

МВД России

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

М. Ю. Литвинов, В. И. Алескеров

**ПРОТИВОДЕЙСТВИЕ
СОВРЕМЕННЫМ ВИДАМ ПРЕСТУПЛЕНИЙ,
СОВЕРШАЕМЫХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

Научно-практическое пособие

Часть 1

2-е издание, переработанное и дополненное

Домодедово
ВИПК МВД России
2026

ББК 67.408.135

Л 64

Авторский коллектив:

М. Ю. Литвинов, кандидат технических наук; **В. И. Алескеров**, кандидат юридических наук, доцент.

Рецензенты:

А. А. Курносенко – первый заместитель Министра внутренних дел Российской Федерации генерал-лейтенант полиции;

С. Н. Лебедев – заместитель Министра – начальник СД МВД России генерал-полковник полиции;

В. В. Голованов – начальник ГУУР МВД России генерал-лейтенант полиции;

О. В. Ильиных – начальник ГУПЭ МВД России генерал-лейтенант полиции;

О. А. Баранов – начальник ГУ МВД России по г. Москве генерал-лейтенант полиции;

В. К. Пауков – начальник ГУ МВД по Московской области генерал-лейтенант полиции;

С. А. Синенко – начальник Академии управления МВД России генерал-лейтенант полиции.

Л 64 Противодействие современным видам преступлений, совершаемых в условиях цифровизации : научно-практическое пособие : в 3 частях : 2-е издание, переработанное и дополненное / М. Ю. Литвинов, В. И. Алескеров. – Домодедово : ВИПК МВД России, 2026.

Часть 1. – 2026. – 255 с.

В научно-практическом пособии раскрываются уголовно-правовая и криминалистическая характеристики преступлений, совершаемых в условиях цифровизации. Рассматриваются проблемные вопросы раскрытия преступлений, совершаемых в сфере телекоммуникаций и компьютерной информации, особое внимание уделено раскрытию преступлений в системе дистанционного банковского обслуживания и преступлений террористического характера и экстремистской направленности.

Авторами даны понятия цифровизации, биллинга, идентификации, технического канала связи, телекоммуникационной сети, тайминга и др., с учетом криминалистического и оперативно-розыскного аспектов; впервые рассмотрены некоторые способы маскирования оперативно значимой информации.

Данное пособие предназначено для сотрудников подразделений специальных технических мероприятий, других оперативных подразделений органов внутренних дел и правоохранительной системы Российской Федерации. Будет полезно курсантам, адъюнктам, профессорско-преподавательскому составу высших учебных заведений юридического профиля правоохранительной системы Российской Федерации.

ББК 67.408.135

© ВИПК МВД России, 2026

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.

Анимешник – человек, который увлекается аниме, т.е. японской анимацией. Анимешники (изначально японская молодежная субкультура) – являются фанатами японских мультфильмов, ориентированных на подростковую и молодежную аудиторию и выполненных в оригинальной прорисовке.

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 компьютерной 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») – 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) – недокументированная возможность в программном обеспечении, оставленная разработчиком умышленно либо при уязвимости в коде, или разновидность вредоносных программ, представляющая 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 – программная или аппаратная система, эмулирующая аппаратное обеспечение компьютера и исполняющая программы для некоторых платформ или виртуализирующая их, создающая на ней среды, изолирующие друг от друга программы и даже операционные системы.

Виртуальный сервер – вид сервера, root-доступ к которому его клиент получает посредством удаленного интернет-соединения (собственные IP-адреса, порты, правила фильтрации, таблицы маршрутизации), 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), обеспечивающая процессы туннелирования и криптографии (образуется соединение, внутри которого передаваемая информация шифруется).

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 достижения определенных противоправных целей (в том числе для рассылки спама). Пользователи при этом могут даже не догадываться, что их машины заражены.

Вредоносная программа – программа, объективными свойствами которой являются модификация, уничтожение, копирование с последующей передачей 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, предоставляющая 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 – уникальное название сайта или иного другого ресурса в сети (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, тысяч «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 дампы памяти переполняются 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 как обналичивание похищенных денег и иных материальных ценностей, так и их дальнейшее перераспределение другим участникам преступной схемы, 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 иных платежных систем на реквизиты, заранее подготовленные злоумышленником.

Залищик – 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, 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 (айпи-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) – вид 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 информационно-коммуникационном пространстве 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 сфере¹.

Кодер – разработчик вредоносного программного обеспечения.

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

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 выступающее посредником для получения наличных денежных средств путем хищения в системе

¹ Чекунов И. Г. Киберпреступность: понятие и классификация // Российский следователь. 2012. № 2. С. 37

дистанционного банковского обслуживания. Данное лицо при помощи безналичных переводов может переводить оставшиеся деньги на другие счета и при этом удерживать комиссию.

Неправомерный и/или 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 впоследствии 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, касающимся преступлений с использованием компьютерных технологий.

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») – 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, позволяют такой программе достаточно качественно маскировать свое присутствие в системе, защищая ее от обнаружения пользователем и антивирусным программным обеспечением.

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 – 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 мобильного устройства или компьютера, 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 – совокупность методов психологического манипулирования, используемых мошенниками для того, чтобы заставить человека выдать конфиденциальную информацию, дать доступ к защищенным ресурсам или перевести денежные средства на счет злоумышленника. Это метод несанкционированного доступа к информации или системам хранения информации без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается одним из разрушительных.

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 не запрошенная 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 – идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправле-

ния или международными организациями, связанные с устрашением населения и/или иными формами противоправных насильственных действий.

Террористическая деятельность – 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.

Траффер – 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 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.

Фолкеры – люди, которые любят народную музыку, танцы, материальную культуру, но, тем не менее, соотносят себя с современным реальным миром, а не фантазийной реальностью (ролевики) или средневековьем (реконструкторы). Как правило, увлечение народной культурой превращается в хобби – игру на соответствующих музыкальных инструментах, танцы, пошив одежды в народном или средневековом стиле и встречи, проводимые с целью потанцевать и пообщаться.

Цифровизация (с учетом криминалистического, оперативно-розыскного и следственного аспектов) – современный этап автоматизации и информатизации в деятельности правоохранительных органов от имени государства и общества, сущностью которого является процесс перехода на современные цифровые технологии, в основе его лежит не только использование возможностей информационно-коммуникационных технологий, но также накопление, систематизация, анализ и хранение полученной оперативно значимой информации в целях дальнейшего использования и прогнозирования оперативно-розыскной и следственной ситуации специально допущенными лицами для выявления, предупреждения, пресечения и раскрытия преступлений, а также расследования уголовных дел.

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 обслуживании 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 активизируется 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 – 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 всту-

пившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности.

Экстремистские материалы – предназначенные для обнаружения 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. Пэй – 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, перенаправления 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 отправляет 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 MSOutlook;
- использование функций WindowsMAPI (инструмент обмена сообщениями в сети).

HTML (от англ. Hyper Text 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 сетях. Отличительной особенностью данного типа червей является отсутствие необходимости в пользователе как звена 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.

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 червь достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по распространению вируса P2P-Worm 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 Вашему 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 преумножить 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-Staling-Ware (вор аккаунтов).

При запуске PSW трояны ищут необходимые им сведения системных файлов, хранящих различную конфиденциальную информацию или реестр. В случае успешного поиска программа отправляет 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.

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

Прежде всего, надо улучшить работу по раскрытию преступлений. Само собой разумеется, в первую очередь тяжких и особо тяжких посягательств против личности и преступлений против собственности граждан.

Особо обращаю внимание, что по итогам 2025 года впервые за длительное время наметился, к сожалению, рост подростковой преступности. При этом доля тяжких и особо тяжких составов среди таких преступлений превысила 40 процентов. Ситуация требует адекватного и оперативного реагирования. МВД России совместно с другими правоохранительными органами необходимо значительно усилить акцент на профилактику и предотвращение подобных преступлений.

Конечно, это общенациональная задача. Разумеется, над этим работать должны все органы власти: и муниципальные, и региональные, и федеральные, – но и роль Министерства внутренних дел здесь высока.

Комплексная, системная, современная, можно сказать, умная и гибкая работа необходима и в борьбе с экстремизмом. За последний год количество преступлений экстремистской направленности тоже, к сожалению, выросло. Задача МВД России – жестко пресекать любые проявления русофобии, ксенофобии, религиозной вражды, расширять профилактическую работу в этой сфере, оперативно выявлять тех, кто стремится раскачать ситуацию в России, в нашем обществе.

Серьезное внимание следует уделять борьбе с киберпреступлениями. В прошлом году их общее количество сократилось, в том числе в отношении наиболее уязвимой социальной группы – наших граждан старшего возраста, пенсионеров. И это, безусловно, в том числе результат системных мер информационно-предупредительного характера, которые реализуются органами внутренних дел, другими нашими специальными службами и правоохранительными органами.

Уверен, что сотрудники МВД России будут и впредь ответственно нести службу. Рассчитываю на ваш профессионализм, преданность долгу и желаю вам новых успехов!

Президент Российской Федерации В.В. Путин²

² Расширенная коллегия МВД России 4 марта 2026 г.

Введение

Уважаемые коллеги, сотрудники других оперативных структурных подразделений органов внутренних дел, на которых возложены функциональные обязанности по своевременному выявлению, пресечению, предупреждению и раскрытию преступлений, в том числе совершаемых в условиях цифровизации, а также следователи (дознаватели) и другие читатели данного научно-практического пособия!

Наш авторский коллектив обращает ваше внимание на то, что все граждане Российской Федерации в это непростое время переживают события, связанные с проведением специальной военной операции³. Данное событие способствовало усилению наших патриотических чувств и потребности реализовать наш гражданский долг, что проявляется в желании многих из нас оказать посильную помощь непосредственным участникам СВО и в потребности активнее реализовывать свою гражданскую позицию любым правомерным способом. Подтверждением данной позиции является ежедневное информирование представителями Министерства обороны Российской Федерации граждан том, что изо дня в день растёт количество добровольцев, желающих непосредственно участвовать в боевых действиях в зоне проведения СВО. Кроме того, граждане Российской Федерации как никогда ярко выражают свой высокий патриотизм путем оказания гуманитарной помощи конкретным подразделениям Вооруженных сил Российской Федерации и другим участникам СВО. Данную гуманитарную помощь оказывают различные организации, учреждения, коммерческие структуры и даже граждане пенсионного возраста.

Одним из самых веских доказательств нашей сплоченности и консолидации общества является пример проведения выборов Президента Российской Федерации в период с 15 по 17 марта 2024 г. В выборах Президента Российской Федерации приняло участие подавляющее большинство граждан нашей страны, включая граждан вновь присоединенных регионов Российской Федерации (ЛНР, ДНР, Запорожская и Херсонская области). Состоявшиеся выборы показали очень высокую явку на всех избирательных участках.

Как бы ни старались страны коллективного Запада, Североатлантического альянса и их бенефициары-сателлиты любыми путями дестабилизировать обстановку путем совершения преступлений с использованием IT-технологий, а также действий террористического характера и экстремистской направленности в условиях цифровизации, они не смогли подорвать нашу веру в Победу, в государство и вновь избранного Президента Российской Федерации В.В. Путина. Президентская кампания показала силу духа российского народа и его сосредоточенность. Весь российский народ был овеян высоким патриотическим чувством и желанием проголосовать за кандидата в президенты Российской Федерации, о чем наглядно свидетельствуют представленные далее схемы.

³ Далее – «СВО».



Схема 1. Центральная избирательная комиссия Российской Федерации

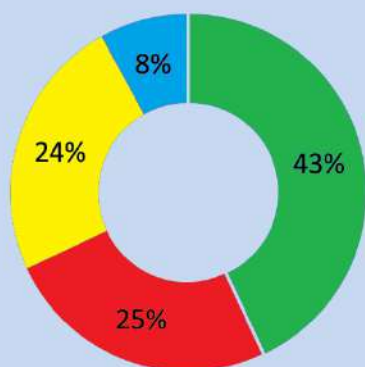


Схема 2. Основные особенности

Статистика 2023 – 2024 года
Всероссийского центра изучения общественного мнения

Участие в выборах

- Принимают участия во всех выборах
- Ходят на выборы при возможности
- Иногда ходят, иногда - нет
- Не ходят на выборы



**Уровень доверия и оценка
легитимности**

- Выборы проходят честно без серьезных нарушений закона
- Заявили об обратном
- Воздержавшиеся от ответа

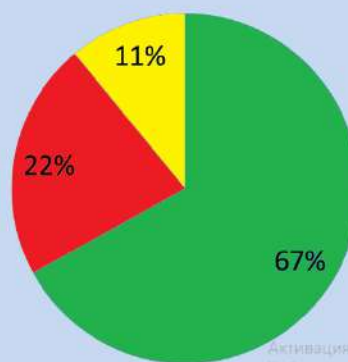


Схема 3. Статистика 2023-2024 года Всероссийского центра изучения общественного мнения

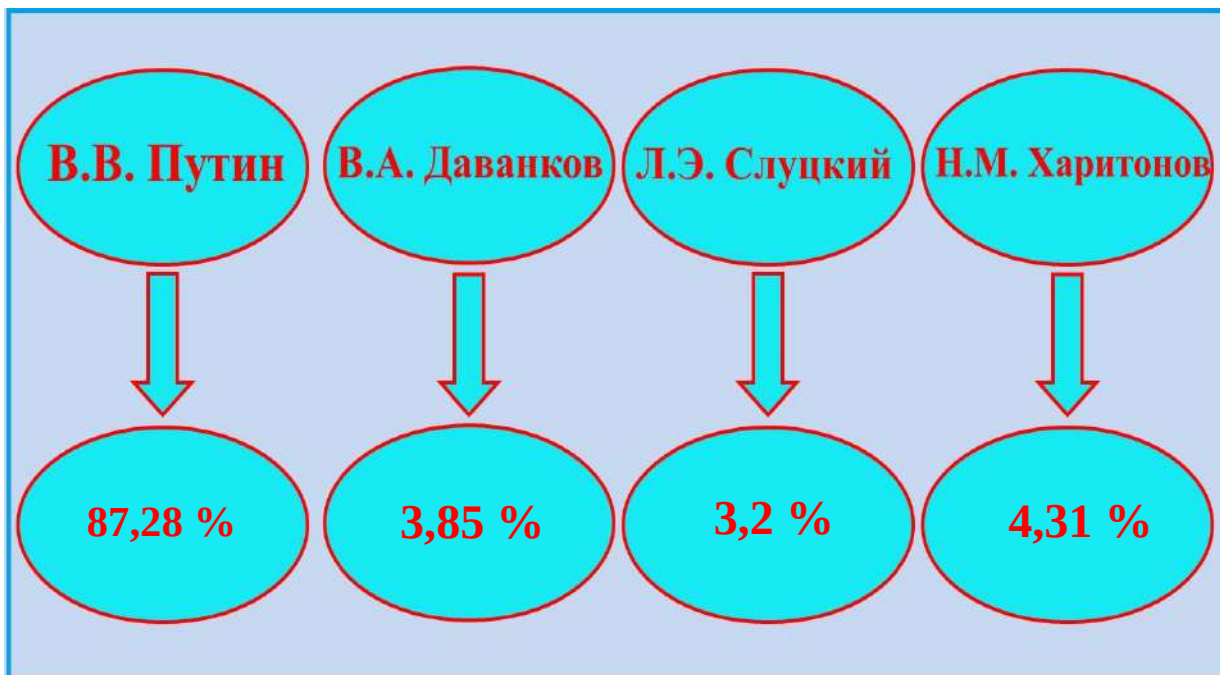


Схема 4. Итоговое подведение выборов Президента Российской Федерации

Во время подготовки данного научно-практического пособия на территории Российской Федерации в г. Москве был совершен ужасающий своей жестокостью и коварством кровавый акт терроризма. В связи с чем авторы научно-практического пособия считают значимым начать исследование заявленной темы с указания на необходимость своевременного противодействия преступлениям, совершаемым в информационно-коммуникационном пространстве в условиях цифровизации. Это имеет первостепенное значение, поскольку данный теракт был подготовлен спецслужбами стран Североатлантического альянса, коллективного Запада и Украины с использованием возможностей информационно-коммуникационной сети, а именно мессенджера «TELEGRAM», где и осуществлялся подбор кандидатов для совершения террористических актов.

Так 22 марта 2024 г. был совершен злодейский, кровавый, варварский террористический акт, начавшийся в 20 часов 15 минут в здании концертного зала-конструктора имени Муслима Магомаева, расположенного на территории комплекса «Крокус Сити Холл». Так, четверо вооруженных автоматами, винтовками и гранатами террористов, экипированных в специальную одежду с рюкзаками за спиной, незадолго до начала концерта группы «Пикник» ворвались в зал и стали жестоко и цинично расстреливать ни в чем не повинных, мирных людей, пришедших послушать выступление артистов.

После совершения этого кровавого и жестокого преступления, квалифицированного как террористический акт, убийцы сели в автомашину «Рено» белого цвета и скрылись с места преступления в неизвестном направлении. К зданию концертного зала оперативно прибыли практически все структурные подразделения ФСБ России, Следственного комитета Российской Федерации, Росгвардии, МВД России, МЧС России и пожарные службы, а также спасатели. Были объявлены планы «Перехват», «Паутина» и др., направленные на обнаружение и поимку преступников.

В целях противодействия преступной деятельности скрывшихся с места преступления четверых террористов были организованы и впоследствии скоординированы мероприятия по установлению направления движения лиц, имеющих намерение скрыться от правосудия. Благодаря тесному взаимодействию сотрудников правоохранительной системы Российской Федерации и проведению комплексных оперативно-розыскных и других поисковых мероприятий все лица, причастные к совершению этого дерзкого и кровавого террористического деяния, вскоре были обнаружены и задержаны недалеко от границы Российской Федерации с Украиной на территории Брянской области. В этот же вечер СК РФ было возбуждено уголовное дело по ст. 205 УК РФ, проведен осмотр места происшествия, где были обнаружены и изъяты следы преступления, которые впоследствии будут признаны вещественными доказательствами, назначены необходимые экспертизы и проведены другие следственные действия.

Виновные лица свою вину признали, и 25 марта 2024 г. ночью в Басманном суде г. Москвы им вынесена мера пресечения «заключение под стражу». Всех четверых подозреваемых в совершении террористического акта арестовали.

