР, СУ, ОД УМВД. 5) При получении новых сведений сотрудники, ответственные за формирование ИПС, осуществляют ввод информации в БД и ее корректировку.	
5	*Мероприятия, проводимые Следственным управлением (СУ), ОД:* Осуществлять взаимодействие с территориальными СОГ. При необходимости осуществить выезд на место происшествия. Обеспечивать контроль за квалификацией возбужденных уголовных дел, качеством проведения следственных действий и полученных результатов, подготовкой ходатайств и получением судебных решений по установленным абонентским номерам. Подготавливать необходимые запросы в банки или иные кредитные организации. Проводить контроль за проставлением соответствующих реквизитов в статистических карточках по форме 1, заполнить реквизит № 26 согласно справочнику 12, где указать способ совершения преступления (49, 50), при использовании мошенниками сети Интернет заполнить реквизит 28, указав значение 100 и 037; - ИПК-ПР (Л), кроме основной информации заполнить способ мошенничества/кражи (реквизит 51 с указанием значения 20 (сотового телефона).	*СУ, ОД*
6	*Мероприятия, осуществляемые Управлением уголовного розыска (УУР), отделом оперативно-розыскной информации (ООРИ) БСТМ МВД России:* Осуществить контроль за проведением ОРМ и получить сведения из территориальных ОВД об абонентских номерах, банковских картах (счетах), используемых злоумышленниками, предоставить информацию дежурному сотруднику отдела «К» и УЭБиПК УМВД России по Энской области; при получении информации от сотрудника отдела «К», ООРИ осуществить проверку установленных владельцев абонентских номеров и банковских карт (счетов) по учетам информационной системы (ИС) оперативно-розыскной информации (ОРИ); полученную информацию предоставить дежурному сотруднику ОУР территориального ОВД для дальнейшего приобщения к материалам уголовного дела.	*УУР* *ООРИ БСТМ МВД России*

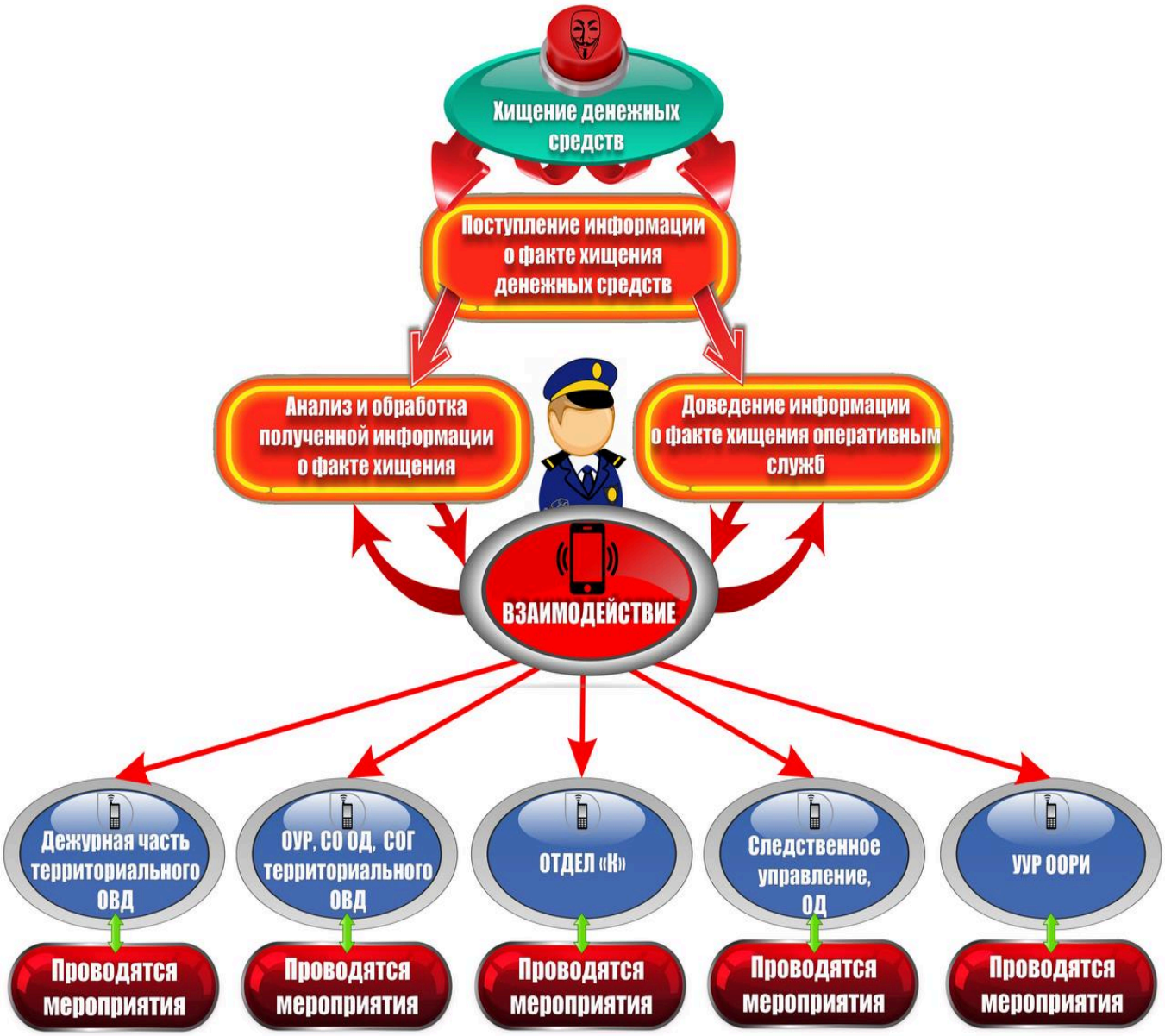


Рис. 45. Схема взаимодействия

3.5. ПРОФИЛАКТИКА ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ В СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

В целях повышения эффективности проводимых мероприятий по предупреждению и раскрытию хищений денежных средств граждан, совершаемых с использованием средств дистанционного банковского обслуживания и мобильной связи, считаем необходимым:

1. Во взаимодействии со следственными подразделениями, судебными органами и прокуратурой региона необходимо разработать проект постановления о возбуждении перед судом ходатайства на проведение оперативно-розыскных мероприятий в виде наведения справок и судебных постановле-

ний, позволяющих получить у представителей операторов связи информацию:

- принадлежность абонентского номера;
- географическое положение аппарата связи, в котором установлена и эксплуатировалась SIM-карта с абонентским номером в интересующий период времени;
- детализацию входящих и исходящих телефонных соединений за интересующий период времени; IMEI-номерах, с которыми эксплуатировалась SIM-карта;
- поступление и списание денежных средств по счету абонентского номера.

2. На базе информационных подразделений необходимо создать единый информационный банк данных указанных преступлений, в котором отражать сведения:

- о потерпевшем;
- о способе хищения денежных средств;
- об абонентских номерах;
- об электронных и банковских счетах.

3. Организовать своевременный взаимообмен информацией с региональными подразделениями УМВД России.

4. На законодательном уровне установить и ограничить сроки исполнения запросов операторам связи, провайдерам и банковским структурам, путем наделения территориальных представителей правами доступа к общим базам данных, установление ответственности за ненадлежащее исполнение, а также вменить в обязанность проведение профилактических мероприятий в адрес клиентов.

5. Постоянно осуществлять профилактическую работу по надежному обеспечению безопасного предоставления услуг дистанционного (удаленного) обслуживания (например, программное обеспечение или определенные алгоритмы) и, в случае совершения хищений, обязать банки и платежные системы возвращать клиентам денежные средства.

6. Согласовать работу определенного рода, направленную на незамедлительное получение информации о совершенных фактах нарушений и преступлений в системе дистанционного банковского обслуживания за конкретный период времени. Исходя из полученных сведений о складывающейся ситуации, осуществлять глубокий анализ криминогенной обстановки и вносить корректировку в действующую систему дистанционного банковского обслуживания населения.

7. Проработать вопрос о расширении страховых услуг денежных средств, находящихся на счетах клиентов организаций, оказывающих банковские услуги.

8. Размещать информацию о фактах мошеннических действий, совершенных с использованием аппаратов сотовой связи (стикеры, баннеры), в организациях, осуществляющих работу с гражданами (РЭУ, пенсионные фонды,

дома культуры, органы соцзашиты и т.д.), на объектах общего пользования (отделения банков, магазины, торговые центры, кафе и т.д.). Данные профилактические мероприятия должны носить в зависимости от возникшей ситуации «адресный» характер и охватывать все слои населения, включая наиболее уязвимые группы.

9. Зональным оперативным сотрудникам, обеспечивающим безопасность дистанционного банковского обслуживания населения, проводить на закрепленных административных участках профилактическую работу, направленную на подробное разъяснение современных способов совершения преступлений, связанных с хищением денежных средств в системе ДБО.

10. Доведение информации гражданам через сотрудников банков о необходимости разъяснения своим клиентам сведений о совершаемых мошенничествах с использованием аппаратов сотовой связи и банковских карт.

11. Постоянно осуществлять размещение статей во всевозможных печатных изданиях и Интернете о современных способах мошенничества и других видов преступлений, связанных с дистанционным банковским обслуживанием и совершенных с использованием аппаратов сотовой связи и банковских карт.

Контрольные вопросы

1. Укажите статьи УК РФ, квалифицирующие хищения денежных средств в системе ДБО.
2. Перечислите нормативные акты, необходимые при квалификации хищений денежных средств в системе ДБО.
3. Что является особенностью объекта и объективной стороны при совершении хищений денежных средств в системе ДБО?
4. Что является окончанием совершения хищений денежных средств в системе ДБО?
5. В чем заключается сущность криминалистической характеристики хищений денежных средств в системе ДБО?
6. Назовите систему криминалистической характеристики хищений денежных средств в системе ДБО?
7. Какие Вы знаете средства хищений денежных средств в системе ДБО?
8. Назовите типичный состав преступной группы, совершающий хищения денежных средств в системе ДБО?
9. В чем заключается сущность способа хищений денежных средств в системе ДБО и какова его структура?
10. Какие Вы знаете способы совершения хищений денежных средств в системе ДБО?
11. Какие Вы знаете способы сокрытия хищений денежных средств в системе ДБО
12. Из каких операций состоит технология обналичивания хищений денежных средств в системе ДБО?
13. Назовите алгоритм действий при организации выявления хищений денежных средств в системе ДБО на стадии возбуждения уголовного дела.
14. В чем сущность криминалистической характеристики хищений денежных средств в системе ДБО?
15. Назовите типичный состав преступной группы, совершающей хищения денежных средств в системе ДБО.
16. Перечислите способы совершения хищений денежных средств в системе ДБО.
17. Перечислите операции и технологии обналичивания хищений денежных средств в системе ДБО.
18. Какие существуют способы подготовки хищений денежных средств в системе ДБО?
19. Что является основанием для проведения 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.

20. Перечислите нормативные документы и назовите Инструкцию по организации информационного обеспечения сотрудничества по линии Интерпола при ситуации выявления фактов трансграничных хищений денежных средств в системе ДБО.

21. Перечислите типичные виды ОРМ, осуществляемые при раскрытии и документировании преступных действий лиц, совершающих хищения денежных средств в системе ДБО.

22. Какие факторы оказывают влияние на характер следственной ситуации первоначального этапа расследования хищения денежных средств в системе ДБО?

23. Перечислите типичные следственные ситуации, возникающие в ходе расследования хищения денежных средств в системе ДБО.

24. В чем заключается особенность производства и тактики следственных действий при расследовании хищений денежных средств в системе ДБО?

25. В чем заключается особенность производства и тактика осмотра места происшествия при расследовании хищений денежных средств в системе ДБО?

26. В чем заключается особенность производства и тактики обыска, а также выемки при расследовании хищений денежных средств в системе ДБО? На какие объекты необходимо обращать особое внимание?

27. Перечислите виды предварительного исследования и судебных экспертиз, производимых при расследовании хищений денежных средств в системе ДБО.

28. В чем заключается особенность допросов подозреваемых (обвиняемых) в ходе расследования хищений денежных средств в системе ДБО?

29. На что может целенаправить знание криминалистической характеристики хищений денежных средств в системе ДБО в ходе раскрытия преступлений данной категории?

30. Какие нормы законов необходимо знать должностному лицу при раскрытии и расследовании хищений денежных средств, совершаемых в системе ДБО?

ГЛАВА IV
ОБЗОР ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СФЕРЫ ТЕЛЕКОММУНИКАЦИЙ И КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В связи с интенсивным развитием информационных технологий, средств связи, банковских услуг, в том числе электронных платежей и внедрением их в повседневную жизнь происходит адаптация схем преступных деяний, направленных на завладение денежными средствами граждан. Наиболее распространенными являются мошеннические действия, совершенные с использованием средств проводной и сотовой связи.

Приведем (рассмотрим) пример из Н-ской области.

По результатам проведенного анализа материалов возбужденных уголовных дел (совместно с УМВД и СУ УМВД) установлено, что в 2018 году на территории Н-ской области было зарегистрировано 792 факта хищения денежных средств мошенническим путем с использованием средств проводной, сотовой связи и сети Интернет.

Наиболее распространенными схемами являются:

– вредоносное программное обеспечение телефонного аппарата на операционной системе «Android» (129 фактов – 16%);

– получение звонков, SMS– сообщений «Ваша карта заблокирована» (118 фактов – 15%);

– размещение объявления в сети Интернет (потерпевший/преступник) (395 фактов – 50%);

– ложная информация – компенсация за «БАДы», «Молитвы», «Экстрасенсы», «Бонусы к пенсии» (47 фактов – менее 6%);

– преступник из окружения потерпевшего получил доступ к карте или потерпевший потерял карту (13 фактов – менее 2%).

Проанализировав ежемесячные сборники «Состояния преступности в России за 2020 год», можно сделать вывод, что злоумышленниками использовались SIM-карты, принадлежащие номерным емкостям филиалов операторов сотовой связи **следующих субъектов Российской Федерации**:

1. г. Москва и Московская область – 185 фактов;
2. г. Санкт Петербург и Ленинградская область – 77 фактов;
3. Самарская область – 67 фактов;
4. Челябинская область – 61 факт;
5. Тульская область – 46 фактов;
6. Свердловская область – 38 фактов;
7. Краснодарский край – 35 фактов;
8. Республика Татарстан – 31 факт;
9. Кемеровская область – 28 фактов;
10. Новосибирская область – 27 фактов;

11. Республика Башкортостан – 26 фактов;
12. Ростовская область – 23 факта;
13. Липецкая область – 20 фактов;
14. Пермский край – 15 фактов;
15. Курганская область – 15 фактов;
16. Белгородская область – 14 фактов;
17. Волгоградская область – 14 фактов;
18. Оренбургская область – 13 фактов;
19. Красноярский край – 12 фактов;
20. Ивановская область – 10 фактов.

Для более наглядного и глубокого понимания складывающейся криминогенной обстановки на территории Российской Федерации приводим сводные данные о преступлениях, совершенных в системе дистанционного банковского обслуживания с использованием компьютерных технологий.

Таблица 12

Динамика краж, совершенных с использованием компьютерных технологий на территории Российской Федерации с 2016 по 2020 гг.

Годы	Количество краж, уголовные дела о которых находились в производстве	В том числе количество преступлений			
		Количество краж, зарегистрированных в отчетном периоде	Из них выявлено сотрудниками подразделений СТМ	По которым установлены лица сотрудниками подразделений СТМ	Уголовные дела, о которых прекращены по реабилитирующим основаниям
2016	2104	1766	901	758	63
2017	2412	1911	1103	826	70
2018	2681	2015	1292	912	78
2019	4173	3891	2994	1512	133
2020	4357	4120	3821	1912	175

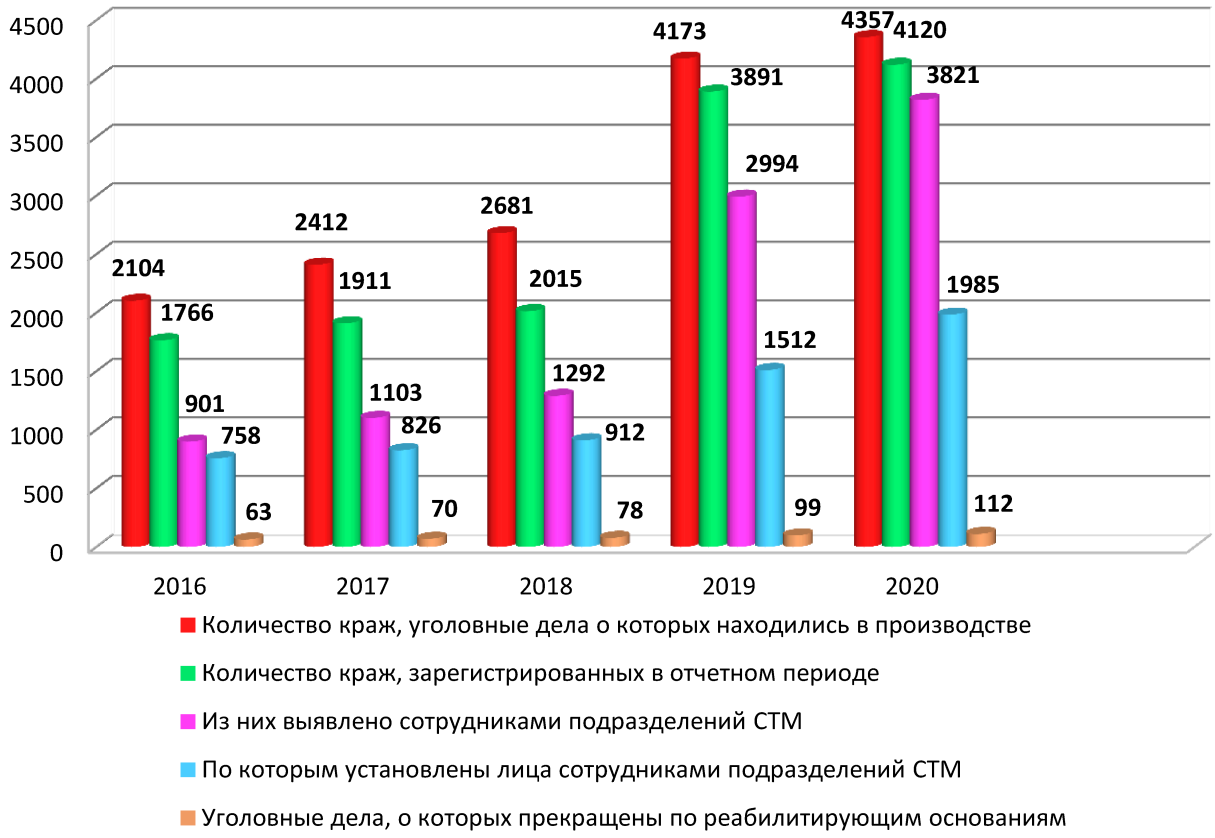


Диаграмма 12. Динамика краж, совершенных с использованием компьютерных технологий на территории России с 2016 по 2020 гг.

Таблица 13

Динамика краж, в том числе количество преступлений с использованием компьютерных технологий и движение уголовных дел

Годы	В том числе количество преступлений, уголовные дела о которых				
	Закончены расследованием либо разрешены в отчетном периоде	Из них		Приостановлены за нерозыском лица либо в случае неустановления лица, совершившего преступление	Из них должностными лицами ОПС ОВД
		Направлено в суд	В том числе должностными лицами ОПС ОВД		
2016	1052	883	721	740	494
2017	1206	956	883	925	617
2018	1341	1008	998	1157	772
2019	2035	1234	1176	1287	912
2020	1985	1347	1311	1395	953

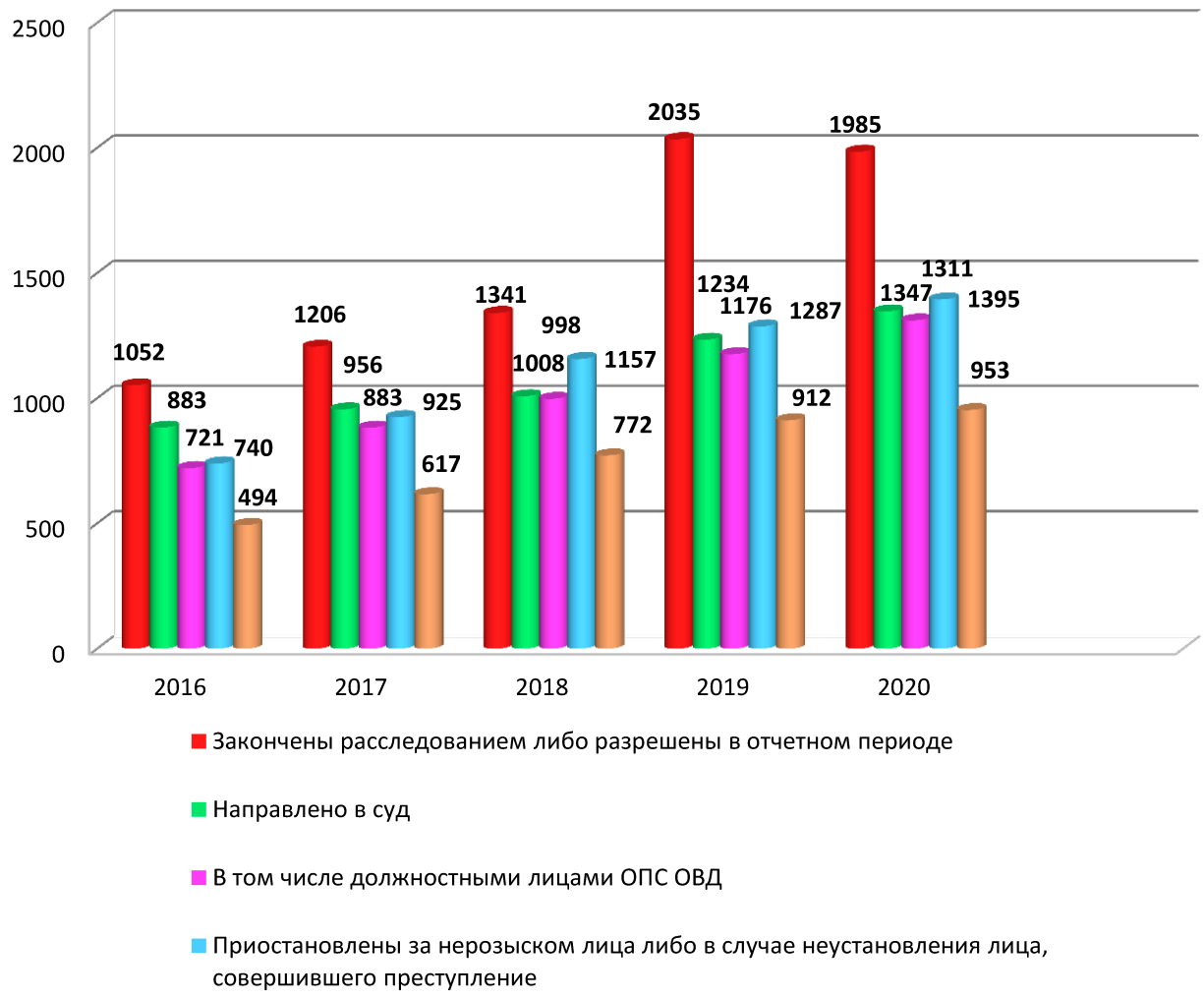


Диаграмма 13. Динамика краж, в том числе количество преступлений с использованием компьютерных технологий и движение уголовных дел

На представленной ниже диаграмме видно, какой процент от общего количества уголовных дел, по которым лица, совершившие преступления, установлены сотрудниками подразделений СТМ, составляют уголовные дела, прекращенные по реабилитирующим основаниям. Таким образом, из этого следует, что в более чем в 90% случаев выявленные сотрудниками ПСТМ и подозреваемые в совершении преступлений лица в последующем несут наказание, соответствующее нормам уголовно-процессуального законодательства (см. диаграмму 14).

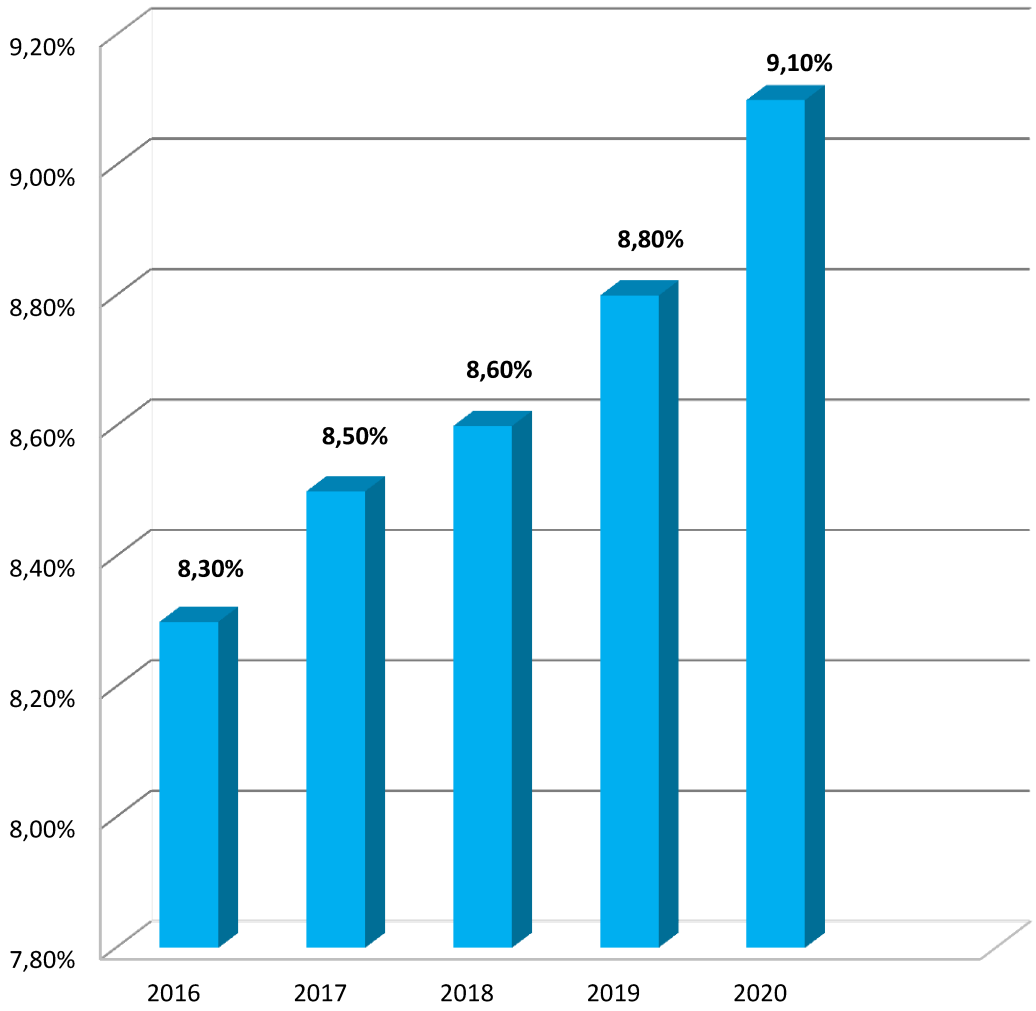


Диаграмма 14. Удельный вес уголовных дел, прекращенных по реабилитирующим основаниям,[1] %

Таблица 14

Динамика уголовных дел в 2016-2020 гг.

Годы	Количество краж, уголовные дела о которых находились в производстве	Закончены расследованием либо разрешены в отчетном периоде	Направлено в суд	Приостановлены за неразыском лица, либо в случае неустановления лица, совершившего преступление
2016	2104	1052	883	740
2017	2412	1206	956	925
2018	2681	1341	1008	1157
2019	4173	2035	1234	1287
2020	4357	1985	1347	1395

[1] *Из числа дел, по которым лица, совершившие преступления данной категории на территории Российской Федерации, установлены сотрудниками подразделений СТМ в 2016-2020 гг.).*

Из следующей диаграммы видно, что количество краж с использованием компьютерных технологий с каждым годом увеличивается.

Диаграмма 15. Динамика уголовных дел в 2016-2020 гг.

Таблица 15

Удельный вес уголовных дел в 2016-2020 гг., %

Год	Количество краж, уголовные дела о которых находились в производстве	Закончены расследованием либо разрешены в отчетном периоде		Приостановлены за нерозыском лица, либо в случае неустановления лица, совершившего преступление	
		Количество	Удельный вес	Количество	Удельный вес
2016	2104	1052	50,00%	740	35,20%
2017	2412	1206	50,00%	925	38,30%
2018	2681	1341	50,01%	1157	43,15%
2019	4173	2035	48,76%	1287	30,84%
2020	4357	1985	45,55%	1395	32,00%

На диаграмме ниже видно, что количество уголовных дел, законченных расследованием либо разрешенных в отчетном периоде, составляет примерно половину от всех уголовных дел, находящихся в производстве. Количество

приостановленных за нерозыском лица, либо в случае неустановления лица, совершившего преступление, составляет около одной трети от всех уголовных дел, находящихся в производстве (см. диаграмму 16).

Диаграмма 16. Удельный вес уголовных дел в 2016-2020 гг., %

Таблица 16

Динамика мошенничеств (ст. 159 УК), совершенных с использованием компьютерных технологий на территории Российской Федерации в 2008-2019 гг.

Годы	Количество мошенничеств, уголовные дела о которых находились в производстве	в том числе количество преступлений			
		количество мошенничеств, зарегистрированных в отчетном периоде	из них	по которым установлены лица сотрудниками подразделений СТМ	уголовные дела, о которых прекращены по реабилитирующим основаниям
			выявлено сотрудниками подразделений СТМ		
2008	897	760	430	260	9
2009	1219	1078	697	370	22
2010	1199	1010	537	190	127
2011	1819	1527	910	582	85
2012	2049	1805	1319	672	99
2013	3148	2748	1399	508	195
2014	2805	2196	1033	459	457
2015	2917	2071	1180	525	402
2016	3058	2172	1238	550	357
2017	3189	2265	1291	574	426
2018	3274	2325	1325	589	548
2019	3356	2475	1399	631	656

Диаграмма 17. Динамика мошенничеств (ст. 159 УК), совершенных с использованием компьютерных технологий на территории Российской Федерации в 2008-2019 гг.

Таблица 17

Динамика мошенничеств с использованием компьютерных технологий и движение уголовных дел в 2008-2019 гг.

Годы	в том числе количество преступлений, уголовные дела о которых				
	Закончены расследованием либо разрешены в отчетном периоде	из них		приостановлены за нерозыском лица либо в случае неустановления лица, совершившего преступление	из них должностными лицами ОПС ОВД
		направлено в суд	в том числе должностными лицами ОПС ОВД		
2008	579	517	435	176	150
2009	717	671	516	237	156
2010	611	597	513	329	290
2011	1019	998	865	404	338
2012	972	957	903	630	504
2013	1333	1255	1134	1113	855
2014	782	665	592	1318	1085
2015	1420	1302	1152	1567	1345
2016	1123	1045	985	1754	1568
2017	987	846	749	1967	1754
2018	1210	1096	957	2015	1865
2019	1513	1421	1233	2312	2001

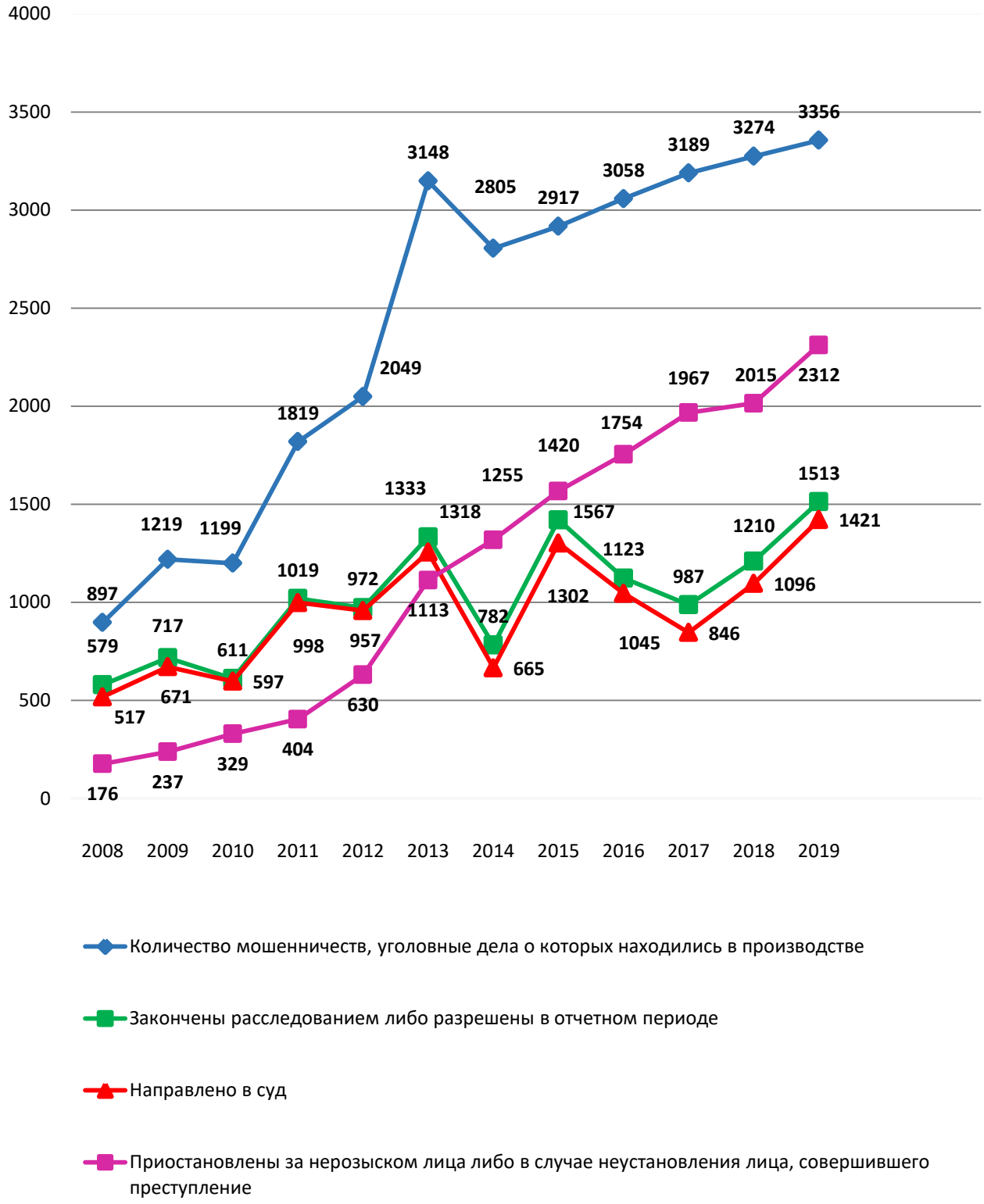


Диаграмма 18. Динамика преступлений в 2008-2019 гг.

Таблица 18

Удельный вес мошенничеств с использованием компьютерных технологий в 2008-2019 гг., %

годы	Количество мошенничеств, уголовные дела о которых находились в производстве	Выявлено сотрудниками подразделений СТМ	
		Количество	Удельный вес
2008	897	430	47,9%
2009	1219	697	57,2%
2010	1199	537	44,8%
2011	1819	910	50,0%
2012	2049	1319	64,4%
2013	3148	1399	44,4%
2014	2805	1033	36,8%
2015	2917	1180	40,5%
2016	3058	1238	40,5%
2017	3189	1291	40,5%
2018	3274	1325	40,5%
2019	3356	1399	41,6%

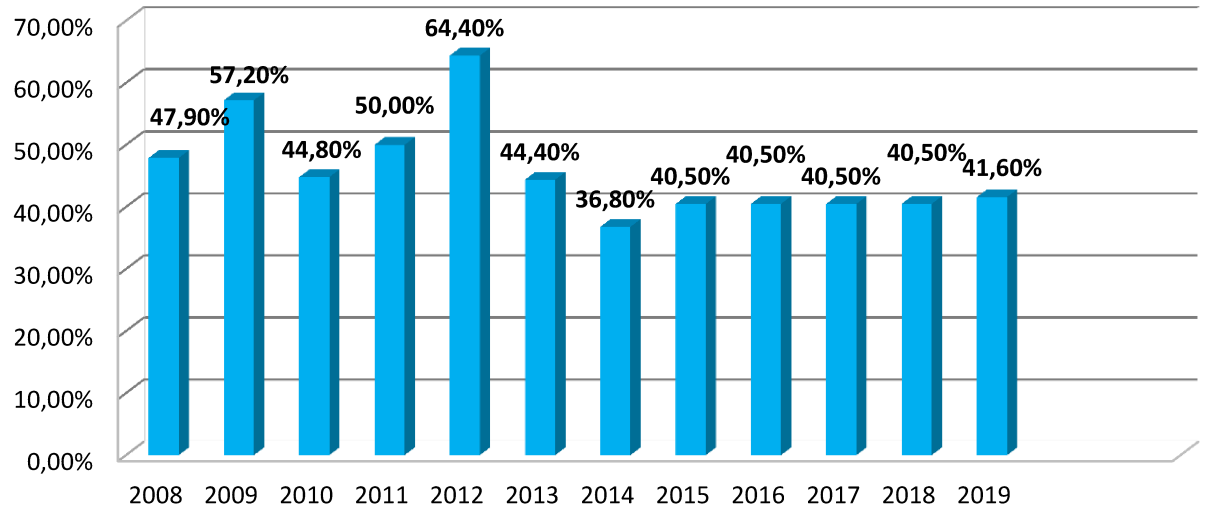


Диаграмма 19. Удельный вес мошенничеств с использованием компьютерных технологий в 2008-2019 гг., %

Таблица 19

Удельный вес прекращенных уголовных дел по реабилитирующим основаниям в 2008-2019 гг., %

Годы	Количество мошенничеств, уголовные дела о которых находились в производстве	Уголовные дела, прекращенные по реабилитирующим основаниям	
		Количество	Удельный вес
2008	897	9	1,0%
2009	1219	22	1,8%
2010	1199	127	10,6%
2011	1819	85	4,7%
2012	2049	99	4,8%
2013	3148	195	6,2%
2014	2805	457	16,3%
2015	2917	402	13,8%
2016	3058	357	11,7%
2017	3189	426	13,4%
2018	3274	548	16,7%
2019	3356	656	19,5%

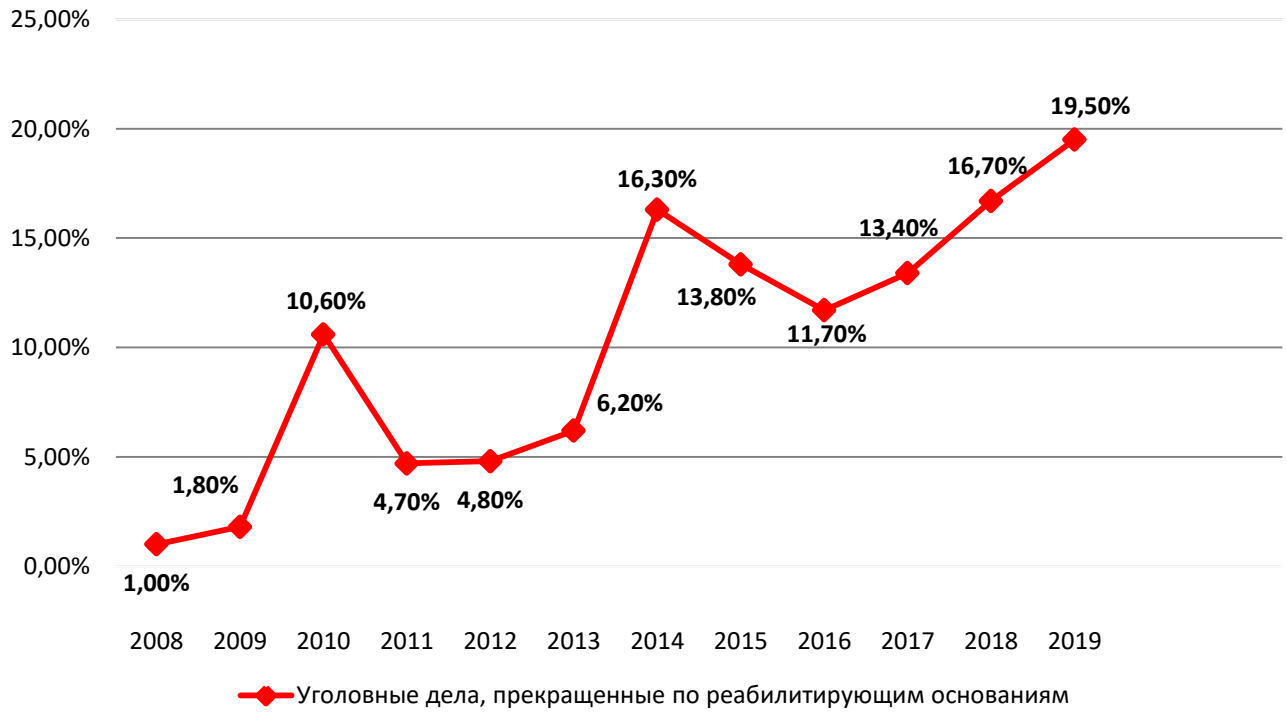


Диаграмма 20. Удельный вес прекращенных уголовных дел по реабилитирующим основаниям в 2008-2019 гг, %

Таблица 20

Удельный вес уголовных дел в 2008-2019 гг., в %

Годы	Количество мошенничеств, уголовные дела о которых находились в производстве	Закончены расследованием либо разрешены в отчетном периоде		Приостановлены за нерозыском лица либо в случае неустановления лица, совершившего преступление	
		Количество	Удельный вес	Количество	Удельный вес
2008	897	579	64,5%	176	19,6%
2009	1219	717	58,8%	237	19,4%
2010	1199	611	51,0%	329	27,4%
2011	1819	1019	56,0%	404	22,2%
2012	2049	972	47,4%	630	30,7%
2013	3148	1333	42,3%	1113	35,4%
2014	2805	782	27,9%	1318	47,0%
2015	2917	1420	48,7%	1567	53,7%
2016	3058	1123	36,7%	1754	57,4%
2017	3189	987	31,0%	1967	61,7%
2018	3274	1210	37,0%	2015	61,5%
2019	3356	1513	45,0%	2312	68,8%

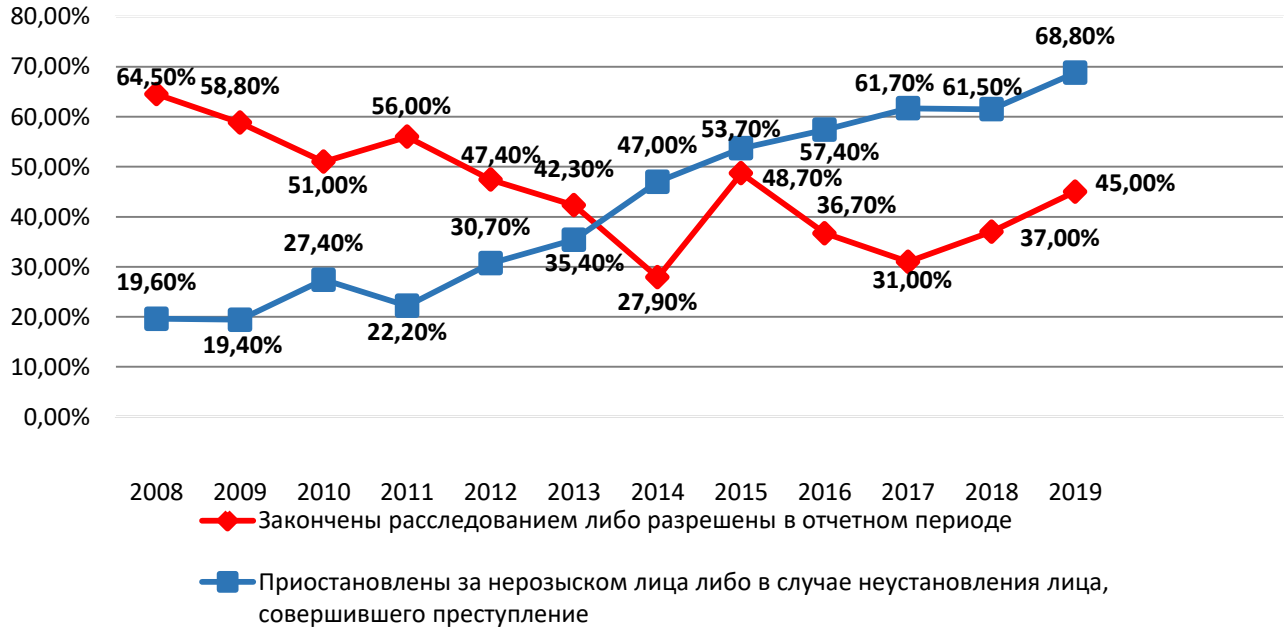


Диаграмма 21. Удельный вес уголовных дел в 2008-2019 гг., %

Таблица 21

Удельный вес уголовных дел, направленных в суд в 2008-2019 гг., %

Годы	Количество мошенничеств, уголовные дела о которых находились в производстве	Направлено в суд	
		Количество	Удельный вес
2008	897	517	57,6%
2009	1219	671	55,0%
2010	1199	597	49,8%
2011	1819	998	54,9%
2012	2049	957	46,7%
2013	3148	1255	39,9%
2014	2805	665	23,7%
2015	2917	1302	44,6%
2016	3058	1045	34,2%
2017	3189	846	26,5%
2018	3274	1096	33,5%
2019	3356	1421	42,3%

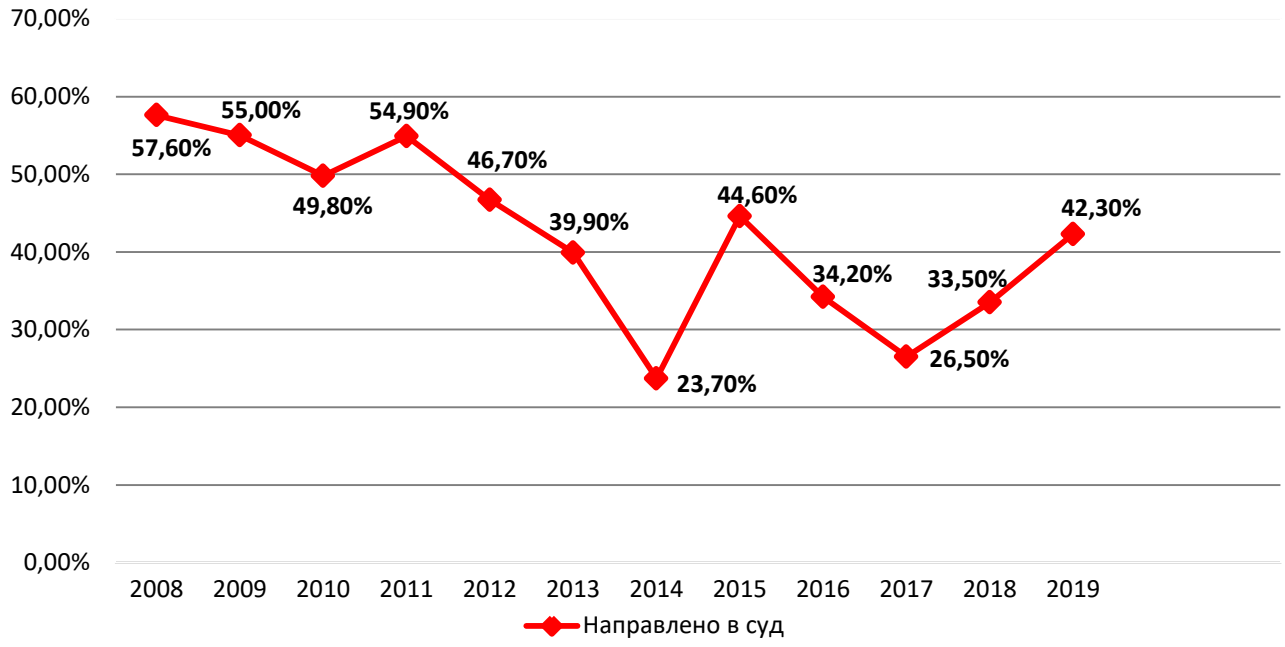


Диаграмма 22. Удельный вес уголовных дел, направленных в суд в 2008-2019 гг., %

ЗАКЛЮЧЕНИЕ

Свобода проявлений себя в информационном пространстве позволяет преступным элементам действовать дерзко и безбоязненно, в связи с чем возможно утверждать, что информатизация общества, обладая, несомненно, множеством позитивных качеств, привела и к информатизации криминальной среды, придала ей ярко выраженный интернациональный и высокотехнологичный характер. Лица, склонные к совершению вышеуказанных преступлений, используют возможности информационно-телекоммуникационных систем, что способствует расширению транснационального масштаба, и, как результат, в конечном итоге определяют и создают угрозу национальной безопасности.[1]

На протяжении многих лет сотрудники органов внутренних дел ведут упорную борьбу, направленную на своевременное предупреждение, выявление, раскрытие и успешное расследование преступлений, совершаемых с использованием возможностей сферы телекоммуникаций и компьютерной информации.

Зачастую данный вид преступлений носит латентный характер. Способы совершения преступлений постоянно видоизменяются, в механизм совершения преступлений вносятся новые ухищрения, в связи с чем раскрытие указанных преступлений становится затруднительным. Такое положение требует от сотрудников правоохранительных органов своевременного получения специальных знаний, умений и навыков в указанной сфере.

Для решения данной задачи необходимо постоянно вести активную работу по подготовке учебно-методических материалов с освещением практического опыта раскрытия рассматриваемых видов преступлений, что благоприятно будет сказываться на профессиональных компетенциях сотрудников органов внутренних дел.

Преступления, совершаемые в сфере телекоммуникаций и компьютерной информации, в большинстве случаев носят корыстный характер. Все чаще мы сталкиваемся с таким распространенным видом преступлений, как мошенничество, которое в настоящее время практически каждый день совершается разными ухищренными способами.

Преступления, совершаемые в этой сфере, позволяют преступникам анонимизироваться. Высокая степень анонимности, обеспечиваемая возможностями глобальной сети Интернет, может существенно облегчить обман предполагаемой жертвы и последующее завладение ее имуществом.

Выбор именно этой разновидности преступлений обусловлен широким распространением мошенничества, многообразием способов его совершения и другими факторами. Мошенники всегда имеют желание максимально обо-

[1] Алескеров В.И., Баранов В.В. Телекоммуникация и киберпространство как средство преступлений экстремистской и террористической направленности//Труды Академии управления МВД России. 2020, №1 (53). С. 104-113.

гатиться в минимальные сроки и без финансовых затрат. В связи с этим единственно верным выходом из такой ситуации будет своевременное, постоянное, максимально полное и эффективное информирование о предполагаемой опасности быть обманутым. Данное информирование должно проходить в рамках правоохранительной деятельности наряду:

- с эффективным проведением профилактической работы, направленной на предупреждение рассматриваемой категории преступлений;
- со своевременным обнаружением преступлений;
- с качественным расследованием преступлений;
- с постоянным информированием населения о результатах деятельности правоохранительных органов по предупреждению и недопущению преступлений;
- с постоянной работой, направленной на более эффективное сотрудничество со средствами массовой информации.

Результаты такой деятельности обеспечат пользователям максимальную безопасность в глобальной сети Интернет.

Информационная среда, в том числе и глобальная сеть Интернет, является сложной технологической системой. Раскрытие преступления как факта его совершения и дальнейшее успешное расследование преступлений в сети Интернет требует от субъекта расследования не только юридических, но и обширных специальных знаний в области информационно-телекоммуникационных технологий, а также новых алгоритмов действий сотрудников органов внутренних дел.

Раскрытие данного вида преступлений всегда зависит от своевременно полученной информации, способа совершения преступления, профессионализма сотрудников и тесного взаимодействия структурных подразделений Министерства внутренних дел с другими правоохранительными органами и ведомствами.

Одновременно с высокими темпами развития общества и расширением сфер его жизнедеятельности все большее внимание уделяется использованию возможностей сферы телекоммуникаций и компьютерной информации, количество пользователей этой сферы растет с каждым годом. В связи с этим возникают и проблемы, которые носят циклический характер, что создает благоприятную основу для совершения новых видов преступлений.

В настоящее время, на наш взгляд, можно выделить следующие основные проблемы, связанные с расследованием различных видов преступлений, совершаемых с помощью глобальной сети Интернет:

1. Недостаточно высокая квалификация лиц, занимающихся расследованием данных преступлений.

2. Недостаток практики расследования некоторых видов интернет-мошенничеств.

3. Относительно большое количество преступлений, остающихся нераскрытыми.

4. Недостаточное количество комментариев специалистов на некоторые проблемные вопросы расследования мошенничеств, совершенных с использованием сети Интернет.

Исходя из выше изложенного, можно сказать, что борьба с мошенничеством, совершаемым с использованием сферы телекоммуникаций и компьютерной информации, с каждым днем все более усложняется. Возникающие оперативно-розыскные и следственные ситуации требуют от должностных лиц высокого профессионализма. Для разрешения этих обстоятельств требуется серьезный подход, и имеющаяся статистика о раскрытии данных видов преступлений говорит о том, что сотрудники органов внутренних дел с ними успешно справляются.

Все чаще через средства массовой информации населению доводятся сведения о новых способах совершения преступлений по фактам мошенничеств, о раскрытии преступлений, совершенных организованными преступными группами, и причиненном ущербе. Данная профилактическая работа положительно сказывается на отношении населения к использованию возможностей современных информационных технологий.

Помимо рассматриваемого вида преступлений такого, как мошенничество, набирают обороты и преступления, совершаемые в системе дистанционного банковского обслуживания.

Анализируя и обсуждая актуальные вопросы, наиболее часто встречающиеся в ходе своевременного раскрытия и дальнейшего успешного расследования преступлений, совершаемых в системе дистанционного банковского обслуживания, необходимо:

1. Постоянно повышать свой уровень профессиональных знаний, касающихся непосредственных особенностей организационного, технического и правового обеспечения раскрытия и расследования преступлений.

2. Постоянно изучать не только нормы уголовного права, уголовного процесса, новейшие достижения науки криминалистики, но и других смежных наук, дающие ответы на сложные вопросы, возникающие в ходе раскрытия рассматриваемой категории преступлений.

3. Постоянно быть в курсе последних нововведений и положений, отраженных в законодательстве банковского, гражданского, информационного, корпоративного права и других смежных отраслей знаний.

4. Своевременно получать информацию об организации и технологии обеспечения ДБО, что положительно будет способствовать раскрытию преступлений, совершаемых в системе ДБО.

5. С целью недопущения пробелов в работе постоянно изучать положения решений Пленумов Верховного Суда Российской Федерации о практике рассмотрения уголовных дел по фактам хищения денежных средств в системе ДБО для получения полной информации о ситуации, складывающейся в настоящее время.

6. Активизировать взаимодействие между регионами Российской Федерации, а также с зарубежными государствами по раскрытию преступлений, совершаемых в системе ДБО.

7. Рассматриваемые виды преступлений в большинстве случаев имеют транснациональный характер. Зачастую, они начинаются в одном регионе того или иного государства, имеют свое продолжение в другой стране, а заканчиваются в третьей. В этих ситуациях разоблачение организованной преступной группы может быть проблематичным. Одной из таких проблем являются различия в национальных уголовных и уголовно-процессуальных законодательствах тех или иных зарубежных государств, что препятствует привлечению к уголовной ответственности лиц, причастных к совершению преступлений.

В связи с изложенным, необходимо принять неотложные меры по урегулированию законодательства в сфере противодействия преступлениям, совершаемым с использованием возможностей телекоммуникаций и компьютерной информации, на международном уровне.

Предложенные меры и сделанные выводы по ключевым вопросам раскрытия и расследования преступлений в сфере телекоммуникаций и компьютерной информации, по нашему мнению, окажут существенную помощь в борьбе с преступностью.

Представленное учебно-практическое пособие позволит сотрудникам органов внутренних дел, призванным по своим функциональным обязанностям раскрывать и расследовать преступления, совершаемые с использованием возможностей сферы телекоммуникаций и компьютерной информации, в достаточном объеме иметь представление о складывающейся криминогенной обстановке. Собранные наработки, взятые из практической деятельности сотрудников правоохранительных органов, касающиеся отечественного и зарубежного опыта борьбы с преступлениями в сфере телекоммуникаций и компьютерной информации, будут способствовать эффективному раскрытию преступлений данного вида.

Авторский коллектив учебно-практического пособия выражает свою глубокую признательность и благодарность в оказании помощи по сбору материалов сотрудникам БСТМ МВД России, территориальных ПСТМ, Академии управления МВД России, Национального исследовательского университета «Высшая школа экономики», а также слушателям, проходившим в разные периоды обучение на кафедре ОТМ ОВД ВИПК МВД России.

ТЕСТОВЫЕ ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ

1. Чем вызвана необходимость установления уголовной ответственности за причинение вреда в связи с незаконным использованием компьютерной информации?

а) возрастающим значением ЭВМ во многих сферах деятельности современного общества;

б) возрастающим значением и широким применением ЭВМ во многих сферах деятельности современного общества;

в) широким применением ЭВМ во многих сферах деятельности современного общества;

г) меняющимся значением и узким применением ЭВМ во многих сферах деятельности современного общества.

2. Какая информация является наиболее уязвимой?

а) графическая;

б) компьютерная;

в) текстовая;

г) звуковая.

3. Что такое «компьютерная информация»?

а) организационно упорядоченная совокупность сведений (сообщений, данных), зафиксированных на машинном носителе;

б) информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ;

в) организационно упорядоченная совокупность сведений (сообщений, данных), зафиксированных на машинном носителе либо в информационно-телекоммуникационной сети с реквизитами, позволяющими их идентифицировать, имеющую собственника либо иного законного владельца;

г) организационно упорядоченная совокупность сведений (сообщений, данных), зафиксированных в информационно-телекоммуникационной сети с реквизитами.

4. Выберите вид преступления, связанного с противоправным вмешательством в работу ЭВМ:

а) изменения в программной части компьютера;

б) изменения в аппаратной части компьютера;

в) хищение, уничтожение и подделка компьютерной информации;

г) нарушение авторских прав.

5. Какое специализированное подразделение было создано для борьбы с преступлениями в сфере компьютерной информации?

а) управление «К» ГУУР МВД России;
б) управление «К» ГУЭБиПК МВД России;
в) управление «К» БСТМ МВД России;
г) управление «К» ГУСБ МВД России.

6. Что является немаловажным значением в раскрытии любого вида компьютерного преступления?
а) характерологическая особенность психологии личности преступника;
б) субъективная особенность личности преступника;
в) психологический профиль преступника;
г) психологические свойства преступника.

7. Что такое «информация» согласно Федеральному закону от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»?
а) обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств;
б) сведения (сообщения, данные) независимо от формы их представления;
в) сигнал (сообщение), устраняющий или снижающий неопределенность;
г) воспринимаемая живым организмом через органы чувств окружающая действительность в виде распределения материи и энергии во времени и в пространстве и процессов их перераспределения.

8. Назовите нормативный документ, в котором заложены основополагающие принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.
а) Федеральный закон от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и о защите информации»;
б) Федеральный закон от 15 июня 2005 г. № 148 «Об информации, информационных технологиях и о защите информации»;
в) Федеральный закон от 01 декабря 2003 г. № 156 «Об информации, информационных технологиях и о защите информации»;
г) Федеральный закон от 15 мая 2007 г. № 124 «Об информации, информационных технологиях и о защите информации».

9. Что такое «телекоммуникационные сети»?
а) сети обмена и распределенной обработки информации; средства передачи и обработки информации ориентированы в них на коллективное использование общесетевых ресурсов – аппаратных, информационных, программных;

б) технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

в) технические механизмы (средства) и устройства информационного обмена, при помощи которых субъекты информационного права могут «обмениваться» информацией и «обращать» информацию в пространстве и времени через каналы электросети (электросвязи), представляющие собой технологические (технологичные) системы с различными видами передач (цифровое телевидение, различные виды работы в Интернете, факсимильная, телеграфная, телефонная и др., включая обмен информацией между ЭВМ и другие виды документальных сообщений);

г) коммуникационные сети, в которых продуктом генерирования, переработки, хранения и использования является информация.

10. Что включает в себя понятие «компьютерная информация»?

а) информация, циркулирующая в компьютере;

б) совокупность сведений, представляющих особую ценность для государства, общества и отдельных граждан, производство, хранение и использование которых осуществляется посредством компьютерной техники

в) информация, содержащая сведения, составляющие государственную или коммерческую тайну, сведения конфиденциального характера и общего пользования;

г) информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ.

11. В каком году было создано специализированное подразделение по борьбе с преступлениями в сфере компьютерной информации?

а) 1992;

б) 1994;

в) 2001;

г) 2011.

12. Какие криминалистические особенности имеют преступления, совершаемые в телекоммуникационных сетях?

а) отсутствие следов преступления;

б) простое и быстрое преобразование из одной объектной формы в другую, возможность сохранения в первоисточнике;

в) отсутствие возможности преобразования из одной объектной формы в другую, возможность сохранения в первоисточнике;

г) отсутствие возможности сохранения в первоисточнике.

13. В какой главе УК РФ отражены статьи, относящиеся к преступлениям, совершаемым в сфере компьютерной информации?

а) 27;
б) 28;
в) 29;
г) 30.

14. Перечислите номера статей, относящиеся к преступлениям, совершаемым в сфере компьютерной информации.
а) Статья 157, Статья 158, Статья 159;
б) Статья 282, Статья 283, Статья 284;
в) Статья 251, Статья 252, Статья 253;
г) Статья 272, Статья 273, Статья 274.

15. Какие некоторые характерные особенности включают в себя преступления, совершаемые в телекоммуникационных сетях?
а) неоднородность объекта посягательства;
б) выступление телекоммуникационной информации, как в качестве объекта, так и в качестве средства преступления;
в) многообразие предметов и средств преступного посягательства;
г) выступление ИТКС либо в качестве предмета, либо в качестве средства совершения преступления.

16. Дайте определение понятию «преступление, совершаемое в телекоммуникационных сетях», исходя из его особенностей.
а) предусмотренное уголовным законом общественно опасное действие;
б) предусмотренное административным законодательством малозначительное преступление;
в) предусмотренное уголовным законом общественно опасное деяние, не относящееся к категории тяжких или особо тяжких;
г) предусмотренное уголовным законом общественно неопасное действие.

17. Что является предметом преступлений, совершаемых в сфере телекоммуникационных сетей?
а) информация, находящаяся в телекоммуникационных сетях;
б) оборудование, обеспечивающее информационно-телекоммуникационные процессы;
в) информация, находящаяся в телекоммуникационных сетях, и оборудование, обеспечивающее информационно-телекоммуникационные процессы;
г) правильный ответ отсутствует.

18. Что такое MAC-адрес?
а) это уникальный идентификатор, сопоставляемый с различными типами оборудования для компьютерных сетей;

б) это уникальный идентификатор, присваиваемый каждой единице аппаратной части компьютера;

в) это уникальный идентификатор, присваиваемый сетевой карте;

г) сетевой адрес активного оборудования для компьютерных сетей.

19. Какие возможности используют террористы для организации «цветных революций» во многих странах мира?

а) использование возможностей ИТКС;

б) использование возможностей ЭВМ;

в) использование возможностей вредоносного программного обеспечения;

г) использование человеческих возможностей.

20. В каком году было создано специализированное подразделение по борьбе с преступлениями экстремистской и террористической направленности?

а) 1992;

б) 1994;

в) 2008;

г) 2011.

21. Деятельность по противодействию экстремизму регламентирует:

а) Федеральный закон от 8 декабря 2003 г. № 162-ФЗ;

б) Федеральный закон от 06 марта 2006 г. № 35-ФЗ;

в) Федеральный закон от 25 июля 1998 г. № 130-ФЗ;

г) Федеральный закон от 25 июля 2002 г. № 114-ФЗ.

22. По российскому законодательству за деяния экстремистского характера предусмотрена ответственность:

а) уголовная;

б) административная и дисциплинарная;

в) гражданско-правовая;

г) уголовная и административная.