Считаем необходимым также отметить обращение к народу Российской Федерации Президента Российской Федерации В.В. Путина, в котором указывается на то, что нашу многонациональную страну никому не удастся сломить, потому что наш народ един, и своим общим усилием **по противодействию** мы сможем победить любое преступное проявление: в Москве, Подмосковье, во всех регионах страны введены дополнительные меры антитеррористического и противодиверсионного характера. Главное сейчас – не дать тем, кто стоит за этой кровавой бойней, совершить новое преступление. Что касается расследования этого преступления и результатов оперативно-розыскных действий, то в настоящее время можно сказать следующее: все четверо непосредственных исполнителей теракта, все те, кто стрелял, убивал людей, найдены и задержаны. Они пытались скрыться и двигались в сторону Украины, где, по предварительным данным, для них с украинской стороны было подготовлено «окно» для перехода государственной границы. Всего задержано 19 человек. ФСБ России и другие правоохранительные органы работают над выявлением, вскрытием всей пособнической базы террористов, тех, кто обеспечивал их транспортом, намечал пути отхода от места преступления, готовил «схроны», тайники с оружием и боеприпасами. Следственные и правоохранительные органы сделают всё, чтобы установить все детали преступления. Уже очевидно, что мы столкнулись не просто с тщательно, цинично спланированным терактом,

а с подготовленным и организованным массовым убийством мирных, беззащитных людей. Преступники хладнокровно и целенаправленно шли именно убивать, расстреливать в упор наших граждан, наших детей. Как когда-то нацисты, творившие расправы на оккупированных территориях, они задумали устроить показательную казнь, кровавую акцию устрашения. Все исполнители, организаторы и заказчики этого преступления понесут справедливое и неизбежное наказание, кем бы они ни были, кто бы их ни направлял. Будут установлены и понесут наказание все, кто стоит за спиной террористов, кто готовил это злодеяние, этот удар по России, по нашему народу. Мы знаем, что такое угроза терроризма. Рассчитываем здесь на взаимодействие со всеми государствами, которые искренне разделяют нашу боль и готовы на деле реально объединять усилия в борьбе с общим врагом – международным терроризмом, со всеми его проявлениями. Террористов, убийц, нелюдей, у которых нет и не может быть национальности ждет одна незавидная участь – возмездие и забвение. Будущего у

них нет! Наш общий долг сейчас, наших боевых товарищей на фронте, всех граждан страны – быть вместе, в одном строю⁴. «Верю! Так и будет, потому что никто и ничто не может поколебать нашу сплоченность и волю, нашу решимость и мужество, силу единого народа России. Никому не удастся посеять ядовитые семена розни, панику и разлад в наше многонациональное общество. Россия не раз проходила через тяжелейшие, порой невыносимые испытания, но становилась еще сильнее, так будет и сейчас», – этими словами было закончено обращение Президента Российской Федерации В.В. Путина к народу России.

В процессе предварительного расследования по возбужденному уголовному делу по мере проведения следственных действий одновременно проводились оперативно-розыскные мероприятия, в том числе и необходимые специальные технические мероприятия, направленные на **установление всех участников организованной преступной группы, начиная с организаторов, аналитиков, пособников, исполнителей и других виновных лиц, причастных к данному преступлению**. По окончании процесса расследования всем членам организованной преступной группы в зависимости от их роли были предъявлены обвинения, материалы уголовного дела направлены в суд для вынесения соответствующего наказания.

2-й Западный окружной военный суд 12 марта 2026 г. огласил приговор фигурантам дела о теракте в концертном зале «Крокус Сити Холл». Гособвинение в прениях сторон потребовало приговорить 15 из 19 фигурантов дела к пожизненным срокам, еще 4-х обвиняемых к лишению свободы на сроки от 19 лет 11 месяцев до 22 лет десяти месяцев. Данное заседание проходило в закрытом режиме⁵. Самый суровый приговор в истории современной России был вынесен 19 участникам террористической атаки на концертный зал «Крокус Сити Холл». Изначально было очевидно, что пожизненное лишение свободы прокуроры запросили четверым непосредственным исполнителям теракта, унесшего жизни 149 человек. Однако в прениях сторон обвинение заявило, что до конца жизни должны быть изолированы 15 участников террористического подполья, предложив сделать относительное снисхождение в виде сроков от 20 до 23 лет лишения свободы лишь нескольким их подручным, предоставлявшим жилье и машины. По мнению надзорного ведомства, отбывать долгие годы в местах лишения свободы лица, получившие пожизненное наказание, должны сначала в условиях не колонии особого режима, а тюрьмы.

Необходимо отметить, что этому предшествовал допрос засекреченного свидетеля. Как оказалось, он не был установлен в ходе предваритель-

⁴ Новостная лента телеканалов «Вести России», «Россия-1» от 23 марта 2024 г.: обращение Президента Российской Федерации В.В. Путина.

⁵ РИА Новости от 12 марта 2026 года.

ного следствия и появился лишь совсем недавно, буквально перед началом судебного слушания. Установлено, что им являлся не имеющий отношения к теракту некий знакомый подсудимых. Дополнительно установлено, что из 19 подсудимых Шамсидину Фаридуни отводилась самая активная роль. Председатель суда вне зала заседаний уточнил личность свидетеля, взял с него подписку о не разглашении сведений. После чего свидетель отвечал на вопросы суда, прокуроров и адвокатов из соседнего помещения измененным голосом. Засекреченным свидетелем были даны подробные показания о подтверждении роли всех подсудимых в причастности к совершенному теракту. В начале заседания перед военными судьями выступили трое гособвинителей. Представитель Генпрокуратуры Евгений Потапов говорил об объективной стороне преступления, его коллега - о доказательствах, подтверждающих вину подсудимых, а сотрудник прокуратуры Московской области огласил сроки наказания, которые, по мнению надзорного ведомства, обвиняемые заслуживают. Изначально было понятно, что для четверых непосредственных исполнителей Шамсидина Фаридуни, Далерджона Мирзоева, Мухаммадсобира Файзова, Саидакрами Рачабализоды, расстреливавших людей в концертном зале и поджигавших помещение, обвинение будет настаивать на пожизненном лишении свободы в колонии особого режима, а интрига заключалась в сроках наказания для их многочисленных сообщников. Необходимо заметить, что в ходе предварительного следствия многие из них давали правдивые и признавательные показания. Однако в зале судебного слушания они признавали свою вину лишь частично для смягчения и «Облегчения своей преступной роли в содеянном». Четверо из них настаивали на том, что они не были осведомлены о планах террористов и лишь оказывали помощь своим братьям по вере, знакомым и родственникам. Впрочем, как заявили в свое время представители следствия, все арестованные были знакомы в той или иной мере с планами террористов. В итоге пожизненное заключение получили 15 подсудимых, среди которых оказались и выходцы из Ингушетии Хусен Медов и Хусейн Халидов, поставившие исполнителям автоматы Калашникова и множество патронов, уже снаряженных в магазины, а оружие было переделано из охолощенных образцов. Государственные обвинители посчитали, что осужденные поступить в исправительные колонии особого режима должны только лишь после того, когда проведут свои наказания

в тюрьме от 8 до 18 лет. Суровость наказания прокуроры обосновали общественной опасностью совершенного им масштабного теракта.

В настоящее время органы прокуратуры намерены инициировать процедуру лишения гражданства Российской Федерации тех подсудимых, у кого оно имеется. Остаться без российского подданства могут

и их родственники. Представители потерпевших, выступавшие вслед за прокурорами, заявили, что поддерживают предложенное прокуратурой наказание: «Мы считаем его адекватным и соразмерным совершенному преступлению, которое находится сверх человеческих представлений радикальных верований». Следователи СКР проделали огромную работу, собрав «исчерпывающие доказательства» вины каждого из фигурантов в зависимости от его роли.

Далее необходимо продолжить наше научное исследование с краткой характеристики состояния преступности в Российской Федерации за январь-декабрь 2023 года.

За 2023 год зарегистрировано 1 947,2 тыс. преступлений, или на 1,0% меньше, чем за аналогичный период прошлого года. Рост регистрируемых преступлений отмечен в 40 субъектах Российской Федерации, что указывает на снижение количества преступлений в 45 субъектах.

92,8% всех зарегистрированных преступлений выявляются органами внутренних дел, причем 6,1% из них – на стадии приготовления и покушения. Всего на этих стадиях выявлено 110,6 тыс. преступлений (+10,9%).

Четыре преступления из пяти (82,9%) регистрируются в городах и поселках городского типа – всего 1,6 млн., шестая часть (16,5%) – в сельской местности, где зарегистрировано 321,5 тыс. преступлений, что на 7,2% меньше, чем за январь-декабрь 2022 года.

В результате преступных посягательств погибло 21,0 тыс. человек, тяжкий вред здоровью причинен 32,4 тыс. человек.

Ущерб от преступлений (по оконченным и приостановленным уголовным делам) составил 587,6 млрд. руб., что на 21,5% меньше аналогичного показателя прошлого года. Причем, более чем три четверти ущерба (84,4%) приходится на преступления, зарегистрированные в городах и поселках городского типа.

Удельный вес тяжких и особо тяжких преступлений, в числе зарегистрированных, возрос с 27,3% в январе-декабре 2022 года до 30,3%.

Больше половины всех зарегистрированных преступлений (53,5%) составляют хищения чужого имущества, совершенные путем: кражи – 583,3 тыс. (-16,4%), мошенничества – 433,7 тыс. (+26,4%), грабежа – 22,2 тыс. (-23,9%), разбоя – 3,4 тыс. (-15,4%). Почти каждая седьмое преступление – кража (13,3%), каждый двадцать седьмой грабеж (3,7%) и почти каждое седьмое разбойное нападение (13,5%) были сопряжены с незаконным проникновением в жилище, помещение или иное хранилище.

В январе-декабре 2023 года зарегистрировано 20,5 тыс. квартирных краж, что на 24,6% меньше по сравнению с аналогичным периодом прошлого года.

Количество выявленных преступлений, связанных с незаконным оборотом оружия, по сравнению с январем-декабрем 2022 года сократилось на 12,8% и составило 19,4 тыс., а количество выявленных фактов хищения и вымогательства оружия, боеприпасов, взрывчатых веществ и взрывных устройств сократилось на 31,5% (578 преступлений).

В январе-декабре 2023 года с использованием оружия, боеприпасов, взрывчатых веществ, взрывных или имитирующих их устройств совершено 5,7 тыс. преступлений (-7,9%).

В январе-декабре 2023 года зарегистрировано 677,0 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 20,7% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 26,5% в январе-декабре 2022 года до 34,8%.

Практически все такие преступления (90,8%) выявляются органами внутренних дел.

Больше половины таких преступлений (50,6%) относятся к категориям тяжких и особо тяжких (342,6 тыс.; +25,9%), более чем $\frac{3}{4}$ (77,8%) совершается с использованием сети «Интернет» (526,8 тыс.; +38,2%), почти половина (44,7%) – средств мобильной связи (302,9 тыс.; +42,2%).

Почти $\frac{2}{3}$ таких преступлений (70,2%) совершается путем кражи или мошенничества: 475,3 тыс. (+28,1%), почти каждое восьмое (12,0%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 81,5 тыс. (+31,0%)⁶.

В 2024 году органами внутренних дел рассмотрено 36,0 млн. заявлений (сообщений) о преступлениях, об административных правонарушениях, о происшествиях, что на 1,1% больше, чем за 2023 год. Из них 9,9 млн. (27,6%) были зарегистрированы как заявления (сообщения) о преступлениях.

Проведенный анализ оперативно-служебной деятельности сотрудников оперативных и следственных подразделений органов внутренних дел позволяет сделать вывод о том, что в большинстве случаев лица, совершившие указанные преступления, прибегали к использованию возможностей современной информационно-коммуникационной среды.

Изучение научно-публицистических источников, актуальных на данное время по теме исследования, показало, что в настоящее время при использовании термина «цифровизация» определение данного понятия

⁶ Статистические сведения сформированы в соответствии с приказом Генерального прокурора Российской Федерации от 3 июля 2023 г. № 429, без учета сведений о преступлениях, совершенных на территориях Донецкой и Луганской народных республик, Запорожской и Херсонской областей.

не сформулировано, поэтому авторами работы предпринята попытка привести свое видение на определение понятия «цифровизация».

Цифровизация (с учетом криминалистического, оперативно-розыскного и следственного аспектов) – новый этап автоматизации и информатизации в деятельности правоохранительных органов от имени государства и общества, сущностью которого является процесс перехода на современные цифровые технологии, в основе его лежит не только использование возможностей информационно-коммуникационных технологий, но также накопление, систематизация, анализ и хранение полученной оперативно значимой информации в целях дальнейшего использования и прогнозирования оперативно-розыскной и следственной ситуации специально допущенными лицами для выявления, предупреждения, пресечения, раскрытия и расследования преступлений.

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 коммуникаций и компьютерной информации, в условиях цифровизации ежегодно имеют тенденцию значительного роста (диаграмма 1).

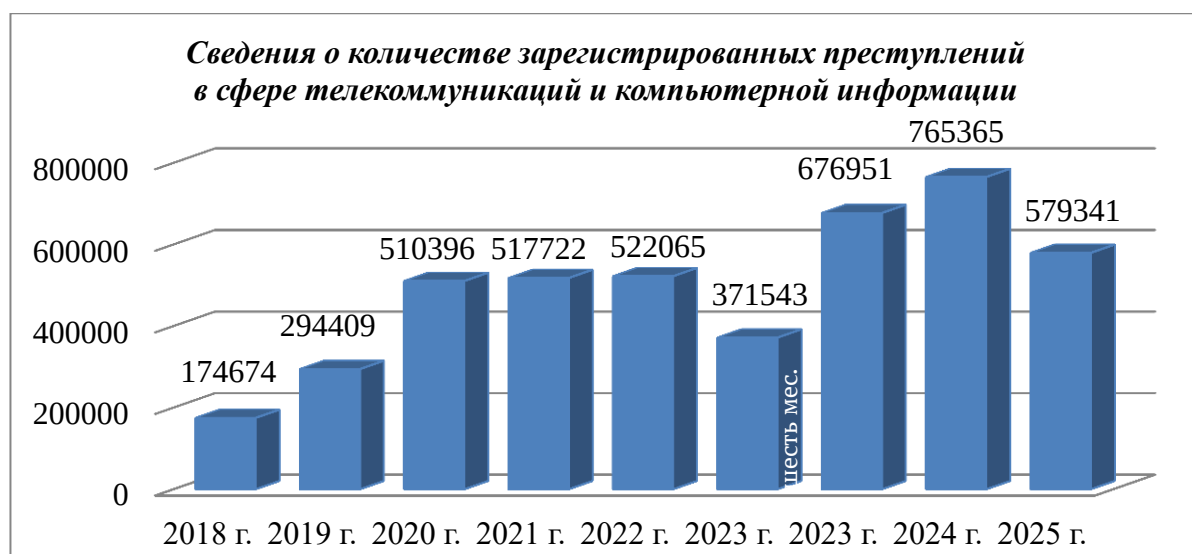


*Диаграмма 1. Сведения о количестве зарегистрированных преступлений
в сфере телекоммуникаций и компьютерной информации*

Приведем сведения ГИАЦ МВД России о состоянии преступности в России за 2021, 2022, 2023, 2024 и 2025 годы.

В январе-декабре 2021 года было зарегистрировано 517,7 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Больше половины таких преступлений (55,7%) относилось к категориям тяжких и особо тяжких (288,3 тыс.; +7,7%), более двух третей (67,9%) совершалось с использованием сети «Интернет» (351,5 тыс.; +17,0%) (см. диаграмму 4), почти половина (42,0%) – средств мобильной связи (217,6 тыс.; -0,5%).

Более чем три четверти таких преступлений (78,4%) совершалось путем кражи или мошенничества: 406,0 тыс. (-1,1%) (см. диаграмму 3), почти каждое десятое (9,9%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 51,4 тыс. (+9,3%) (см. диаграмму 2)⁷.

В январе-декабре 2022 года было зарегистрировано 522,1 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 0,8% больше, чем за аналогичный период прошлого года.

В общем числе зарегистрированных преступлений их удельный вес увеличился с 25,8% в январе-декабре 2021 года до 26,5%.

Больше половины таких преступлений (52,1%) относилось к категориям тяжких и особо тяжких (272,2 тыс.; -5,6%), почти три четверти (73,0%) совершалось с использованием сети «Интернет» (381,1 тыс.; +8,4%) (см. диаграмму 4), более трети (40,8%) – средств мобильной связи (213,0 тыс.; -2,1%).

Почти три четверти таких преступлений (71,1%) совершалось путем кражи или мошенничества: 371,2 тыс. (-8,6%) (см. диаграмму 3), почти каждое восьмое (11,9%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 62,2 тыс. (+20,9%) (см. диаграмму 2)⁸.

В январе-июле 2023 года зарегистрировано 371,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 27,9% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 24,9% в январе-июле 2022 года до 32,6%. Все указанные преступления 98,7% выявляются органами внутренних дел.

Больше половины таких преступлений 52,5% относится к категориям тяжких и особо тяжких (194,8 тыс.; +26,8%), более чем три четверти (76,8%) совершается с использованием сети «Интернет» (285,2 тыс.; +34,3%), почти половина (45%) – средств мобильной связи (167,3 тыс.; +49,1%). Почти три четверти рассматриваемых преступлений (70,8%) совершается путем кражи или мошенничества: 263,0 тысячи (28,2%),

⁷ Состояние преступности в России за январь-декабрь 2021 года / ФКУ «Главный информационно-аналитический центр МВД России», Москва.

⁸ Состояние преступности в России за январь-декабрь 2022 года / ФКУ «Главный информационно-аналитический центр МВД России», Москва.

каждое восьмое (12,8%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 47,7 тыс. (+34,9%)⁹.

В 2024 году органами внутренних дел рассмотрено 36,0 млн. заявлений (сообщений) о преступлениях, об административных правонарушениях, о происшествиях, что на 1,1% больше, чем за 2023 год. Из них 9,9 млн. (27,6%) были зарегистрированы как заявления (сообщения) о преступлениях. По каждому шестому сообщению о преступлении (15,2%) принято решение о возбуждении уголовного дела. Всего возбуждено 1511,8 тыс. уголовных дел, что на 4,6% меньше значения этого показателя за 2023 год.

В 2024 году зарегистрировано 1911,3 тыс. преступлений или на 1,8% меньше, чем за 2023 год. Рост регистрируемых преступлений отмечен в 28 субъектах Российской Федерации, снижение – в 57 субъектах.

Наибольший рост отмечается в Республике Марий Эл (10630; +28,1%), Ханты-Мансийском АО – Югре (26394; +25,5%), республиках Северная Осетия – Алания (10479; +20,8), Мордовия (9642; +20,6%), Адыгея (4503; +18,6%).

Удельный вес тяжких и особо тяжких преступлений, в числе зарегистрированных, вырос с 30,3% в 2023 году до 32,3%.

В 2024 году сохранилась позитивная тенденция снижения регистрации наиболее опасных преступлений против личности: убийство и покушение на убийство – на 9,8%, умышленное причинение тяжкого вреда здоровью – на 8,1%.