23. Основанием для признания организации экстремистской и запрета ее деятельности на территории Российской Федерации являются:

а) Указы Президента Российской Федерации;

б) Постановления Правительства Российской Федерации;

в) Судебные решения;

г) Решения Генеральной прокуратуры Российской Федерации.

24. Органы государственной, законодательной и исполнительной власти осуществляют следующие меры по предупреждению экстремисткой деятельности:

а) профилактические меры;
б) воспитательные и пропагандистские меры;
в) законодательные и оперативные;
г) все вышеперечисленное.

25. Под понятие «экстремистская деятельность» подпадают:
а) пропаганда и публичное демонстрирование нацистской атрибутики или символики, сходной с нацистской;
б) уничтожение, повреждение или захват транспортных средств или иных объектов;
в) посягательство на жизнь государственного или общественного деятеля;
г) похищение людей и захват заложников.

26. Предупреждение о недопустимости экстремистской деятельности общественному или религиозному объединению выносит:
а) Генеральный прокурор Российской Федерации или подчиненным ему соответствующий прокурор;
б) Федеральный орган исполнительной власти в сфере юстиции или его соответствующий территориальный орган;
в) Судебный орган;
г) Генеральный прокурор Российской Федерации или подчиненный ему соответствующий прокурор, также федеральный орган исполнительной власти в сфере юстиции или его соответствующий территориальный орган.

27. Террористическая деятельность – это:
а) деятельность, направленная на совершение преступлений террористического характера, включающая в себя организацию, планирование, подготовку и совершение террористических акций;
б) подстрекательство к осуществлению террористических акций, призывы к насилию, организация незаконных военизированных формирований или преступных группировок с целью совершения террористических акций, а равно участие в них;
в) вербовка, вооружение или использование террористов в террористических акциях, а также обучение их террористическим навыкам, финансирование террористической организации или террористов, пособничество в подготовке и совершении террористической акции;
г) все вышеперечисленное.

28. Определение «терроризм» закреплено:
а) в Конституции Российской Федерации;
б) в Федеральном законе Российской Федерации от 25 июля 2002 г. № 114-ФЗ;

в) в Федеральном законе Российской Федерации от 6 марта 2006 г. № 35-ФЗ;

г) в Уголовном кодексе Российской Федерации от 13 июня 1996 г. № 63-ФЗ.

29. Основанием для признания организации террористической и ее ликвидации является:

а) решение суда;

б) Указ Президента Российской Федерации;

в) Постановление Правительства Российской Федерации;

г) Постановление Пленума Верховного Суда Российской Федерации.

30. Какое определение «террористическая организация» является верным?

а) Организация, созданная в целях осуществления террористической деятельности или признающая возможность использования в своей деятельности терроризма;

б) Группа лиц, объединившихся в целях осуществления террористической деятельности;

в) Организация, в отношении которой вынесено соответствующее судебное решение;

г) Организация, созданная по национальному признаку и признающая возможность осуществления террористической деятельности.

31. Укажите основные направления противодействия экстремистской деятельности:

а) предупреждение, выявление, пресечение экстремистской и террористической деятельности;

б) борьба с похищением людей и захватом заложников, пресечение деятельности незаконных вооруженных формирований, противодействие финансированию террористической и экстремистской деятельности;

в) принятие профилактических мер, направленных на предупреждение экстремистской деятельности, в том числе на выявление и последующее устранение причин и условий, способствующих осуществлению экстремистской деятельности, выявление, предупреждение и пресечение экстремистской деятельности общественных и религиозных объединений, иных организаций, физических лиц;

г) все ответы правильные.

32. Что является объективной стороной компьютерных преступлений и, в частности, преступлений, совершаемых в телекоммуникационных сетях?

а) нарушение прав и интересов пользования информации, находящейся в телекоммуникационной сети;

б) незаконное создание, копирование и распространение информации;

в) нарушение авторских прав информации при её копировании и распространении;

г) отсутствие доказательной базы.

33. Что является субъективной стороной компьютерных преступлений, а также преступлений, совершаемых в телекоммуникационных сетях?

а) следы, оставляемые при совершении преступления;

б) умышленная вина;

в) наличие существенного ущерба;

г) адекватность преступника.

34. Какие первоначальные следственные действия возможны, если подозреваемые задержаны сразу после совершения преступления:

а) личный обыск и допрос задержанных, обыск по месту жительства, месту работы и месту задержания;

б) личный обыск и опрос задержанных, обследование по месту жительства, работы и месту задержания;

в) личный обыск, арест подозреваемого;

г) личный обыск, ограничение свободы подозреваемого.

35. В каком году появился вирус, который не причинял вреда, а лишь выводил сообщение на экран:

а) 1960;

б) 1975;

в) 1986;

г) 1990.

36. Что такое дамп памяти?

а) нарушение работоспособности жесткого диска;

б) процесс копирования информации на жестком диске;

в) копия содержимого оперативной памяти, находящаяся на жёстком диске или другом энергонезависимом устройстве памяти;

г) повреждение загрузочного сектора.

37. Что такое DoS-атака?

а) атака на вычислительную систему;

б) создание таких условий, при которых легальные пользователи системы могут получить доступ к предоставляемым системным ресурсам (серверам);

в) атака на вычислительную систему с целью довести ее до отказа, то есть, создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднен;

г) атака на вычислительную систему с целью получения доступа к предоставляемым системным ресурсам (серверам).

38. Что такое DDoS-атака?

а) DoS-атака, выполняемая с использованием VPN-канала;

б) DoS-атака, выполняемая ботом;

в) DoS-атака, выполняемая посредством прокси-сервера;

г) DoS-атака, выполняемая одновременно с большого числа компьютеров.

39. Что такое телефонное мошенничество?

а) преступление с использованием средств проводной связи;

б) преступление с использованием IP-телефонии;

в) преступление с использованием средств мобильной связи;

г) правильный ответ отсутствует.

40. Что отрицательно влияет на развитие ДБО (дистанционного банковского обслуживания)?

а) попытки неправомерного получения персональной информации пользователей систем ДБО, недостаток доверия со стороны клиентов;

б) слабый интерес со стороны бизнеса, ненадежность подобных систем;

в) проблемы совместимости с операционными платформами, недостаточное финансирование;

г) недостатки по части информационной безопасности, отсутствие перспектив развития.

41. Что вызывает необходимость существенных дополнений в Главу 28 УК РФ?

а) увеличение количества выявляемых преступлений в сфере телекоммуникаций;

б) увеличение количества выявляемых преступлений в сфере телекоммуникаций и компьютерной информации и их;

в) постоянная модификация преступлений в сфере телекоммуникаций и компьютерной информации;

г) все вышеперечисленные ответы.

42. Какая кредитная организация осуществляет выпуск и обслуживание банковских карт?

а) Банк – эмитент;

б) Банк эквайер;

в) Web money$;

г) ЦБР.

43. Какая вредоносная программа проникает и устанавливается в индивидуальное электронное устройство потерпевшего, фиксирует вводимый пользователем логин и пароль в момент доступа к удаленному банковскому сервису?

а) Программа скрытого управления;
б) Программа считывания пароля;
в) Программа удаленного доступа;
г) «Зеркальный сайт».

44. Согласно закону «О противодействии дистанционному хищению денежных средств» банк может приостановить исполнение операций по переводу денег на срок:

а) не более одного рабочего дня;
б) не более двух рабочих дней;
в) не более трех рабочих дней;
г) не более недели.

45. Как называется операция, состоящая в переводе денежных средств с одного счета на другой?

а) Акцепт;
б) Аннуитет;
в) Транзакция;
г) Вексель.

46. Какая вредоносная программа проникает и устанавливается в мобильный телефон, рассылает с него СМС-сообщения, управляя банковским счетом владельца через услугу «Мобильный банк»?

а) Программа скрытого управления;
б) Программа считывания пароля;
в) Программа удаленного доступа;
г) «Зеркальный сайт».

47. Какое максимальное наказание, согласно действующему законодательству, предусмотрено за хищение денежных средств с банковского счета в особо крупном размере?

а) 5 лет лишения свободы;
б) 10 лет лишения свободы;
в) 15 лет лишения свободы;
г) 20 лет лишения свободы.

48. Какая программа необходима любому банку, действующему на территории Российской Федерации, для предоставления финансовой отчетности в Банк России за определенный период времени?

а) 1С;

б) АРМ КБР;
в) СУФД (система удаленного финансового документооборота);
г) СЭД.

49. Уникальный идентификатор, присваиваемый каждой единице активного оборудования (устройства) или некоторым их интерфейсам в компьютерных сетях Ethernet.
а) IP-адрес;
б) BIOS;
в) MAC-адрес;
г) DNS-адрес.

50. Какая вредоносная программа предварительно устанавливается на электронное устройство и позволяет в режиме реального времени отправлять на него команды управления через сеть Интернет и перечислять похищенные денежные средства?
а) Программа скрытого управления;
б) Программа считывания пароля;
в) Программа удаленного доступа;
г) «Зеркальный сайт».

51. С какого момента мошенничество признается оконченным, если предметом преступления является безналичные денежные средства?
а) С момента поступления в незаконное владение;
б) Когда виновное лицо получило возможность пользоваться денежными средствами;
в) Когда виновное лицо получило возможность распоряжаться денежными средствами;
г) С момента поступления в незаконное владение виновного лица, и когда это лицо получило реальную возможность пользоваться или распоряжаться по своему усмотрению.

52. Как называется отдельная программа-клиент, которая хранит все свои данные (выписки по счетам, платежные документы)?
а) Классический «Банк-Клиент»;
б) Интернет-банкинг;
в) Мобильный банкинг;
г) Внешние сервисы.

53. Система дистанционного банковского обслуживания, работающая через обычный Интернет-браузер, с помощью которой можно осуществлять все те же действия, что и через традиционные системы, с тем отличием, что не требуется установка дистрибутива, системы на компьютер пользователя?
а) Классический «Банк-Клиент»;

б) Интернет-банкинг;
в) Мобильный банкинг;
г) Внешние сервисы.

54. Технологии ДБО с использованием устройств банковского самообслуживания (банкоматов, платежных терминалов, информационных киосков):
а) Классический «Банк-Клиент»;
б) Интернет-банкинг;
в) Мобильный банкинг;
г) Внешние сервисы.

55. Как называется оказание услуг ДБО с использованием телефонной связи?
а) Классический «Банк-Клиент»;
б) Интернет-банкинг;
в) Мобильный банкинг;
г) Внешние сервисы.

56. Под какие статьи УК РФ подпадают действия злоумышленников при совершении преступлений в сфере ДБО?
а) ст. 158, ст. 159;
б) ст. 165, ст. 167, ст.168, ст.169;
в) ст. 158, ст. 159, ст. 272, ст. 273;
г) ст. 172, ст. 172.1, ст. 187.

57. На основании какого федерального закона в 2012 году в Уголовный кодекс были введены шесть новых видов мошеннических действий?
а) № 207-ФЗ;
б) № 149-ФЗ;
в) № 126-ФЗ;
г) № 3-ФЗ.

58. Перечислите типичные виды ОРМ, осуществляемые при раскрытии и документировании преступных действий лиц, совершающих хищения денежных средств в системе ДБО:
а) наведение справок, исследование предметов и документов, наблюдение, прослушивание телефонных переговоров, снятие информации с технических каналов связи;
б) наведение справок, отождествление личности, контрольная закупка, опрос, контролируемая поставка;
в) получение компьютерной информации, отождествление личности, сбор образцов для сравнительного исследования, контрольная закупка;
г) Все выше перечисленные.

59. Что является основанием для проведения ОРМ, ограничивающих 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?

а) Постановление суда;

б) Рапорт должностного лица;

в) Распоряжение руководителя органа, осуществляющего ОРД;

г) Рапорт руководителя органа, осуществляющего ОРД.

60. Система ДБО позволяет клиенту контролировать:

а) банковские счета;

б) обмен электронными документами с банком;

в) осуществлять операции со счетами;

г) все выше перечисленное верно.

61. Виртуальный банк – это:

а) предоставление банковских услуг через электронные каналы передачи информации, в т.ч. через Интернет;

б) банк, не имеющий традиционного офиса, обслуживающий клиентов посредством телефона, Интернета и при необходимости почты;

в) предоставление банковских услуг по договору;

г) верный ответ 1 и 2.

62. К какой главе УК РФ относятся статьи 158, 159?

а) 20;

б) 21;

в) 22;

г) 23.

63. Как называется сеть компьютеров, зараженных вредоносной программой, позволяющей киберпреступникам удаленно управлять зараженными машинами (каждой в отдельности, частью компьютеров, входящих в сеть, или всей сетью целиком) без ведома пользователя?

а) Дроп;

б) Ботнет;

в) Трафер;

г) Социальная сеть.

64. Что является одним из способов первичного средства выявления вредоносных программ на телефоне?

а) использование антивирусных программ;

б) использование VPN-приложений;

в) установка приложения Office Suite;

г) наличие посторонних программ на телефоне.

65. Какие данные владельца «электронного кошелька» оперативный сотрудник может узнать при осуществлении соответствующего запроса?

а) персональные данные владельца кошелька;

б) MAC-адрес устройства;

в) IMEI телефона;

г) тип операционной системы устройства.

66. Куда направляется изъятый у потерпевшего сотовый телефон после выявления факта вмешательства вредоносной программы в код операционной системы?

а) в ближайшее отделение полиции;

б) в отдел «К»;

в) в экспертно-криминалистическое подразделение;

г) в управление уголовного розыска.

67. В каком году удельный вес (в %) прекращенных уголовных дел по реабилитирующим основаниям (от количества уголовных дел, находящихся в производстве на территории Российской Федерации с 2005 по 2019 гг. был наименьшим?

а) в 2019;

б) в 2007;

в) в 2015;

г) в 2017.

68. Преступления в сфере компьютерной информации преимущественно совершают:

а) люди пожилого возраста;

б) лица от 14 до 35 лет;

в) сотрудники банков;

г) женщины.

69. Что означает понятие «фейковый»?

а) поддельный;

б) симметричный;

в) безопасный;

г) социальный.

70. Что происходит в настоящее время с динамикой количества совершенных преступлений мошеннического характера?

а) количество преступлений снижается;

б) количество преступлений возрастает;

в) количество преступлений остается неизменным;

г) преступления мошеннического характера искоренены.

71. Какие интернет-ресурсы наиболее подвержены атакам с хищением денежных средств?

а) государственные ресурсы;

б) блоги и форумы;

в) интернет-торговля;

г) сайты СМИ.

72. Что такое технический канал связи?

а) одна из составляющих частей телекоммуникационной сети, состоящая из технических средств и устройств, обеспечивающих проводную и беспроводную связь по передаче и обмену информацией во времени и в пространстве;

б) одна из составляющих частей телекоммуникационной сети;

в) одна из составляющих частей, где имеются технические средства и устройства;

г) беспроводная связь по передаче и обмену информацией во времени и в пространстве.

Правильные ответы к предлагаемым тестам см. в конце учебно-практического пособия.

ЛИТЕРАТУРА

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ);

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.07.2017).

3. Комментарий к Уголовному кодексу Российской Федерации (постатейный) (12-е издание, переработанное и дополненное) / Отв. ред. А.И. Рарога – «Проспект», 2017;

4. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 01.09.2017).

5. О государственной тайне: Закон Российской Федерации от 21 июля 1993 г. № 5485-1.

6. Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ.

7. О Центральном банке Российской Федерации (Банке России): Федеральный закон от 10 июля 2002 г. № 86-ФЗ.

8. О связи: Федеральный закон от 7 июля 2003 г. № 126-ФЗ.

9. О коммерческой тайне: Федеральный закон от 29.07.2004 № 98-ФЗ.

10. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ.

11. О стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы: Указ Президента Российской Федерации от 9 мая 2017 г. № 203.

12. Об утверждении Положения о защите информации в платежной системе: постановление Правительства Российской Федерации от 13 июня 2012 г. № 584.

13. Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств: указание Банка России от 9 июня 2012 г. № 2831-У.

14. О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности: письмо Банка России от 24 марта 2014 г. № 49-Т.

15. Об утверждении типовых Требований к плану мероприятий по внедрению технических средств для проведения оперативно-розыскных мероприятий: приказ Мининформсвязи, ФСБ России от 15 января 2008 г. № 5/8.

16. Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: приказ МВД РФ, МО РФ, ФСБ РФ, ФСО РФ, ФТС РФ, СВР РФ, ФСИН РФ,

ФСКН РФ, СК РФ от 27 сентября 2013 г. № 776/703/509/507/ 1820/42/535/398/68.

17. Состояние преступности за 2008-2012 гг.: сборник / ФКУ «ГИАЦ МВД России».

18. Акопов, Г.Л. Интернет и политика. Модернизация политической системы на основе инновационных политических интернет-коммуникаций. – Москва: Кнорус, 2014. – 238 с.

19. Алескеров, В.И. Уголовно-правовая и криминалистическая характеристика современных видов преступлений в сфере компьютерной информации: лекция / В.И. Алескеров, И.А. Максименко. – Домодедово: ВИПК МВД России, 2011.

20. Алескеров, В.И. Преступления, совершаемые в телекоммуникационных сетях, как разновидность преступлений в сфере компьютерной информации: аналитический сборник / В.И. Алескеров, Ф.А. Куц. – Домодедово: ВИПК МВД России, 2014.

21. Алескеров, В.И. Особенности раскрытия преступлений в сфере компьютерной информации: учебно-практическое пособие / В.И. Алескеров, О.Н. Колокольчикова. – Домодедово: ВИПК МВД России, 2015.

22. Алескеров, В.И. Раскрытие преступлений в сфере телекоммуникаций и компьютерной информации: учебно-практическое пособие/ В.И. Алескеров, О.Н. Колокольчикова. – Домодедово: ВИПК МВД России, 2018.

23. Алескеров, В.И. Выявление и раскрытие преступлений экстремистской и террористической направленности, совершаемых с использованием сферы телекоммуникаций и компьютерной информации: учебно-практическое пособие / В.И. Алескеров, О.Н. Колокольчикова, А.И. Федоткин. – Домодедово: ВИПК МВД России, 2018.

24. Алескеров, В.И. Раскрытие преступлений в системе дистанционного банковского обслуживания: учебно-практическое пособие/ В.И. Алескеров, О.Н. Колокольчикова, Л.В. Василенко. – Домодедово: ВИПК МВД России, 2020.

25. Алпатов, А.С. Мошенничество и причинение имущественного ущерба путем обмана или злоупотребления доверием / А.С. Алпатов // Трибуна молодого ученого. – 2016. – № 2. – С. 16-37.

26. Баулин, В.В. Методы совершения хищений денежных средств через систему дистанционного банковского обслуживания / В.В. Баулин, Д. Волков, В.В. Баранов, А.А. Рыжков // Сборник трудов XXIII Всероссийской конференции «Информатизация и информационная безопасность правоохранительных органов». – Москва, 2014.

27. Дуленко, В.А. Преступление в сфере высоких технологий: учебное пособие / В.А Дуленко, Р.Р. Мамлеев, В.А. Пестриков. – Москва: ЦОКР МВД России, 2010. – 200 с.

28. Еферин, В.П. Организация деятельности территориальных органов МВД России на районном уровне по противодействию терроризму и экстре-

мизму: учебное пособие / В.П. Еферин, Ю.П. Хорькин. – Домодедово: ВИПК МВД России, 2014.

29. Историческая и социально-образовательная мысль. Всероссийский научный журнал. – 2014. – № 4 (26).

30. Кочои, С. Ответственность за неправомерный доступ к компьютерной информации / С. Кочои, Д. Савельев // Рос. юстиция. – 1999. – № 1.

31. Крылов, В.В. Информация как элемент криминальной деятельности/ В.В. Крылов // Российская юстиция. – № 5. – 2000. – С.35.

32. Маторин, М.А. Актуальные вопросы формирования Маторина Ю.Н. правовой системы противодействия терроризму / М.А. Маторин // Оперативник (сыщик). – 2014. – № 2 (39).

33. Медведев, В.Н. Правовое регулирование снятия информации с технических каналов связи в оперативно-розыскной деятельности: диссертация на соискание ученой степени кандидата юридических наук / В.Н. Медведев. – Санкт-Петербург: Санкт-Петербургский университет, 2003.

34. Мельников, Д.А. Организация и обеспечение безопасности информационно-телекоммуникационных сетей и систем: учебник / Д.А. Мельников. – Москва: ИД КДУ, 2015. – 598 с.

35. Мирошников, Б.Н. Сетевой фактор. Интернет и общество / Б.Н. Мирошников. – Москва: Кучково поле, 2015.

36. Россинская, Е.Р. Судебная экспертиза в гражданском, административном и уголовном процессе / Е.Р. Россинская. – Москва: Норма, 2020.

37. Сайт Центра исследований компьютерной преступности [Электронный ресурс]. – URL: http://www.crime-research.ru (дата обращения: 20.01.2018).

38. Сейджман, М. Сетевые структуры терроризма / М. Сейджман. – Москва: Идея-Пресс, 2008. – 268 с.

39. Синякин, И.И. Терроризм с использованием оружия массового уничтожения: международно-правовые вопросы противодействия: монография / И.И. Синякин. – Москва: Норма, 2012.

40. Сорокин, А.В. Судебная практика по делам о преступлениях в сфере компьютерной информации / А.В. Сорокин [Электронный ресурс]. – URL: http://www.zaural.ru/procur/my_page.htm (дата обращения: 20.01.2021).

41. Теория оперативно-розыскной деятельности: учебник. – 3-е изд., перераб. и доп. / под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова. – Москва: ИНФРА-М, 2014. – 712 с.

42. Терроризм в современном мире. – 2-е изд. / под ред. В.Л. Шульца; Центр исслед. проблем безопасности РАН. – Москва: Наука, 2011.

43. Тищенко, В.И., Жуков Т.И., Попков Ю.С. Сетевые взаимодействия. Предмет исследования и объект моделирования / В.И. Тищенко, Т.И. Жуков, Ю.С. Попков. – Москва: Ленанд, 2014. – 352 с.

44. Ткаченко, В.В. Российский терроризм. Проблемы уголовной ответственности: монография / В.В. Ткаченко. – Москва: ИНФРА-М, 2014.

45. Троицкий, С.В. Международно-правовые формы сотрудничества государств по противодействию терроризму / С.В. Троицкий// Государство и право. – 2014. – № 2.

46. Ульянова, В.В. Проблемы реализации уголовной ответственности за содействие террористической деятельности в форме финансирования терроризма / В.В. Ульянова //Актуальные проблемы российского права. – 2014. – № 3.

47. Фатьянов, А.А. Правовое обеспечение безопасности информации в Российской Федерации: учебное пособие / А.А. Фатьянов. – Москва, 2001.

48. Чекунов, И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений / И.Г. Чекунов // Право и кибербезопасность. – 2012. – № 1.

49. Шаталов, А.С. Криминалистические алгоритмы и программы. Теория. Проблемы. Прикладные аспекты / А.С. Шаталов. – Москва: Лига Разум, 2000.

50. Шаталов, А.С. Уголовно-процессуальное право Российской Федерации: академический курс по направлению «Юриспруденция» / А.С. Шаталов, А.А. Крымов. – М.: Проспект, 2018.

51. Шаталов, А.С. Уголовно-процессуальный кодекс Российской Федерации в схемах: учебное пособие / А.С. Шаталов. – Москва: Проспект, 2021.

52. Шеннон, К. Работы по теории информации и кибернетике / К. Шеннон. – Москва, 1963.

53. Шмонин, А.В. Организация выявления и раскрытия хищений денежных средств с использованием дистанционного банковского обслуживания / А.В. Шмонин // Сборник трудов XXIII Всероссийской конференции «Информатизация и информационная безопасность правоохранительных органов». Москва, 2014.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1

ПАМЯТКИ
В ЦЕЛЯХ ПРОФИЛАКТИКИ МОШЕННИЧЕСТВА

Памятка 1

1. **Если поступило SMS-сообщение «Ваша карта заблокирована»:**

- ни в коем случае не следовать рекомендациям подозрительных SMS-сообщений;
- при поступлении SMS о блокировке карты нужно сразу же позвонить сотрудникам банка по телефону, который указан на банковской карте, официальном сайте банка или в договоре;
- банковские сотрудники никогда не просят назвать пин-код Вашей карты (в том числе ни по телефону, ни в электронном письме). Поэтому если Вы всё-таки позвонили по указанному в SMS номеру, и Вам предлагают прогуляться до ближайшего банкомата, чтобы ввести определённую комбинацию цифр, знайте: это мошенник! Банковские карты нельзя разблокировать через обычный терминал;
- если банкомат принял карту и пин-код – значит она не заблокирована.

2. **«Мобильный банк»**

Если у Вас украли телефон или Вы потеряли SIM-карту, то нужно сразу же обратиться в банк и отключить по данному номеру услугу «Мобильный банк». Ни в коем случае не выбрасывайте неактивные SIM-карты, чтобы мошенники ими не воспользовались**!**

3. **Ложная информация «проблема у родственника»:**

- ни в коем случае не следовать рекомендациям позвонивших;
- в ходе разговора задать уточняющие вопросы (Куда именно попал? В какой отдел? А на каком автомобиле? В каком районе? и т.д.), после чего преступники не захотят разговаривать;
- осуществить звонок родственникам или лицам, с ними проживающим, при невозможности дозвониться родственнику (выключен телефон) не поддаваться панике и сообщить в полицию о поступившем звонке.

4. Покупка, продажа товаров, трудоустройство на работу по объявлениям, размещенным в сети Интернет:

- ни в коем случае не следовать рекомендациям покупателя, продавца, работодателя по передаче им информации по имеющейся банковской карте, а именно, сведений с тыльной стороны карты, а также сведений из SMS-сообщений с одноразовым кодом (денежные средства на банковскую карту можно зачислить, зная только ее номер на лицевой стороне (16 или 18 цифр);
- не перечислять в качестве задатка денежные средства на банковские карты и абонентские номера;
- осуществить проверку принадлежности абонентских номеров продавца, покупателя к региону Российской Федерации (программы в интернете или же программы для телефонов Android, ИОС) и сравнить с объявлением;
- задавать продавцу, покупателю уточняющие вопросы по месту нахождения, расположения, особенностям предмета и т.д.

Памятка2

Справочная информация для подготовки запросов

Информация, которую можно получить по сайтам:

- по названию сайта можно получить информацию о его полном доменном имени, которое состоит из непосредственного имени домена и далее имён всех доменов, в которые он входит, разделённых точками. Например, полное имя «ru.wikipedia.org» обозначает домен третьего уровня «ru», который входит в домен второго уровня «wikipedia», который входит в домен верхнего уровня «org», который входит в безымянный корневой домен «.» (точка);
- регистратор доменного имени – организация, имеющая полномочия создавать (регистрировать) новые доменные имена и продлевать срок действия уже существующих доменных имён в домене, для которого установлена обязательная регистрация. Таковыми доменами являются: домен нулевого уровня (корневой домен); все домены верхнего уровня (первого уровня);
- компания хостер – организация, оказывающая услуги по предоставлению вычислительных мощностей для размещения информации на сервере, постоянно находящемся в сети Интернет.

В сети Интернет на специальных информационных сайтах (например, 2ip.ru, nic.ru) можно установить регистратора доменного имени и компанию хостера по названию сайта. При свободной политике конфиденциальности может быть указано лицо, регистрировавшее доменное имя. На ресурсах регистратора доменного имени также при свободной политике конфиденциальности может быть указано лицо, регистрировавшее доменное имя.

При направлении запроса в компанию хостер может быть получена информация об ip-адресах, с которых осуществляется администрирование сайта и реквизиты, использующиеся клиентом при оплате хостинга (при платной услуге).

Регистратор доменного имени по запросу также может предоставить регистрационные данные, указанные при получении доменного имени клиентом, а также ip-адреса, с которых происходила регистрация.

Электронные почтовые ящики

Операторы электронной почты сохраняют сведения о регистрации пользователей и сеансах последнего доступа за различный период времени. Также сохраняется содержимое электронной переписки, если пользователь не удалял свою корреспонденцию самостоятельно.

Возможно получить сведения от операторов связи, действующих на территории Российской Федерации (Mail.ru. Rambler.ru. Yandex.ru). Информацию об адресах электронной почты, расположенных за пределами Российской Федерации, необходимо запрашивать через НЦБ Интерпола.

ООО «Мэйл.Ру» сохраняет сведения о регистрации пользователя, а также о последних 10-15 сеансах доступа пользователя к ящику, приблизительно за несколько месяцев. Запрос в ООО «Мэйл.Ру» направляется почтой. Срок исполнения зависит от времени предоставления запроса.

ООО «Рамблер Интернет Холдинг» сохраняет сведения о регистрации пользователя, а также о последних сеансах доступа пользователя к ящику, приблизительно 1-2 месяца. Запрос направляется почтой. Срок исполнения составляет около 2-3 недель.

ООО «Яндекс» сохраняет сведения о регистрации пользователя, а также о последних сеансах доступа пользователя к ящику, приблизительно 1-2 месяца. Запрос направляется почтой. Срок исполнения составляет около месяца.

Информация по электронным почтовым ящикам, расположенным на собственных почтовых серверах различных сайтов, может быть получена только у администрации ресурса или у компании хостера.

Выемка электронной переписки проводится по постановлению суда в офисах компаний.

Социальные сети

В сети Интернет действует значительное количество социальных сетей, как правило, в большинстве случаев используются самые распространённые: «ВКонтакте» и «Одноклассники», реже «Мой Мир». При запросе сведений у оператора социальной сети необходимо указывать в запросе идентификатор учетной записи либо ссылку на страницу интересующего пользователя.

Недопустимо указывать в запросах общее описание учетной записи (имя, фамилия, возраст, город и т. п.).

Операторы социальных сетей сохраняют у себя следующую информацию:

- сведения о регистрации учетной записи: указанные пользователем анкетные данные, дату и время регистрации, IP-адрес доступа к сети Интернет при регистрации, как правило, также – абонентский номер сотовой связи, использованный для подтверждения регистрации;

- сведения о доступе пользователя к своей учетной записи в виде зафиксированных моментов даты и времени с соответствующим IP-адресом. Сведения о доступе хранятся, как правило, 2-3 месяца;

- сведения о платежных операциях, проведенных пользователем;

- электронную переписку пользователя, в случае, если она не была удалена владельцем.

ООО «В Контакте» располагает сведениями о доступе пользователя к учетной записи около 2 недель с момента получения организацией запроса. Таким образом, установить сведения о более ранних сеансах доступа пользователя не представляется возможным.

Исключением является момент регистрации пользователя, сведения о котором хранятся постоянно.

Запросы в ООО «В Контакте» направляются почтой, срок исполнения составляет в среднем около 2-3 недель. В запросе необходимо указывать конкретный идентификатор учетной записи. При необходимости допустимо запрашивать сведения о группах, сообществах, указывая в таком случае идентификатор группы. Допустимо запрашивать сведения о наличии жалоб пользователей социальной сети в адрес интересующего идентификатора. В запросе должны быть указаны основания направления запроса (КУСП, обращение) образец ссылки vk.com/id654654654 или vk.com/sdkjfh.

В случае, когда необходимо получить содержимое электронной переписки пользователя, в адрес ООО «В Контакте» приложением к запросу направляется заверенная копия соответствующего постановления.

По удаленным анкетам информация не сохраняется.

ООО «Одноклассники» аналогично постоянно сохраняет сведения о моменте регистрации пользователя в социальной сети, а сведения о доступе пользователя к странице хранит более продолжительное время, порядка 3-4 месяцев. Сведения об электронной переписке пользователя аналогично предоставляются при наличии постановления суда.

Запрос в ООО «Одноклассники» направляется почтой. В запросе должны быть указаны основания направления запроса (КУСП, обращение) и ссылка на аккаунт или группу ok.ru/klclkjklj. Выемки проводятся на основании постановления в офисах компаний. По удаленным анкетам информация не сохраняется.

Электронные платежные системы

В сети Интернет действует значительное количество электронных платежных систем, как правило, в большинстве случаев используются самые распространённые: «КИВИ», «Яндекс.Деньги», «ВебМани» и т.п. При запросе сведений у оператора платежной системы необходимо указывать в запросе идентификатор учетной записи пользователя.

Операторы платежных систем сохраняют у себя следующую информацию:

- сведения о регистрации учетной записи: указанные пользователем анкетные данные, дату и время регистрации, IP-адрес доступа к сети Интернет при регистрации, как правило, также – абонентский номер сотовой связи, использованный для подтверждения регистрации;
- сведения о доступе пользователя к своей учетной записи в виде зафиксированных моментов даты и времени с соответствующим IP-адресом. Сведения о доступе хранятся, как правило, последние 2-3 месяца;
- сведения о платежных операциях, проведенных пользователем.

КИВИ Банк (АО). Предоставляет информацию по электронным кошелькам системы КИВИ: сведения о регистрации кошелька, движении денежных средств. Сведения о регистрации кошелька и закрепленных к нему картах сохраняются постоянно, сведения о доступе к кошельку хранятся около 2-3 месяцев, сведения о платежных операциях – продолжительное время.

Время исполнения составляет около 3-4 недель. Целесообразно указывать в запросе отдельным пунктом сведения о конкретной платежной операции. Ответы в большинстве случаев поступают с приложением электронных документов (таблицы) на CD-R диске.

Яндекс.Деньги. Сведения о регистрации кошелька сохраняются постоянно, сведения о доступе к кошельку хранятся около 2-3 месяцев, сведения о платежных операциях – продолжительное время.

Запросы в Яндекс.Деньги направляются почтой, время исполнения составляет около 1-2 месяцев.

ВебМани. ООО «ВебМани.Ру» занимается обслуживанием электронных платежных средств ВебМани. При этом следует понимать, что при регистрации пользователь сначала получает общую учетную запись, именуемую WMID, к которой затем самостоятельно закрепляет электронные кошельки. Данные кошельки различаются в зависимости от типа валюты (курс аналогичен обычному банковскому): рублевые, долларовые и т.п. Тип кошелька определяется по первой букве в его наименовании: R – для рублевых, Z – для долларовых, E – для евро, B – для белорусских рублей и т.п.

Запросы по рублевым кошелькам направляются непосредственно в ООО «ВебМани.Ру», запросы по кошелькам иного типа валюты адресуются головной компании WM Transfer Ltd., и направляются в адрес ООО «ВебМани.Ру» для передачи на исполнение.

Терминалы КИВИ

ЗАО «Киви» является оператором платежных терминалов, которые широко распространены на территории Российской Федерации, и наиболее часто используются для совершения платежных операций в адрес абонентских номеров сотовой связи, банковских карт и т.п. В указанной организации (не путать с КИВИ Банк (АО) допустимо запрашивать информацию о том, в каких именно терминалах оплачивался абонентский номер.

Запрос в ЗАО «КИВИ» направляется почтой, время исполнения составляет около месяца, иногда более.

Объявления

Оператором системы электронных объявлений **«Авито»** является ООО «КЕХ Коммерц». Организация может предоставить сведения по электронному объявлению: дата и время размещения, IP-адреса, контактная информация, наличие жалоб на автора объявления, а также другие объявления, которые размещались данным пользователем. В большинстве случаев необходимо указывать конкретный номер объявления, в порядке исключения (если сведения утрачены) дать как можно более подробное описание объявления: примерную дату публикации (время обнаружения объявления заявителем), реализуемый товар (точно передать описание), контактные данные, которые были указаны в объявлении (телефон, адрес электронной почты и т. п.).

Запрос направляется почтой, время исполнения зависит от скорости доставления запроса в организацию.

Ip-адреса

Для установления оконечного оборудования, которому присваивался ip-адрес, необходимо знать точную дату и время присвоения с точностью до секунды. В некоторых случаях необходимо знать ресурс обращения (IP-адрес) и порт соединения.

Для получения информации об IP-адресе необходимо направить запрос провайдеру. Определить провайдера, которому принадлежит IP-адрес можно из открытых источников 2ip.ru, nic.ru.

Памятка3

Платежные системы и банки:

- **ПАО «Сбербанк».** Адрес: Россия, 117997 г. Москва, ул. Вавилова д. 19.
- **ООО «НКО Вестерн Юнион ДП Восток»**. Адрес: 125171, г. Москва, Ленинградское шоссе, д. 16 «А», строение 1. Телефоны: 8 (495) 797-21-87, факс 797-21-88;
- **ЗАО ТКС Банк (Тинькофф)**. Адрес: 123060, г. Москва, 1-й Волоколамский проезд, д. 10, строение 1. Телефоны: 8 (495) 645-59-09;
- **ЗАО «Банк Связной»**. Адрес: 115280, г. Москва, Ленинская Слобода, д. 19. Телефоны: 8 (495) 796-90-05, 796-90-03;
- **ООО НКО ЭПС «РБК Мани»**. Адрес: 117393, г. Москва, ул. Профсоюзная, д. 56. Телефоны: 8 (495) 648-68-58;
- **ООО НКО «Яндекс Деньги»**. Адрес: 119021, г. Москва, а/я 57. Телефоны: 8 (495) 739-23-25, 739-22-11;
- **ЗАО «Национальная сервисная компания» (RURU)**. Адрес: 127473, г. Москва, ул. Краснопролетарская, д. 16, строение 2. Телефоны: 8 (495) 544-36-98, факс 544-36-97;
- **ООО КБ «Интеркоммерц»**. Адрес: 119435, г. Москва, Большой Савинский пер., д. 2-4-6, строение 10. Телефоны: 8 (800) 333-36-89;
- **ООО «ВебМани.Ру»**. Адрес: 119049, г. Москва, ул. Коровий вал, д. 7, строение 1, секция 9. Телефоны: 8 (495) 228-14-09;
- **КИВИ Банк (АО)**. Адрес: 117648, г. Москва, мкр. Чертаново Северное, д. 1А. Телефоны: 8 (495) 231-36-46;
- **ОАО «КиберПлат»**. Адрес: 123610, г. Москва, ЦМТ, Краснопресненская Набережная, д. 12, подъезд 7. Телефоны: 8 (495) 967-02-20, 967-02-08;
- **ООО «Дельта Телеком»** (платежная система DeltaPay). Адрес: 111024, г. Москва, а/я 148. Телефоны: 8 (495) 987-10-90;
- **ООО «О2» (Единый кошелек)**. Адрес: 123317, г. Москва, ММДЦ «Москва-Сити», Пресненская набережная, д. 10 «С», офис 448. Телефоны: 8 (495) 777-11-25, 8 (3532) 336-603;
- **ООО НКО «Деньги. Мэйл.Ру»**. Адрес: 125167, г. Москва, Ленинградский пр-т, д. 39, строение 79;
- **ООО НКО «Рапида»**. Адрес: 125190, г. Москва, ул. Усиевича, д. 20, корпус 2. Телефоны: 8 (495) 380-1555, факс 380-15-43;
- **ООО «Платежный»**. Адрес: 129090, г. Москва, Олимпийский пер., д. 14. Телефоны: 8 (495) 783-83-93;
- **ООО «Система электронных расчетов»**. Адрес: 125190, г. Москва, Ленинградский проспект, д. 80, корп. 17, офис 20. Телефоны: 8 (495) 788-91-57;
- **ООО «Мастеркард»**. Адрес: 107051, г. Москва, Цветной бульвар, д. 2, БЦ «Легенда». Телефоны: 8 (495) 937-7735, 937-7711;

- **ПАО «МТС Банк»**. Адрес: 115035, г. Москва, ул. Садовническая, д. 75. Телефоны: факс 8 (495) 232-27-54, 921-28-00 (доб. 3399);
- **ЗАО «Океан-Банк» (Робокасса)**. Адрес: 119334, г. Москва, Канатчиковский проезд, д. 1, стр. 1. Телефоны: факс 8 (495) 98-013-30, 8 (800) 100-55-11.

Ресурсы сети Интернет

1. **«Одноклассники»**

Адрес: Ленинский проспект, д. 39, стр. 79, БЦ «Skylight» г. Москва, 125167;

2. **«В Контакте»**

Адрес: ул. Херсонская, д. 12-14, лит. «А», г. Санкт Петербург, 191024;

3. **«Мэйл.Ру»**

Адрес: Ленинский проспект, д. 39, стр. 79, БЦ «Skylight» г. Москва, 125167;

4. **«Рамблер»**

Адрес: Варшавское шоссе, д. 9, стр. 1, г. Москва, 117105;

5. **«Яндекс»**

Адрес: ул. Льва Толстого, д. 16, г. Москва, 119021;

6. **«Авито»**

Адрес: ул. Лесная, д. 7, ООО «КЕХ еКоммерц», г. Москва, 125047;

7. **«Мамба»**

Адрес: ул. 2-я Звенигородская, д. 13, стр. 42, г. Москва, 123022;

8. **«РБК (qip.ru, loveplanet.ru)»**

Адрес: ул. Профсоюзная, д. 78, стр. 1, ГК «РосБизнесКонсалтинг», г. Москва, 117393

9. **«Молоток.ру» (ООО «Е-Коммерс груп»)**

Адрес: 125258, г. Москва, Ленинградский проспект, д. 31/а стр. 1; тел. +7(495) 739-47-41 (с 10-00 до 18-00); факс +7(495) 739-47-41.

10. **«Из рук в руки» (ООО «Пронто-Москва»)**

Адрес: 115432, г. Москва, 2-й Южнопортовый пр-д, д.27 «а», строение 1тел.(495)229-29-92.

Регистраторы

АО «Регистратор Р01» (http://r01.ru)

Адрес: 123308, г. Москва, а/я 99 – для почты; тел. (495) 783-3-783, факс (495) 930-88-00.

АО «РСИЦ» (Региональный Сетевой Информационный Центр)

Адрес: 123308, г. Москва, 3-я Хорошевская ул., д. 2, стр. 1; телефон: (495) 737-06-48 , факс: (495) 737-76-73.

ООО «Регистратор»
Адрес: ул. Воронцовская 35Б, корпус 2 , этаж 4, помещение II, комната 7, г. Москва, 109147.

ООО «Регистратор доменных систем РЕГ.РУ»
Адрес: ул. 2-я Звенигородская, д. 13, стр. 43, оф. 326, г. Москва, 123007.

АО «Региональный Сетевой Информационный Центр»
Адрес: ул. 3 Хорошевская, д. 2, стр. 1, Москва, 123308.

Операторы связи

ООО «Кловертел» (предоставляет услуги IP- телефонии)
Адрес: ул. Бехтерева, д.47, к. 1, кв. 105, г. Москва, 115516, info@clovertel.ru.

ООО «МАТРИКС телеком» (предоставляет услуги IP- телефонии)
Адрес: Пер. Милютинский, д. 3, а/я 618, 101000. info@matrixmobile.ru.

ОАО «Межрегиональный Транзит Телеком» (предоставляет услуги IP- телефонии)
Адрес: ул. Марксистская, д. 22, стр. 1, г. Москва, 109147.

ООО «Системы Связи» (предоставляет услуги IP- телефонии)
Адрес: а/я 26, г. Белгород-7, 308007.

ООО «ТЕЛЛАН» (предоставляет услуги IP- телефонии)
Адрес: ул. Шарикоподшипниковская, 13, корп.2, г. Москва, 115088. Телефон: +7(495) 777-3770. Электронная почта: info@tellan.ru.

Памятка 4

Образец заявления гражданина

Директору Н-ского филиала
ПАО «Ростелеком»
Г.Н. Кузъменко
от гражданина ФИО
зарегистрирован_____
паспорт_____

Заявление

Прошу Вас предоставить информацию о соединениях принадлежащего мне абонентского номера _____ за период с _____ по _____. Прошу информацию предоставить сотрудникам полиции.

Фамилия И.О. *подпись*
дата

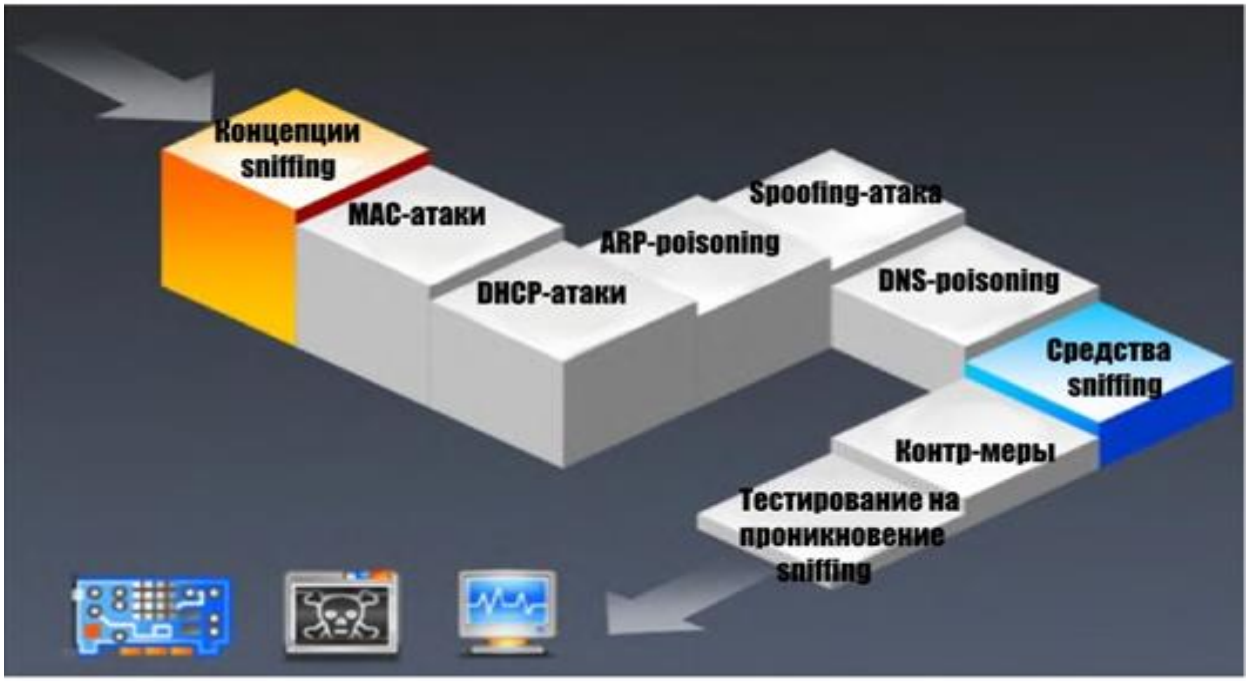
Памятка5

СЕТЕВЫЕ АТАКИ

Модуль задач

- Sniffing пакетов
- Угрозы sniffing
- Типы sniffing-атак
- Аппаратные анализаторы протоколов
- MAC-flooding
- Как работает DHCP
- Атака DHCP-сервера
- Методы ARP-spoofing
- Средства ARP-poisoning
- Как защититься от ARP-poisoning
- Угрозы spoofing-атаки
- Как защититься от MAC-spoofing
- Методы DNS-poisoning
- Как защититься от DNS-spoofing
- Средства sniffing
- Как защититься от sniffing
- Как обнаружить sniffing
- Тестирование на проникновение sniffing

Концепции sniffing

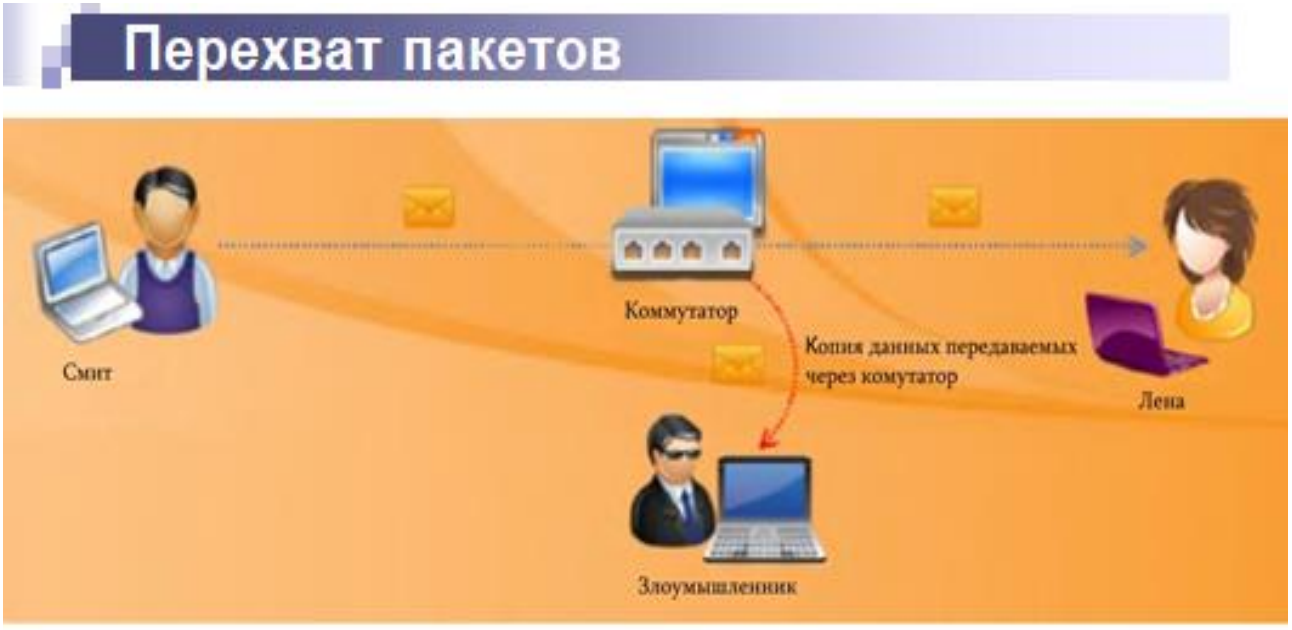


Прослушивание

1. Wiretapping – процесс мониторинга телефонных и интернет разговоров третьей стороной
2. Злоумышленники подсоединяют подслушивающее устройство к схеме переноса информации между двумя телефонами или интернет хостами
3. Это позволяет злоумышленнику читать, перехватывать и записывать информацию, содержащуюся в потоке данных коммуникационной сети

Законное прослушивание

Устройство доступа собирает трафик, обслуживающего интернет-провайдера сети, сортирует трафик по IP-доменам и подает на системы декода и восстановления перехваченного трафика в оригинальном формате. Это достигается с помощью протоколов, таких как POP3,IMAP,SMTP,P2p и FTP,Telnet,и других.



- Перехват пакетов является процессом мониторинга и захвата всех пакетов данных, проходящих через данную сеть с использованием программного обеспечения (приложений) или аппаратного устройства
- Это является одной из форм подслушивания применительно к компьютерным сетям
- Злоумышленники используют анализаторы перехватываемых пакетов данных, содержащих конфиденциальную информацию, такую как пароли, учетную информацию и т.д.
- Злоумышленники получают информацию, читая незашифрованные пакеты данных
- Когда злоумышленник подключается к порту он может контролировать весь транслируемый трафик на этот порт и доступ к конфиденциальной информации, имеющейся в незашифрованном трафике

Хотя большинство сетей сегодня применяют Switch-технологию, сниффинг пакетов по-прежнему эффективен. Потому что установка удаленных программ на сетевые компоненты с плотными потоками трафика, такие как серверы и маршрутизаторы, становится легкой. Это позволяет прослеживать и предоставляет доступ ко всему сетевому трафику с одной точки доступа. Используя сниффинг пакетов, возможен перехват пакетов данных, содержащие конфиденциальную информацию, такую как пароли, учетную информацию и т.д. Таким образом, вам будет доступно чтение паролей в незашифрованном виде, действительные электронные почты, номера кредитных карт, финансовые операции, и т.д. А также это позволяет вам узнатьь SMTP, POP, IMAP трафик, POP, IMAP, HTTP Basic, аутентификацию Telnet, SQL Databse, SMB, NFS, FTP-трафик.

Сниффер – программа и /или устройство, которое проверяет данные, передвигаясь по сети. Снифферы могут быть использованы для законной деятельности, например, управление сетью, а также для незаконной деятельности, например, кража информации, найденной в сети. Некоторые из самых простых пакетов используют командную строку интерфейс и сброс захваченных данных на экран, в то время как продвинутые лица используют графический интерфейс и график статистики трафика ; они также могут отслеживать множество сеансов и предлагать несколько вариантов конфигурации. Сниффер пакетов способен на захват пакетов информации только в данной подсети. Обычно любой ноутбук можно подключить к сети и получить доступ. Порты коммутаторов многих предприятий являются открытыми. Размещая сниффер пакетов в сеть в прослушивающий режим, возможен захват и анализ всего сетевого трафика.

Как работает sniffer

- Sniffer переводит NIC системы в прослушивающий режиме, так что он слушает все данные, передаваемые на своем сегменте
- Sniffer может постоянно следить за всем сетевым трафиком на компьютере через сетевую карту путем декодирования информации, инкапсулированную в пакете данных

Наиболее распространенный способ объединения компьютеров осуществляется через Ethernet. Компьютер, подключенный к локальной сети, имеет два адреса. Одним из них является MAC-адрес, который однозначно идентифицирует каждый узел в сети и хранится на сетевой карты. MAC-адрес используется протоколом Ethernet при построении «фреймов» для передачи данных в систему и из системы. Другой адрес -это IP-адрес. Этот адрес используется приложениями. Канальный уровень использует заголовок Ethernet с MAC-адресом целевой машины, а не IP-адрес. Сетевой уровень отвечает за отображение сетевого IP-адреса в MAC-адрес в соответствии с требованиями протокола передачи данных. Первоначально ищет MAC-адрес целевой машины в таблице, обычно называемую ARP-кэшем. Если запись не найдена для IP-адреса, ARP-трансляция пакетов запроса выводится на всех машинах локальной подсети. Машина с конкретным адресом отвечает исходной машине с ее MAC-адресом. Этот MAC-адрес будет добавлен в ARP-кэш исходной машины. Исходная машина, во всех своих контактах с целевой машиной, использует этот MAC-адрес. Есть два основных типа сред Ethernet, и снифферы работают немного различным образом в обоих случаях. Этими двумя типами сред Ethernet являются:

Общий Ethernet

В общей среде Ethernet все узлы соединены с одной и той же шиной и конкурируют между собой за пропускную способность. В этой среде все остальные машины получают пакеты, предназначенные для одной машины. Таким образом, когда машина 1 хочет поговорить с машиной 2, он отправляет

пакет на сети с назначением MAC-адреса машины 2 вместе с собственным исходным MAC-адресом. Другие машины в общей Ethernet (машина 3 и машина 4) сравнивают назначеный MAC-адрес фрейма со своим собственным. Если они не совпадают, то кадр отбрасывается. Тем не менее, машинный запуск сниффера игнорирует это правило и принимает все кадры. Сниффинг в общей среде Ethernet полностью пассивный и, следовательно, трудно обнаружаемый.

Switched Ethernet

Среда Ethernet, в которой хосты подключены к коммутатору, а не к концентратору, называется Switch Ethernet. Коммутатор поддерживает таблицы отслеживания MAC-адресов каждого компьютера ,и физический порт, с которым связан MAC-адрес, доставляет пакеты, предназначенные для конкретной машины. Коммутатор – устройство, которое посылает пакеты только на предназначенный компьютер и не транслирует его на все остальные компьютеры в сети. Это приводит к лучшей утилизации доступной пропускной способности и повышению безопасности. Таким образом, процесс перехода NIC в прослушивающий режим, чтобы собрать пакеты, не работает. В результате, многие люди думают, что коммутируемые сети являются абсолютно безопасными и невосприимчивыми к сниффингу.

Тем не менее, это не так.

SPAN для анализатора коммутируемых портов Cisco, также известный как зеркалирование портов, является методом, который позволяет контролировать сетевой трафик от одного или нескольких портов коммутатора. Это

также помогает анализировать и отлаживать данные, выявлять ошибки и исследовать на несанкционированный сетевой доступ.

Когда включено зеркалирование портов, сетевой коммутатор будет отправлять копию сетевых пакетов из исходного на порт назначения, где сетевые пакеты исследуются с помощью сетевого анализатора. Может быть, один или несколько источников, но должен быть только один порт назначения на коммутаторе. Исходные порты -порты, чьи сетевые пакеты отмониторены и зазеркалены. Вы можете одновременно контролировать трафик из нескольких портов. Например, вы можете контролировать трафик на всех портах конкретной VLAN.

Модель OSI (модель взаимодействия открытых систем) имеет систему коммуникаций, которая делится на более мелкие части. Каждая часть известна как уровень. Каждый уровень занимается предоставлением услуг для его верхнего уровня и приемом услуги из нижнего. OSI имеет сетевой фреймворк для реализации в семи уровнях. Канальным является второй уровень модели OSI. На этом уровне пакеты данных кодируются и декодируются в биты. Снифферы перехватывают пакеты из канального уровня. Снифферы оперируют на канальном уровне модели OSI. Они не придерживаются таким же правилам, как приложения и сервисы, которые находятся выше по стеку. Если один уровень взломан, коммуникации нарушаются без уведомления других уровней о проблеме.

MAC-flooding- Тип сниффинговой атаки, флудящей коммутатор пакетами данных (зачастую MAC-адресами), препятствуя передаче данных между обычными пользователями. Данные вместо передачи от отправителя к получателю разносятся по всем портам. Таким образом, взломщики могут следить за данными в сети.

DNS-poisoning-Процесс, при котором пользователь засылается на фиктивный сайт из-за ложных данных предоставленных DNS-сервером. Этот вебсайт выглядит схоже с истинным, но находится под контролем нарушителя.

ARP-poisoning-атака, при которой нарушитель пытается ассоциировать свой MAC-адрес с IP-адресом жертвы, таким образом трафик предназначенный для IP-адреса пересылается нарушителю.

DHCP-атаки-DHCP подвержен двум типам атак. 1) DHCP-starvation :процесс взлома DHCP-сервера посредством отсылки огромного количества запросов на сервер. 2) Атака вредоносного DHCP-сервера: Взломщик настраивает вредоносный DHCP-сервер выдавать себя за законный DHCP-сервер в LAN. Вредоносный сервер может начать выдачу лизинга клиента DHCP-сети. Информация поставленная клиентам обрывает их доступ к сети по причине DoS.

Сниффинг паролей – метод кражи паролей посредствам мониторинга трафика, циркулирующего в сети, вытягивания данных, содержащих пароли. Пароли внутри системы отображаются в незашифрованном тексте, который

облегчает нарушителю задачу идентификации и сопряжения с именами пользователей. В случаях, когда пароль зашифрован, нарушители могут воспользоваться алгоритмами дешифрования для его расшифровки. После получения паролей нарушители смогут добиться контроля над сетью и получить доступ к аккаунтам, конфиденциальной информации и т.д.

Spoofing-атаки- ситуация, когда нарушитель успешно притворился кем-то с помощью фальсификации данных, тем самым заполучил доступ к определенным ресурсам или выкрал персональную информацию. Нарушитель в состоянии воспользоваться IP-адресом жертвы для доступа к чужим аккаунтам, отсылки подставных емэйлов и настройки поддельных веб-сайтов для приобретения конфиденциальной информации, такой как пароли, детали аккаунтов и т.д. Нарушители в состоянии даже настроить поддельную беспроводную точку доступа и симулировать законных пользователей для подключения через нелегальное соединение.

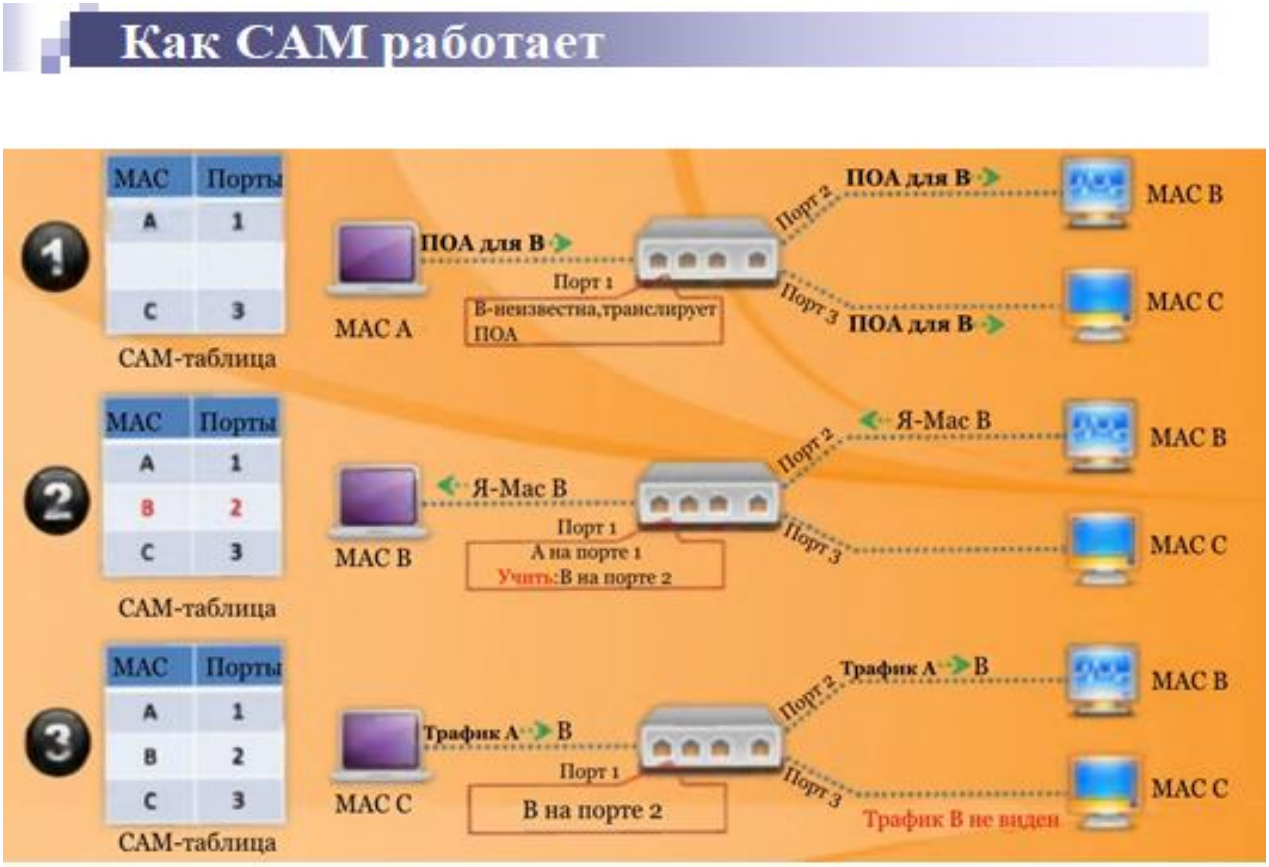
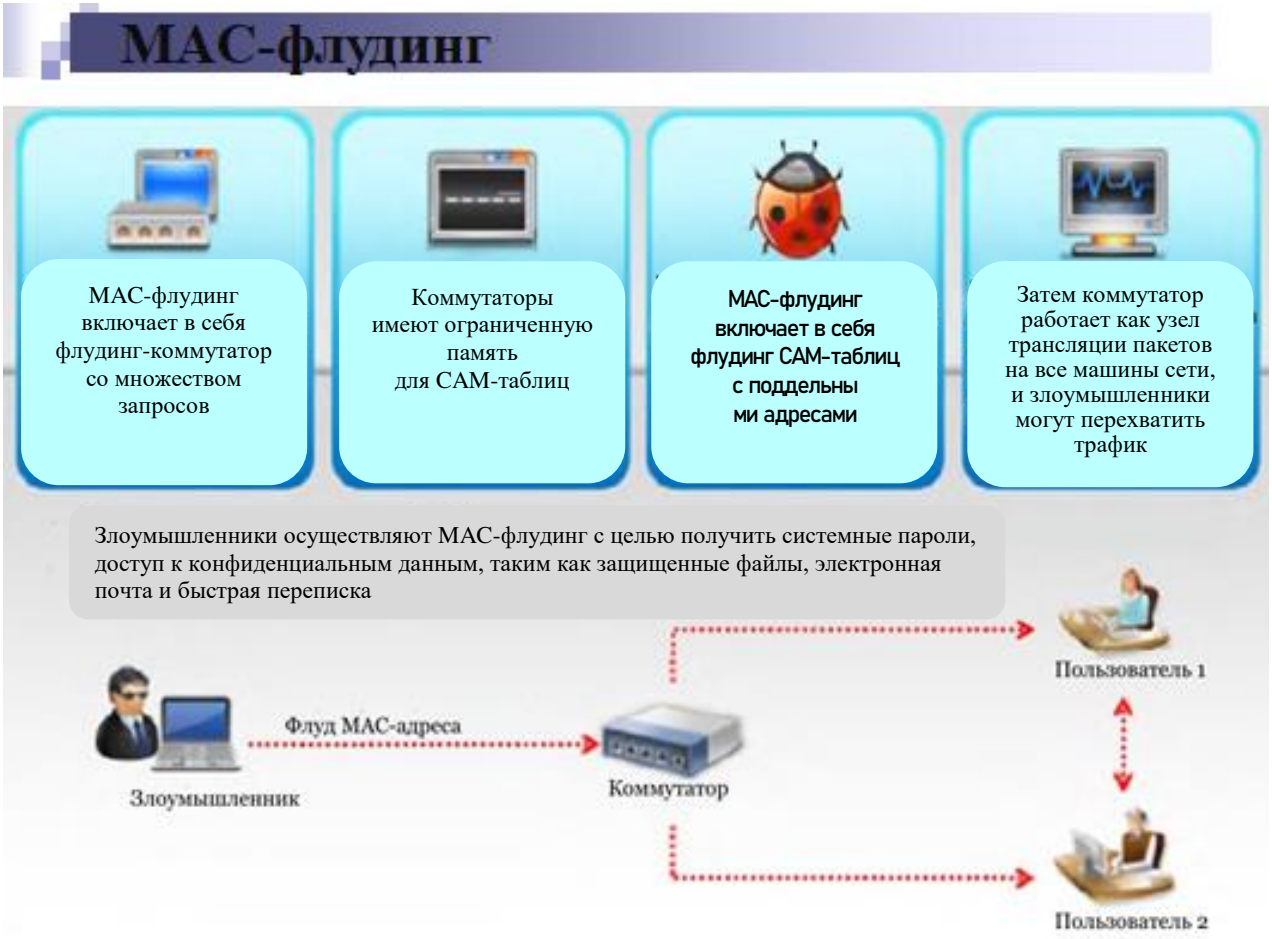


Таблица CAM – контент адресной таблицы памяти, который относится к динамической форме контента и используется с помощью коммутатора Ethernet. Коммутатор Ethernet поддерживает связи между портами. Таблица CAM отслеживает расположение путей MAC-адресов коммутатора с ограниченным размером. Если таблица CAM флудится с MAC-адресами большего размера, то коммутатор становится концентратором. Таблица CAM работает таким образом, чтобы обеспечить доставку данных назначенному узлу.