Больше половины всех зарегистрированных преступлений (50,5%) составляют хищения чужого имущества, совершенные путем: кражи – 499,6 тыс. (-14,3%), мошенничества – 445,7 тыс. (+2,8%), грабежа – 17,6 тыс. (-20,7%), разбоя – 2,8 тыс. (-16,3%). Почти каждая девятая кража (10,7%), каждый двадцать седьмой грабеж (3,8%) и почти каждое седьмое разбойное нападение (13,8%) были сопряжены с незаконным проникновением в жилище, помещение или иное хранилище.

Наибольшее снижение числа зарегистрированных краж наблюдается в Ненецком автономном округе (-31,4%), в республиках Ингушетия (-30,6%), Бурятия (-28,4%), Курганской области (-28,4%), Чукотском автономном округе (-28,2%), г. Севастополе (-27,9%).

В 2024 году зарегистрировано 14,6 тыс. квартирных краж. По сравнению с 2023 годом их число сократилось на 28,7%.

Количество выявленных преступлений, связанных с незаконным оборотом оружия, по сравнению с 2023 годом уменьшилось на 4,2% и составило 18,6 тыс., а количество выявленных фактов хищения

⁹ Состояние преступности в России за январь-июль 2023 года / ФКУ «Главный информационно-аналитический центр МВД России», Москва.

и вымогательства оружия, боеприпасов, взрывчатых веществ и взрывных устройств уменьшилось на 6,2% (542 преступления).

В 2024 году с использованием оружия, боеприпасов, взрывчатых веществ, взрывных или имитирующих их устройств совершено 5,8 тыс. преступлений (+0,8%).

Наибольшее количество зарегистрированных преступлений данной категории отмечается в Белгородской (491), Брянской (324), Курской (261) областях, Республике Дагестан (179), г. Москве (164), Свердловской (149) и Московской (144) областях.

С использованием огнестрельного, газового оружия, боеприпасов совершено 3,9 тыс. преступлений (-3,4%).

В 2024 году количество зарегистрированных преступлений экономической направленности, выявленных правоохранительными органами, практически осталось на уровне 2023 года и составило 105,4 тыс. преступлений, их удельный вес, в общем числе зарегистрированных, составил 5,5%.

Материальный ущерб от указанных преступлений (по оконченным и приостановленным уголовным делам) составил 295,7 млрд. руб., а сумма возмещенного ущерба – 306,4 млрд. руб.

Две трети (64,3%) в общем числе выявленных преступлений экономической направленности составили тяжкие и особо тяжкие преступления.

Подразделениями органов внутренних дел выявлено 83,8 тыс. преступлений экономической направленности, их удельный вес в общем массиве преступлений экономической направленности составил 79,5%.

Подразделениями экономической безопасности и противодействия коррупции органов внутренних дел выявлено 65,5 тыс. преступлений экономической направленности; их удельный вес в общем массиве преступлений экономической направленности составил 62,1%.

Материальный ущерб от указанных преступлений (по оконченным и приостановленным уголовным делам) составил 204,6 млрд. руб., а сумма возмещенного ущерба – 242,3 млрд. руб.

Более трети (40,0%) зарегистрированных в 2024 году преступлений совершается с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (всего 765,4 тыс.; +13,1%).

В общем числе зарегистрированных преступлений их удельный вес увеличился с 34,8% в 2023 году до 40,0%.

Почти половина таких преступлений (48,2%) относится к категориям тяжких и особо тяжких (369,3 тыс.; +7,8%), четыре преступления из пяти

(84,8%) совершаются с использованием сети «Интернет» (649,1 тыс.; +23,2%) (см. диаграмму 4), почти половина (45,2%) – средств мобильной связи (346,0 тыс.; +14,3%). Почти две трети таких преступлений (63,5%) совершается путем кражи или мошенничества: 486,3 тыс. (+2,3%) (см. диаграмму 3), почти каждое восьмое (12,4%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 94,6 тыс. (+16,1%) (см. диаграмму 2).

В 2024 году наблюдается рост (+3,7%) регистрации фактов незаконного оборота наркотиков. Всего было выявлено 198,0 тыс. таких преступлений. При этом сотрудниками органов внутренних дел выявлено 191,8 тыс. преступлений (+3,3%). По сравнению с 2023 годом на 7,0% выросло число выявленных преступлений, совершенных с целью сбыта наркотических средств, психотропных веществ или их аналогов. Также вырос их удельный вес в числе преступлений, связанных с незаконным оборотом наркотиков, с 66,1% в 2023 году до 68,2%.

Не раскрыто 929,7 тыс. преступлений, что на 2,0% больше аналогичного показателя за 2023 год. Из этого количества на тяжкие и особо тяжкие преступления приходится 33,1% (в 2023 году – 32,8%). Остались нераскрытыми 381 убийство и покушение на убийство (+62,8%), 293 факта умышленного причинения тяжкого вреда здоровью (-12,8%), 283,6 тыс. краж (-18,4%), 2,2 тыс. грабежей (-37,2%), 115 разбойных нападений (-20,7%).

902,3 тыс. преступлений (+1,5%) остались нераскрытыми в связи с неустановлением лица, подлежащего привлечению в качестве обвиняемого.

В 2024 году раскрыто 41,0 тыс. преступлений прошлых лет, что на 12,8% меньше, чем в 2023 году. Почти половину (42,4%) раскрытых преступлений прошлых лет составляют кражи (17,4 тыс.) и пятую часть (19,2%) мошенничества (ст.159-159.6 УК РФ) – всего 7,9 тыс.

Организованными группами или преступными сообществами совершено 36,1 тыс. тяжких и особо тяжких преступлений (+17,1%), причем их удельный вес в общем числе расследованных преступлений этих категорий увеличился с 11,6% в 2023 году до 13,8%.

В январе-декабре 2025 года зарегистрировано 1771,2 тыс. преступлений, или на 7,3 % меньше, чем за аналогичный период прошлого года. Рост регистрируемых преступлений отмечен в 5 субъектах Российской Федерации, снижение – в 80 субъектах.

88,9 % всех зарегистрированных преступлений выявляется органами внутренних дел, причем 8,9% их них – на стадии приготовления

и покушения. Всего на этих стадиях выявлено 140,9 тыс. преступлений (+19,3%).

Четыре преступления из пяти (83,7%) регистрируются в городах и поселках городского типа – всего 1,5 млн., седьмая часть (14,6%) – в сельской местности, где зарегистрировано 259,4 тыс. преступлений, что на 13,0% меньше, чем за январь-декабрь 2024 года.

В результате преступных посягательств погибло 19,5 тыс. человек (-17,1%), здоровью 26,5 тыс. человек причинен тяжкий вред (-17,3%). На сельскую местность приходится 34,7% погибших (6,7 тыс. чел.), на города и поселки городского типа – 65,4% лиц, здоровью которых причинен тяжкий вред (17,3 тыс. чел.).

Ущерб от преступлений (по окончанным и приостановленным уголовным делам) составил 767,8 млрд. руб. Значительная часть ущерба (82,1%) приходится на преступления, зарегистрированные в городах и поселках городского типа.

Удельный вес тяжких и особо тяжких преступлений, в числе зарегистрированных, возрос с 32,3% в январе-декабре 2024 года до 35,5%.

Почти половину всех зарегистрированных преступлений (49,8%) составляют хищения чужого имущества, совершенные путем: кражи – 453,3 тыс. (-9,3%), мошенничества – 411,7 тыс. (-7,6%), грабежа – 14,4 тыс. (-18,3%), разбоя – 2,5 тыс. (-11,2%). Почти каждая двенадцатая кража (8,6%), каждый двадцать восьмой грабеж (3,6%) и каждое седьмое разбойное нападение (14,3%) были сопряжены с незаконным проникновением в жилище, помещение или иное хранилище.

В январе-декабре 2025 года зарегистрировано 10,7 тыс. квартирных краж, что на 21,7% меньше по сравнению с аналогичным периодом прошлого года.

Количество выявленных преступлений, связанных с незаконным оборотом оружия, по сравнению с январем-декабрем 2024 года сократилось на 11,9 % и составило 16,4 тыс., а количество выявленных фактов хищения и вымогательства оружия, боеприпасов, взрывчатых веществ и взрывных устройств сократилось на 10,7% (484 преступления).

В январе-декабре 2025 года с использованием оружия, боеприпасов, взрывчатых веществ, взрывных или имитирующих их устройств совершено 5,4 тыс. преступлений (-6,9%).

В январе-декабре 2025 года зарегистрировано 675,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 11,8% меньше, чем за аналогичный период прошлого года. В общем числе зарегистриро-

ванных преступлений их удельный вес уменьшился с 40,0% в январе-декабре 2024 года до 38,1% (см. диаграмму 4).

Практически все такие преступления (98,2%) выявляются органами внутренних дел. Больше половины таких преступлений (52,2%) относится к категориям тяжких и особо тяжких (352,2 тыс.; -4,6%).

Почти две трети таких преступлений (63,5%) совершается путем кражи или мошенничества: 429,0 тыс. (см. диаграмму 3), почти каждое шестое (17,4%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 117,5 тыс. (+24,2%) (см. диаграмму 2).

По сравнению с январем-декабром 2024 года на 1,7% возросло число преступлений экономической направленности, выявленных правоохранительными органами. Всего выявлено 107,2 тыс. преступлений данной категории, удельный вес этих преступлений, в общем числе зарегистрированных, составил 6,1%.

Материальный ущерб от указанных преступлений (по оконченным и приостановленным уголовным делам) составил 363,4 млрд. руб.

Тяжкие и особо тяжкие преступления в общем числе выявленных преступлений экономической направленности составили 67,6%.

Подразделениями органов внутренних дел выявлено 82,3 тыс. преступлений экономической направленности, их удельный вес в общем массиве преступлений экономической направленности составил 76,8%.

В январе-декабре 2025 года выявлено 214,8 тыс. преступлений, связанных с незаконным оборотом наркотиков, что на 8,4% больше, чем за аналогичный период прошлого года. При этом сотрудниками органов внутренних дел выявлено 207,0 тыс. преступлений (+7,9%). По сравнению с январем-декабром 2024 года на 17,6% возросло число выявленных преступлений, совершенных с целью сбыта наркотических средств, психотропных веществ или их аналогов. Также возрос их удельный вес в числе преступлений, связанных с незаконным оборотом наркотиков, с 68,2% в январе-декабре 2024 года до 73,9%.

В январе-декабре 2025 года зарегистрировано 5920 преступлений террористического характера (+59,4%) и 2241 преступление экстремистской направленности (+30,4%).

Из общего числа зарегистрированных преступлений террористического характера 3091 (+50,8%) преступление совершено в текущем году, в том числе:

- пресечено на стадии приготовления и покушения – 394 (+38,2%);
- за пределами Российской Федерации – 161 (+4,5%).

Не раскрыто 849,7 тыс. преступлений, что на 8,6% меньше аналогичного показателя за январь-декабрь 2024 года. Из этого количества на тяжкие и особо тяжкие преступления приходится 35,2% (в январе-декабре 2024 года – 33,1%). Остались нераскрытыми 210 убийств и покушений на убийство (-44,9%), 366 фактов умышленного причинения тяжкого вреда здоровью (+24,9%), 249,8 тыс. краж (-11,9%), 1,7 тыс. грабежей (-25,1%), 109 разбойных нападений (-5,2%).

788,3 тыс. преступлений (-12,6%) остались нераскрытыми в связи с неустановлением лица, подлежащего привлечению в качестве обвиняемого.

Преступлений прошлых лет в январе-декабре 2025 года раскрыто 36,9 тыс., что на 10,1% меньше, чем за аналогичный период прошлого года, 34,0% из них составляют тяжкие и особо тяжкие преступления (всего – 12,5 тыс.).

Организованными группами или преступными сообществами совершено 48,8 тыс. тяжких и особо тяжких преступлений (+35,4%), причем их удельный вес в общем числе расследованных преступлений этих категорий возрос с 13,8% в январе-декабре 2024 года до 17,7%.



Диаграмма 2. Сведения о количестве зарегистрированных преступлений, совершенных с целью незаконного производства, сбыта или пересылки наркотических средств в сфере телекоммуникаций и компьютерной информации



Диаграмма 3. Сведения о количестве зарегистрированных преступлений, совершенных путем кражи или мошенничества в сфере телекоммуникаций и компьютерной информации



Диаграмма 4. Сведения о количестве зарегистрированных преступлений, совершенных с использованием сети «Интернет» в сфере телекоммуникаций и компьютерной информации

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 сопровождается 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 и в целом с использованием возможностей IT-технологий.

В недалеком прошлом 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. долл. 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 стран 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.

В процессе комплексной работы и при международном взаимодействии сотрудниками 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 лет 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.

Далее хотелось бы отметить то, что в складывающейся ситуации участились случаи телефонных и интернет-мошенничеств. Для улучшения обстановки в виде профилактических мероприятий по предупреждению указанных преступлений эти вопросы постоянно обсуждаются на Стратегической сессии в Правительстве. Благодаря принимаемым мерам количество таких преступлений в нашей стране снизилось. Входящие звонки от компаний маркируются, а банки блокируют подозрительные денежные переводы. Только в прошлом году отменили более 27 млн. таких транзакций. Необходимо внимательней быть самим гражданам – не называть посторонним коды на подозрительные смс и не отвечать на звонки, якобы, от госструктур. С августа 2025 года операторы связи передают сообщения с данными, необходимыми для входа на портал госуслуг только после окончания телефонного разговора. С момента, когда начала действовать эта мера, заблокировано уже свыше 13 млн. таких смс. Вызовы с подменных номеров теперь пресекаются на уровне сети и не доходят до абонента. Постоянно расширяется и внедряется набор инструментов, который помогает гражданам самостоятельно защитить себя и свои средства. Практически 800 тыс. человек установили самозапрет на оформление новых сим-карт, свыше 20 млн. – на получение потребительских займов. В результате уже принятых мер впервые с июля текущего года зафиксировано снижение количества зарегистрированных цифровых преступлений¹⁰.

В настоящее время все чаще дети-школьники как старших, так и младших классов стали использовать смартфоны, в том числе

¹⁰ Новостная лента. Выступление Председателя Правительства Российской Федерации М.В. Мишустина на Стратегической сессии в Правительстве. – РИА Новости, 2026.

с выходом в глобальную сеть Интернет, что в последующем может негативно сказаться на психологии несформировавшейся личности подрастающего школьника. Родители не всегда проводят разъяснительные беседы по поводу рекомендаций общения в случае поступления непредвиденных звонков или смс-сообщений, что плачевно сказывается на безопасности самого школьника и его семьи, а также близкого окружения. Таким образом, школьники являются потенциальными жертвами не только мошеннических действий со стороны злоумышленников, которые получают информацию о сбережениях семьи, как в денежном выражении, так и на электронных счетах их родителей. Еще тяжелее может сложиться обстановка, когда возникают ситуации, где со школьниками и порастающим поколением начинают свое общение сотрудники спецслужб зарубежных государств, враждебно настроенных против политики Российского государства, а именно стран Западной Европы, Североатлантического альянса и Украины. Участились случаи, когда наша молодежь поддается на их различного рода ухищрения. В результате психологического воздействия и путем подкупа школьники, сами того не зная, попадают на уловки злоумышленников, выраженные в доставке в съемные квартиры сим-боксов и антенн, их активации и последующей рассылки мошеннических сообщений, а также проведении последующих миллионных звонков через незаконно установленное вышеназванное оборудование. Таким образом, наша молодежь становится жертвой обмана, совершая тяжкие и особо тяжкие преступления. В их отношении возбуждаются уголовные дела по преступлениям против собственности (статья 159 УК РФ) и общественной безопасности (статья 205 УК РФ), после чего они оказываются на скамье подсудимых и получают значительные сроки наказания, как правило, от 15 до 20 лет лишения свободы.

С целью недопущения таких нежелательных тяжелых последствий сотрудники правоохранительных органов активизируют свою работу по своевременному получению оперативно значимой информации, после чего осуществляют специальные рейды, направленные на изобличение организованных групп и преступных сообществ, которые дают свои результаты.

Стало известно о проведенной совместной крупной операции ФСБ и МВД России. Упреждающий удар по кибермошенникам проведен сразу по нескольким российским регионам. В результате чего были задержаны почти 20 человек, все администраторы так называемых сим-боксов. Достоверно известно, что именно с помощью таких устройств украинские аферисты подменяют телефонные номера на российские. В результате использования мошенниками из украинских колл-центров технических возможностей сим-боксов и аналогичных устройств происходит отбор у наших граждан накопленных сбережений.

По данным ФСБ России, такие сим-боксы и сим-шлюзы, роутеры и ноутбуки украинские спецслужбы используют для координации подрывной и диверсионно-террористической деятельности. В Российской Федерации с 1 сентября 2026 года незаконное использование сим-боксов будет уголовно наказуемо до шести лет лишения свободы.¹¹

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 изоэтно, 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 своих преступных замыслов.

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 сфере¹².

¹¹ Новостная лента. Выступление Председателя Правительства Российской Федерации М.В. Мишустина на Стратегической сессии в Правительстве. – РИА Новости, 2026.

¹² Историческая и социально-образовательная мысль // Всероссийский научный журнал. 2014. № 4 (26). С. 350.

Исходя из складывающихся оперативно-розыскных и следственных ситуаций в ходе раскрытия преступлений, совершаемых в **сфере телекоммуникаций и компьютерной информации и в целом с использованием возможностей ИТ-технологий**, было и предложено данное научно-практическое пособие.

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 оперативных подразделений и следственных органов внутренних дел Российской Федерации 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 обеспеченности, место жительства, а также места проведения досуга и возможная принадлежность к определенной субкультуре¹³. 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 ориентирует и приблизит оперативных сотрудников и следователей к проведению оперативно-розыскных, специальных технических мероприятий¹⁴ 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

¹³ Ворошилова Т.В. Социальная и психологическая характеристика личности компьютерного преступника. Москва, 2009. С. 5.

¹⁴ Далее – «ОРМ», «СТМ».

Российской Федерации от 13 июня 1996 г. № 63-ФЗ¹⁵ 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 отношения¹⁶.

Проанализировав нормы из различных отраслей права, можно сделать ряд выводов¹⁷:

1. Информация – сведения (сообщения, данные) независимо от формы их представления¹⁸.

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

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

4. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)¹⁹.

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

Конфиденциальной в соответствии с законом является информация:

- содержащая государственную тайну²⁰;
- передаваемая путем переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений²¹;
- содержащая служебную тайну, коммерческую тайну²², налоговую или банковскую тайну²³, личную тайну и семейную тайну²⁴, информация, являющаяся объектом прав, смежных с авторами²⁵;

¹⁵ Далее – «УК РФ».

¹⁶ Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. Домодедово: ВИПК МВД России. 2013. № 2 (26).

¹⁷ Историческая и социально-образовательная мысль // Всероссийский научный журнал. 2014. № 4 (26). С. 351.

¹⁸ Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ.

¹⁹ Там же – Ст. 5.

²⁰ О государственной тайне: Федеральный закон от 21 июля 1993 г. № 5485-1; УК РФ. Ст. 275, 276, 283, 284.

²¹ Конституция РФ. Ст. 23.Ч.2; УК РФ. Ст. 138.

²² УК РФ. Ст. 183.

²³ Там же.

²⁴ Там же – Ст. 137.

²⁵ Гражданский кодекс Российской Федерации от 30 ноября 1994 г. № 51-ФЗ. Гл. 71, далее – ГК РФ; УК РФ. Ст. 146.

- непосредственно затрагивающая права и свободы гражданина или персональные данные²⁶ 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»²⁷. Начальные шаги в теории информации были сделаны еще в первой половине XX в.: в 1928 году Р. Хартли впервые дал количественное определение информации, а в 1948 году вышла знаменитая книга К. Шеннона «Математическая теория связи», где информация и дается уже как статистическое определение.

Винер Н., 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»²⁸. К. Шеннон, который сыграл не меньшую роль в развитии кибернетики, рассматривал информацию как сигнал (сообщение), устраняющий или снижающий неопределенность²⁹.

Фатьянов А.А. 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 –

²⁶ Об информации, информатизации и защите информации: Федеральный закон. УК РФ. Ст.140.

²⁷ Большой энциклопедический словарь. Москва, 2004. С. 421.

²⁸ Винер Н. Кибернетика и общество. Москва, 2003. С. 35.

²⁹ Шеннон К. Работы по теории информации и кибернетике. Москва, 1963. С. 59.

как информация, циркулирующая по электронным каналам связи. Кибернетика доказала, что информация имеет непосредственное отношение к процессам управления и развития, обеспечивающим функционирование любых систем³⁰.

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, внесенные Федеральным законом Российской Федерации от 31 июля 2025 г. № 282-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», вступили в силу с 1 сентября 2025 г.

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)³¹. В соответствии со ст. 5 Федерального закона от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и о защите информации», информация в зависимости от порядка ее предоставления или распространения подразделяется:

- 1) на информацию, свободно распространяемую;
- 2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- 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 г. № 5485-1 «О государственной тайне» (в ред. Федеральных законов от 4 августа 2023 г. № 432-ФЗ, от 8 августа 2024 г. № 249-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;

³⁰ Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. Домодедово: ВИПК МВД России. 2013. № 2 (26). С. 32-37.

³¹ Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации: учеб. пособие. Москва, 2001. С. 10.

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») неотделимы 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 таковой³².

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

³² 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.

в форме, доступной восприятию ЭВМ»³³. Комиссаров В.С. 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»³⁴. По нашему мнению, понятия, предложенные С.А. Пашиным и В.С. Комиссаровым, 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 государства³⁵.

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 и программные 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), 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) (см. рис. 1).

³³ Комментарий к Уголовному кодексу Российской Федерации / под общ. ред. Ю.И. Скуратова, В.М. Лебедева. Москва, 2001. С. 696.

³⁴ Уголовное право России / под ред. В.С. Комиссарова. Москва, 2006. С. 307.

³⁵ Дуленко В.А., Мамлеев Р.Р., Пестриков В.А. Преступление в сфере высоких технологий: учебное пособие. Москва, 2010. С. 196.

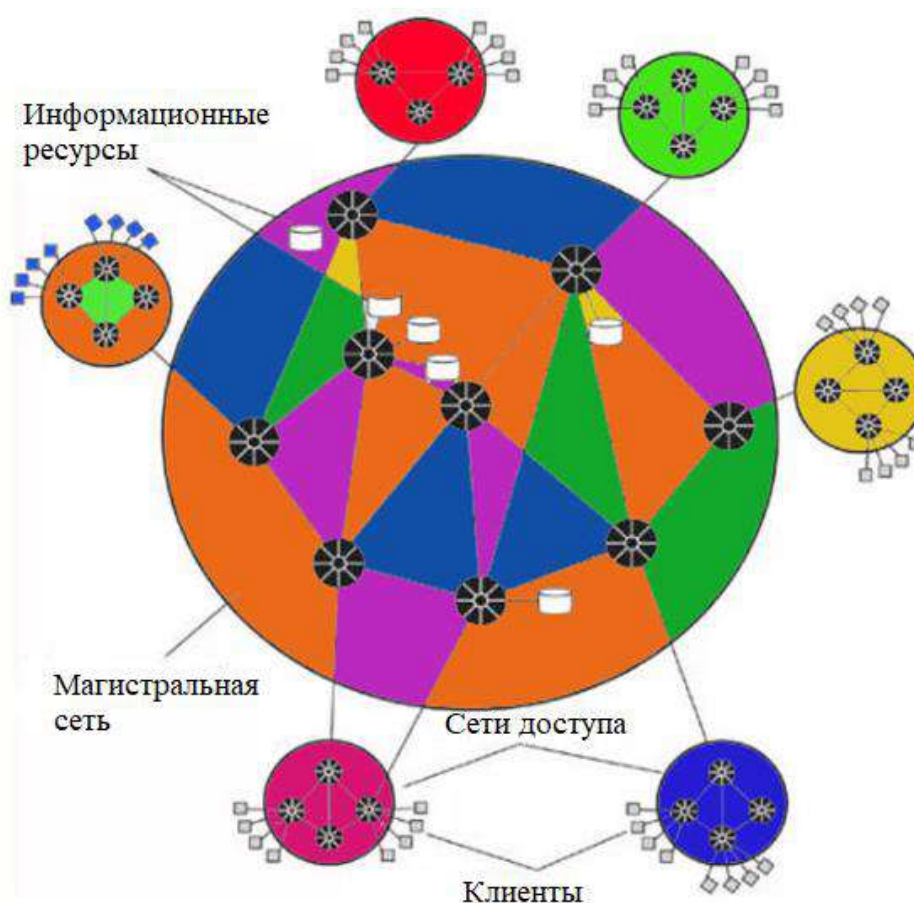


Рис. 1. Телекоммуникационная сеть

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 норм³⁶.

³⁶ Вестник Всероссийского института повышения квалификации сотрудников МВД России. Домодедово: ВИПК МВД России. 2013. № 2 (26). С. 32-37.

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»³⁷**. 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»³⁸.

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...»³⁹. Отсюда можно сделать вывод, что информация становится объектом гражданского законодательства.

³⁷ Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. №149-ФЗ. Ст. 2.

³⁸ Крылов В.В. Информация как элемент криминальной деятельности // Вестник Московского университета. Сер. 11. Москва: Право, 1998. № 4.

³⁹ Копылов В.А. Информационное право. Москва: Юристъ, 1997. С. 23.

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 «**Преступления 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 оперативных подразделений органов внутренних дел Российской Федерации 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**⁴⁰:

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 злоумышлен-

⁴⁰ Вестник ВИПК МВД России. Домодедово: ВИПК МВД России. 2012. № 3 (23). С. 69.

никам 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;
- 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;
- статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования;
- статья 274.3. Незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции;
- статья 274.4. Организация деятельности по передаче абонентских номеров с нарушением требований законодательства Российской Федерации;
- статья 274.5. Организация деятельности по передаче информации, необходимой для регистрации и (или) авторизации пользователя сети «Интернет» для получения доступа к функциональным возможностям информационного ресурса.

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 сейфе⁴¹.

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.

⁴¹ Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // Рос. юстиция. 1999. № 1. С. 44-45.

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 предусмотренные уголовным законом общественно опасные действия, совершенные 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 государства⁴².

Однако выстроенные глобальные информационные сети, востребуемые современным цивилизованным обществом, все чаще используются и лицами, склонными к совершению различного рода преступлениям. К нашему сожалению, статистические данные говорят, что такое незаконное использование сферы телекоммуникаций и компьютерной информации из года в год растет, но в 2025 году просматривается некоторое снижение на 12,24% по соотношению с 2024 годом (см. диаграмму 5).

⁴² Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2012. № 1. С. 9-10.

Состояние преступности в сфере компьютерных и телекоммуникационных технологий

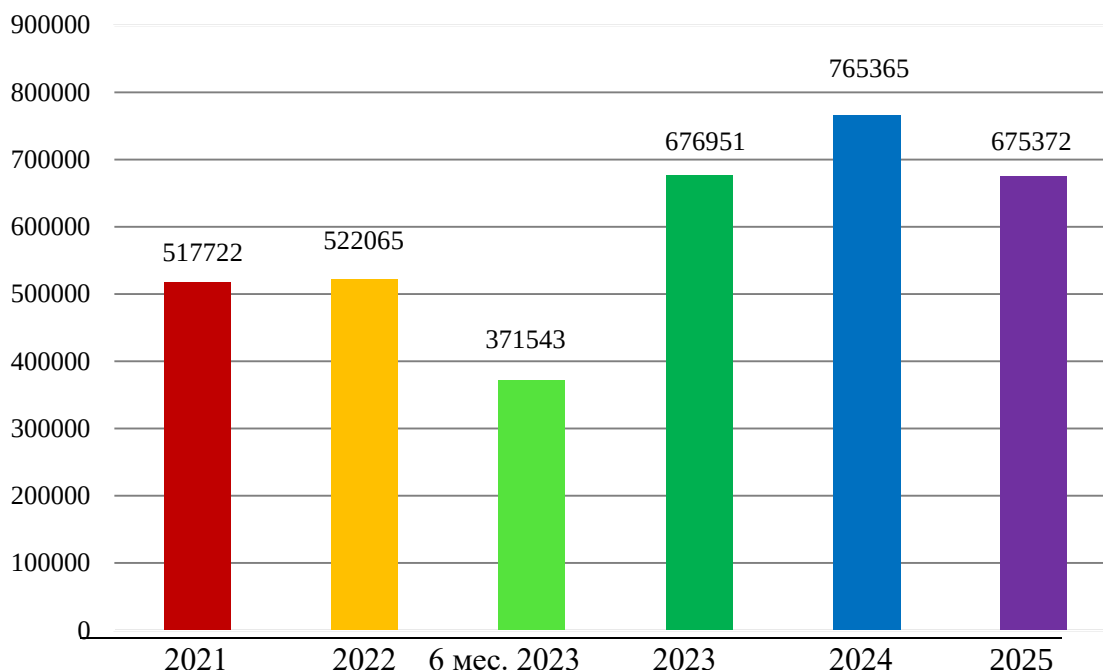


Диаграмма 5. Сведения о количестве зарегистрированных преступлений
в сфере телекоммуникаций и компьютерной информации

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. Точное количество всех существующих в мире вирусов невозможно определить, так как они постоянно создаются и модифицируются. По данным на начало 2026 года, в мире насчитывалось более 1 миллиарда вредоносных программ. При этом ежедневно выявлялось около 560 тыс. новых образцов вредоносного программного обеспечения.

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 компьютерных программ»). 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»⁴³, сохранить его и ввести в официальную судебную статистику как условное наименование не только преступлений, предусмотренных главой 28 УК РФ, но и совокупности с ними по другим

⁴³ Скоромников К.С. Неправомерный доступ к компьютерной информации и его исследование // Прокурорский надзор и следственная практика. 1998. № 1. С. 168.

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 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 модификации 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 7 декабря 2011 г. № 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 вирусов⁴⁴.

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

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 вредоносной⁴⁵.

⁴⁴ Ляпунов Ю.И., Максимов С.В. Указ. соч. С.12.

⁴⁵ Комментарий к Уголовному кодексу Российской Федерации / под общ. ред. Ю.И. Скуратова и В.М. Лебедева. С. 704.

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

Субъектом преступления является лицо, достигшее 16 лет⁴⁶. 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;
- 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 условий⁴⁷.

⁴⁶ Комментарий к Уголовному кодексу Российской Федерации [Электронный ресурс]. URL: http://rfuk.ru/comment_273.html.

⁴⁷ Смирнова Т.Г. Указ. соч. С. 26.

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 подразделений специальных технических мероприятий органов внутренних дел Российской Федерации⁴⁸ со службой безопасности ОАО «Сбербанка России» и Центра информационной безопасности ФСБ России⁴⁹, взятые из практики.

В результате проделанной работы сотрудниками ПСТМ ОВД 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 «StelsAPK», нацеленной на компрометацию 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 ПСТМ ОВД совместно с ЦИБ ФСБ России и 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 преступной деятельности в различных регионах Российской Федерации и Украины, связанной с разработкой, распространением и использованием вредоносных программ для операционной системы «Android» 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).

⁴⁸ Далее – «ПСТМ ОВД».

⁴⁹ Далее – «ЦИБ ФСБ России».

Распространение машинного носителя с программой для ЭВМ – это передача его третьим лицам в любой форме⁵⁰.

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 лет⁵¹. 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 вред⁵².

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 деяние, 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.

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 пользования⁵³.

⁵⁰ Смирнова Т.Г. Указ. соч. С. 26.

⁵¹ Комментарий к Уголовному кодексу Российской Федерации [Электронный ресурс]. URL: http://rfuk.ru/comment_274.html.

⁵² Комментарий к Уголовному кодексу Российской Федерации Указ. соч.

⁵³ Там же.

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, 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 указанной 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 июля 2017 г. 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 – причинение 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 ч. 4 ст. 274.1 УК РФ предусматривает те же деяния, рассматриваемые чч. 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 указывает 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.

В завершении рассмотрения главы 28 УК РФ предлагаем проанализировать ключевые понятия, ст. 274.2 УК РФ «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования» (статья введена Федеральным законом от 14 июля 2002 года № 260-ФЗ).

Под должностным лицом в настоящей статье понимается лицо, постоянно, временно либо по специальному полномочию выполняющее управленческие, организационно-распорядительные или административно-хозяйственные функции в коммерческой или иной организации.

1. Бланкетная диспозиция статьи связана с п. 5¹ ст. 46, п. 3 ст. 65¹ Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» и Постановлением Правительства РФ от 30 августа 2025 г. № 1333 «Об утверждении Правил установки, эксплуатации и модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования».

2. Объект преступления – общественные отношения, обеспечивающие безопасность целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования.

3. Объективная сторона выражается в альтернативно предусмотрительных действиях (бездействии). При этом в ч. 1 статьи установлена ответственность, говоря в целом, за эксплуатационные нарушения в процессе деятельности соответствующих технических средств, тогда как в ч. 2 – за неиспользование таких средств при организации функционирования на территории Российской Федерации сети «Интернет» и сети связи общего пользования.

4. Условием привлечения к уголовной ответственности является предшествующее двукратное привлечение к административной ответственности за соответствующее деяние в течение года перед совершением уголовно-наказуемого деяния.

5. Субъект специальный – индивидуальный предприниматель или должностное лицо, ответственные за соблюдение соответствующих требований и ранее привлеченные к административной ответственности. Определение должностного лица в примечании к статье не совпадает с данным в п. 1 примечаний к ст. 285 УК РФ и распространяется только на комментируемую статью.

6. Субъективная сторона – умышленная форма вины.

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 обеспечения, 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 удастся 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 облике **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 «**тройского коня**», а не вредоносную программу.

Имеется еще одна *разновидность вредоносных программ* – «*преумножение тройского коня*». 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 «тroyанского 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 не-санкционированного 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, перенадресация 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) (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 использу-

ется 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 выявление 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 напрямую у провайдера (фирма, предоставляющая пользователю доступ в Интернет).

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:

- 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 конструктивных 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 McAfee;

- 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, направленных на использование различных систем аппаратной защиты ЭВМ от несанкционированного доступа (например, система электронных ключей);
- использование всевозможных видов шифрования информации, выражающееся 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.

Глава II.

Раскрытие преступлений, совершаемых в сфере телекоммуникаций и компьютерной информации

В настоящее время невозможно представить функционирование любого министерства, ведомства, управления, какой-либо 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 «CNewsAnalytics», общее число частных пользователей систем дистанционного банковского обслуживания в 2018 году составило 133,6 млн. чел., в 2019 году – 150,1 млн. чел., в 2020 году – 168 млн. чел., в 2021 году – 170 млн. чел., в 2022 году – 183 млн. чел., в 2023 году – 197 млн. чел., в 2024 году – 198 млн. чел., в 2025 году – 199 млн. чел. (см. диаграмму 6). 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 ДБО (см. диаграмму 7)⁵⁴.

⁵⁴ Научно-практический электронный журнал «Аллея Науки». 2023 // URL: Alley-science.ru.

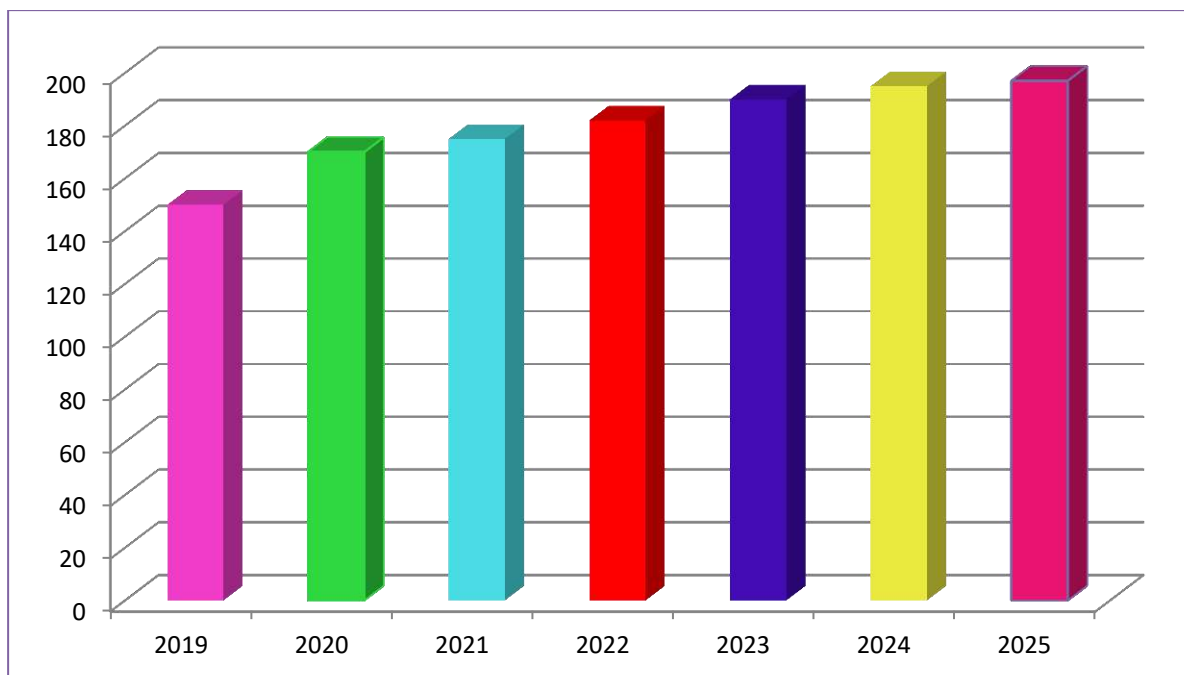


Диаграмма 6. Число частных пользователей систем дистанционного банковского обслуживания в России



Диаграмма 7. Прогноз количества преступлений, совершаемых в системе ДБО⁵⁵

⁵⁵ Данные взяты из статистических данных ФКУ «Главный информационно-аналитический центр МВД России».