Злоумышленники используют эту уязвимость в таблице CAM для сниффинга сети передачи данных. Если атакующий имеет возможность подключения к общему коммутатору сегмента Ethernet, то он или она может легко перехватить данные.



Типичный MAC-flooding включает флудинг коммутатора с многочисленными запросами с поддельными исходными MAC-адресами. Проблем не возникает до тех пор, пока таблица MAC-адресов не будет заполнена. После того, как таблица MAC-адресов заполнится, любые дальнейшие запросы могут заставить коммутатор перейти в «failopen-режим».

Коммутатор в «failopen-режиме» действует как концентратор, транслирует данные для всех машин в сети.

Таким образом, злоумышленники могут легко перехватить трафик и могут украсть конфиденциальную информацию.

CAM-таблица заполненная поддельными MAC-адресами

Таблица CAM содержит информацию сети, такую как MAC-адреса, доступные на физических портах коммутатора и связанные с параметрами VLAN. Но эти CAM таблицы ограничены в размерах. С помощью MAC-flooding можно организовать нападение. MAC-flooding осуществляет бомбардировки коммутатора через поддельные исходные MAC-адреса до того, пока CAM таблица не заполнится. После того, как это будет сделано, коммутатор начинает флудить весь входящий трафик на всех портах. Затем коммутатор работает как концентратор, через который можно контролировать фреймы, передаваемые от хоста жертвы на другой хост без записи в CAM таблицы. Эта атака заполняет также CAM таблицы смежных коммутаторов.

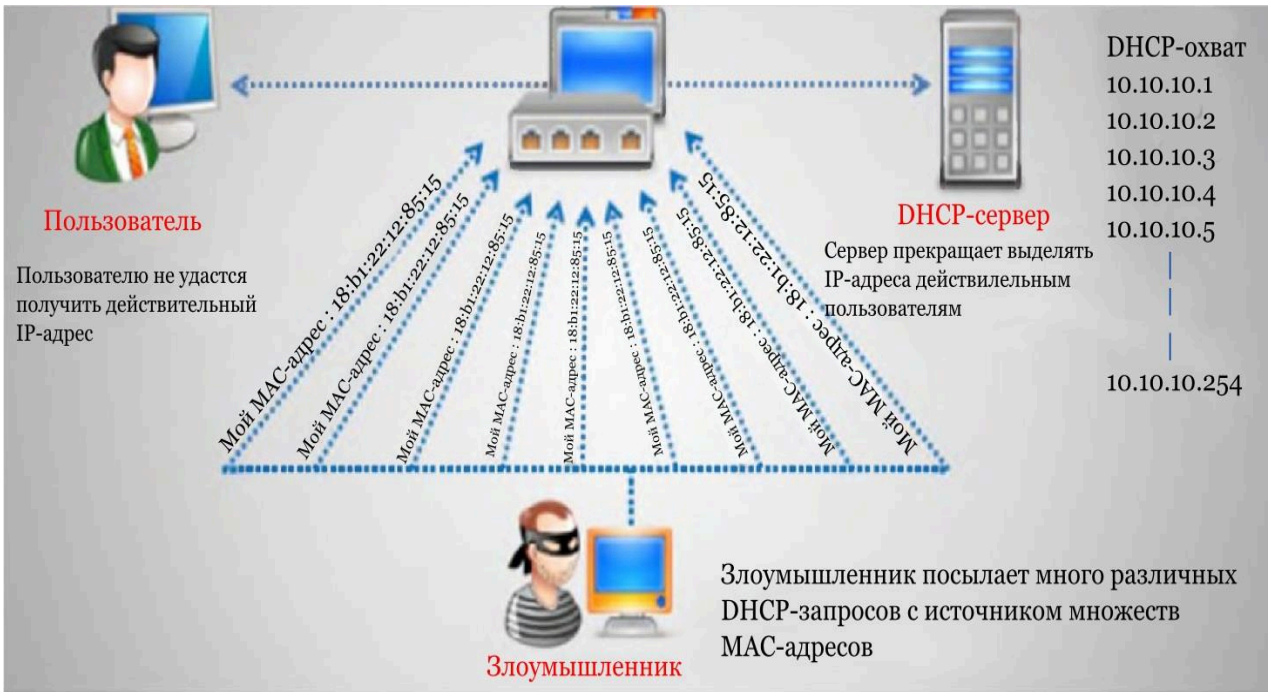
DNCP В ДЕЙСТВИИ

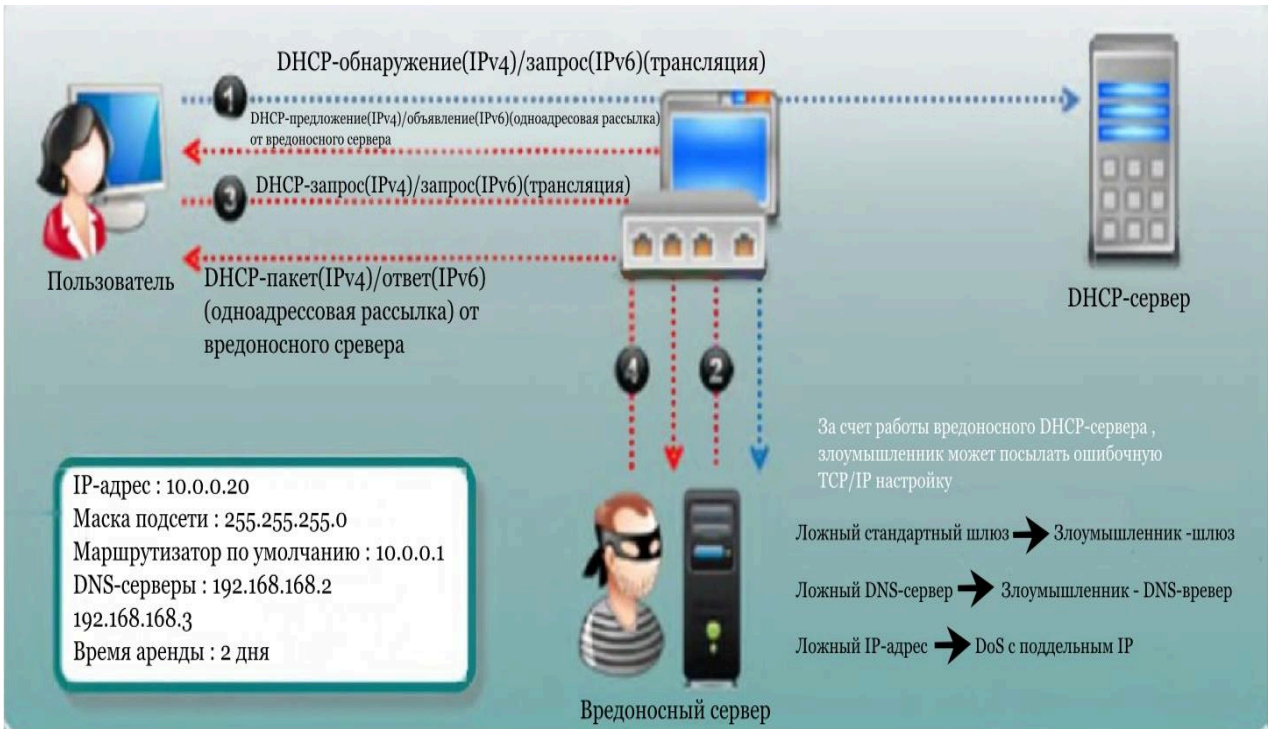
В атаках DHCP Starvation, злоумышленник производит flooding DHCP-сервера, посылая большое количество DHCP-запросов и использует все доступные IP-адреса, которые DHCP-сервер может выдать.

В результате, сервер не может выдать больше никаких IP-адресов, что приводит к отказу в обслуживании (DoS атаке). Из-за этой проблемы, действительные пользователи не могут получить или продлить их IP-адреса, и поэтому не имеют доступ к сети.

Злоумышленник передает DHCP запросы с поддельным MAC адресами с помощью таких инструментов, как Gobbler.

DHCP-истощающая атака

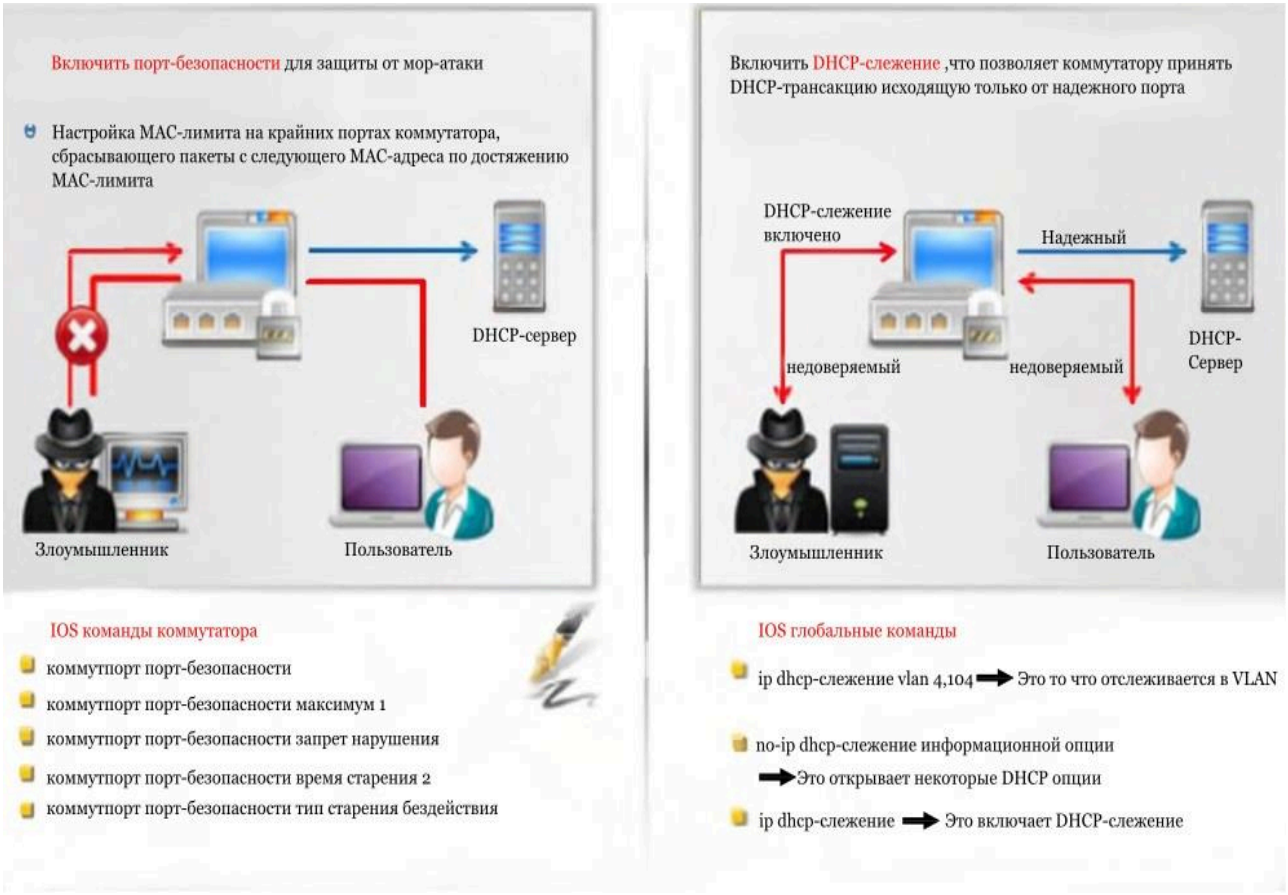




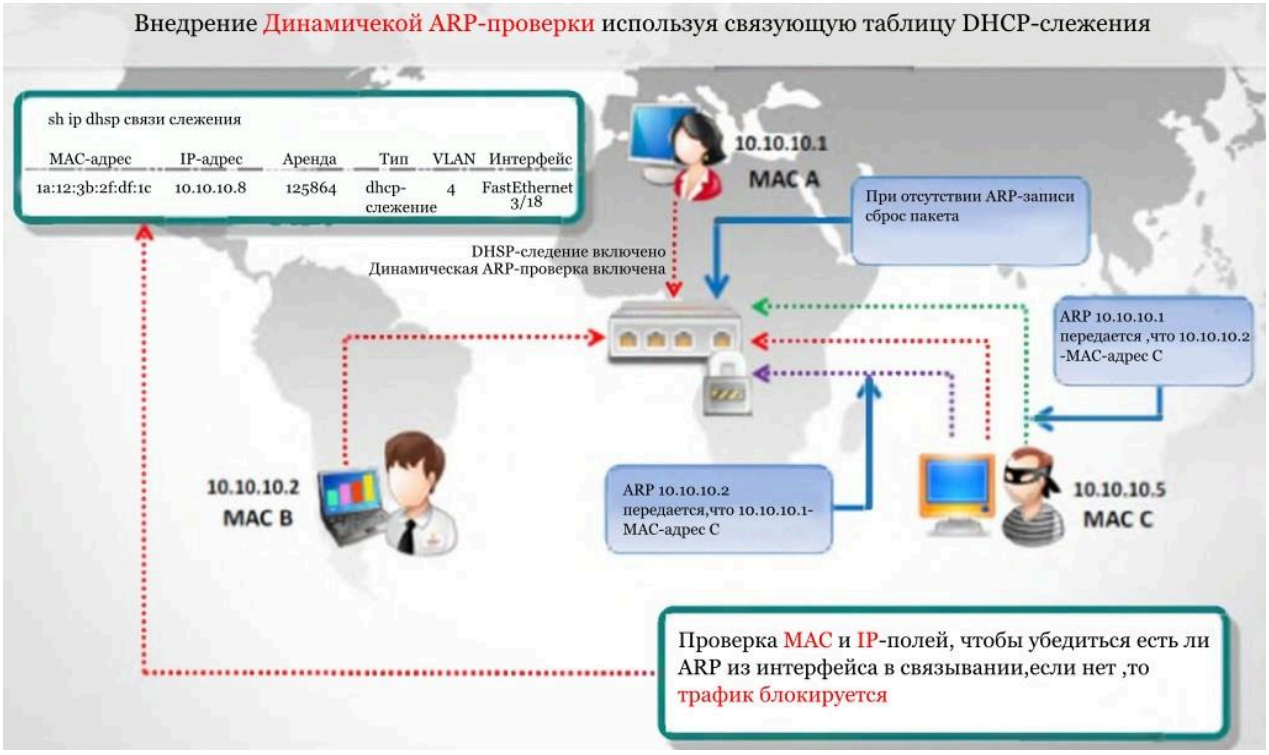
В атаках вредоносного DHCP сервера, злоумышленник будет вводить вредоносный сервер в сеть. Этот сервер имеет способность реагировать на открытые DHCP запросы клиентов. Хотя оба сервера отвечают на запрос, т.е. вредоносный сервер и реальный DHCP сервер, сервер, который отвечает первым, выбирается клиентом. В случае, когда мошенник сервер дает ответ раньше, чем реальный сервер DHCP, клиент принимает ответ вредоносного сервера. Информация, предоставляемая клиентам этим вредоносным сервером, может нарушить их доступ к сети, в результате чего DOS. Ответ DHCP от DHCP сервера атакующего может присвоить IP-адрес злоумышленника в качестве шлюза клиента по умолчанию. В результате, весь трафик от клиента будет отправлен на IP-адрес злоумышленника. Затем злоумышленник захватывает весь трафик и направляет этот трафик в соответствующий шлюз по умолчанию. С точки зрения клиента вроде бы все работает правильно. Этот тип атаки не может быть обнаружен клиентом в течение длительного времени. Иногда клиент вместо стандартного DHCP сервера, использует вредоносный DHCP сервер. Вредоносный сервер направляет клиента посетить поддельные веб-сайты с целью получения его данных.

Для смягчения атаки вредоносного DHCP-сервера, установите интерфейс, к которому вредоносный сервер подключен как ненадежный. Это действие будет блокировать проникновению в DHCP-сервер сообщений от этого интерфейса.

Как защититься от DHCP-Starvation(мор) атаки и атаки вредоносного сервера



Как защититься от ARP-poisoning



ARP –poisong-атаки могут быть предотвращены путем внедрения динамической проверки ARP (DAI). DAI- функция безопасности, которая позволяет проверить Address Resolution Protocol (ARP) пакетов в сети. Когда DAI включен в сеть VLAN, все порты на VLAN считаются ненадежным по умолчанию. DAI проверяет пакеты ARP, используя DHCP Snooping таблицы привязок . Следовательно, необходимо включить DHCP Snooping до включения DAI. Если вы включили DHCP Snooping после включения DAI, то никакой связи между VLAN у устройств не будет установлено на основе ARP. Следовательно, это может привести к добровольному отказу в обслуживании на любом устройстве в этом VLAN.

Для того чтобы проверить пакет ARP, DAI осуществляет обязательный осмотр привязки IP и MAC адреса, хранящейся в базе данных отслеживания DHCP перед передачей пакета в его пункт назначения. Если любой неправильная привязка IP и MAC-адреса встречается, то DAI удаляет соответствующий ARP-пакет. Таким образом, исключается риск man-in-the-middle атак. DAI гарантирует, что только нормальные запросы и отклики ARP передадутся.

MAC-spoofing/дублирование

MAC дублирующая атака запускается перехватом MAC-адресов клиентов, которые активно связаны с портом коммутатора и повторно используют один из этих адресов.

Перехватывая трафик в сети, злоумышленник может перехватить и использовать MAC-адрес законного пользователя, чтобы получить весь трафик, предназначенный для пользователя.

Эта атака позволяет атакующему получить доступ к сети и присвоить себе чью-то личность уже в сети.

MAC дублирующая атака запускается перехватом MAC-адресов клиентов, которые активно связаны с портом коммутатора и повторно используют один из этих адресов.

Перехватывая трафик в сети, злоумышленник может перехватить и использовать MAC-адрес законного пользователя, чтобы получить весь трафик, предназначенный для пользователя.

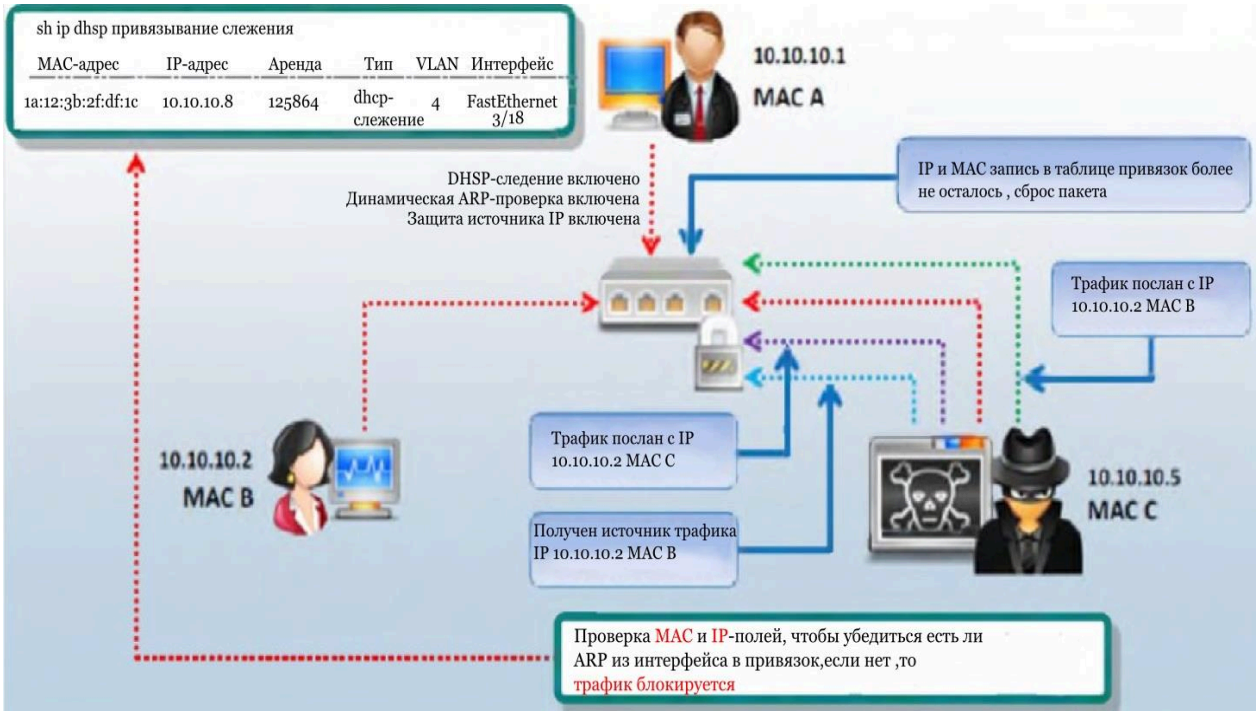
Эта атака позволяет атакующему получить доступ к сети и присвоить себе чью-то личность уже в сети.

Как защититься от spoofing-атаки

Выполнение оценки безопасности является основной целью хакера. «Этичные» хакеры выполняют различные нападения на сети или организации с целью поиска лазеек в архитектуре безопасности. Но на этом их работа не заканчивается. Поиск лазеек безопасности организации – второстепенная задача. Основной и важнейшей задачей этичного взлома является применение соответствующих контрмер к найденным лазейкам, чтобы их исправить.

После того как проверена сеть на MAC-spoofing атаки и обнаружены лазейки в безопасности, необходимо применить контрмеры для защиты сети против MAC-spoofing. Есть много контрмер для MAC-spoofing , которые пригодны в различных ситуациях. В зависимости от архитектуры безопасности сети и найденных лазеек, возможно применить соответствующие контрмеры к сети. Лучший способ защиты от подделки MAC-адресов является размеще-

ние серверов позади маршрутизатора, т.к. маршрутизаторы зависят только от IP-адресов, в то время как переключатели зависят от MAC-адресов для коммуникации в сети. Настройка интерфейса безопасности портов – другой способ смягчить MAC-spoofing. После того, как команда безопасности порта включена, она позволяет указать MAC-адрес системы подключенной к определенному порту. Она также позволяет задать действия, которые следует предпринять, если возникает нарушение безопасности порта.



Возможные методы для защиты от атак с подделкой адресов MAC:

- DHCP Snooping Binding Таблица: DHCP Snooping фильтрует не надежные DHCP-сообщения и помогает строить и связывать DHCP-таблицы привязок. Эта таблица содержит MAC-адрес, IP-адрес, занимаемое время, типы связывания, номер VLAN, и информационный интерфейс для соответствия с ненадежными интерфейсами переключателя. Он действует как брандмауэр между ненадежными узлами и DHCP-серверами. Это также помогает в дифференциации между надежными и ненадежными интерфейсами.

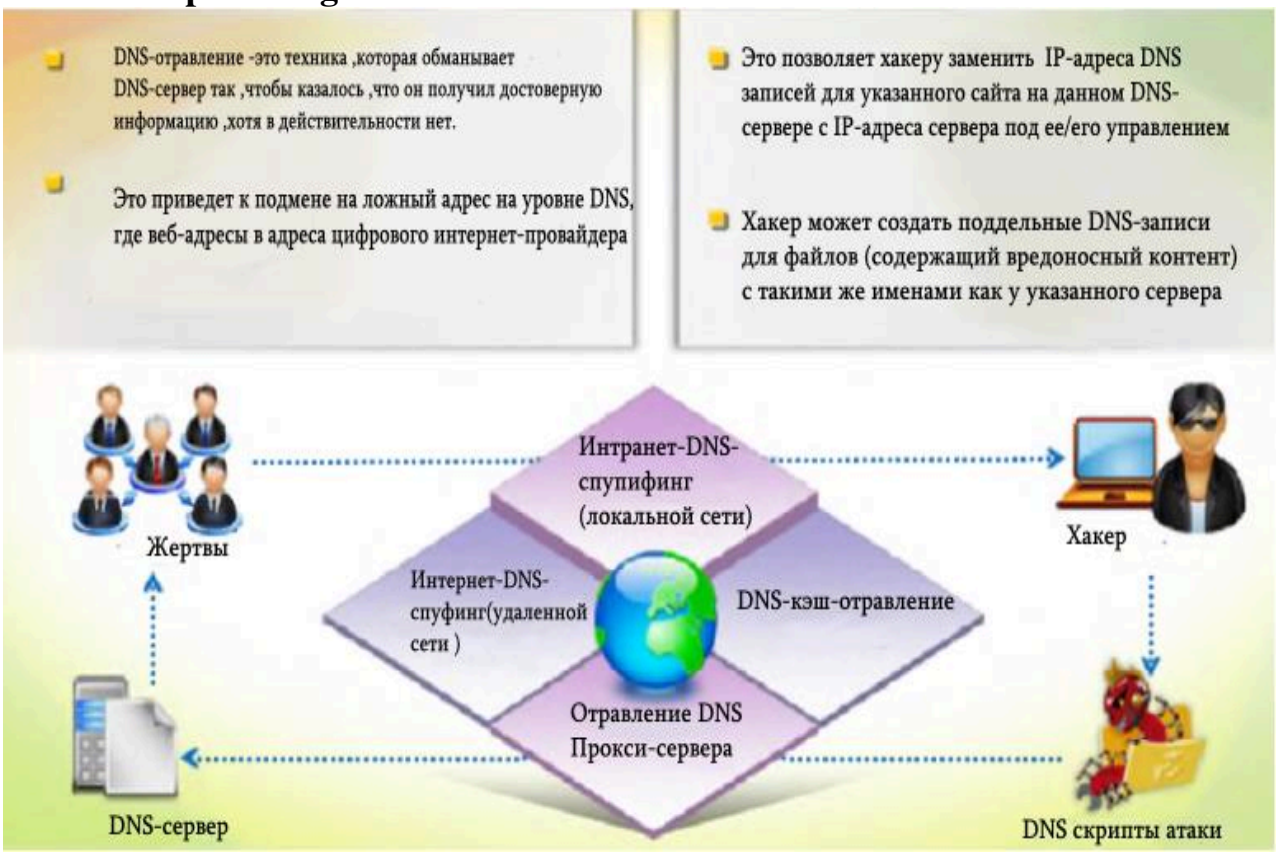
- Функцию Dynamic ARP Inspection(проверка динамического ARP): Она проверяет связи IP-адресов к MAC адресам для каждого ARP-пакета в сети. Если какие-либо не действительные привязки найдены, то они будут отброшены на проверке динамического ARP.

- Функция IP Source Guard: Функция IP Source Guard является функцией безопасности, которая поможет вам ограничить трафик IP на ненадежном слое 2 портов путем фильтрации трафика на основе DHCP Snooping базу данных привязок. Это поможет вам избежать spoofing-атаку, когда атакующий пытается подменить или использовать IP-адрес другого хоста.

- Кодировка: коммуникация должна быть зашифрована между точкой доступа и компьютером, чтобы избежать MAC-spoofing.

- Извлечение MAC-адреса: вы всегда должны получать MAC-адреса непосредственно из сетевого адаптера вместо получения его из операционной системы.

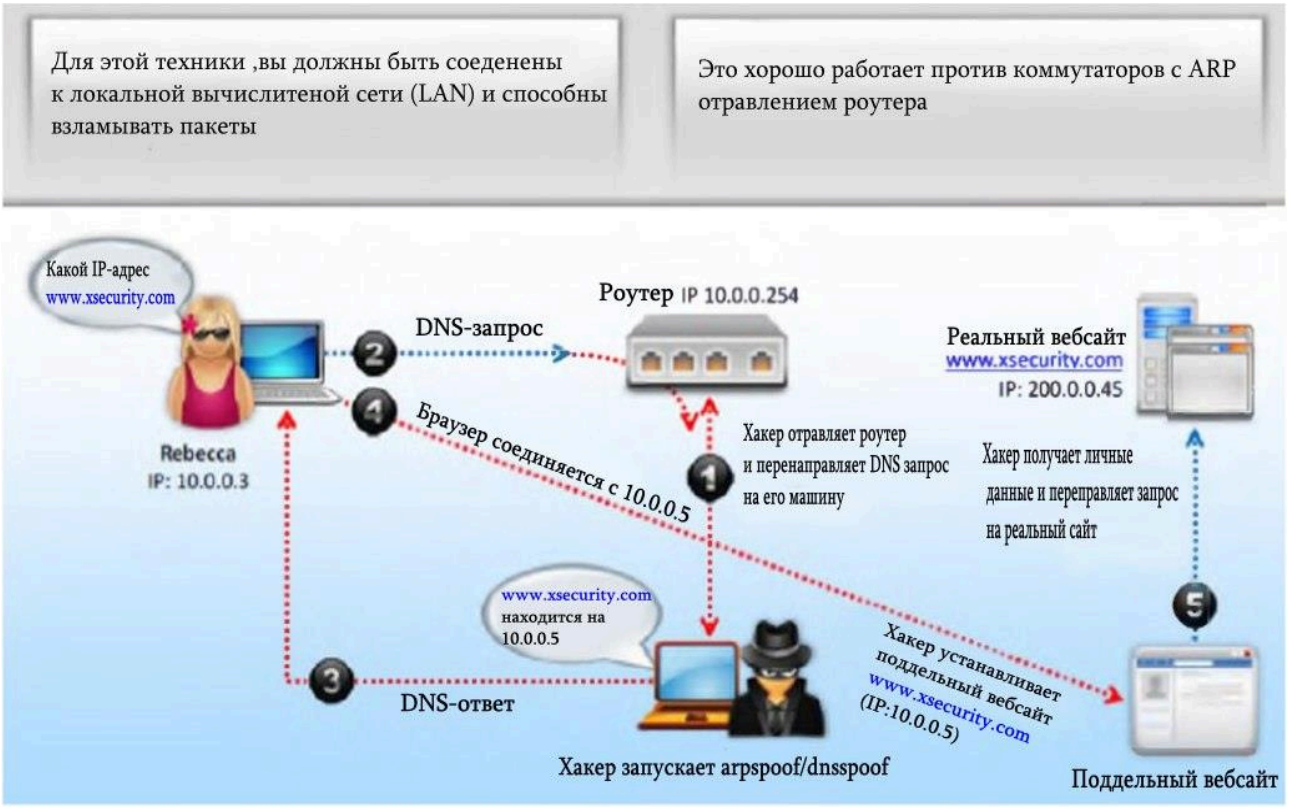
DNS-poisoning



DNS (Domain Name Service) является протоколом, который переводит доменное имя (например, www.google.com) в IP-адрес (например, 8.8.8.8). Для поддержания DNS, используются таблицы DNS, которые содержат имя домена и его эквивалент IP адрес, сохраненный в распределенной большой базе данных. DNS-poisoning, которая также называется DNS-spoofing, является атака, в которой злоумышленник пытается перенаправить жертву на вредоносный сервер вместо настоящего. Злоумышленник может совершить этот тип атаки, манипулируя записями таблицы DNS в системе DNS. Предположим, жертва хочет получить доступ к веб-сайту ABC.com, злоумышленник манипулирует записями в таблице DNS таким образом, что жертва перенаправляется на сервер злоумышленника. Это может быть сделано путем изменения IP-адреса ABC.com на IP-адрес сервера злоумышленника. Таким образом, жертва подключается к серверу злоумышленника без ведома. После того, как жертва подключается к серверу злоумышленника, злоумышленник может скомпрометировать систему жертвы и украсть данные.