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 операционной системы⁵⁶ 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

⁵⁶ Далее – «ОС».

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» хакер⁵⁷. Обычно хакеры используют схему двоичного кода (рис. 3).



Рис 3. Схема двоичного кода

Классификация компьютерных вирусов

Рассмотрим детально, что собой представляет указанная выше классификация (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.

⁵⁷ Материал электронной энциклопедии ЗАО «Лаборатория Касперского» // URL: <https://encyclopedia.kaspersky.ru/>.

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 за циклируется 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-интерпретаторы.

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 системного 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 определенных временных или информационных условиях для осуществления вредоносных действий. Многие вредоносные программы, такие как вирусы или черви, часто содержат логические бомбы, которые срабатывают в заранее определенное время или при выполнении определенных 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 несообщенным заранее последствиям для пользователей. Таким образом, отключение определенной 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 привести к нарушению 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 оперативной 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. Так же, 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 программного обеспечения⁵⁸, 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.

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;

⁵⁸ Далее – «ПО».

- получения управления макропрограммой без вмешательства пользователя (автоматические или стандартные макросы). Описанным условиям удовлетворяют редакторы MS Word, MS Office и AmiPro, а также электронная таблица MS Excel. Эти системы содержат в себе макроязыки (MS Word – Word Basic, MS Excel и MS Office – Visual Basic), при этом:

- макропрограммы привязаны к конкретному файлу (AmiPro) или находятся внутри файла (MS Word/Excel/Office);

- макроязык позволяет копировать файлы (AmiPro) или перемещать макропрограммы в служебные файлы системы и редактируемые файлы (MSWord /Excel/Office);

- 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).

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 макровирусов.

Макровирусы, поражающие файлы Word, Excel или Office, 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 полувirusы, 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. Существуют, однако, вирусы, использующие приемы скрытия своего кода и хранящие свой код в виде не макросов. 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: пользователь зараженного макровирусом редактора, сам того не подозревая, рассылает «инфицированные» письма своим адресатам, а они рассылает 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 нерезидентными.

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 получают 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, РНР. 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. 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 г.).

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, файлы 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 года известная компания McAfee обнародовала данные, показывающие, что они собрали 250 тыс. 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 года 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 заголовков 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» (ЕРО-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 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 каталоге 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. Данным способом самозапуска пользуются также многие компьютерные черви и троянские программы.

Вирусы-ссылки.

Вирусы-ссылки или link-вирусы не изменяют физического содержания 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 IBMTrusteer сообщили, что раскрыли масштабную мошенническую операцию, в которой использовались огромные фермы эмулято-

ров мобильных устройств, при помощи которых преступники выводили миллионы долларов со счетов в онлайн-банках в США и ЕС⁵⁹.

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.

Для настройки эмуляторов мошенники применяли специальный инструмент, способный загружать спецификации устройств из базы ранее скомпрометированных девайсов, сопоставляя каждое при этом поддельное устройство 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, срочно завершить операцию и немедленно уничтожить все следы.

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

Данный факт свидетельствует о том, что хакеры ни 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.

⁵⁹ Журнал «Хакер» [Электронный ресурс] // URL: <http://www.hacker.ru>. (дата обращения: 18 декабря 2023 г.).

Пример 2.

В интернет-журнале «Хакер» в статье «Rotexu. Как действовал один из опаснейших троянов 2022 года»⁶⁰ было указано, что с момента появления трояна Rotexu 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 Rotexu в последние годы и его устройство.

Если разобрать исторический аспект, то Rotexu, по сути, – это помесь банкера и вымогателя. Он появился в 2018 году и провел десятки тысяч атак на различные устройства российских пользователей. Исследования функционирования Rotexu показали, что в течение всего 2020 года активность вредоноса постоянно снижалась, но в октябре – ноябре был зафиксирован его рост. Как долго продолжится его активность, покажет время.

Если рассматривать атакующие действия Rotexu, 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 Rotexu 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 обфусцируются с помощью частных криптов.

У рассматриваемого вредоноса Rotexu 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.

⁶⁰ Статья опубликована 17 декабря 2022 г.

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 распространялся 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 MacOS 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 постоянно растет число активно действующих вирусов, вызывая создание новых антивирусных программ (ревизоров, детекторов, «вакцин», «фагов»).

По данным «Лаборатории Касперского», в первом квартале 2026 года ее системы зафиксировали следующие показатели:

- более 343 млн. атак с различных интернет-ресурсов, 50 млн. уникальных вредоносных ссылок, на которые среагировал веб-антивирус;

- более 15 млн. вредоносных и потенциально нежелательных объектов, заблокированных файловым антивирусом;
- 2 938 новых модификаций шифровальщиков (программ-вымогателей);
- более 77 тыс. пользователей, столкнувшихся с атаками шифровальщиков;
- более 260 тыс. пользователей, подвергшихся атакам майнеров (программ для несанкционированного майнинга криптовалюты).

Кроме того, с начала 2026 года «Лаборатория Касперского» выявила почти 100 тыс. кибератак, в которых злоумышленники распространяли вредоносное программное обеспечение под видом популярных ИИ-сервисов (ChatGPT, Claude, Gemini). Также было обнаружено более 15 тыс. образцов вредоносного программного обеспечения, маскировавшегося под агентные ИИ-инструменты, включая поддельные версии OpenClaw.

Проблема вирусов начинает принимать глобальный характер примерно с 1990 года. 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 SymantecNortonAntivirus. Начало 1991 года отмечено массовой эпидемией полиморфного загрузочного вируса Tequila. Летом 1991 году 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 полиморфных-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 года 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», отмечается широкое распространение на данный момент файлового вируса Win32.Rmnet.12, с помощью которого злоумышленники создали бот-сеть, насчитывающую более миллиона инфицированных компьютеров. Уже по состоянию на 15 апреля 2017 г., ботнет Win32.Rmnet.12 состоял 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 файрволов 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 ИТ-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 девяти 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 расследования 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 немедленно 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 экспертом статуса «вредоносной» 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 опреде-

лить: 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 (см. рис. 5).

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, раскаялся в содеянном, заключил досудебное соглашение о сотрудничестве, по месту жительства и работы.

Суд признал Рыжова А.Н. виновным в совершении преступления, предусмотренного ст. 273 ч. 3 УК РФ, и назначил 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, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации».

В недалеком прошлом некий гражданин 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. 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 10 000 рублей.

Пример 3. Ст. 273 ч.1 УК РФ.

ОРП УМВД СУ УМВД России по г. Борисоглебску 11.02.2022 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 факту того, что 02.02.2022 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 являлся Крутинин Г.В., 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 Крутина 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 75 млн. 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 граждан К. и гражданин В. сознались в совершении преступления, предусмотренного ч. 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 ч. 3 ст. 273 УК РФ. Осужденному гражданину К. суд назначил наказание в виде 6 лет 6 месяцев лишения свободы 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 оперативно-розыскной деятельности, 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 ПСТМ 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 «Хакер.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 осуществлял 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 посредством 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 установление 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 «Скуре» 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 определялся 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 компьютерной 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 предоставленном USB-флеш-носителе?

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

По итогам проведенного исследования **собранного научно-практического 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 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 БСТМ МВД России 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 «ВТБ24», ОАО «Банк Москвы», ОАО «Альфа-Банк», 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 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 БСТМ МВД России 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 окончании 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 БСТМ МВД России 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, привязанной 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 УК РФ «Кража» и 273 УК РФ «Создание и распространение вредоносных компьютерных программ».

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 масштабного вовлечения несовершеннолетних в преступную деятельность, как связанную с написанием вредоносных программ, так и распространением компьютерных вирусов, а также все чаще стали встречаться случаи вербовки иностранными спецслужбами нашей молодежи с целью последующего их использования в подготовке и совершении террористических актов и преступлений экстремистской направленности.

Об этом на расширенном заседании коллегии МВД России, состоявшейся 4 марта 2026 года, конкретно заявил Президент Российской Федерации В.В. Путин: «Особую тревогу вызывают случаи агрессивного поведения подростков в школах, колледжах, а также в общественных местах. МВД России совместно с другими правоохранительными органами необходимо значительно усилить акцент на профилактику и на предотвращение подобных преступлений. Президент отметил, что в 2025 году впервые за долгое время наметился рост подростковой преступности. Молодежь

часто втягивают в незаконные дела и вербуют в криминальную среду». Далее он отметил, что подростков, в том числе с проблемами в семьях необходимо вовлекать в волонтерское движение и занятием спортом, в работу молодежных общественных объединений, делать все, чтобы ребятам помочь не допустить трагическую ошибку, найти себя в жизни, преодолеть трудности, реализовать свой талант, способности, которые есть у каждого. Тех, кто подталкивает несовершеннолетних к преступлениям, будут наказывать вплоть до пожизненного заключения»⁶¹.

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 правоохрнительным органам в раскрытии преступлений, на установление фигурантов и их 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

⁶¹ См. Материалы коллегии МВД России от 4 марта 2026 года. Выступление Президента Российской Федерации В.В. Путина.

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 лица⁶² (см. рис. 6).

⁶² Кесарева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. канд. юрид. наук: 12.00.08. Москва, 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 **научно-практической 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 информации 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 распространены 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 личности⁶³.

Носители информации, имеющие отношение к расследуемому преступлению, изымаются, упаковываются соответствующим образом, исследуются, оцениваются, признаются вещественными доказательствами и приобщаются к материалам уголовного дела⁶⁴ с соблюдением норм, установленных Уголовно-процессуальным кодексом Российской Федерации.

Для участия в обыске и выемке целесообразно приглашать специалиста⁶⁵ 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.

⁶³ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Ст. 176, 182, 183.

⁶⁴ УПК РФ. Ст. 81-82.

⁶⁵ Там же. Ст. 58.

Злоумышленник, зная о том, что неблагоприятная ситуация может возникнуть в любое время, заранее программирует свое оборудование для идентификации «себя» с использованием **тайминга**, и если через определенный период времени не будет подтверждения «себя», то в этом случае вся информация будет искажена или уничтожена. 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 данных⁶⁶.

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;

⁶⁶ Криминалистика. Полный курс: учебник для вузов / под общ. ред. А.Г. Филиппова. 5-е изд., перераб. и доп. Москва: Юрайт, 2020. 855 с. Серия: Бакалавр. Углубленный курс.

ж) выключить подачу энергии в компьютер и далее действовать по схеме «компьютер не работает»⁶⁷.

Если компьютер не работает, следует:

а) точно отразить в протоколе следственного действия и на прилагаемой к нему схеме местонахождение компьютера и его периферийных устройств;

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 отдельно 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)**⁶⁸.

Наиболее эффективным и простым способом фиксации данных из ОЗУ является распечатка на бумагу информации, появляющейся на мониторе. Также можно использовать специализированное программное обеспечение для сохранения и последующей визуализации дампа памяти.

Дамп памяти – это копия содержимого оперативной памяти, находящаяся на жестком диске или другом энергонезависимом устройстве памяти⁶⁹. Естественно, дампом может быть не вся оперативная память, а только какая-то определенная её часть, которая, так сказать, интересует в данный момент ту программу, которая делает этот дамп.

Если компьютер не работает, информация может находиться в ВЗУ и других компьютерах информационной системы или в «почтовых ящиках» электронной почты или сети ЭВМ.

⁶⁷ Криминалистика. Полный курс. Указ. соч.

⁶⁸ Там же. С. 417.

⁶⁹ Юдин М., Куприянова А., Матвеев М. Windows XP. Полное руководство 2010 // Наука и Техника. 2010. Ст. 65.

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 обвиняемого⁷⁰.

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;

⁷⁰ Криминалистика. Полный курс: учебник для вузов / под общ. ред. А.Г. Филиппова. С. 417.

- *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 технологию⁷¹.

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 системах⁷².

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, разрешения уголовных дел по существу⁷³. *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.

⁷¹ Россинская Е.Р. Судебная экспертиза в гражданском, административном и уголовном процессе. Москва: Норма, 2005. С. 458-467.

⁷² Криминалистика. Полный курс. Указ. соч. С. 417.

⁷³ УПК РФ – Ст. 85-89.

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 форме⁷⁴.

*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.

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** (рис. 7).



Рис. 7.

⁷⁴ Криминалистика. Полный курс. Указ. соч. С. 417.

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.

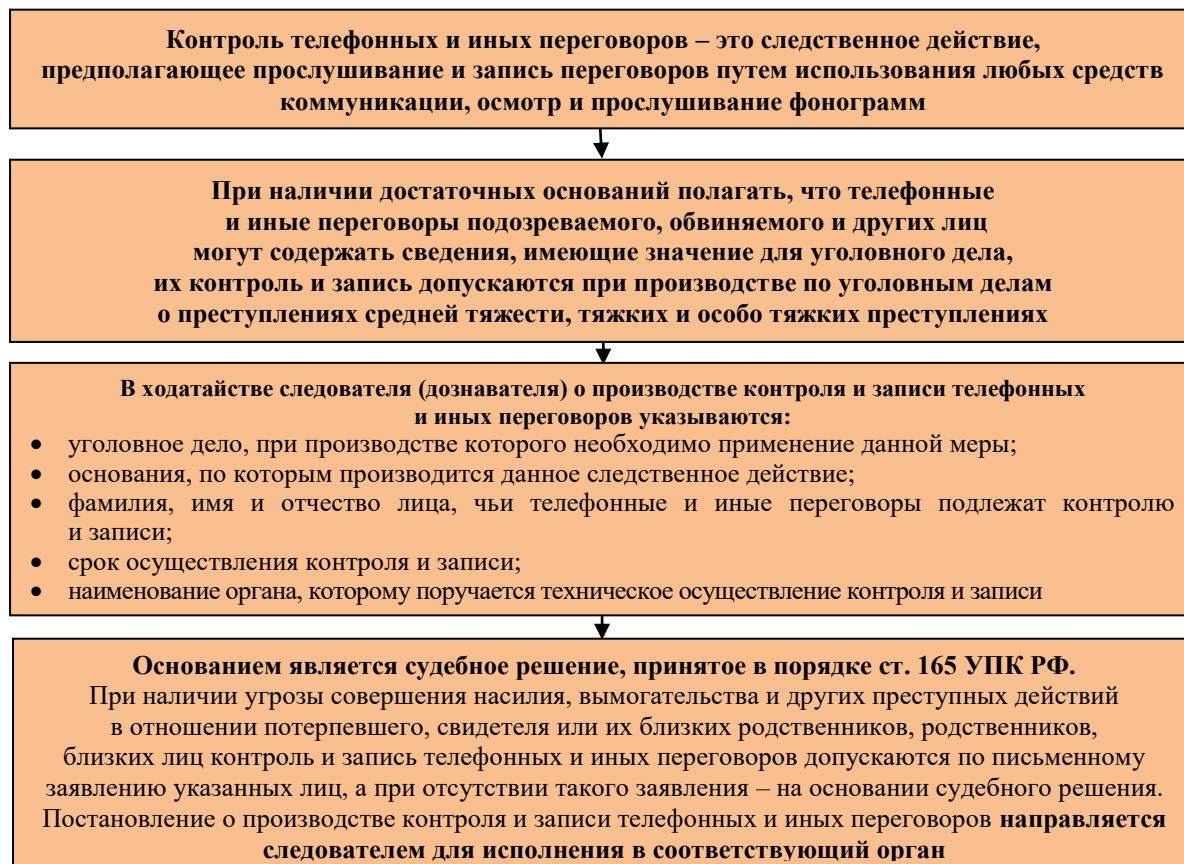
Специфика уголовно-правовых отношений, возникающих в связи с совершением общественно-опасных деяний, обуславливает особенности механизма осуществления как оперативно-розыскных, в том числе и специальных технических мероприятий, так и параллельное сопровождение их во время производства следственных действий и до окончания уголовного судопроизводства, а в исключительных случаях и на некоторое время и после него⁷⁵. В таких случаях, когда ведется уголовное преследование лица, предпологаемо виновного в совершении средней тяжести, тяжкого и особо тяжкого преступления, его привлечение к уголовной 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.

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 РФ⁷⁶ (схема 5).

⁷⁵Алескеров В.И. Применение мер безопасности к участникам уголовного судопроизводства // Вестник Российской Правовой Академии Министерства Юстиции. 2007. № 4. С. 70 – 73.

⁷⁶Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ.

Контроль и запись переговоров (ст. 186 УПК РФ)⁷⁷



Хотя некоторыми специалистами задолго до появления указанной статьи в российском уголовно-процессуальном законодательстве приводились не столько убедительные, сколько эмоциональные доводы против введения этого следственного действия⁷⁸. 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 значение⁷⁹. В связи с чем в целях

⁷⁷ Шаталов А.С. Уголовно-процессуальный кодекс Российской Федерации в схемах: учебное пособие. Москва; Проспект, 2021. 816 с.

⁷⁸ Савицкий В.М. Правосудие и личность // Советское государство и право. 1983. № 5. С. 58.

⁷⁹ 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.

обеспечения соблюдения конституционного права граждан на тайну телефонных и иных переговоров в УПК РФ была включена специальная статья⁸⁰. 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 служб⁸¹. В соответствии с п. 11 ч. 2 ст. 29 УПК РФ разрешение на производство данного следственного действия уполномочен давать суд в порядке, предусмотренном статьей 165 УПК РФ. Однако необходимо отметить, что при наличии угрозы совершения насилия, вымогательства и других преступных действий в отношении свидетеля⁸², потерпевшего⁸³ или их близких родственников⁸⁴, близких лиц⁸⁵, контроль и запись переговоров допускаются по их письменному заявлению, а при его отсутствии – на основании судебного решения, вынесенного по ходатайству следователя⁸⁶. Согласно нормам статьи 186 УПК РФ 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. схему 6).

⁸⁰ УПК РФ. Ст. 186.

⁸¹ Там же. Ст. 38. п. 4.

⁸² 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.

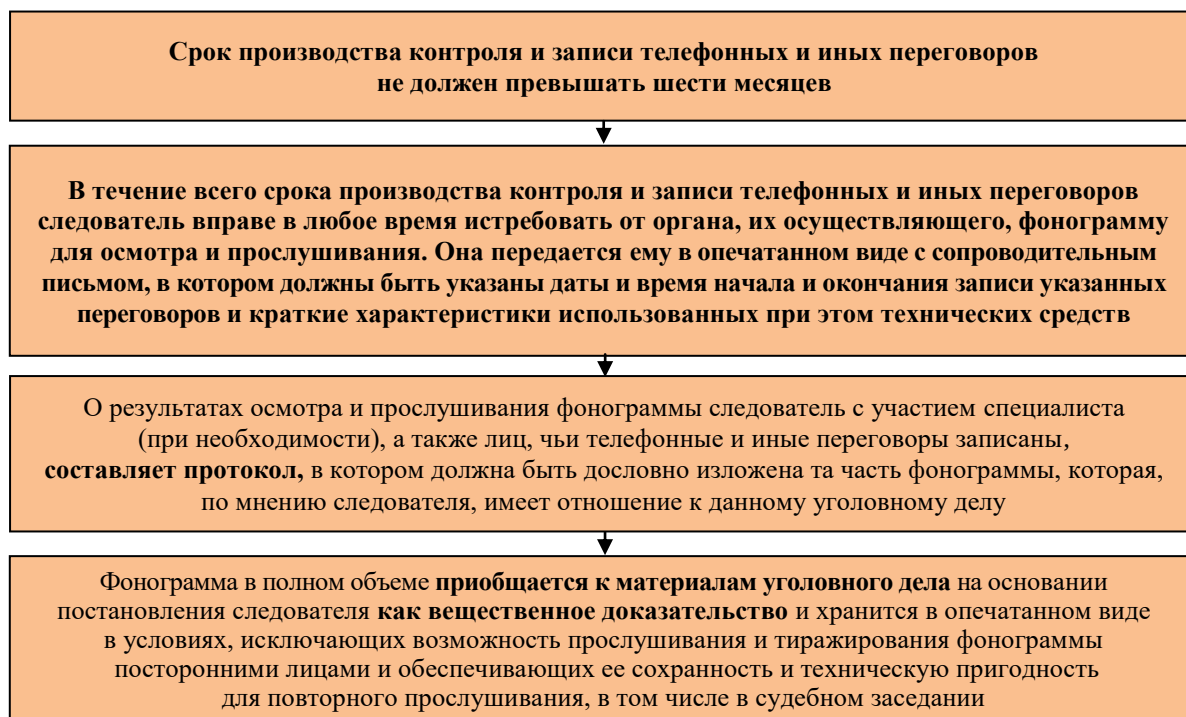
⁸³ В соответствии с частью первой ст. 42 УПК РФ потерпевшим является физическое лицо, которому преступлением причинен физический, имущественный, моральный вред, а также юридическое лицо в случае причинения преступлением вреда его имуществу и деловой репутации.

⁸⁴ Близкие родственники – супруг, супруга, родители, дети, усыновители, усыновленные, родные сестра и братья, дедушка, бабушка, внуки. УПК РФ – Ст. 5.п. 4.

⁸⁵ 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. УПК РФ – Ст. 5. п. 3.

⁸⁶ По законодательству США, например, прослушивание должно быть прекращено не только по окончании срока, но и сразу после того, как были получены искомые доказательства. Махов В.Н., Пешков М.А. Уголовный процесс США (досудебные стадии): учебное пособие. Москва: 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. 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.

Общие правила контроля и записи переговоров (ст. 186 УПК РФ)⁸⁷



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 печатанном 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 печатанном виде в условиях, исключающих возможность ее прослушивания и тиражирования посторонними лицами и обеспечивающих, кроме того, сохранность и техническую пригодность фонограммы для необходимого последующего прослушивания⁸⁸. Такова законодательная рекомендация порядка производства контроля и записи переговоров.

⁸⁷ Шаталов А.С. Уголовно-процессуальный кодекс Российской Федерации в схемах: учебное пособие. Москва; Проспект, 2021. 816 с.

⁸⁸ УПК РФ – Ст. 186. Ч. 5-8.

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 лиц⁸⁹.

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 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 коммуникации⁹⁰.

⁸⁹ Шаталов А.С. Контроль и запись переговоров на предварительном следствии: правовые основания, тактические условия, технология проведения ... С. 57-84.

⁹⁰ Действующими нормативными актами предусматривается обязательная установка и эксплуатация оборудования в учреждениях связи для проведения следственных действий и оперативно-розыскных мероприятий. 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 января 2008 г. № 6.

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 оперативно-го 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 заключается 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 predeterminedены не только строгим соблюдением законодательных предписаний, имеющих прямое отношение к проведению специальных технических мероприятий, но и применением криминалистической технологии, учитывающей самые разнообразные закономерные связи⁹¹. Полученная криминалистически значимая информация имеет универсальный характер

⁹¹ 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. Россинская Е.Р. Криминалистика: учебник для вузов / Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г. [и др.]; под ред. Р.С. Белкина. Москва, 1999. С. 549-678; Юрина Л.Г., Юрин В.М. Указ. соч. – С. 69 и др.

и, в принципе, может применяться для познания каждого из обстоятельств, входящих в предмет доказывания по уголовному делу⁹². 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 окончательном 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 для практической реализации в процессе доказывания преступной деятельности разрабатываемых лиц, подозреваемых в совершении преступления.

Для наглядности приведем один из примеров, взятый из практических наработок ПСТМ МВД России:

Сотрудниками ПСТМ МВД 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 «взятничество».

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

⁹² Шаталов А.С. Контроль и запись переговоров на предварительном следствии: правовые основания, тактические условия, технология проведения ... С. 57-84.

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 отличаются. 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 РФ, 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 ситуации⁹³.

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 основу⁹⁴ 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, имеющих 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, создание всех вышеперечисленных условий – задача очень непростая. Однако ее реше-

⁹³ Шаталов А.С. Контроль и запись переговоров на предварительном следствии: правовые основания, тактические условия, технология проведения ... С. 57-84.

⁹⁴ УПК РФ – Ст. 7.Ч. 4.

ние 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 2018-2023 гг. можно отметить высокую эффективность по их тесному взаимодействию, слаженность следственных действий и оперативно-розыскных мероприятий, 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, совершаемые в информационно-коммуникационных 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 поддается 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. схему 7).

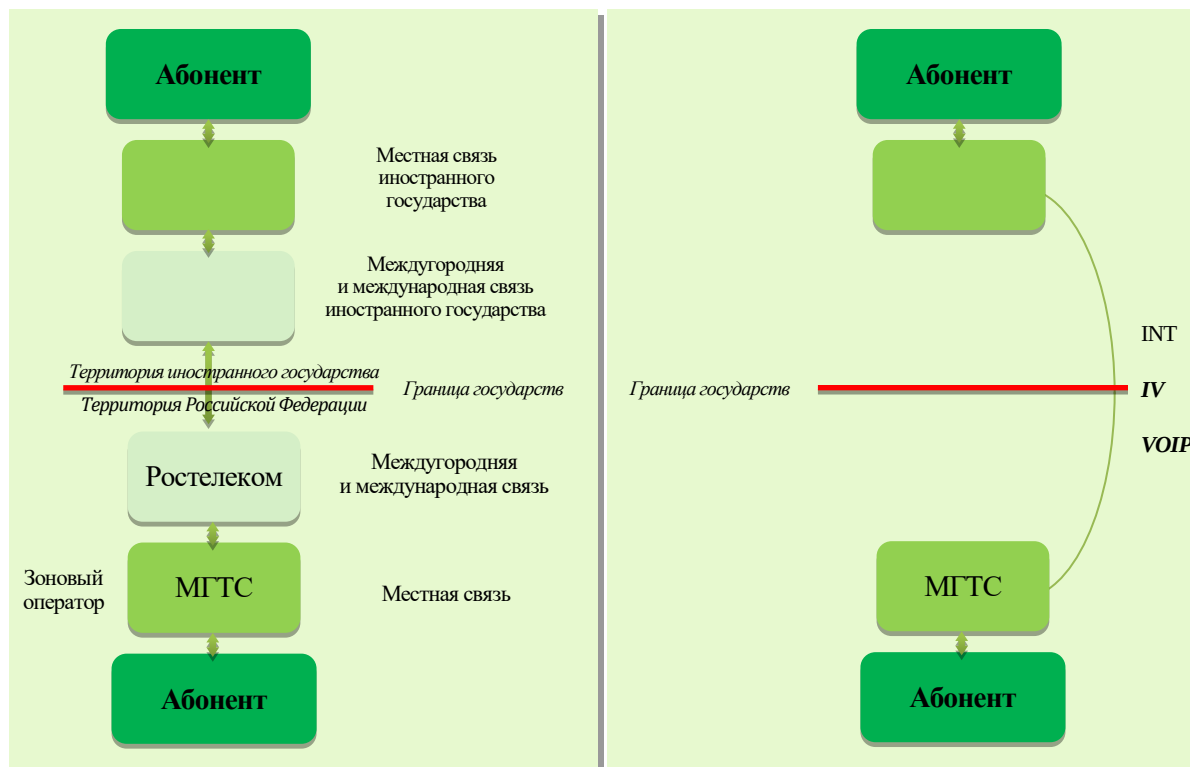


Схема 7. Работа операторов фиксированной (проводной) связи

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, PBX⁹⁵, IP-PBX⁹⁶) путем использования изъянов (уязвимостей) в настройках УАТС (функции DISA, командного интерфейса, стека протоколов TCP/IP) со стороны злоумышленников реализуется следующими способами.

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 (см. схему 8): 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.).

⁹⁵ 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.

⁹⁶ 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.

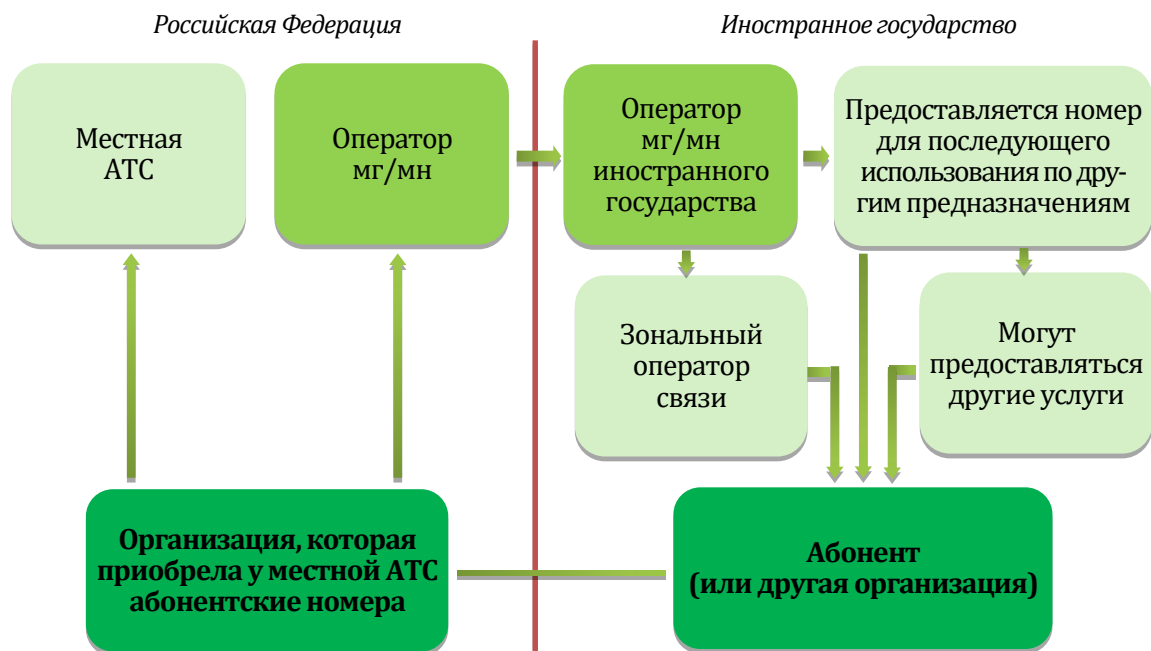


Схема 8. Схема работы несанкционированного доступа к УАТС с целью генерации трафика на абонентские номера с услугой звонка за дополнительную плату (платные номера) международных операторов

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 м/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.

в) организация ISUP-шлюзов на сетях операторов связи для нелегальной терминции междугороднего и международного трафика, в том числе с подменой вызывающего номера.

Предпосылками для совершения данных деяний являются:

- во-первых, большое различие в тарифах за терминцию трафика на международном и зоновом уровнях и очень низких тарифах за терминцию VOIP-трафика;

- во-вторых, существование бирж по продаже VOIP-трафика (например, voipexchange.com), и, наконец, **отсутствие нормативной базы по вопросам регулирования терминции 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 лицо⁹⁷ подключается к интернет-провайдеру, затем **устанавливает VOIP-шлюз**, 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 терминции трафика на сеть оператора связи, к которому присоединен, по определенному тарифу. Биржа продает заявленные им услуги по терминции трафика на рынке **«серого»** трафика.

Данная схема терминции 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 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-разыскных мероприятий»;

- условиям лицензий операторов местной связи при приеме и шлюзовании международного трафика от зарубежных операторов на своем

⁹⁷ Устройство, имеющее подключение к нескольким сетям с различными видами технологий доступа, таких как IP-сети (Интернет, IP-PBX-предприятия, VoIP-оператор и т.д.), аналоговыми линиями сетей фиксированной связи, E1TDM-потокам, с одной стороны, и к сети радиодоступа (RAN) GSM/CDMA/UMTS-оператора – с другой.

оконечном оборудовании связи через сети передачи данных (IP-сети, Интернет) и его терминирования 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.

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 междооператорного, междугородного и международного трафика. В основе этой распространенной схемы получения дохода от нелегальной схемы терминирования 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 терминирование трафика. С другой стороны, он подключается к интернет-провайдеру, реализуя связь между сетями (рис. 8). Далее злоумышленник регистрируется на бирже трафика и объявляет о возможности терминирования трафика на сеть оператора связи, sim-карты которого используются в шлюзе, по определенному тарифу. Биржа продает заявленные им услуги по терминированию трафика на рынке «серого» трафика. Данный вид правонарушений является широко распространенным: так, например, на сети московских операторов мобильной связи факты работы GSM-шлюзов выявляются еженедельно.



Рис. 8. 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. 9. 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 контролирующими 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 г. 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. 10. 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. 11. Интервью информационному телеканалу «РОССИЯ – 24»

3. 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. 12. Интервью информационному телеканалу «РОССИЯ – 24»



Рис. 13. Интервью информационному телеканалу «РОССИЯ – 24»

4. 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. 14. Студия информационного телеканала «РОССИЯ – 24»

5. «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, 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 исправительном 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. 15. 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 потенциальных 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 Подмоскowie 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 РФ, которые предусматривают для получения необходимой информации привлечение к расследованию специалистов, обладающих специальными знаниями в области банковской деятельности, 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 Солнцево и Коммунарке. Девушка из «сервиса по восстановлению сим-карт» была задержана в Подмоскowie, 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 отбывтия 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, 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. 16).

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. 16. 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 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 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 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 также 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 ПСТМ 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 госпошину, 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 ничем 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. Вышеуказанный вид нарушения осуществляются и в настоящее время.

Приведем пример преступления данного вида.

В результате проведенных 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. 2 ст. 165 УК РФ «Причинение имущественного ущерба путем обмана или злоупотребления доверием».

Вышеперечисленные 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 сотрудниками 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 млн. рублей.

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 «WesternUnion» 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 г., в Москве 24 февраля 2021 г. задержали мужчину, который занимался аферами в сети Интернет. Он предлагал людям мобильные телефоны известного бренда, электронику «Премиум-класса». Товар выставял 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 постоянно 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 развитие сети Интернет способствует увеличению активности и возможности фальсификаторов и кибермошенников в финансовой сфере, спамеров, фишеров, вымогателей, которые требуют выкуп за нераспространение персональных данных.

В связи с этим, разработчики компьютерных программ в разных странах 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 Blockchain и криптовалюта Биткоин позволила достаточно четко определить новые подходы к обеспечению целостности информации, передаваемой между абонентами, не имеющими оснований доверять друг другу.



Рис. 17. Соотношение децентрализованных распределенных систем

Биткоин (от англ. BitCoin – 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 условием для работы с платежной системой является наличие установленного клиента. Протокол платформы Биткоин и программный код базового клиента (BitcoinCore) 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 постоянно 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.

Максимальная децентрализация. Прежде всего, идеальное решение должно обеспечить децентрализацию данных (данные хранятся децентрализованно, 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 дефицитные, 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 Биткойн, 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 попадают на глаза пользователям сети Биткойн. В основном, они хранятся в файлах бумажника, а манипуляции ключами выполняет программное обеспечение кошелька – разумеется, по инициативе владельца.

Таким образом, в рамках сети Биткойн адреса обеспечивают анонимность пользователей. Не существует способа ассоциировать биткойн-адрес с конкретным физическим или юридическим лицом. Но эта анонимность поддерживается только в рамках сети Биткойн. Использование токенов на криптобиржах или магазинах, принимающих криптовалюту, в большинстве случаев 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 биткойн-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 биткойн-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 имеющем прямого соединения с Интернетом. Разумеется, такой способ обеспечивает 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, учитывающая технологию изготовления:

1. Веб-кошельки (или онлайн-кошельки). Идеально подходят для новичков, не желающих самостоятельно администрировать собственное программное обеспечение, или обладателей «маломощной» вычислительной техники. Популярны онлайн- (браузерные) кошельки: Матби, Coinbase, Blockchain.info, Cryptopay, Харо, 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).

2. 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 та-

кие значимые для телефона ресурсы, как память и трафик. Популярны кошельки для мобильных устройств: Blockchain Mobile; Bitcoin Wallet; Electrum; Mycelium; Coin Pocket; Харо 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.

3. Локальные кошельки (устанавливаются на персональный компьютер или ноутбук). Подразделяются на два вида.

«Толстые» или «тяжелые» – такие кошельки загружают на компьютер весь блокчейн, возводя пользователя в ранг полноценного участника сети Биткойн 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 синхронизироваться с блокчейном.

4. 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).

5. 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 Биткойн 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, но 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:

1. 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 достигнет определенного порога, она выводится с кошелька.

Способ борьбы весьма прост: загружайте кошельки с прямых ссылок на сайте криптовалюты или производителя проверенного кошелька.

2. 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 веб-сайты, 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 спама 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.

3. 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 сразу 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 произошел в Турции, когда в апреле 2021 года без вести пропал основатель турецкой криптобиржи Thodex Фарук Фатих Озер. Как сообщало турецкое агентство ДНА, топ-менеджер выехал из Турции с \$2 млрд. инвесторов в криптовалюте. Thodex внезапно приостановила торги тоже в апреле, 22 апреля она объявила, что ей не хватает финансового обеспечения для продолжения операций.

4. 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.

5. 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.

6. 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 (служит 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 использования 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 оборудовании – ASIC-майнеры.

В недалёком прошлом криптовалюты 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 криптовалют и по сей день добываются при помощи видеокарт и процессоров, но при добыче Биткоина это стало не выгодно, так как счета за электричество превышали доход от «добычи» криптовалюты.

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 криптовалюты 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 криптокошелек. Вернуть добытые монеты, конечно же, не получится.