Аналогичным образом, может быть поставлена под угрозу система путем проведения DNS-poisoning атак.

Интернет-DNS-spoofing



Для запуска DNS-poisoning атаки обычно выполняются следующие действия:

1) Устанавливается фальшивый веб-сайт на вашем компьютере.

2) Устанавливается treewalk и измените файл, упомянутый в readme.txt к вашему IP адресу.Treewalk сделает вас DNS-сервером.

3) Изменяется файл DNS-spoofing.bat и замените IP-адрес на ваш.

4) Троянизируется файл DNS-spoofing.bat и отправьте его к Ребекке (например: chess.exe).

5) Когда хост нажмет файл с трояном, он заменит DNS-запись Ребекки в ее свойствах TCP / IP на соответсвующую вашей машине.

6) DNS-сервер для Ребекки и ее DNS-запросы будут проходить через злоумышленника.

7) Когда Ребекка вводит XSECURITY, сайт на который она перейдет - это поддельный сайт XSECURITY. Затем, перехватывается пароль и отправляется на реальный сайт.

Есть четыре типа атак DNS-poisonong, с помощью которых вы можете поставить под угрозу систему:

- Intranet DNS spoofing (локальной сети)
- Internet DNS spoofing (удаленной сети)
- DNS poisoning Proxy-сервера
- DNS cache poisoning

Как видно из диаграммы, сначала атакующий отравляет маршрутизатор, запустив ARPSpoof / dnsspoof для того, чтобы перенаправлять DNS-

запросы клиентов на машину злоумышленника. Когда клиент (Ребекка) посылает DNS-запрос к маршрутизатору, отравленый маршрутизатор посылает пакет DNS-запроса к машине злоумышленника. После получения DNS-запроса, злоумышленник посылает поддельные DNS-ответы, которые перенаправляют клиента на фальшивый сайт, созданный злоумышленником. Так как веб-сайт принадлежит атакующему, злоумышленник может увидеть всю информацию, представленную клиентом для этого сайта. Таким образом, злоумышленник может перехватить конфиденциальные данные, такие как пароли и т.д., представленных поддельному веб-сайту. После того, как злоумышленник получает необходимую информацию, он или она перенаправляет клиента на реальный сайт.

ПРИЛОЖЕНИЕ 2

ЛАБОРАТОРНЫЕ РАБОТЫ

ЛАБОРАТОРНАЯ РАБОТА № 1

АНАЛИЗ ЗАЩИЩЕННОСТИ ПРОТОКОЛА MODBUS TCP

1 Цель лабораторной работы

Целью лабораторной работы является изучение открытого коммуникационного протокола Modbus и проведение сетевой атаки на протокол.

В ходе выполнения лабораторной работы обучающиеся получат следующие основные навыки:

- выявление уязвимостей сетевых индустриальных протоколов на примере протокола Modbus;
- подготовка полезной нагрузки для возможности списания определенного объема топлива.
- подготовка скрипта для проведения replay-атаки с использованием сформированной ранее полезной нагрузки.

Время выполнения работы – два академических часа.

2 Краткие теоретические сведения

Modbus — открытый коммуникационный протокол, основанный на архитектуре ведущий-ведомый (master-slave). Широко применяется в промышленности для организации связи между электронными устройствами. Может использоваться для передачи данных через последовательные линии связи RS-485, RS-422, RS-232, и сети TCP/IP (Modbus TCP, см. рис. 1).

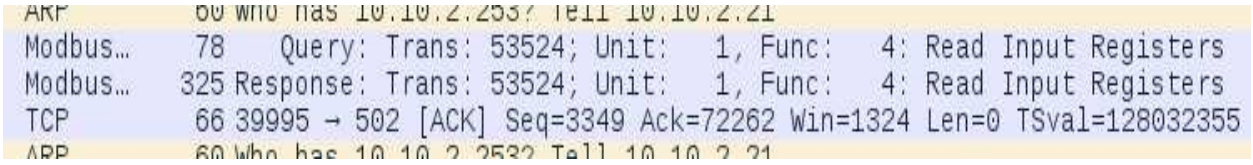


Рисунок 1 – Пример Modbus TCP трафика

Обычно в сети есть только одно ведущее, так называемое, «главное» устройство, и несколько ведомых — «подчинённых» устройств. Главное устройство инициирует транзакции (передаёт запросы). Мастер может адресовать запрос индивидуально любому подчиненному или инициировать передачу широковещательного сообщения для всех подчиненных устройств. Подчинённое устройство, опознав свой адрес, отвечает на запрос, адресованный именно ему. При получении широковещательного запроса ответ подчинёнными устройствами не формируется.

Спецификация Modbus описывает структуру запросов и ответов. Их основа — элементарный пакет протокола, так называемый PDU (Protocol Data Unit). Структура PDU не зависит от типа линии связи и включает в себя код

функции и поле данных. Код функции кодируется однобайтовым полем и может принимать значения в диапазоне 1…127. Диапазон значений 128…255 зарезервирован для кодов ошибок. Поле данных может быть переменной длины (см. таблицу 1). Размер пакета PDU ограничен 253 байтами.

Для передачи пакета по физическим линиям связи PDU помещается в другой пакет, содержащий дополнительные поля. Этот пакет носит название ADU (Application Data Unit). Формат ADU зависит от типа линии связи.

Следует обратить внимание, что поле контроля ошибок в Modbus TCP отсутствует, так как целостность данных обеспечивает TCP/IP-стек.

Таблица 1 – Параметры таблиц данных модулей

Номер регистра	Адрес регистра	Тип	Название	Тип
1-9999	0000 до 270E	Чтение-запись	Discrete Output Coils	DO
10001-19999	0000 до 270E	Чтение	Discrete Input Contacts	DI
30001-39999	0000 до 270E	Чтение	Analog Input Registers	AI
40001-49999	0000 до 270E	Чтение-запись	Analog Output Holding Registers	AO

Рассмотрим пакет инициализации соединения (см. таблицу 2).

Таблица 2 – Инициализация Modbus TCP соединения

00 01	ID транзакции (обычно – нули)
00 00	ID протокола
00 06	Длина
01	Идентификатор юнита
04	Функция 4 – чтение входных регистров (см. *Таблица 3)*
10 00 00 7d	Данные

Таблица 3 – Функции Modbus TCP соединения

Код функции	Что делает функция		Тип значения	Тип доступа
01 (0x01)	Чтение DO	Read Coil Status	Дискретное	Чтение
02 (0x02)	Чтение DI	Read Input Status	Дискретное	Чтение
03 (0x03)	Чтение AO	Read Holding Registers	16 битное	Чтение
04 (0x04)	Чтение AI	Read Input Registers	16 битное	Чтение
05 (0x05)	Запись одного DO	Force Single Coil	Дискретное	Запись
06 (0x06)	Запись одного AO	Preset Single Register	16 битное	Запись
15 (0x0F)	Запись нескольких DO	Force Multiple Coils	Дискретное	Запись
16 (0x10)	Запись нескольких AO	Preset Multiple Registers	16 битное	Запись

Рассмотрим ответный пакет на создание соединения (см. рис. 2).

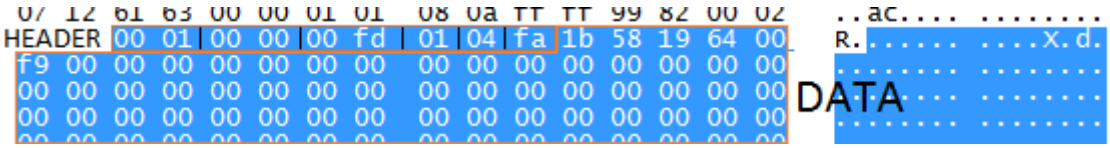


Рисунок 2 – Ответный Modbus TCP пакет

В пакете явно выделяются заголовок и блок данных (см. таблицу 4)

Таблица 4 – Ответный пакет Modbus TCP соединения

Заголовок	
«00 01»	Номер пакета в сессии
«00 00»	Функциональный код Function Code
«00 fd» = 253 байт	Длина
«01»	Идентификатор юнита
«04»	Функция 4 – чтение входных регистров
«fa» = 250 байт	Количество считанных байт
Блок данных	
«1b 58» = 7000	Значение 1
«19 64» = 6500	Значение 2
«00 f9» = 249	Значение 3

2.1 Описание стенда

Управление состоянием стенда осуществляется посредством переключения кнопки «Питание» в правом верхнем углу приложения (см. рис. 3).

Рисунок 3 – Стенд выключен (слева), стенд включен (справа)

Управление состоянием топливного склада осуществляется путем отправки запросов на заправку из топливного склада в левом нижнем углу приложения (см. рис. 4) нажатием на кнопку, соответствующую требуемому объему жидкости

Рисунок 4 – Кнопки управления объемом топлива

3 Описание инструментария

Для выполнения работы потребуется анализатор сетевого трафика.

3.1 Утилита tcpdump tcpdump является инструментом позволяющим перехватывать и анализировать сетевой трафик, проходящий через компьютер, на котором запущена данная программа.

Типичный вызов tcpdump выглядит следующим образом:

$ tcpdump –i $eth dst $ip and port $port

где:

– $eth – это название интерфейса, от которого должна осуществиться отправка пакета;

– $ip – это имя или IP-адрес сервера имен для запроса;

– $port – это номер порта для подключения к серверу.

Параметры запроса:

– -i интерфейс: Задает интерфейс, с которого необходимо анализировать трафик (без указания интерфейса – анализ «первого попавшегося»).

– -n: Отключает преобразование IP в доменные имена. Если указано -nn, то запрещается преобразование номеров портов в название протокола.

– -e: Включает вывод данных канального уровня (например, MAC-адреса).

– -v: Вывод дополнительной информации (TTL, опции IP).

– -s размер: Указание размера захватываемых пакетов. (по-умолчанию – пакеты больше 68 байт).

– -w имя_файла: Задать имя файла, в который сохранять собранную информацию.

– -r имя_файла: Чтение дампа из заданного файла.

– -p: Захватывать только трафик, предназначенный данному узлу. (по-умолчанию – захват всех пакетов, например в том числе широковещательных).

– -q: Переводит tcpdump в «бесшумный режим», в котором пакет анализируется на транспортном уровне (протоколы TCP, UDP, ICMP), а не на сетевом (протокол IP).

– -t: Отключает вывод меток времени.

Фильтрующие параметры tcpdump:

– dst хост: Проверяет, совпадает ли адрес получателя IP-пакета с указанным значением. Возможно, задавать как IP, подсеть в формате 10.0.0.1/24, так и имя хоста.

– src хост: Проверяет, совпадает ли адрес отправителя IP пакета с указанным значением. Возможно, задавать как IP, подсеть в формате 10.0.0.1/24, так и имя хоста.

– host хост: Проверяет, совпадает ли адрес отправителя или получателя с заданным значением. Возможно задавать как IP, подсеть в формате 10.0.0.1/24, так и имя хоста.

– net имя_сети: Проверяется, находится ли адрес отправителя/получателя в заданной сети. Возможно указание сети в формате CIDR (например 10.0.0.1/22), либо указание имени сети, заданной в файле /etc/networks.

– ip | arp | rarp | tcp | udp | icmp [хост]: Проверяет, принадлежит ли пакет одному из указанных протоколов и при указании адреса хоста проверяет,

совпадает ли адрес отправителя\получателя с заданным. Возможно, задавать как IP, подсеть в формате 10.0.0.1/24, так и имя хоста.

– [tcp | udp] dst port номер_порта: Проверяется, принадлежит ли пакет протоколу TCP/UDP и равен ли порт назначения заданному. Можно указать номер порта, либо имя, заданное в файле /etc/services.

– [tcp | udp] src port номер_порта: Проверяется, принадлежит ли пакет протоколу TCP/UDP и равен ли порт источника заданному. Можно указать номер порта, либо имя, заданное в файле /etc/services.

– [tcp | udp] port номер_порта: Проверяется, принадлежит ли пакет протоколу TCP/UDP и равен ли порт назначения или источника заданному. Можно указать номер порта, либо имя, заданное в файле /etc/services.

– ip broadcast: Проверяется, является ли IP пакет широковещательным.

– ether { src | dst | host } MAC_адрес: Проверяется, принадлежит ли сетевой пакет источнику, назначению, источнику или назначению имеющему заданный MAC-адрес.

– ether broadcast: Проверяется, является ли ARP-пакет широковещательным.

Пример использования:

1) Вывод сетевой статистики с интерфейса ppp0 без преобразования IP в DNS тех фреймов, у которых MAC-адресом источника равен 11:20:b3:d8:d8:2c:

$ tcpdump –n –I ppp0 ether src 11:20:b3:d8:d8:2c

2) Вывод широковещательного трафика с интерфейса vlan0:

$ tcpdump –n –e –I vlan0 ether broadcast

3) Фильтровать сетевые пакеты, где IP-адрес указан как источник или как получатель пакета:

$ tcpdump –n –I eth0 host 192.168.66.1

4) Фильтровать сетевые пакеты, где IP-адрес указан как источник пакета:

$ tcpdump –n –I eth0 src 192.168.66.1

5) Сохранение сетевых пакетов с интерфейса «eth0» в файл «capture.pcap» по пути «/var/tmp»:

$ tcpdump –ni eth0 –s0 –w /var/tmp/capture.pcap.

3.2 Утилита Wireshark

Wireshark является программой-анализатором трафика для компьютерных сетей Ethernet и некоторых других. Имеет графический пользовательский интерфейс.

Функциональность, которую предоставляет Wireshark, очень схожа с возможностями программы tcpdump, однако Wireshark имеет графический пользовательский интерфейс и гораздо больше возможностей по сортировке и фильтрации информации. Программа позволяет пользователю просматривать весь проходящий по сети трафик в режиме реального времени, переводя сетевую карту в неразборчивый режим (promiscuous mode).

3.3 Утилита python

Для выполнения лабораторной работы достаточно воспользоваться предварительно созданным скриптом на языке Python, в который необходимо будет внести изменения на основе данных, полученных в течение работы. Поля «ip» и «port» должны быть заполнены данными удаленной машины, к которой будет осуществлено подключение. Поле «payload» должно быть заполнено данными, необходимыми для проведения атаки на протокол.

```
import socket
ip = “127.0.0.1”
port = 65535
payload = ‘\x00\x00\x00\x00’


s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((ip, port))
s.send(payload)
```

4 Используемое методическое и лабораторное обеспечение

1) Виртуальная машина «KP_ASU_SCADA_SRV» с установленной ОС Ubuntu Linux 3.19.0, содержащую в себе ПО клиентской части стенда АСУ ТП (интерфейс SCADA) с использованием протокола Modbus.

2) Виртуальная машина «KP_ASU_PLC_1» с установленной ОС Linux Debian 3.2.68, содержащую в себе ПО серверной части стенда АСУ ТП (эмуляция ПЛК) с использованием протокола Modbus.

3) Виртуальная машина обучаемого с установленной ОС Kali Linux, содержащую в себе следующее программное обеспечение: tcpdump, wireshark, python 2.7.

5 Порядок выполнения работы

Лабораторная работа состоит из нескольких заданий. Задача лабораторной работы – собрать ключевую информацию (указана в задании) из сетевого трафика, проанализировать его, найти возможность выполнения вектора атаки на проприетарный сетевой протокол и сформировать отчет по проведенной атаке.

5.1 Ход работы

1) Подключиться к клиентской виртуальной машине обучающегося.

Логин – root, пароль – qwe123!@#.

2) В утилите Wireshark, используя синтаксис утилиты tcpdump, для записанного между клиентом и сервером образца трафика, определить функции, используемые в течение сетевого взаимодействия компонентов сети.

3) На основе полученной информации необходимо сформировать собственный пакет, который позволит установить значение воды в баке равным необходимому в задании. Значение можно отслеживать, подключившись к удаленной машине «zero-rel» в левой верхней части приложения (см. рис. 6).

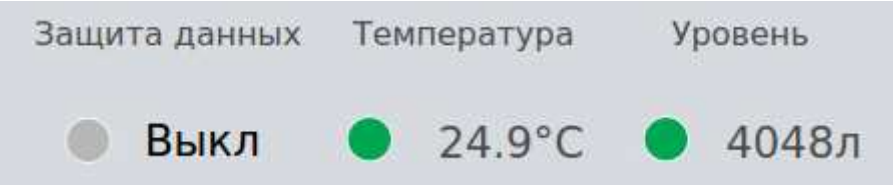


Рисунок 5 – Уровень топлива в интерфейсе

5.2 Завершение работы

Выключить виртуальные машины «KP_ASU_SCADA_SRV», «KP_ASU_PLC_1».

6 Содержание отчёта о выполненной работе

В отчёте о выполненной лабораторной работе необходимо указать в виде таблицы найденную ключевую информацию.

6.1 Пример задания

1) Подключиться к клиентской виртуальной машине обучающегося.

2) В утилите Wireshark, используя синтаксис утилиты tcpdump, для записанного между клиентом и сервером образца трафика, определить функции, используемые в течение сетевого взаимодействия компонентов сети.

3) На основе полученной информации необходимо сформировать собственный пакет, который позволит установить значение воды в баке равным необходимому в задании.

6.2 Пример отчета

Отчет может выполняться как на компьютере, так и на бумажном носителе в зависимости от требований преподавателя.

№	Задание	Значение
1	Получение номера и названия функции записи протокола Modbus	
2	Написание полезной нагрузки	
3	Написание и эксплуатация Pyhton-скрипта с полезной нагрузкой, получение нового значения объема топлива	

7 Контрольные вопросы

1) Объясните основную концепцию протокола Modbus.
2) Назовите причину возможности проведения атаки на протокол.
3) Предложите решения, позволяющие устранить возможность атаки на протокол.

8 Бланк отчета

8.1 Задание

1) Подключиться к клиентской виртуальной машине обучающегося.

2) В утилите Wireshark, используя синтаксис утилиты tcpdump, для записанного между клиентом и сервером образца трафика, определить функции, используемые в течение сетевого взаимодействия компонентов сети.

3) На основе полученной информации необходимо сформировать собственный пакет, который позволит установить значение воды в баке равным необходимому в задании.

8.2 Ответы

№	Задание	Значение
1	Получить номер и название функции записи протокола Modbus	
2	Написать полезную нагрузку	
3	Написать и выполнить Pyhton-скрипт с полезной нагрузкой для получения нового значения объема топлива	

ЛАБОРАТОРНАЯ РАБОТА № 2

АНАЛИЗ ЗАЩИЩЕННОСТИ ПРОГРАММИРУЕМОГО ЛОГИЧЕСКОГО КОНТРОЛЛЕРА (ПЛК)

1 Цель лабораторной работы

Целью лабораторной работы является изучение методов анализа сети и атака перебором с использованием словаря.

В ходе выполнения лабораторной работы обучающиеся получат следующие основные навыки:

– навыки подключения к АСУ ТП различными способами;

– работа с языком Python для решения задачи перебора пароля с использованием словаря.

Время выполнения работы – два академических часа.

2 Краткие теоретические сведения

Атака полным перебором (bruteforce) — метод атаки, использующий перебор всех возможных в пределах данного набора символов последовательностей для решения задачи. Как правило, используется для неправомерной аутентификации.

Атака является самым простым и универсальным способом получения неправомерного доступа, однако, в зависимости от мощности алфавита перебираемого сообщения, и длины сообщения, перебор может занимать огромное количество времени.

Например, при алфавите мощностью равной 36, длине сообщения в 10 символов и скорости перебора равной 100000 сообщений в секунду, перебор займет 1162 года.

По причине того, что атака может не принести результата в необходимые сроки, она используется в нескольких случаях:

1) Вместе со словарем — набором популярных пользовательских паролей, которые перебираются вместо генерируемого набора случайных символов. Этот способ использования атаки полным перебором будет использоваться в данной работе.

2) Если заведомо известно, что перебор сообщений займет приемлемое для атакующего время.

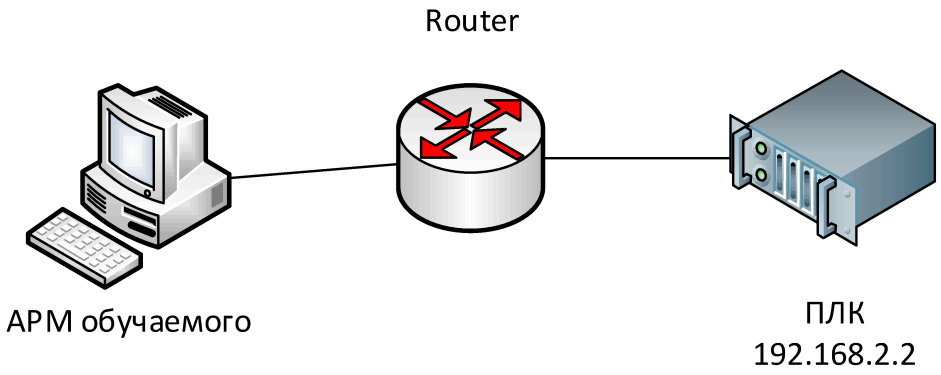
Python — высокоуровневый язык программирования общего назначения, ориентированный на повышение производительности разработчика и читаемости кода. Синтаксис ядра Python минималистичен. В то же время стандартная библиотека включает большой объём полезных функций.

Python, по причине невысокой сложности в освоении и приемлемой скорости работы имеет популярность, как язык написания скриптов вредо-

носной направленности. Скрип написанный на Python будет использоваться в данной работе.

Предполагается, что обучаемый самостоятельно нашел скрипт и адаптировал его для своих нужд, что является близким к жизни сценарием.

2.1 Схема стенда



3 Инструментарий

Terminal — это приложение, внутри которого выполняется командный интерпретатор. Его еще часто называют интерфейсом командной строки. Он интерпретирует команды специального языка скриптов.

По умолчанию используется командный интерпретатор Bash. Это улучшенный вариант интерпретатора Bourne Shell, который обычно называют просто «Shell». В настоящее время Bash – фактически стандарт де-факто в большинстве Unix-подобных систем.

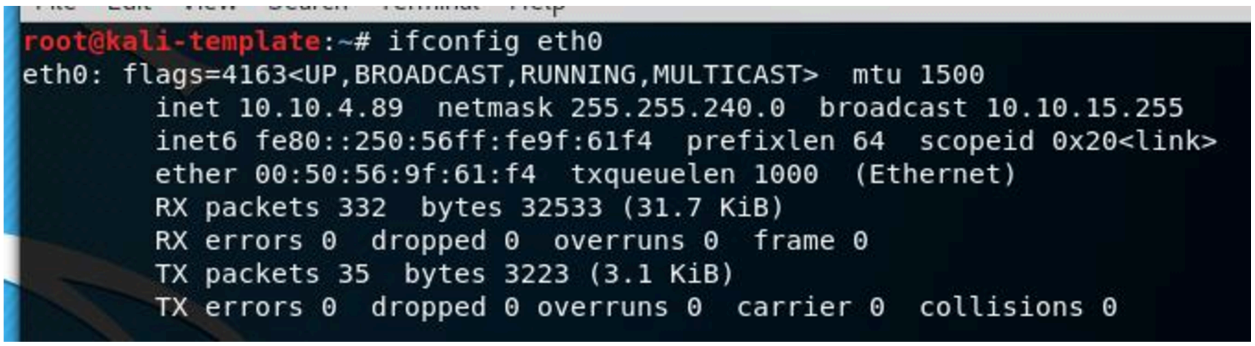


Рисунок 6 –Скриншот работы Terminal

Работа с приложением реализована с помощью ввода команд в окно терминала.

Командная строка начинается с пользователя (root), после «@» следует его имя (kali-template), затем следует название текущего каталога — по умолчанию открывается домашний каталог пользователя, который в Unix-системах обозначается знаком «~» (тильда). Далее следует знак «#», который называется приглашением – приглашением вводить команды интерпретатору.

Формат команд:

[команда] [аргументы …]

Примеры основных команд:

– Определение текущей директории.

pwd

– Смена директории.

cd [путь]

В частности:

cd .. — сменит директорию на вышестоящую над текущей

cd / — сменит директорию на корневую

cd ~ — переместит в домашнюю папку

– Отображение всех файлов и директорий в текущей директории.

ls [опции] [файл]

– Поиск файла или директории по имени. Команда поддерживает регулярные выражения.

find [директория начала поиска] [опции]

Пример:

find . –type d –name *cookie* — поиск, начиная с текущей директории, исключительно папок, в названии которых содержится «cookie»

– Поиск файла по его содержимому.

grep [опции] [путь]

– Удаление файла.

rm [опции] [путь]

– Чтение файла, объединение файлов, создание файла.

cat [опции] [путь]

– Вывод списка работающих процессов.

ps [опции]

– Задание приоритета процессу.

nice [опции] [ID процесса]

Также, работая с терминалом, необходимо знать о функциях некоторых клавиш:

– Дозаполнение названия файла или директории. При введении нескольких букв, нажмите Tab, чтобы набор был завершен автоматически.

– Остановка текущего процесса.

Ctrl+C

– Перемещение по истории введенных команд.

↑ и ↓

Nmap (Network Mapper) — свободная утилита, предназначенная для разнообразного настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети (портов и соответствующих им служб).

Часто используется для анализа сетей с целью обнаружения уязвимых мест — открытых портов и др.

Формат команд:

nmap [тип сканирования] [опции] [цель сканирования]

Пример команды:

– Сканирование первых 1024 портов первой половины из всех доступных подсетей адресного пространства 10.10.

nmap –p 1-1024 10.10.0-255.0-127

4 Используемое методическое и лабораторное обеспечение

1) Виртуальная машина «KP_ASU_PLC_1» с установленной ОС Linux Debian 3.2.68, содержащую в себе ПО серверной части стенда АСУ ТП (эмуляция ПЛК) с использованием протокола Modbus.

2) Виртуальная машина обучаемого с установленной ОС Kali Linux, содержащую в себе следующее программное обеспечение: tcpdump, wireshark, python 2.7.

5 Порядок выполнения работы

Лабораторная работа состоит из нескольких заданий. Задача лабораторной работы – собрать необходимые сведения (указана в задании) с помощью различных инструментов, проанализировать их, использовать собранную информацию для эксплуатации уязвимостей и сформировать отчет, содержащий полученные сведения.

5.1 Ход работы

1) Обучающиеся должны просканировать порты ПЛК,

2) Обучающимся надо проверить реакцию порта на попытку подключения.

3) Обучающиеся должны написать на Python скрипт для атаки перебором.

5.2 Завершение работы

Выключить виртуальную машину «KP_ASU_PLC_1».

6 Содержание отчёта о выполненной работе

В отчёте о выполненной лабораторной работе необходимо указать в виде таблиц с заполненными значениями.

6.1 Пример задания

1) Обнаружить открытый порт ПЛК.
2) Подключиться к 9108 порту.
3) Подобрать пароль с помощью скрипта и словаря.

6.2 Пример отчета

Отчет может выполняться как на компьютере, так и на бумажном носителе в зависимости от требований преподавателя.

№	Задание	Значение
1	Обнаружить открытый порт ПЛК	
2	Подключиться к 9108 порту	
3	Подобрать пароль с помощью скрипта и словаря.	

7 Контрольные вопросы

1) Укажите ключевую слабость атаки полным перебором.
2) Назовите популярные словари, используемые для проведения атаки полным перебором.
3) На каком уровне модели OSI работает используемый скрипт? Почему? (ответить на примере исходного кода)
4) Для чего в скрипте используется проверка на пустую строку? Можно ли избежать этой проверки?

8 Бланк отчета

8.1 Задание

1) Обнаружить открытый порт ПЛК.
2) Подключиться к 9108 порту.
3) Подобрать пароль с помощью скрипта и словаря.

8.2 Ответы

№	Задание	Значение
1	Обнаружить открытый порт ПЛК	
2	Подключиться к 9108 порту	
3	Подобрать пароль с помощью скрипта и словаря.	

ЛАБОРАТОРНАЯ РАБОТА № 3

АНАЛИЗ ЗАЩИЩЕННОСТИ SCADA-СЕРВЕРА

1 Цель лабораторной работы

Целью лабораторной работы является изучение способов поиска возможности удаленного подключения к серверу, а также анализ режимов шифрования для дальнейшего нелегитимного получения пароля.

В ходе выполнения лабораторной работы обучающиеся получат следующие основные навыки:

– навыки подключения к АСУ ТП различными способами;

– навыки выявления слабых режимов шифрования;

– работа со специальным программным обеспечением для выполнения анонимных подключений типа reverse_tcp.

Время выполнения работы – два академических часа.

2 Краткие теоретические сведения

ECB (Electronic Code Book) — это режим шифрования, при котором исходное сообщение делится на блоки длины k и каждый блок последовательно и независимо шифруется с использованием одного и того же ключа.

Шифрование:

Пусть дано сообщение P (открытый текст, последовательность бит, данные).

Во время шифрования выполняются следующие действия:

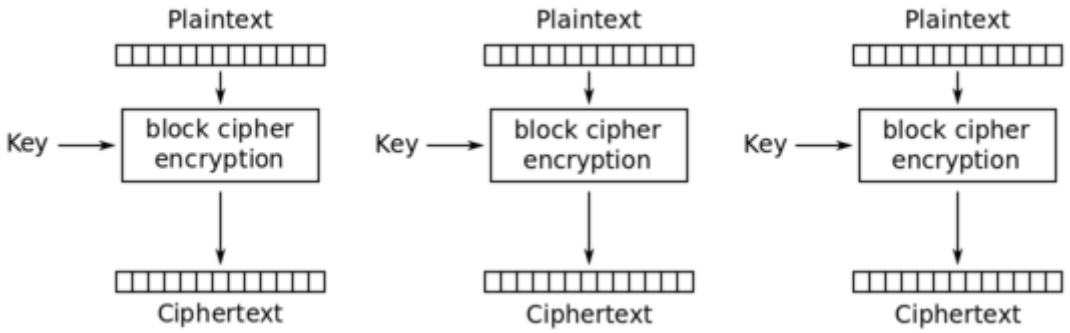


Рисунок 7 –Режим шифрования «ECB»

Сообщение делится на блоки одинакового размера. Размер (длина) блока равен n и измеряется в битах. В результате получается последовательность блоков P_1, P_2, $P_{3...}$ P_q. Последний блок при необходимости дополняется до длины n.

Каждый блок P_i шифруется алгоритмом шифрования E_k с использованием ключа k:

$C_i = E_k (P_i, k)$,

где:

i — номер блока;

k — ключ;

P_i — блок сообщения (открытый текст);

C_i — зашифрованный блок (шифротекст);

E_k — функция, выполняющая блочное шифрование.

В результате получаются зашифрованные блоки C_1, C_2, $C_{3...}$ C_q.