Для предотвращения подобного рода мошенничеств следует приобретать айсики у надежного поставщика и проверять его на отсутствие вредоносных программ. Также следует постоянно мониторить свой крипто-кошелек на количество «добытых» криптовалют, 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, которые 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 криптовалюты 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 криптовалют, советуясь с другими пользователями Telegram-группы и опытными людьми, профессионально занимающимися инвестициями в криптовалюты.



Рис. 18. 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, приносящими весьма жестокие и порой непоправимые последствия (рис. 19).

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. 19. 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 (см. диаграмму 8).

Сведения о количестве зарегистрированных преступлений террористического характера и экстремистской направленности

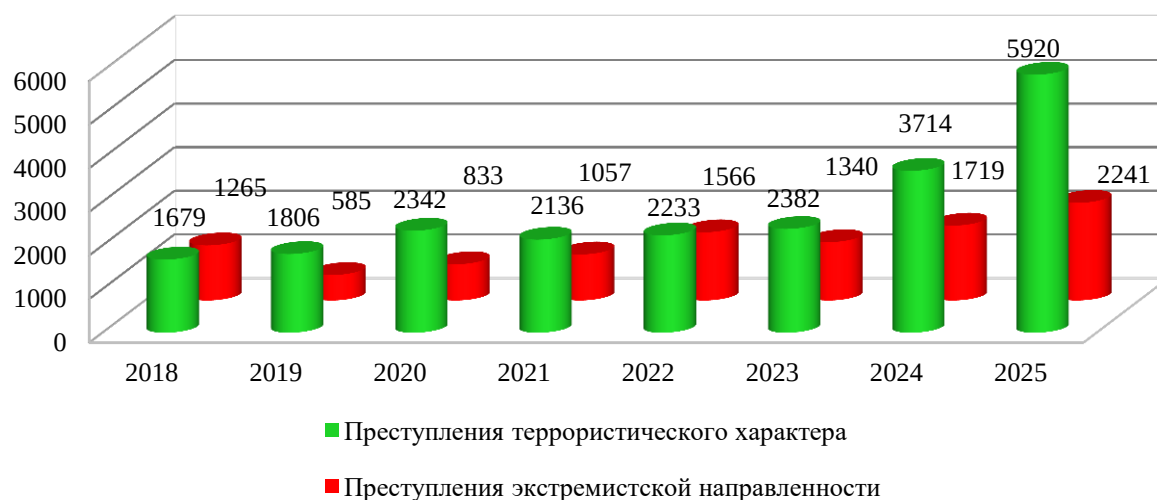


Диаграмма 8. Сведения о количестве зарегистрированных преступлений террористического характера и экстремисткой направленности

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. 20. 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 МВД России⁹⁸.

Основными направлениями оперативно-служебной деятельности ГУПЭ МВД России являются:

1. Противодействие экстремистской деятельности и терроризму.
2. Организация и участие в формировании основных направлений государственной политики по вопросам своей деятельности.
3. Организация взаимодействия подразделений Министерства внутренних дел 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. 21).

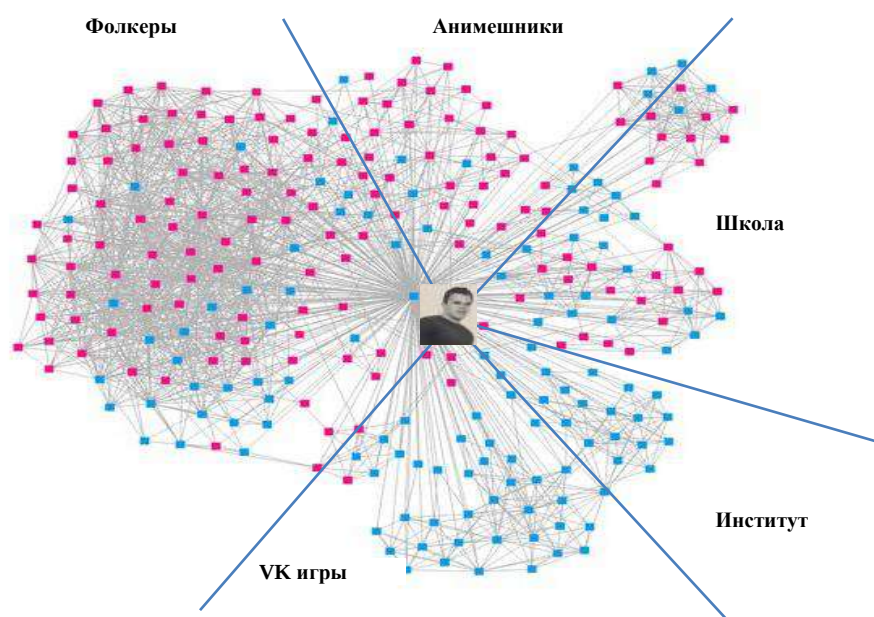


Рис. 21. Пример визуализации связей в социальной сети

⁹⁸ ГУПЭ МВД России – Главное управление по противодействию экстремизму Министерства внутренних дел Российской Федерации.

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 С.Т. 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 «obeIkanobe – hiphopistkrieng – 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 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», главу 29 «Преступления против основ Конституционного строя и безопасности государства». Рассмотрим некоторые примеры:

Пример 1.

В марте 2022 года в ходе регулярно проводимого мониторинга информационных ресурсов сети Интернет выявлена 165 страница социальной сети «ВКонтакте» с призывами к участию в шествии и митинге против СВО, которые на тот момент не были согласованы 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 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 лиц, склонных к совершению правонарушений. Принятыми мерами количество участников акции минимизировано, экстремистских проявлений и иных правонарушений в период проведения митинга не допущено.

Пример 2.

Сотрудниками Центров по противодействию экстремизму⁹⁹ регионального уровня в рамках постоянно проводимого мониторинга информационных 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 – «Пропаганда либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами»; ст. 20.29 КоАП РФ – «Производство и 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 (см. рис. 22).

⁹⁹ Далее – «ЦПЭ».



Рис. 22. Сбор информации о лицах и группах лиц, причастных к организации и осуществлению экстремистской деятельности

В настоящее время возможности глобальной сети Интернет 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 центрифуг, 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 недавно¹⁰⁰.

¹⁰⁰ Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2012. № 1. С. 11.

Факторы, влияющие на распространение идей экстремизма и терроризма в сети Интернет:



- > огромное количество людей – пользователей сети Интернет (более миллиарда человек);
- > транснациональность. Проникновение во все сферы жизнедеятельности человека;
- > анонимность пользователей и конспирация местоположения;
- > законодательная неурегулированность среды Интернет;
- > универсальность и многоликость среды как средства связи, коммуникаций, хранения данных;
- > средства массовой информации и др.

Рис. 23. 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. 24). К ним могут относиться 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. 25) на основе беспилотного воздушного судна (БВС), которые предназначены для оперативного и достоверного получения информации об объектах различного происхождения, проведения инженерной разведки, выявления электронных компонентов минно-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.

3. Осуществления наблюдения и охраны районов сосредоточения экстремистских и террористических группировок при проведении специальных мероприятий.



Рис. 24. Использование новых информационных технологий и радиотехнических методов в борьбе с преступностью

В начале января 2018 года международными террористами были использованы так называемые летательные самодельные беспилотники (см. рис. 25). Данные беспилотные воздушные судна начинались боеком-

плектами 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. 25. 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 взрывопожароопасные 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 России 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 межрегиональной ячейки, в отношении которых приняты различного рода процессуальные решения.

В конце лета 2020 года ФСБ России задержала шестерых «финансировщиков», 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 были 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 террористической 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 для последующего вовлечения 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 люди, 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 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 г. 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 «ЛизаАлерт» 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 г. 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 хранил в целях распространения, а также распространял материалы с порнографическими изображениями несовершеннолетних, в отношении лица, не достигшего четырнадцатилетнего

возраста, с использованием информационно-телекоммуникационных сетей (включая сеть Интернет).

Игнатъев Д.В. с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) совершил распространение порнографических материалов. Указанное преступление подсудимый совершил при следующих обстоятельствах.

Игнатъев 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 программа представляла собой файлообменную сеть, то есть одноранговую компьютерную сеть для совместного использования файлов. Программа была 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.

Игнатъев 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 Игнатъев Д.В. свою вину в предъявленных ему по пп. «а», «г» ч. 2 ст. 242.1, п. «б» ч. 3 ст. 242 УК РФ обвинениях не признал.

Руководствуясь ст. 296-300, 302-304, 307-313 Уголовно-процессуального кодекса Российской Федерации, суд приговорил Игнатъева Д.В. признать виновным в совершении преступлений, предусмотренных пп. «а», «г» ч. 2 ст. 242.1, п. «б» ч. 3 ст. 242 Уголовного кодекса Российской Федерации и назначить наказания:- по пп. «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 Игнатъеву Денису Вячеславовичу 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 возможности файлообменной сети, незаконно распространил через сеть Интернет материалы с порнографическими изображениями несовершеннолетних.

Оперуполномоченными ПСТМ 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 пп. «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. 307-309, 316 УПК РФ, суд приговорил признать Дутова М. В. виновным в совершении преступления, предусмотренного пп. «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, пп. «а, в» ч. 2 ст. 242.2 (совершил незаконное собирание сведений о частной жизни лица, составляющих его личную тайну, без его согласия (видеосъемка 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, используя 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. 307, 308, 309 УПК РФ, суд приговорил Ж. виновным в совершении преступлений, предусмотренных ч. 1 ст. 137, п.п. «а», «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-антиэкстремизма»», 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-антиэкстремизма»» 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 Х, то есть публично, изображения с текстом «Х». 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. 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 экстремистской 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 «ВКонтакте» 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 Рукавишникова. 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 экстремистской организации, которая предположительно была связана с черногорскими мафиозными кланами. Радикалы маскировались под футбольных фанатов. При обыске у них было обнаружено и изъято оружие. Следствие считает, что их наняли главарь 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 сообщества¹⁰¹.

¹⁰¹ Белград, 8 февраля 2021 г. – РИА Новости.

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 2022 год, указывают на резкий скачок данных преступлений с 2391 зарегистрированных преступлений в 2019 году до 3799 преступлений, зарегистрированных в 2022 году, что составляет 58,89% роста. В январе-декабре 2023 года зарегистрировано 2382 преступления террористического характера (+ 6,7%) и 1340 преступлений экстремистской направленности (-14,4 %). Из общего числа зарегистрированных преступлений террористического характера 1098 (+ 29,0 %) преступлений совершены в текущем году, в том числе:

- пресечено на стадии приготовления и покушения – 213 (+ 76,0 %);
- за пределами Российской Федерации – 223 (- 31,6 %).

В январе-декабре 2025 года зарегистрировано 5920 преступлений террористического характера (+ 59,4%) и 2241 преступлений экстремистской направленности (+30,4 %). Из общего числа зарегистрированных преступлений террористического характера 3091 (+50,8 %) преступлений совершены в текущем году, в том числе:

- пресечено на стадии приготовления и покушения – 394 (+38,2 %);
- за пределами Российской Федерации – 161 (+4,5 %) (диаграмма 9).

**Динамика зарегистрированных преступлений
террористического характера и экстремистской направленности**

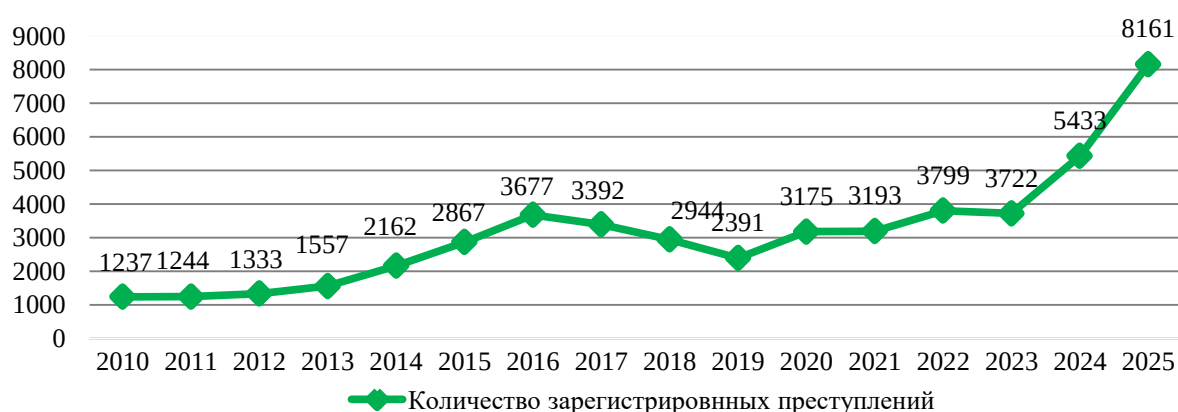


Диаграмма 9. Динамика зарегистрированных преступлений террористического характера и экстремистской направленности

Ежедневная практическая деятельность, направленная на эффективную работу по вопросу раскрытия рассматриваемых видов преступлений, осуществляется путем тесного взаимодействия сотрудников БСТМ МВД России, ГУПЭ МВД России 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» (диаграмма 10).



Диаграмма 10. Динамика раскрываемости преступлений террористического характера и экстремистской направленности

Согласно приведенным сведениям о состоянии преступности в России¹⁰² за I полугодие 2022 г. было выявлено 1332 преступления террористического характера, за аналогичный период 2021 года их было выявлено 1271. Данное количество преступлений указывает на то, что за I полугодие 2022 года их было выявлено на 61 преступление больше, что составляет 4,8% роста.

Среди преступлений экстремистской направленности за I полугодие 2022 г. было выявлено 775 фактов, тогда как за аналогичный период 2021 года их было выявлено 603, что на 172 случая больше и в процентном соотношении составляет рост на 28,5% (см. диаграмму 11).

Согласно приведенным сведениям о состоянии преступности в России¹⁰³ за 2022 год было выявлено 2233 преступлений террористического характера, за 2021 год их было выявлено 2136. Данное количество преступлений указывает на то, что за 2022 год их было выявлено на 27 преступлений меньше, что составляет 4,5%.

Согласно приведенным сведениям о состоянии преступности в России¹⁰⁴ за 2023 год было выявлено 2382 преступления террористического характера, за 2022 год их было выявлено 2233. Данное количество преступлений указывает на то, что за 2023 год их было выявлено на 149 преступлений больше, что составляет 6,3%.

Согласно приведенным сведениям о состоянии преступности в России¹⁰⁵ за 2024 год было выявлено 3714 преступления террористического характера, за 2023 год их было выявлено 2382. Данное количество преступлений указывает на то, что за 2024 год их было выявлено на 1332 преступления больше, что составляет 25,9%.

Согласно приведенным сведениям о состоянии преступности в России¹⁰⁶ за 2025 год было выявлено 5920 преступлений террористического характера, за 2024 год их было выявлено 3714. Данное количество преступлений указывает на то, что за 2025 год их было выявлено на 2206 преступления больше, что составляет 27,3%.

¹⁰² Состояние преступности в России ФКУ «Главный информационно-аналитический центр МВД России» за I полугодие 2022 г., Москва.

¹⁰³ Там же.

¹⁰⁴ Состояние преступности в России ФКУ «Главный информационно-аналитический центр МВД России» за 2023 год, Москва.

¹⁰⁵ Состояние преступности в России ФКУ «Главный информационно-аналитический центр МВД России» за 2024 год, Москва.

¹⁰⁶ Состояние преступности в России ФКУ «Главный информационно-аналитический центр МВД России» за 2025 год, Москва.

**Динамика преступлений террористического характера
и экстремистской направленности за 1 полугодие 2022 года
по отношению к 1 полугодю 2021 года и первое полугодие
2023 года по отношению к 1 полугодю 2022 года**

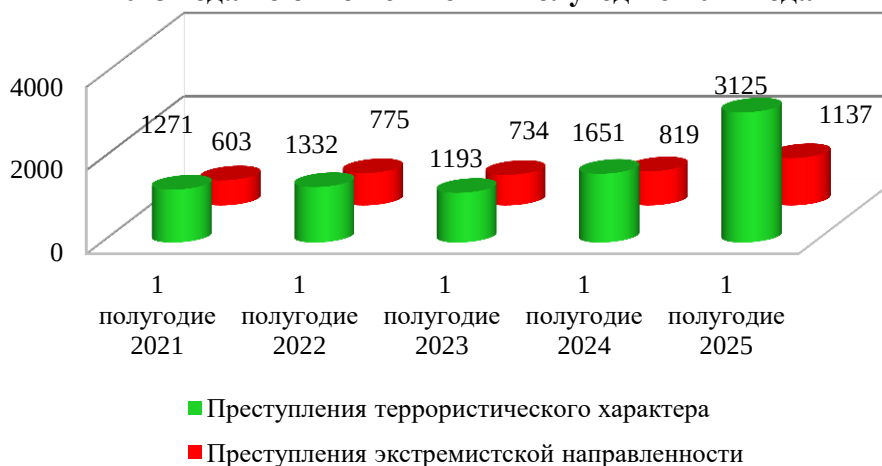


*Диаграмма 11. Динамика преступлений террористического характера
и экстремистской направленности за I полугодие с 2021 по 2025 гг.*

Среди преступлений экстремисткой направленности за 2022 год было выявлено 1566 фактов, тогда как за 2021 год их было выявлено 1057, что на 509 случаев больше и в процентном соотношении составляет рост на 48,2% (см. диаграмму 12).

Среди преступлений экстремисткой направленности за 2023 год было выявлено 1340 фактов, тогда как за 2022 год их было выявлено 1566, что на 226 случаев меньше и в процентном соотношении составляет снижение на 16,8% (см. диаграмму 12).

Среди преступлений экстремисткой направленности за 2024 год было выявлено 1719 фактов, тогда как за 2023 год их было выявлено 1340, что на 379 случаев больше и в процентном соотношении составляет рост на 7,8% (см. диаграмму 12).

Среди преступлений экстремисткой направленности за 2025 год было выявлено 2241 фактов, тогда как за 2024 год их было выявлено 1719, что на 522 случая больше и в процентном соотношении составляет рост на 23,7% (см. диаграмму 12).

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.