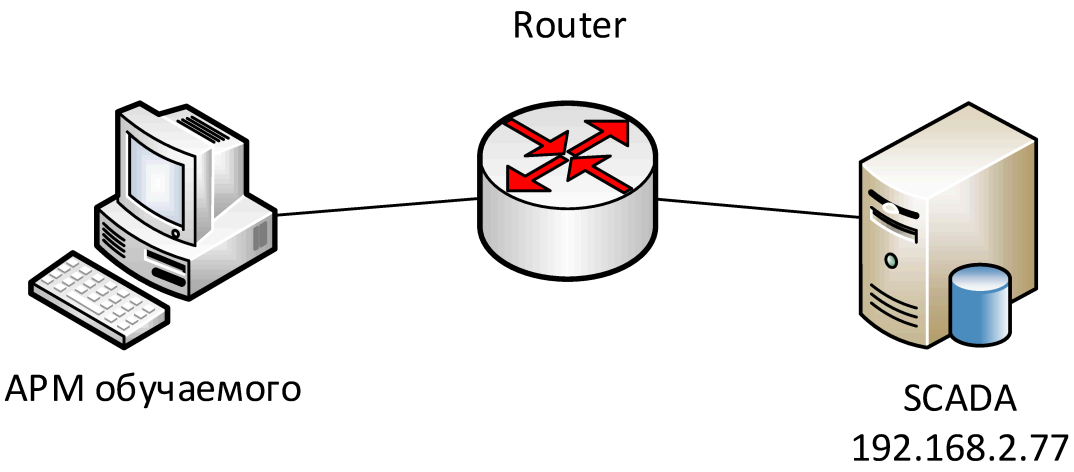
Расшифровка:

выполняется функцией D_k с использованием того же ключа k:

$C_i = E_k (P_i, k)$.

Недостатком ECB является сохранение статистических особенностей открытого теста.

2.1 Схема стенда



3 Инструментарий

Terminal — это приложение, внутри которого выполняется командный интерпретатор. Его еще часто называют интерфейсом командной строки. Он интерпретирует команды специального языка скриптов.

По умолчанию используется командный интерпретатор Bash. Это улучшенный вариант интерпретатора Bourne Shell, который обычно называют просто «Shell». В настоящее время Bash – фактически стандарт де-факто в большинстве Unix-подобных систем.

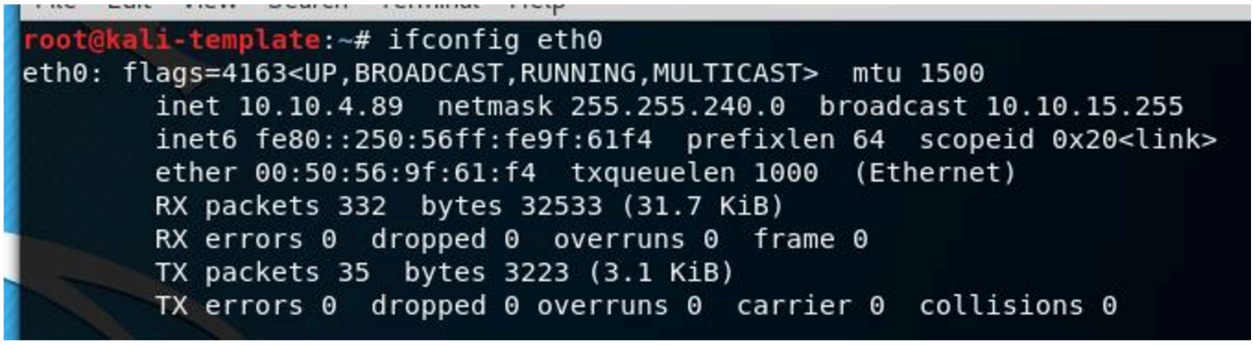


Рисунок 8 –Скриншот работы Terminal

Работа с приложением реализована с помощью ввода команд в окно терминала.

Командная строка начинается с пользователя (root), после «@» следует его имя (kali-template), затем следует название текущего каталога — по умолчанию открывается домашний каталог пользователя, который в Unix-системах обозначается знаком «~» (тильда). Далее следует знак «#», который называется приглашением – приглашением вводить команды интерпретатору.

Формат команд:

[команда] [аргументы …]

Примеры основных команд:

– Определение текущей директории.

pwd

– Смена директории.

cd [путь]

В частности:

cd .. — сменит директорию на вышестоящую над текущей

cd / — сменит директорию на корневую

cd ~ — переместит в домашнюю папку

– Отображение всех файлов и директорий в текущей директории.

ls [опции] [файл]

– Поиск файла или директории по имени. Команда поддерживает регулярные выражения.

find [директория начала поиска] [опции]

Пример:

find . –type d –name *cookie* — поиск, начиная с текущей директории, исключительно папок, в названии которых содержится «cookie»

– Поиск файла по его содержимому.

grep [опции] [путь]

– Удаление файла.

rm [опции] [путь]

– Чтение файла, объединение файлов, создание файла.

cat [опции] [путь]

– Вывод списка работающих процессов.

ps [опции]

– Задание приоритета процессу.

nice [опции] [ID процесса]

Также, работая с терминалом, необходимо знать о функциях некоторых клавиш:

Дозаполнение названия файла или директории. При введении нескольких букв, нажмите Tab, чтобы набор был завершен автоматически.

– Остановка текущего процесса.

Ctrl+C

– Перемещение по истории введенных команд.

↑ и ↓

Nmap (Network Mapper) — свободная утилита, предназначенная для разнообразного настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети (портов и соответствующих им служб).

Часто используется для анализа сетей с целью обнаружения уязвимых мест — открытых портов и др.

Формат команд:

nmap [тип сканирования] [опции] [цель сканирования]

Пример команды:

– Сканирование первых 1024 портов первой половины из всех доступных подсетей адресного пространства 10.10.

nmap –p 1-1024 10.10.0-255.0-127

Wireshark — — программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других. Имеет графический пользовательский интерфейс. Программа позволяет пользователю просматривать весь проходящий по сети трафик в режиме реального времени, переводя сетевую карту в неразборчивый режим (promiscuous mode).

Функционал Wireshark включает в себя «прослушивание» сети, возможность экспорта медиа-информации и др.

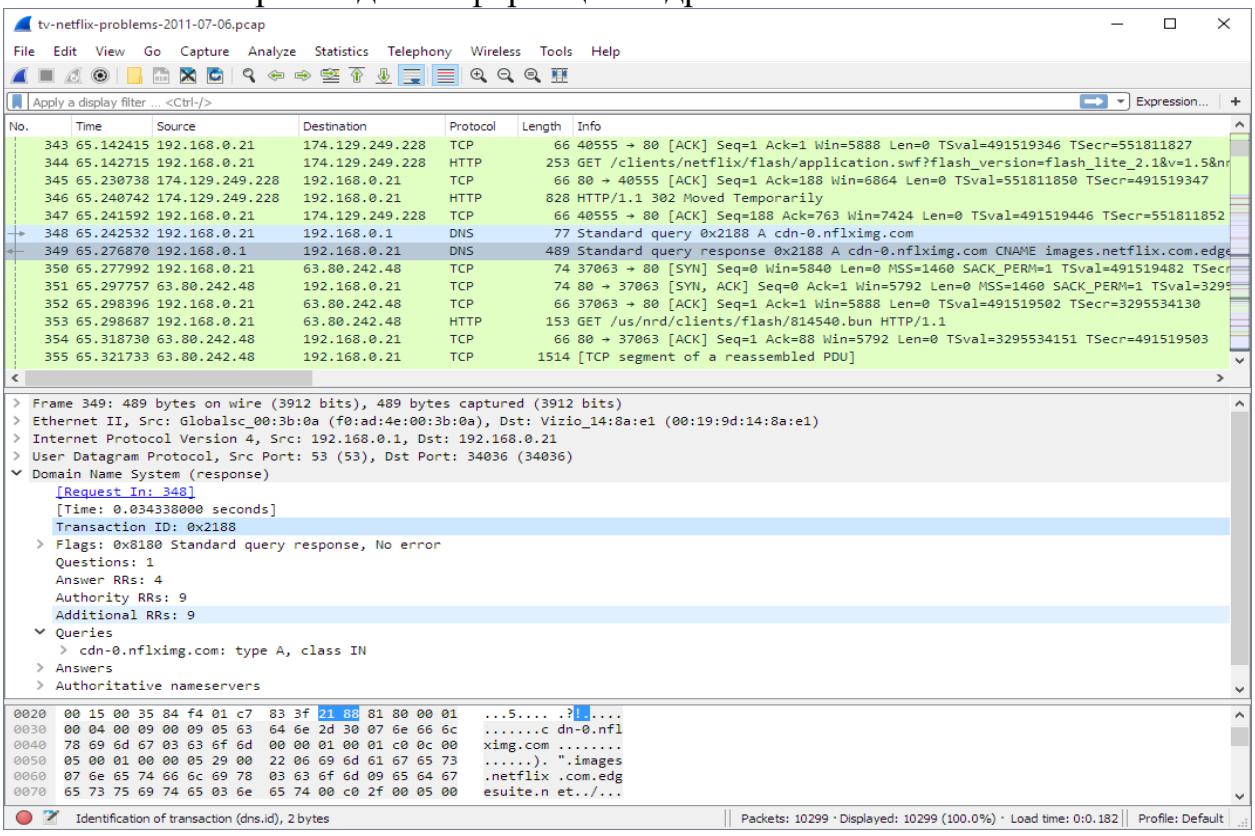


Рисунок 9 –Скриншот работы Wireshark

netcat — утилита Unix, позволяющая устанавливать соединения TCP и UDP, принимать оттуда данные и передавать их. Несмотря на свою полезность и простоту, данная утилита не входит ни в какой стандарт (например, POSIX).

Формат команд:

nc [опции] [IP хоста] [порт]

Ключи:

-h — Справка; ничего не делается

-v — Дополнительная диагностика (verbose)

-o — выходной_файл Выводить дампы данных

-i — Задержка между отправляемыми данными (в секундах)

-t — Совместимость с Telnet

-z — Не посылать данные (сканирование портов)

-u — Подключаться по UDP (вместо TCP)

-l — Пассивный режим (прослушивание порта)

-p — Локальный номер порта (для -l)

-s — Использовать заданный локальный («свой») IP-адрес

-n — Отключить DNS и поиск номеров портов по /etc/services

-w — Задать тайм-аут (в секундах)

-q — Задать время ожидания после EOF на входе (в секундах)

-e — Запустить указанную программу для обмена данных с сетью (вместо стандартных ввода и вывода)

-c —То же, в виде команды для /bin/sh

4 Используемое методическое и лабораторное обеспечение

1) Виртуальная машина «KP_ASU_SCADA_SRV» с установленной ОС Ubuntu Linux 3.19.0, содержащую в себе ПО клиентской части стенда АСУ ТП (интерфейс SCADA) с использованием протокола Modbus.

2) Виртуальная машина обучаемого с установленной ОС Kali Linux, содержащую в себе следующее программное обеспечение: tcpdump, wireshark, python 2.7.

5 Порядок выполнения работы

Лабораторная работа состоит из нескольких заданий. Задача лабораторной работы – собрать необходимые сведения (указана в задании) с помощью различных инструментов, проанализировать их, использовать собранную информацию для эксплуатации уязвимостей и сформировать отчет, содержащий полученные сведения.

5.1 Ход работы

1) Подключиться к виртуальной машине «KP_ASU_SCADA_SRV».
2) Найти открытый порт удаленного сервера

3) Подключиться к открытому порту, совершить попытку аутентификации
4) Определить ключ генерации пароля нового пользователя
5) Определить пароль администратора сервера
6) Получить IP-адрес SCADA-сервера с помощью netcat.
7)

5.2 Завершение работы

Выключить виртуальную машину «KP_ASU_SCADA_SRV».

6 Содержание отчёта о выполненной работе

В отчёте о выполненной лабораторной работе необходимо указать в виде таблиц с заполненными значениями.

6.1 Пример задания

1) Подключиться к виртуальной машине «KP_ASU_SCADA_SRV».
2) Найти открытый порт удаленного сервера
3) Подключиться к открытому порту, совершить попытку аутентификации
4) Определить ключ генерации пароля нового пользователя
5) Определить пароль администратора сервера
6) Получить IP-адрес SCADA-сервера с помощью netcat

6.2 Пример отчета

Отчет может выполняться как на компьютере, так и на бумажном носителе в зависимости от требований преподавателя.

№	Задание	Значение
1	Найти открытый порт удаленного сервера	
2	Подключиться к порту, совершить попытку авторизации и регистрации.	
3	Определить длину ключа шифра	
4	Определить пароль администратора	
5	Получить IP необходимый для завершения аутентификации	
6	Запустить generator	

7 Контрольные вопросы

1) Назовите достоинства режима ECB.
2) Назовите недостатки ECB.

8 Бланк отчета

8.1 Задание

1) Подключиться к виртуальной машине «KP_ASU_SCADA_SRV».
2) Найти открытый порт удаленного сервера
3) Подключиться к открытому порту, совершить попытку аутентификации
4) Определить ключ генерации пароля нового пользователя
5) Определить пароль администратора сервера
6) Получить IP-адрес SCADA-сервера с помощью netcat

8.2 Ответы

№	Задание	Значение
1	Найти открытый порт удаленного сервера	
2	Подключиться к порту, совершить попытку авторизации и регистрации.	
3	Определить длину ключа шифра	
4	Определить пароль администратора	
5	Получить IP необходимый для завершения аутентификации	
6	Запустить generator	

ЛАБОРАТОРНАЯ РАБОТА № 4

АНАЛИЗ ЗАЩИЩЕННОСТИ LOG-СЕРВЕРОВ

1 Цель лабораторной работы

Целью лабораторной работы является изучение методов анализа сети и атака перебором с использованием словаря.

В ходе выполнения лабораторной работы, обучающиеся получат следующие основные навыки:

– навыки проведения атаки типа «Path Traversal»;

– навыки работы со специальным программным обеспечением для проведения сетевых атак

– навыки осуществления анонимного сетевого подключения типа «reverse_tcp»

Время выполнения работы – два академических часа.

2 Краткие теоретические сведения

Path Traversal — атака, направленная на несанкционированное получение доступа к директории, к которой атакующий не имеет доступа, из директории, к которой он имеет доступ.

Это осуществляется, например, манипуляциями с содержимым адресной строки (в веб-интерфейсе), или с содержимым команды перехода в unix-оболочках.

Один из вариантов Path Traversal — введение в адресную строку адреса директории, к которой у атакующего есть доступ, затем использование специальных символов для перехода в директорию более высокого уровня (необходимого для получения доступа к требуемой директории), и далее написание адреса искомой директории.

При этом сервер может быть сконфигурирован таким образом, чтобы предотвращать Path Traversal путем фильтрации адресной строки.

Пусть атакующий имеет доступ к директории /home, а ему нужно попасть в директорию /etc, сервер находится по адресу 192.168.2.222.

Варианты манипуляций с адресной строкой:

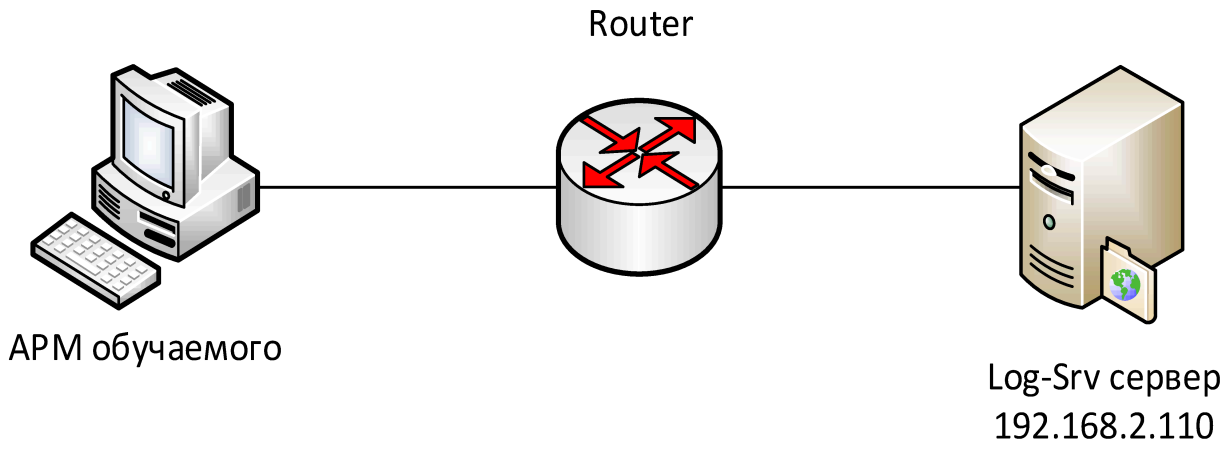
1) 192.168.2.222/home/../etc
2) 192.168.2.222/home/%2e%2e/etc

%2e: «2e» — номер символа «.» в таблице ASCII

3) 192.168.2.222/home/%252e%252e/etc

%252e: «25» — номер символа «%» в таблице ASCII

2.1 Схема стенда



3 Инструментарий

Terminal — это приложение, внутри которого выполняется командный интерпретатор. Его еще часто называют интерфейсом командной строки. Он интерпретирует команды специального языка скриптов.

По умолчанию используется командный интерпретатор Bash. Это улучшенный вариант интерпретатора Bourne Shell, который обычно называют просто «Shell». В настоящее время Bash – фактически стандарт де-факто в большинстве Unix-подобных систем.

```
root@kali-template:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.4.89  netmask 255.255.240.0  broadcast 10.10.15.255
        inet6 fe80::250:56ff:fe9f:61f4  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:9f:61:f4  txqueuelen 1000  (Ethernet)
        RX packets 332  bytes 32533 (31.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35  bytes 3223 (3.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Рисунок 10 –Скриншот работы Terminal

Работа с приложением реализована с помощью ввода команд в окно терминала.

Командная строка начинается с пользователя (root), после «@» следует его имя (kali-template), затем следует название текущего каталога — по умолчанию открывается домашний каталог пользователя, который в Unix-системах обозначается знаком «~» (тильда). Далее следует знак «#», который называется приглашением – приглашением вводить команды интерпретатору.

Формат команд:

[команда] [аргументы …]

Примеры основных команд:

– Определение текущей директории.

pwd

– Смена директории.

cd [путь]

В частности:

cd .. — сменит директорию на вышестоящую над текущей

cd / — сменит директорию на корневую

cd ~ — переместит в домашнюю папку

– Отображение всех файлов и директорий в текущей директории.

ls [опции] [файл]

– Поиск файла или директории по имени. Команда поддерживает регулярные выражения.

find [директория начала поиска] [опции]

Пример:

find . –type d –name *cookie* — поиск, начиная с текущей директории, исключительно папок, в названии которых содержится «cookie»

– Поиск файла по его содержимому.

grep [опции] [путь]

– Удаление файла.

rm [опции] [путь]

– Чтение файла, объединение файлов, создание файла.

cat [опции] [путь]

– Вывод списка работающих процессов.

ps [опции]

– Задание приоритета процессу.

nice [опции] [ID процесса]

Также, работая с терминалом, необходимо знать о функциях некоторых клавиш:

Дозаполнение названия файла или директории. При введении нескольких букв, нажмите Tab, чтобы набор был завершен автоматически.

– Остановка текущего процесса.

Ctrl+C

– Перемещение по истории введенных команд.

↑ и ↓

netcat — утилита Unix, позволяющая устанавливать соединения TCP и UDP, принимать оттуда данные и передавать их. Несмотря на свою полезность и простоту, данная утилита не входит ни в какой стандарт (например, POSIX).

Формат команд:

nc [опции] [IP хоста] [порт]

Ключи:

-h — Справка; ничего не делается

-v — Дополнительная диагностика (verbose)

-o — выходной_файл Выводить дампы данных

-i — Задержка между отправляемыми данными (в секундах)
-t — Совместимость с Telnet
-z — Не посылать данные (сканирование портов)
-u — Подключаться по UDP (вместо TCP)
-l — Пассивный режим (прослушивание порта)
-p — Локальный номер порта (для -l)
-s — Использовать заданный локальный («свой») IP-адрес
-n — Отключить DNS и поиск номеров портов по /etc/services
-w — Задать тайм-аут (в секундах)
-q — Задать время ожидания после EOF на входе (в секундах)
-e — Запустить указанную программу для обмена данных с сетью (вместо стандартных ввода и вывода)
-c —То же, в виде команды для /bin/sh

Burpsuite — это платформа для проведения аудита безопасности веб-приложений. Содержит инструменты для составления карты веб-приложения, поиска файлов и папок, модификации запросов, фаззинга, подбора паролей и многого другого.

После включения и настройки Burpsuite и браузера, программа выступает в роли прокси для трафика, получаемого браузером и исходящим от него. При этом пользователь контролирует передачу пакетов с возможностью их модификации.

Настройка Burpsuite:

1) Подготовить браузер к использованию утилиты Burpsuite.

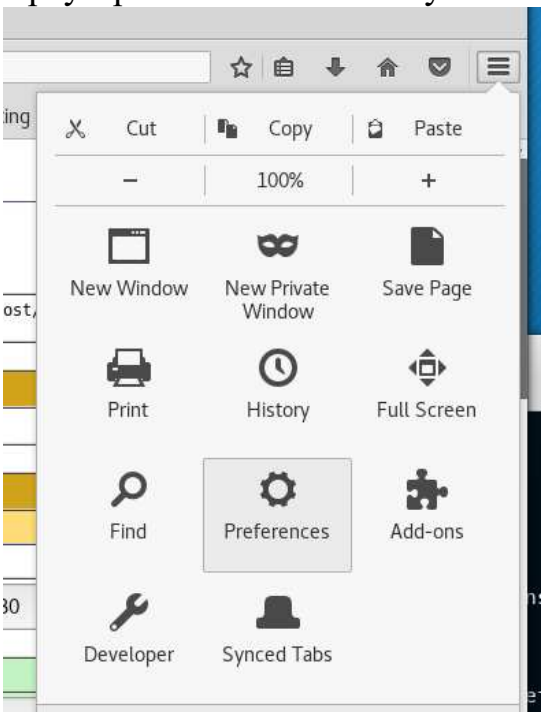


Рисунок 11 – Меню настройки браузера FireFox

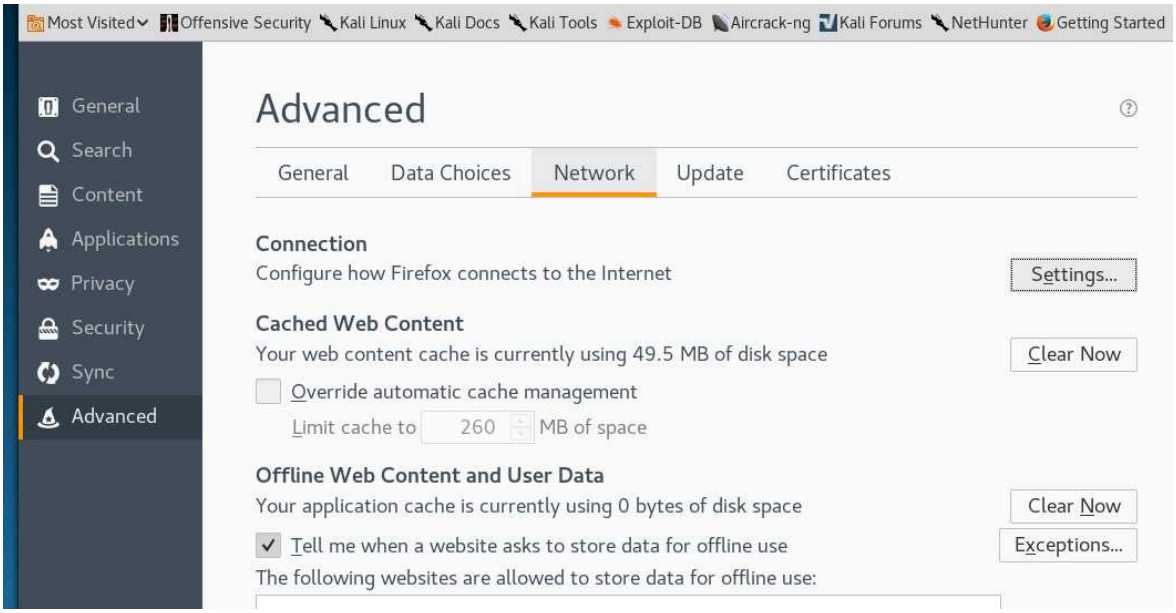


Рисунок 12 – Вкладка «Advanced»

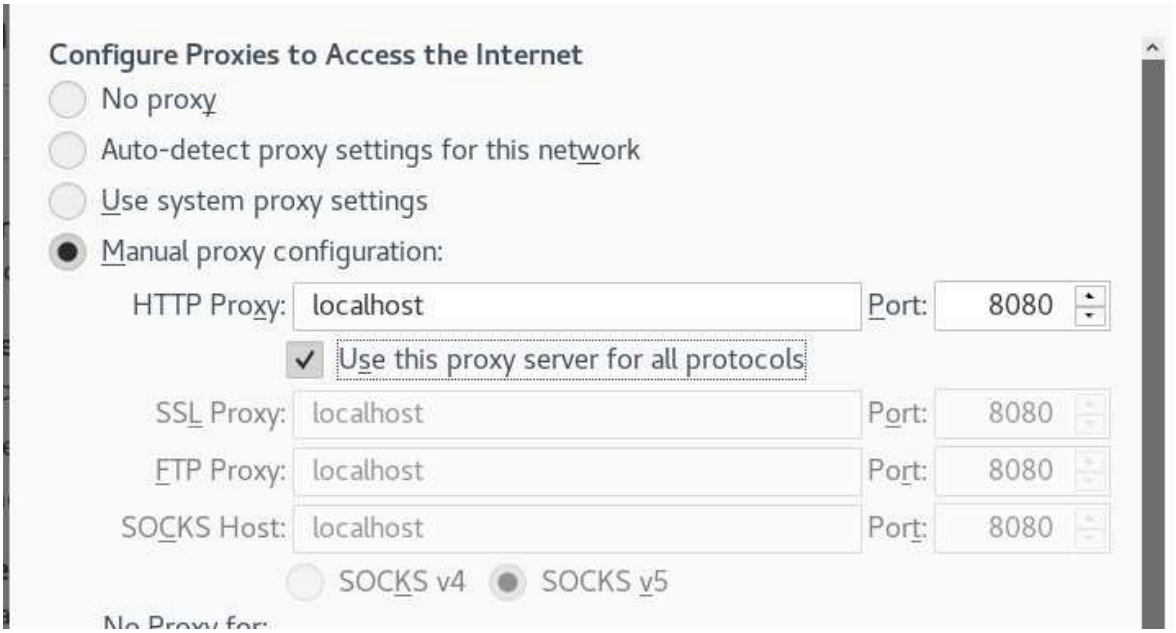


Рисунок 13 – Настройка proxy-сервера браузера

2) Запустить BurpSuit

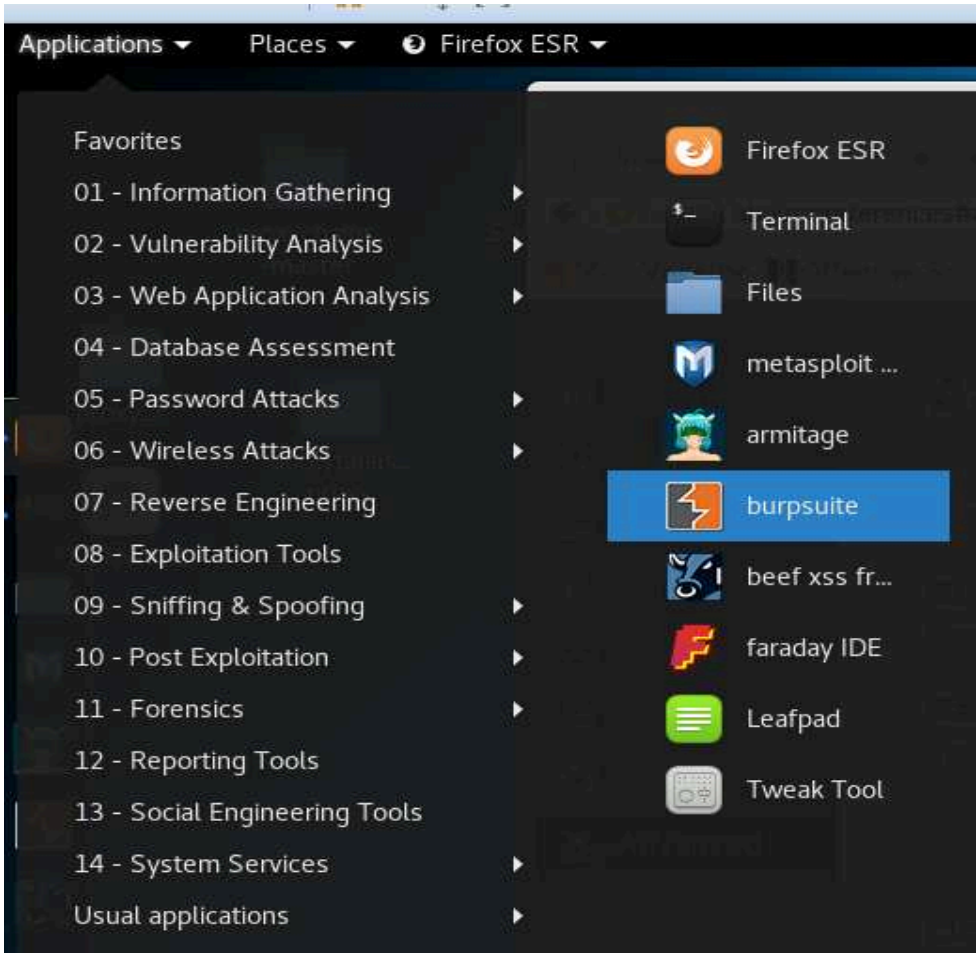


Рисунок 14 – Локация приложения «burpsuite»

3) Выбрать «I Accept»

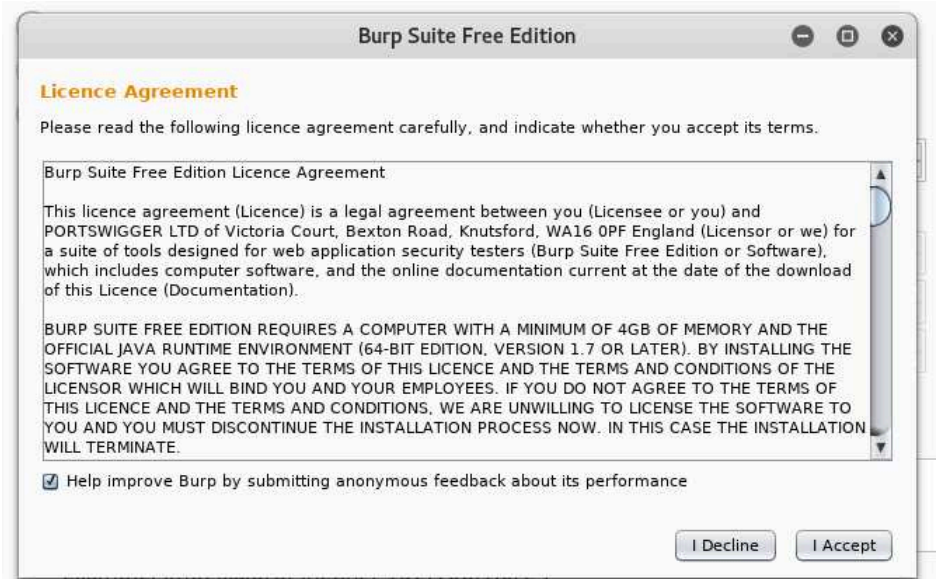


Рисунок 15 – Окно пользовательского соглашения

Далее, «Next»

Рисунок 16 – Окно выбора проекта по умолчанию

Далее, «Start burp»

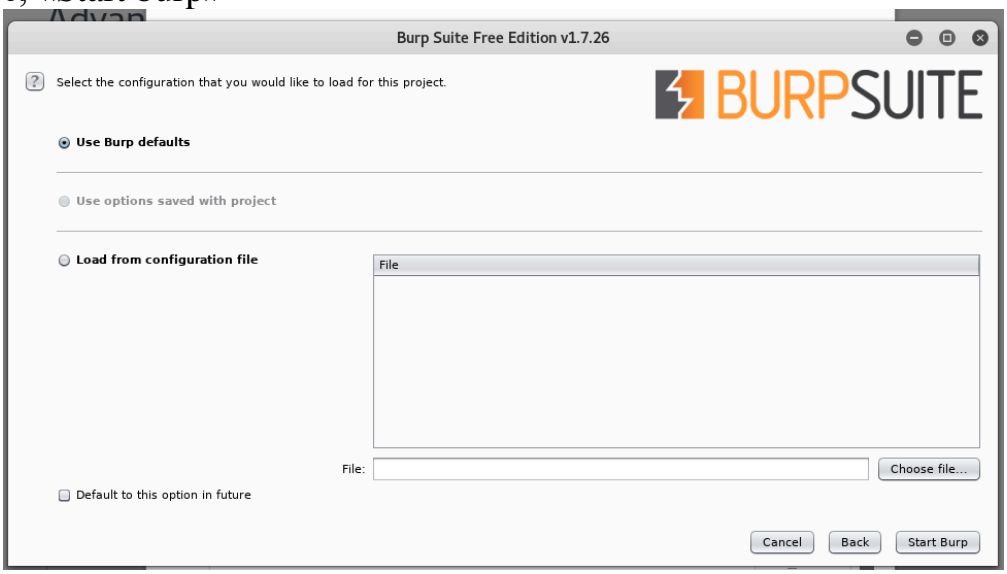


Рисунок 17 – Окно запуска burpsuite

4) Настройка Proxy в Burpsuite.

Перейти во вкладку Proxy, а затем во вкладку Options и установить перехват с порта 8080.

Для этого в настройках Proxy Listeners выделить listener и нажать на кнопку Edit. В появившемся окне перейти во вкладку Binding и установить номер перехватываемого порта – 8080, перехватываемый адрес – Loopback.

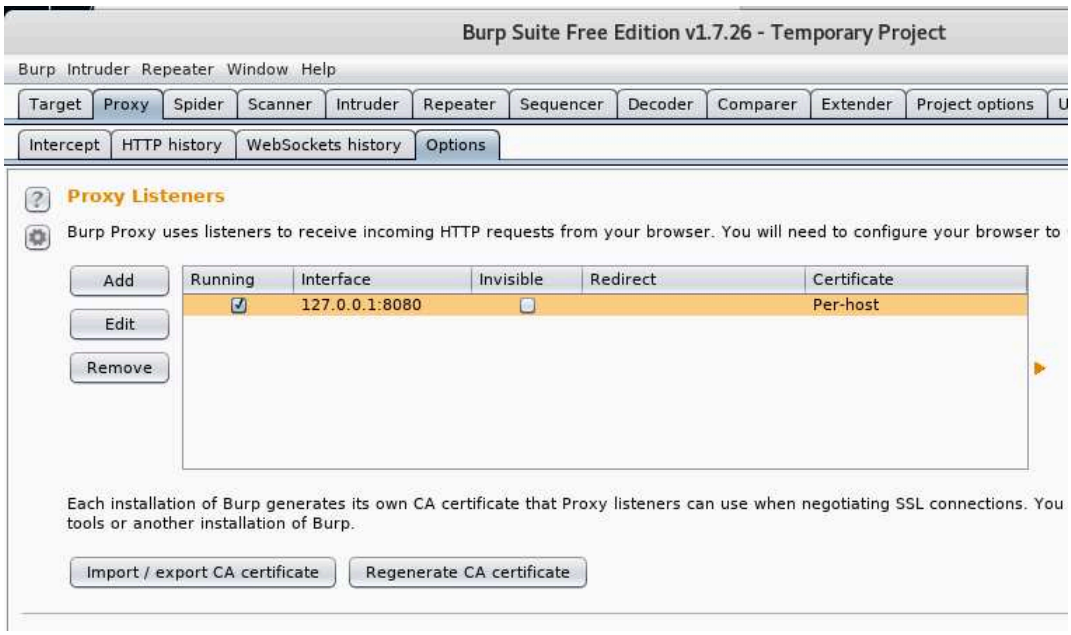


Рисунок 18 – Настройки proxy-сервера burpsuite

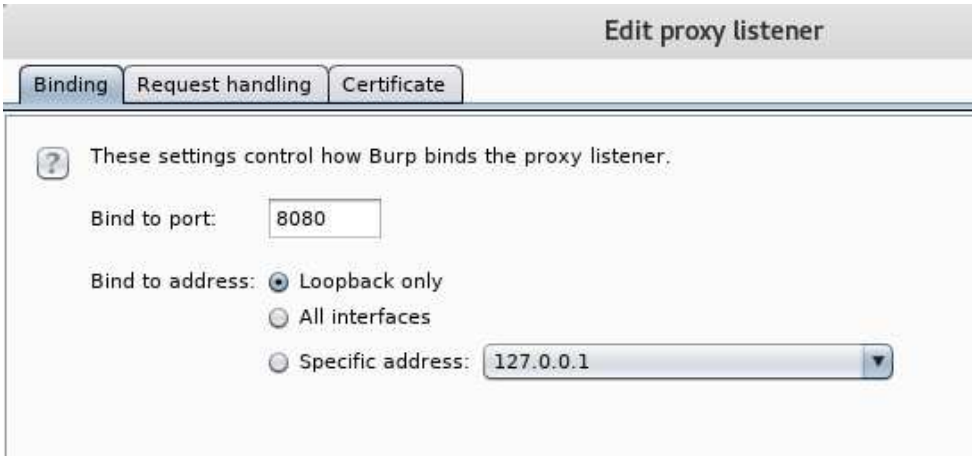


Рисунок 19 –Настройки Listener в Burpsuite

5) Запустить перехватчик трафика Proxy Listener:
Для этого поставить галочку в колонке «Running».

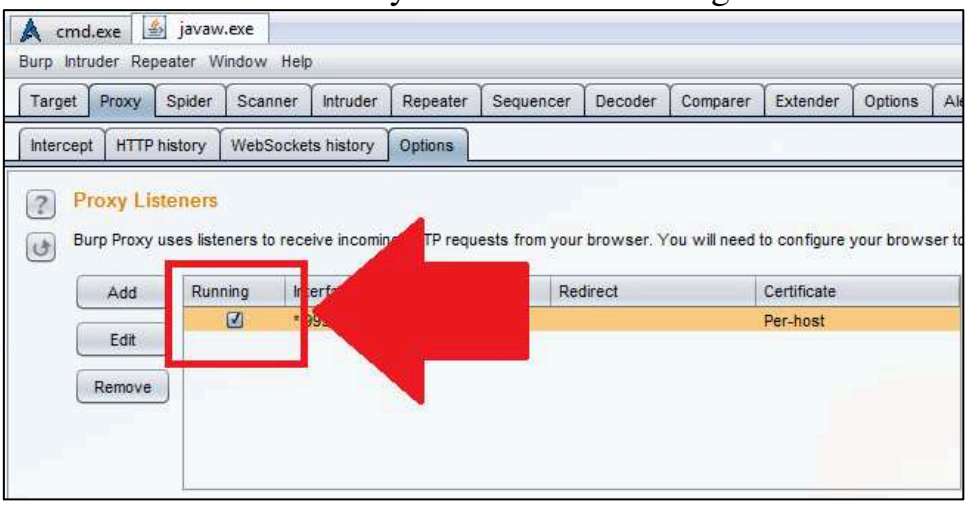


Рисунок 20 –Настройки burpsuite

Для просмотра перехвата и редактирования перейти во вкладку Intercept.

Рисунок 21 – Включение перехвата трафика

6) Далее необходимо удалить существующую cookie.

Важно знать, что адреса ресурсов сервера, к которым обращается пользователь посредством браузера сохраняются в cookie этого браузера. Чтобы Burpsuite работал корректно необходимо периодически удалять cookie из браузера.

Сделать это можно следующим образом: в Mozilla Firefox (браузер по умолчанию в Kali Linux) открыть «Preferences»:

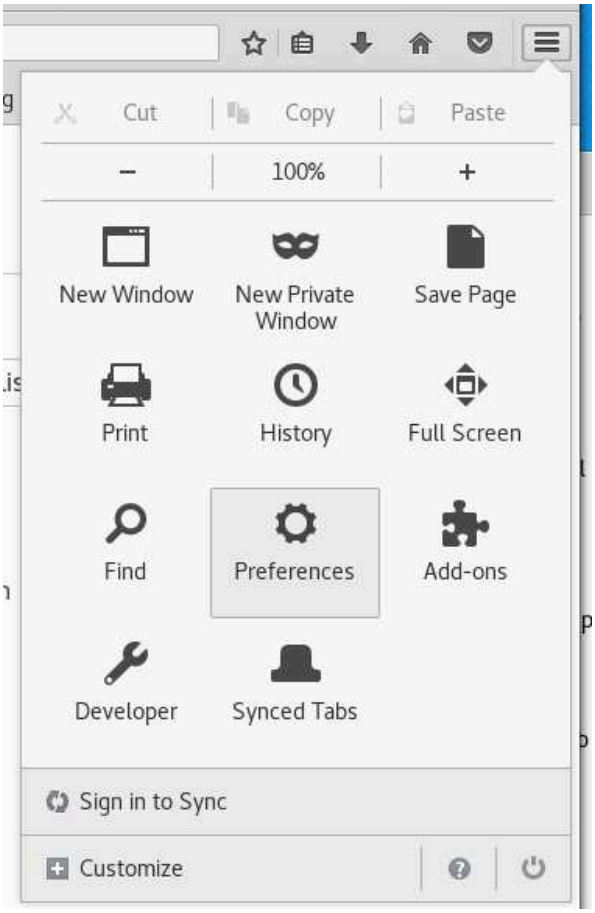


Рисунок 22 – Меню настройки браузера FireFox

7) Выбрать вкладку «Privacy» и нажать «remove individual cookies»:

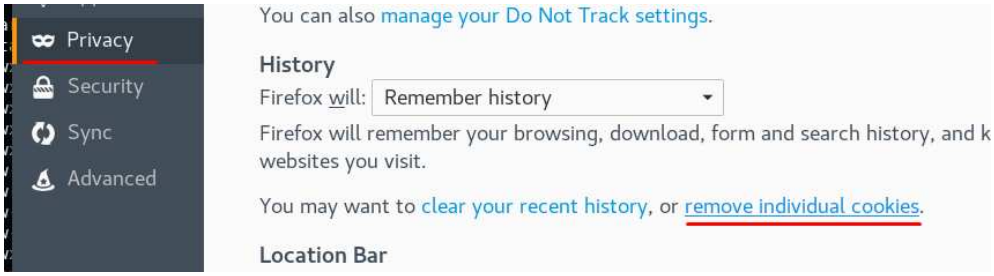


Рисунок 23 – Вкладка «Privacy»

8) Выбрать cookie адреса 192.168.2.110 (адрес Log-сервера) и нажать «remove selected».

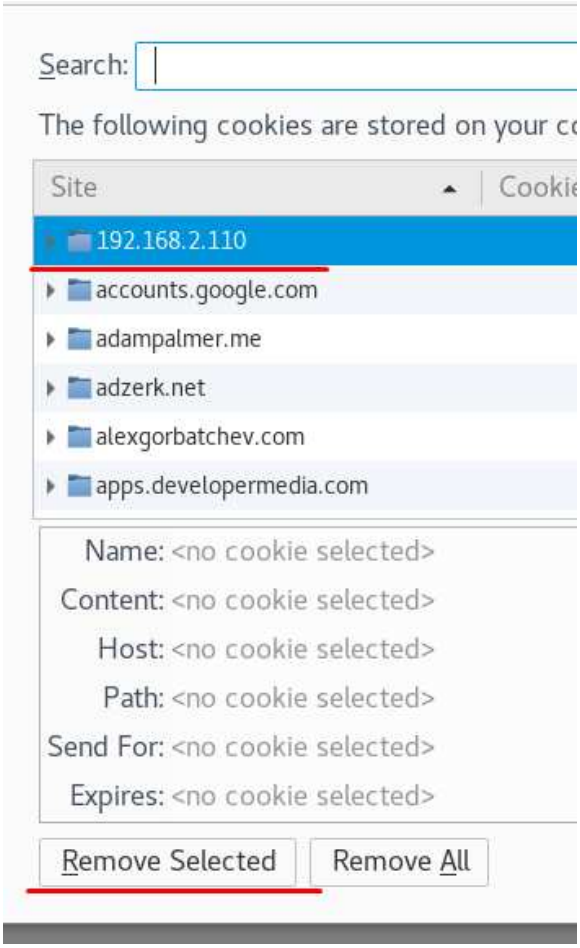


Рисунок 24 – Удаление существующих cookie

Использование Burpsuite:

Для включения или выключения Intercept-режима в Burpsuite необходимо нажать «Intercept is On/Off».

9) Перехват ответа на выбранный пакет.

Нажать кнопку «Action» интерфейса Burpsuite, далее «Do Intercept» и «Response to this request». После этого отправить пакет адресату кнопкой «Forward».

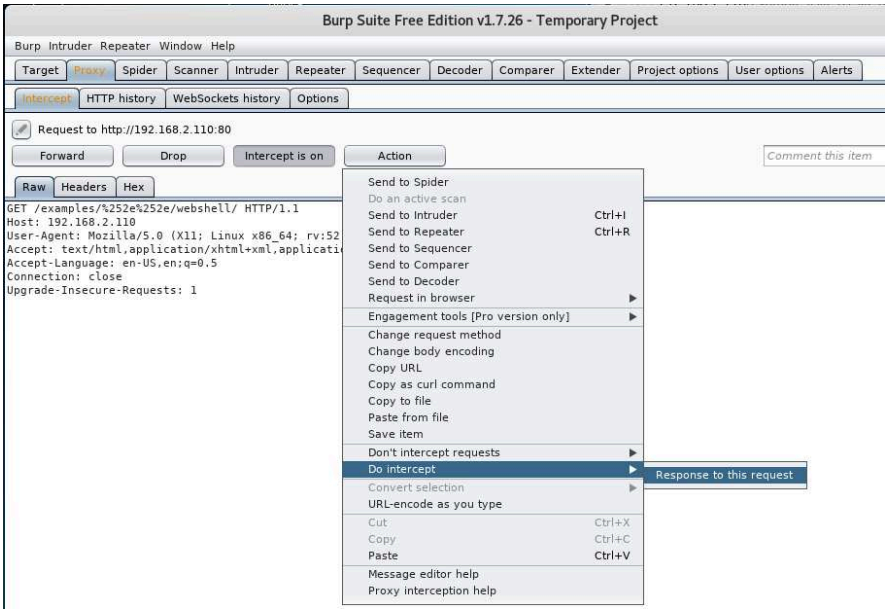


Рисунок 25 – Включение режима перехвата ответов на запрос

10) Модификация пакета.

Содержимое пакетов отображается во вкладке Raw (подвкладка Proxy, затем Intercept). Перед отправкой пакета можно менять его содержимое в поле, в котором оно отображается. Например, поменять значение параметра «Path»:

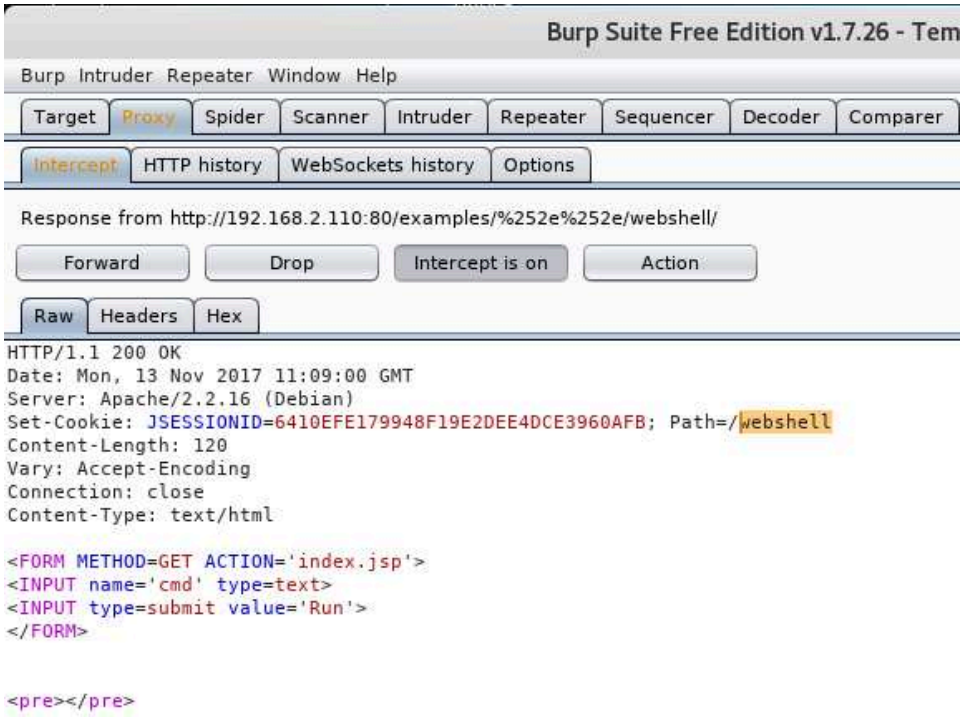


Рисунок 26 – Содержимое входящего пакета

Далее нажать «Forward» для передачи пакета адресату.

4 Используемое методическое и лабораторное обеспечение

1) Виртуальная машина «KP_ASU_SCADA_LOG» с установленной ОС Kali Linux, содержащую в себе ПО клиентской части стенда АСУ ТП (Log-сервер) с использованием сервисов apache2 и tomcat6.

2) Виртуальная машина обучаемого с установленной ОС Kali Linux, содержащую в себе следующее программное обеспечение: tcpdump, wireshark, python 2.7.

5 Порядок выполнения работы

Лабораторная работа состоит из нескольких заданий. Задача лабораторной работы – собрать необходимые сведения (указана в задании) с помощью различных инструментов, проанализировать их, использовать собранную информацию для эксплуатации уязвимостей и сформировать отчет, содержащий полученные сведения.

5.1 Ход работы

1) Подключиться к виртуальной машине обучающегося.

2) Осуществить атаку типа Path Traversal и получить доступ к управляющей консоли.

3) Залить shell на сервер «KP_ASU_SCADA_LOG»

4) Получить доступ к webshell

5) Осуществить reverse shell

5.2 Завершение работы

Выключить виртуальную машину «KP_ASU_SCADA_LOG».

6 Содержание отчёта о выполненной работе

В отчёте о выполненной лабораторной работе необходимо указать в виде таблиц с заполненными значениями.

6.1 Пример задания

1) Осуществить атаку типа Path Traversal и получить доступ к управляющей консоли.
2) Залить webshell на сервер «KP_ASU_SCADA_LOG»
3) Получить доступ к webshell
4) Осуществить reverse shell

6.2 Пример отчета

Отчет может выполняться как на компьютере, так и на бумажном носителе в зависимости от требований преподавателя.

№	Задание	Значение
1	Осуществить атаку типа Path Traversal и получить доступ к управляющей консоли.	
2	Установить webshell на сервер.	

3	Перейти в webshell.	
4	Осуществить reverse shell.	

7 Контрольные вопросы

1) На что направлены атаки типа «Path Traversal»?
2) Почему необходимо изменять значение /path в cookie во время атаки «Path Traversal»?

8 Бланк отчета

8.1 Задание

1) Осуществить атаку типа Path Traversal и получить доступ к управляющей консоли.
2) Установить webshell на сервер «KP_ASU_SCADA_LOG»
3) Получить доступ к webshell
4) Осуществить reverse shell

8.2 Ответы

№	Задание	Значение
1	Осуществить атаку типа Path Traversal и получить доступ к управляющей консоли.	
2	Установить webshell на сервер.	
3	Перейти в webshell.	
4	Осуществить reverse shell.	

ПРАВИЛЬНЫЕ ОТВЕТЫ К ТЕСТОВЫМ ВОПРОСАМ

1. Чем вызвана необходимость установления уголовной ответственности за причинение вреда в связи с незаконным использованием компьютерной информации?

б) возрастающим значением и широким применением ЭВМ во многих сферах деятельности современного общества.

2. Какая информация является наиболее уязвимой?

б) компьютерная.

3. Что такое «компьютерная информация»?

в) организационно упорядоченная совокупность сведений (сообщений, данных), зафиксированных на машинном носителе либо в информационно-телекоммуникационной сети с реквизитами, позволяющими их идентифицировать, имеющую собственника либо иного законного владельца.

4. Выберите вид преступления, связанного с противоправным вмешательством в работу ЭВМ?

в) хищение, уничтожение и подделка компьютерной информации.

5. Какое специализированное подразделение было создано для борьбы с преступлениями в сфере компьютерной информации?

в) управление «К» БСТМ МВД России.

6. Что является немаловажным значением в раскрытии любого вида компьютерного преступления?

а) характерологическая особенность психологии личности преступника.

7. Что такое «информация» согласно Федеральному закону от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»?

б) сведения (сообщения, данные) независимо от формы их представления.

8. В каком нормативном документе заложены основополагающие принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации?

а) ФЗ № 149 от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации».

9. Что такое «телекоммуникационные сети»?

в) технические механизмы (средства) и устройства информационного обмена при помощи, которых субъекты информационного права могут «обмениваться» информацией и «обращать» информацию в пространстве и времени через каналы электросети (электросвязи), представляющие собой технологические (технологичные) системы с различными видами передач (цифровое телевидение, различные виды работы в Интернете, факсимильная, телеграфная, телефонная и др., включая обмен информацией между ЭВМ и другие виды документальных сообщений).

10. Что включает в себя понятие «компьютерная информация»?

г) это информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ.

11. В каком году было создано специализированное подразделение по борьбе с преступлениями в сфере компьютерной информации?

в) 2001.

12. Какие криминалистические особенности имеют преступления, совершаемые в телекоммуникационных сетях?

б) простое и быстрое преобразование из одной объектной формы в другую, возможность сохранения в первоисточнике.

13. В какой главе УК РФ отражены статьи, относящиеся к преступлениям, совершаемым в сфере компьютерной информации?

б) 28.

14. Перечислите номера статей, относящиеся к преступлениям, совершаемым в сфере компьютерной информации:

г) Статья 272, Статья 273, Статья 274.

15. Какие некоторые характерные особенности включают в себя преступления, совершаемые в телекоммуникационных сетях?

а) неоднородность объекта посягательства;

б) выступление телекоммуникационной информации, как в качестве объекта, так и в качестве средства преступления;

в) многообразие предметов и средств преступного посягательства;

г) выступление ИТКС либо в качестве предмета, либо в качестве средства совершения преступления.

16. Дайте определение понятию «преступление, совершаемое в телекоммуникационных сетях», исходя из его особенностей.

а) предусмотренное уголовным законом общественно опасное действие.

17. Что является предметом преступлений, совершаемых в сфере телекоммуникационных сетей?

в) информация, находящаяся в телекоммуникационных сетях, и оборудование, обеспечивающее информационно-телекоммуникационные процессы.

18. Что такое MAC-адрес?

а) это уникальный идентификатор, сопоставляемый с различными типами оборудования для компьютерных сетей.

19. Какие возможности используют террористы для организации «цветных революций» во многих странах мира?

а) использование возможностей ИТКС.

20. В каком году было создано специализированное подразделение по борьбе с преступлениями экстремистской и террористической направленности?

в) 2008.

21. Деятельность по противодействию экстремизму регламентирует:

г) Федеральный закон от 25 июля 2002 г. № 114-ФЗ.

22. По российскому законодательству за деяния экстремистского характера предусмотрена ответственность:

г) уголовная и административная.

23. Основанием для признания организации экстремистской и запрета ее деятельности на территории Российской Федерации являются:

в) Судебные решения.

24. Органы государственной, законодательной и исполнительной власти осуществляют следующие меры по предупреждению экстремисткой деятельности:

г) все вышеперечисленное.

25. Под понятие «экстремистская деятельность» подпадают:

а) пропаганда и публичное демонстрирование нацистской атрибутики или символики, сходной с нацистской.

26. Предупреждение о недопустимости экстремистской деятельности общественному или религиозному объединению выносит:

г) Генеральный прокурор Российской Федерации или подчиненный ему соответствующий прокурор, также федеральный орган исполнительной власти в сфере юстиции или его соответствующий территориальный орган.

27. Террористическая деятельность – это:

г) все вышеперечисленное.

28. Определение «терроризм» закреплено:

в) в Федеральном законе Российской Федерации от 6 марта 2006 г. № 35-ФЗ.

29. Основанием для признания организации террористической и ее ликвидации является:

а) решение суда.

30. Какое определение «террористическая организация» является верным?

а) Организация, созданная в целях осуществления террористической деятельности или признающая возможность использования в своей деятельности терроризма.

31. Укажите основные направления противодействия экстремистской деятельности:

в) принятие профилактических мер, направленных на предупреждение экстремистской деятельности, в том числе на выявление и последующее устранение причин и условий, способствующих осуществлению экстремистской деятельности, выявление, предупреждение и пресечение экстремистской деятельности общественных и религиозных объединений, иных организаций, физических лиц.

32. Что является объективной стороной компьютерных преступлений и, в частности, преступлений, совершаемых в телекоммуникационных сетях?

а) нарушение прав и интересов пользования информации, находящейся в телекоммуникационной сети.

33. Что является субъективной стороной компьютерных преступлений, а также преступлений, совершаемых в телекоммуникационных сетях?

б) умышленная вина.

34. Какие первоначальные следственные действия возможны, если подозреваемые задержаны сразу после совершения преступления:

а) личный обыск и допрос задержанных, обыск по месту жительства, месту работы и месту задержания.

35. В каком году появился вирус, который не причинял вреда, а лишь выводил сообщение на экран:

б) 1975.

36. Что такое дамп памяти?

в) копия содержимого оперативной памяти, находящаяся на жёстком диске или другом энергонезависимом устройстве памяти.

37. Что такое DoS-атака?

в) атака на вычислительную систему с целью довести ее до отказа, то есть, создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднен.

38. Что такое DDoS-атака?

г) DoS-атака, выполняемая одновременно с большого числа компьютеров.

39. Что такое телефонное мошенничество?

в) преступление с использованием средств мобильной связи.

40. Что отрицательно влияет на развитие ДБО? (дистанционное банковское обслуживание)?

а) попытки неправомерного получения персональной информации пользователей систем ДБО, недостаток доверия со стороны клиентов.

41. Что вызывает необходимость существенных дополнений в Главу 28 УК РФ?

г) все выше перечисленные ответы.

42. Какая кредитная организация осуществляет выпуск и обслуживание банковских карт?

а) Банк – эмитент.

43. Какая вредоносная программа проникает и устанавливается в индивидуальное электронное устройство потерпевшего, фиксирует вводимый

пользователем логин и пароль в момент доступа к удаленному банковскому сервису?

б) Программа считывания пароля.

44. Согласно закону «О противодействии дистанционному хищению денежных средств» банк может приостановить исполнение операций по переводу денег на срок:

б) не более двух рабочих дней.

45. Как называется операция, состоящая в переводе денежных средств с одного счета на другой?

в) Транзакция.

46. Какая вредоносная программа проникает и устанавливается в мобильный телефон, рассылает с него СМС-сообщения, управляя банковским счетом владельца через услугу «Мобильный банк»?

а) Программа скрытого управления.

47. Какое максимальное наказание, согласно действующему законодательству, предусмотрено за хищение денежных средств с банковского счета в особо крупном размере?

б) 10 лет лишения свободы.

48. Какая программа необходима любому банку, действующему на территории Российской Федерации, для предоставления финансовой отчетности в Банк России за определенный период времени?

б) АРМ КБР.

49. Уникальный идентификатор, присваиваемый каждой единице активного оборудования (устройства) или некоторым их интерфейсам в компьютерных сетях Ethernet.

в) MAC-адрес.

50. Какая вредоносная программа предварительно устанавливается на электронное устройство и позволяет в режиме реального времени отправлять на него команды управления через сеть Интернет и перечислять похищенные денежные средства?

в) Программа удаленного доступа.

51. С какого момента мошенничество признается оконченным, если предметом преступления является безналичные денежные средства?

г) С момента поступления в незаконное владение виновного лица, и когда это лицо получило реальную возможность пользоваться или распоряжаться по своему усмотрению.

52. Как называется отдельная программа-клиент, которая хранит все свои данные (выписки по счетам, платежные документы)?

а) Классический «Банк-Клиент».

53. Система дистанционного банковского обслуживания, работающая через обычный Интернет-браузер, с помощью которой можно осуществлять все те же действия, что и через традиционные системы, с тем отличием, что не требуется установка дистрибутива, системы на компьютер пользователя?

б) Интернет-банкинг.

54. Технологии ДБО с использованием устройств банковского самообслуживания (банкоматов, платежных терминалов, информационных киосков):

г) Внешние сервисы.

55. Как называется оказание услуг ДБО с использованием телефонной связи?

в) Мобильный банкинг.

56. Под какие статьи УК РФ подпадают действия злоумышленников при совершении преступлений в сфере ДБО?

в) ст. 158, ст. 159, ст. 272, ст. 273.

57. На основании какого федерального закона в 2012 году в Уголовный кодекс были введены шесть новых видов мошеннических действий?

а) № 207-ФЗ.

58. Перечислите типичные виды ОРМ, осуществляемые при раскрытии и документировании преступных действий лиц, совершающих хищения денежных средств в системе ДБО:

а) наведение справок, исследование предметов и документов, наблюдение, прослушивание телефонных переговоров, снятие информации с технических каналов связи.

59. Что является основанием для проведения ОРМ, ограничивающих 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?

а) Постановление суда.

60. Система ДБО позволяет клиенту контролировать:

г) все выше перечисленное верно.

61. Виртуальный банк – это:

г) верный ответ 1 и 2.

62. К какой главе УК РФ относятся статьи 158, 159?

б) 21.

63. Как называется сеть компьютеров, зараженных вредоносной программой, позволяющей киберпреступникам удаленно управлять зараженными машинами (каждой в отдельности, частью компьютеров, входящих в сеть, или всей сетью целиком) без ведома пользователя?

б) Ботнет.

64. Что является одним из способов первичного средства выявления вредоносных программ на телефоне?

а) использование антивирусных программ.

65. Какие данные владельца «электронного кошелька» оперативный сотрудник может узнать при осуществлении соответствующего запроса?

а) персональные данные владельца кошелька.

66. Куда направляется изъятый у потерпевшего сотовый телефон после выявления факта вмешательства вредоносной программы в код операционной системы?

в) в экспертно-криминалистическое подразделение.

67. В каком году удельный вес (в %) прекращенных уголовных дел по реабилитирующим основаниям (от количества уголовных дел, находящихся в производстве на территории Российской Федерации с 2005 по 2019 гг. был наименьшим?

б) в 2007.

68. Преступления в сфере компьютерной информации преимущественно совершают:

б) лица от 14 до 35 лет.

69. Что означает понятие «фейковый»?

а) поддельный.

70. Что происходит в настоящее время с динамикой количества совершенных преступлений мошеннического характера?

б) количество преступлений возрастает.

71. Какие интернет-ресурсы наиболее подвержены атакам с хищением денежных средств?

в) интернет-торговля.

72. Что такое технический канал связи?

а) одна из составляющих частей телекоммуникационной сети, состоящая из технических средств и устройств, обеспечивающих проводную и беспроводную связь по передаче и обмену информацией во времени и в пространстве.

ОГЛАВЛЕНИЕ

Учебное издание

АЛЕСКЕРОВ ВАГИФ ИСМАИЛОВИЧ,

КОЛОКОЛЬЧИКОВА ОЛЬГА НИКОЛАЕВНА,

ВАСИЛЕНКО ЛЮДМИЛА ВЛАДИМИРОВНА,

ЛОМАКИН СЕРГЕЙ НИКОЛАЕВИЧ

СФЕРА ТЕЛЕКОММУНИКАЦИЙ И КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК ПЛАТФОРМА ДЛЯ СОВЕРШЕНИЯ СОВРЕМЕННЫХ ВИДОВ ПРЕСТУПЛЕНИЙ

Редактирование, техническое редактирование И.В. Карась

Подписано в печать 30.03.2022. Формат 60х84 1/16. Объем 24,5 уч.-изд. л.
Тираж 350 экз. Заказ 3/22. Цена договорная.

РИО ВИПК МВД России
Ул. Пихтовая, д. 3, мкр. Авиационный, г. Домодедово,
Московская обл., 142007