**Динамика преступлений террористического характера
и экстремистской направленности за 2022 год
по отношению к 2021 году, за 2023 год по отношению
к 2022 году, за 2024 год по отношению к 2023 году и за 2025 год
по отношению к 2024 году**

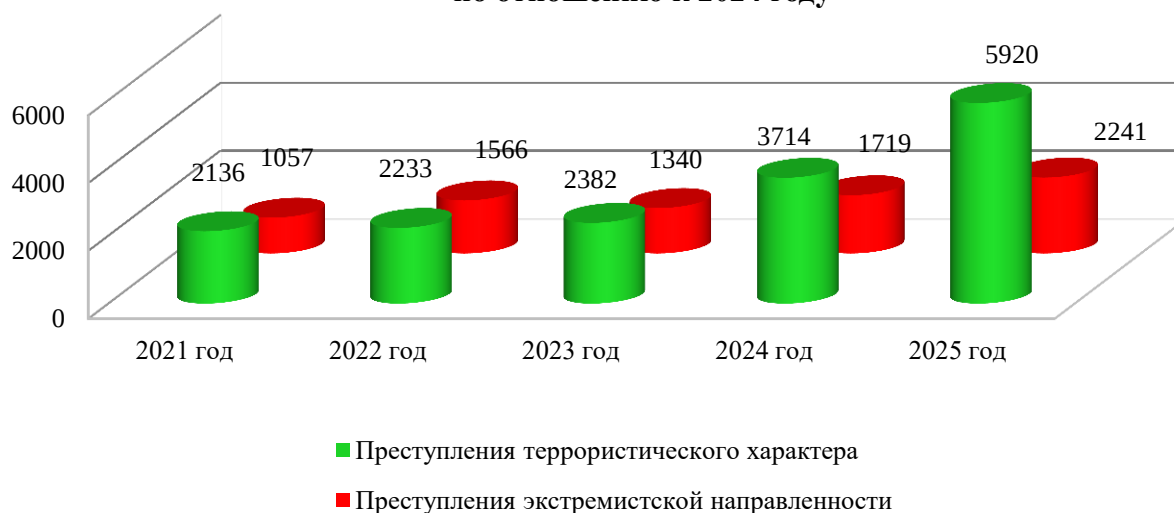


*Диаграмма 12. Динамика преступлений террористического характера
и экстремистской направленности с 2021 по 2025 гг.*

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 безопасности¹⁰⁷.

¹⁰⁷Алескеров 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.

2.8. Основные направления совершенствования системы противодействия кибертерроризму в деятельности органов внутренних дел Российской Федерации

Авторы работы считают необходимым остановиться на буднях сегодняшнего времени. Все мировое сообщество знает и понимает тяжелое положение, складывающееся по вине западных спецслужб, которые на протяжении тридцати лет целенаправленно подрывали экономику Украины и путем ненавистно-агрессивной идеологии, а порой и открытой вражеской пропаганды по отношению к Российской Федерации, настраивали народ Украины против дружественной политики России. Для предотвращения окончательного развала приграничных территорий Украины и во спасение народа Украины руководство и правительство Российского государства были вынуждены начать специальную военную операцию. В этих целях во избежание больших потерь со стороны защитников Российской Федерации активно используются **возможности информационно-телекоммуникационных сетей и высокопрофессиональной деятельности сотрудников Министерства обороны, Росгвардии и МВД России.**

Участники СВО Российской Федерации в целях установления местоположения большого скопления подразделений ВСУ активно используют возможности телекоммуникационной системы, в частности, квадрокоптеры (дроны), при помощи которых выявляют дислокации вражеских сил и принимают все необходимые меры по их обезвреживанию и ликвидации.

В условиях динамично меняющихся обстоятельств ключевым фактором становится скорость обработки и передачи полученной информации. Особенно важным это становится в боевых условиях (во время проведения СВО) и при противодействии странам Североатлантического альянса и их бенефициаров, планируемым террористические угрозы, посредством или через боевиков осуществляющих террористические действия на приграничных районах республик ДНР и ЛНР, а также на территориях Запорожской и Херсонской областей.

Развитие средств связи и протоколов обмена данными на текущем этапе позволяет использовать сложно организованные сети передачи данных на базе беспилотных летательных аппаратов, которые можно быстро развернуть и выдвинуть в район разведки для сбора информации.

Также с помощью беспилотных летательных аппаратов можно развернуть телерадиокоммуникационную сеть, увеличивающую дальность контроля дронов и зону уверенного приема сигналов посредством дрона-ретранслятора (радиосигнал в обычных обстоятельствах обеспечивает зону уверенного приема в пределах пяти километров, при использовании дрона-ретранслятора зона уверенного приема сигнала существенно увеличивается).

Использование разных моделей дронов с различными характеристиками и, соответственно, разными возможностями позволяет выстроить многоуровневую шифрованную информационную сеть, в рамках которой каждый элемент будет выполнять свою задачу.

В условиях, когда отсутствует возможность прямой связи между базовыми станциями или же станциями боевой связи, сформированная из дронов шифрованная информационно-телекоммуникационная сеть **позволит** не только обеспечить связь в самых сложных условиях и самых отдаленных от базовой станции местах, но и **даст возможность контроля территории**, сбора информации и быстрой ее обработки для принятия своевременного решения, а также передачи этого решения для исполнения.

Предлагаемая схема информационно-телекоммуникационной сети имеет три уровня (схема 9).

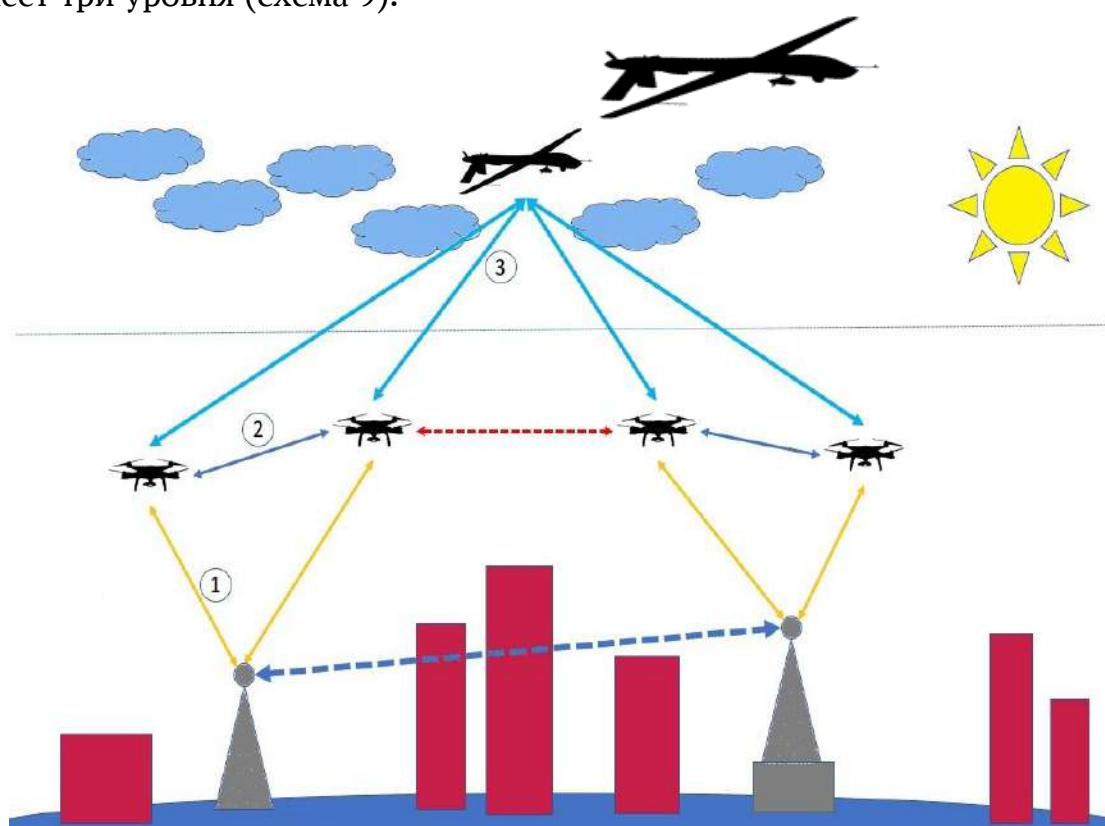


Схема 9. Многоуровневая информационно-телекоммуникационная сеть передачи данных

Первый уровень составляют базовые станции связи (статичные) и мобильные станции связи (командно-штабная машина). Они обеспечивают связь и передачу информации в обычных условиях, а также принимают и передают информацию на сеть дронов-ретрансляторов.

Второй уровень составляет «рой» дронов-ретрансляторов, главными задачами которых является прием и передача поступающей информации, увеличение зоны покрытия и дальности связи, а также сбор и передача разведданных на третий уровень.

Третьим уровнем является высотный беспилотник (беспилотники), осуществляющий контроль за дронами-ретрансляторами и обеспечивающий их управляемость даже в условиях постановки помех, а также служащий ретранслятором в случае, когда связь между дронами-ретрансляторами второго уровня потеряна или нарушена. Аналогом высотного беспилотника также может служить спутник связи при наличии соответствующих модулей приема-передачи спутникового сигнала на дронах-ретрансляторах.

В результате тактически грамотного использования возможностей информационно-телекоммуникационной сети сотрудниками органов внутренних дел в тесном взаимодействии со специалистами ФСБ России, Министерства обороны Российской Федерации, Росгвардии и иных правоохранительных органов Российской Федерации с большим успехом определяется наиболее вероятное скопление вооруженных сил Украины и их наемников для последующей ликвидации (схема 10).

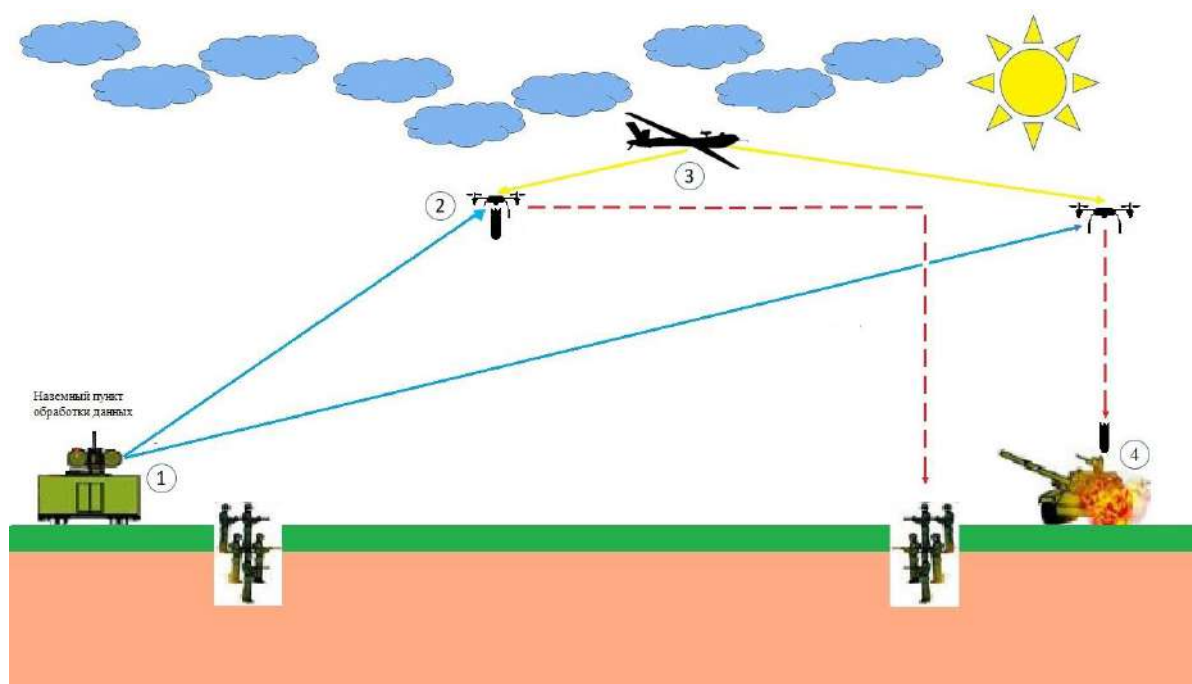


Схема 10. Нанесение точечного удара по противнику за счет полученной информации с БПЛА при использовании информационно-телекоммуникационной сети

В настоящее время, используя радио-электронную телекоммуникационную сеть, все чаще стали использоваться дроны, питающиеся и управляемые через провод питания от электромодуля, а также провод

данных управления. Они используются как быстровозводимые вышки сотовой сети, а также как средство массового поражения в условиях активной радиоэлектронной борьбы.

Как понимает мировое сообщество сам термин кибертерроризм?

Кибертерроризм – это использование современных технологий, в первую очередь компьютерных систем и Интернета, для совершения террористических актов. Кибертерроризм включает в себя преднамеренное нападение на компьютерные сети, информационные системы и цифровые инфраструктуры с целью причинения вреда, полного или частичного их разрушения или оказания деструктивного психологического воздействия на соответствующие целевые аудитории.

Кибертеррористы могут использовать такие методы, как взлом, (кража) данных, распространение вредоносного ПО (вирусов), а также проведение скоординированных кибератак на критически важную инфраструктуру или правительственные системы.

Кибертерроризм представляет значительную угрозу информационной и психологической безопасности личности. Он предполагает использование современных информационно-коммуникационных технологий для осуществления политически мотивированных атак с целью вызвать страх, панику или беспорядки. Осуществляя «нападение» на критически важную инфраструктуру, сети или персональные устройства, кибертеррористы могут украсть конфиденциальную информацию, поставить под угрозу конфиденциальность в целом, что может привести к психологическому стрессу и потере доверия к цифровым системам. Защита от кибертерроризма требует надежных мер кибербезопасности и осведомленности людей для защиты индивидуальной информации и поддержания личного психологического благополучия.

По нашему мнению, **суть понятия информационно-психологической безопасности** заключается в обеспечении благополучия личности, общества и государства путем их защиты от информационных рисков и угроз. Это предполагает обеспечение полной и необходимой доступности, целостности, конфиденциальности и надежной защиты информации, а также содействие психологическому благополучию и устойчивости. Данное понятие также включает меры по предотвращению несанкционированного доступа, манипулированию или раскрытию информации, а также устранению психологических уязвимостей, возникающих в результате связанных с информацией проблем, таких как дезинформация, кибератаки или онлайн-преследование. В конечном итоге информационная и психологическая безопасность направлены **на укрепление доверия, стабильности и чувства безопасности внутри личности, общества и государства.**

КОМПОНЕНТЫ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ

1. РАЗВЕДКА УГРОЗ

Сбор и анализ информации о потенциальных киберугрозах, включая мониторинг хакерской деятельности, выявление вредоносных программ и отслеживание субъектов угроз

2. ЦЕНТР УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ

Централизованное подразделение, отвечающее за непрерывный мониторинг, обнаружение и реагирование на киберугрозы. В его состав входят аналитики безопасности, специалисты по реагированию на инциденты и передовые инструменты безопасности

3. СИСТЕМЫ ОБНАРУЖЕНИЯ/ПРЕДОТВРАЩЕНИЯ ВТОРОЖЕНИЙ (IDS/IPS)

Эти системы помогают отслеживать сетевой трафик, обнаруживать подозрительные действия и предотвращать несанкционированный доступ или атаки

4. ЗАЩИТА КОНЕЧНЫХ ТОЧЕК

Развертывание антивирусного программного обеспечения, решений для обнаружения и реагирования на конечные точки (EDR), а также других мер безопасности для защиты отдельных устройств от киберугроз

5. УПРАВЛЕНИЕ СОБЫТИЯМИ И ИНФОРМАЦИЕЙ О БЕЗОПАСНОСТИ (SIEM)

Собирает и анализирует журналы событий безопасности из различных сетей и устройств безопасности, обеспечивая централизованный мониторинг и обнаружение потенциальных угроз

6. БРАНДМАУЭРЫ

Устройства сетевой безопасности, которые контролируют входящий и исходящий сетевой трафик, обеспечивают соблюдение политик безопасности и блокируют вредоносный трафик

7. СОТРУДНИЧЕСТВО И ОБМЕН ИНФОРМАЦИЕЙ

Содействие сотрудничеству между организациями, государственными учреждениями и международными партнерами для обмена информацией об угрозах, передовым опытом и координации реагирования на кибератаки

8. ОСВЕДОМЛЕННОСТЬ И ОБУЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ

Обучение сотрудников, пользователей и заинтересованных сторон киберугрозам, безопасным онлайн-практикам и важности поддержания протоколов безопасности

9. ПРАВОВАЯ И ПОЛИТИЧЕСКАЯ БАЗА

Разработка и обеспечение соблюдения законов, правил и политики по борьбе с кибертерроризмом, включая соглашения о международном сотрудничестве, законы о защите данных и наказания для киберпреступников

10. ПЛАН РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

Установление заранее определенного набора процедур, которым необходимо следовать в случае киберинцидента, включая шаги по сдерживанию, искоренению и восстановлению

Представленная схема компонентов системы противодействия кибертерроризму представляет собой общий обзор и может варьироваться в зависимости от конкретных потребностей и возможностей организации, ведомства или правительства.

Для эффективного обеспечения информационной и психологической безопасности личности, общества и государства можно принять ряд мер:

1. Информированность и образование: повышение уровня осведомленности и информационной грамотности людей по вопросам онлайн-безопасности, защиты конфиденциальности и психологического благополучия, включая распознавание и устранение киберугроз, психологических манипуляций и дезинформации.

2. **Надежная кибербезопасность:** внедрение строгих мер кибербезопасности для защиты критически важной инфраструктуры, личных данных и конфиденциальной информации от кибератак. Данное понятие включает использование брандмауэров, систем шифрования, антивирусного программного обеспечения и осуществление его регулярного обновления.

3. **Защита конфиденциальности:** соблюдение мер предосторожности при размещении личной информации в информационно-коммуникационном пространстве, а именно: установление правил и методов защиты персональных данных с целью их ответственного использования, поощрение пользователей, соблюдающих эти правила, и предоставление им инструментов для эффективного управления настройками конфиденциальности.

4. **Эффективное законодательство:** необходимо разрабатывать и обеспечивать соблюдение законов, регулирующих сбор, хранение и использование персональных данных, устанавливая подотчетность и наказание для тех, кто злоупотребляет доверием граждан или ставит под угрозу информационное и психологическое благополучие отдельных лиц.

5. **Медиаграмотность:** повышение медиаграмотности общества с целью обучения критическому оцениванию источников информации, различать достоверный и вводящий в заблуждение контент, понимать потенциальные психологические последствия воздействия средств массовой информации.

6. **Поддержание информационно-психического здоровья:** создание доступных ресурсов и систем поддержания психического здоровья для решения психологических проблем, возникающих из-за информационной перегрузки, онлайн-преследований и различного рода манипуляций в информационной среде; поощрение открытых дискуссий на темы психического здоровья и предоставление консультационных услуг. В настоящее время имеет место КИБЕРБУЛЛИНГ – это травля в цифровом пространстве (оскорбление, злые шутки в комментариях или сообщениях), публикация личной информации (адреса, номера телефона, интимных фотографий), посты с угрозами.

7. **Международное сотрудничество:** активизация международного сотрудничества для борьбы с глобальными киберугрозами и кампаниями по дезинформации и психологическим манипуляциям в отношении современного общества. Обмен передовым опытом, разведанными и совместная борьба с киберугрозами могут повысить общую безопасность.

8. **Этичное использование информационных технологий:** поощрение ответственного, с точки зрения этики, развития и использования современных технологий, включая искусственный интеллект, гарантирующих достижение полезного эффекта для отдельных лиц, общества и государства без ущерба для их информационной безопасности или психологического благополучия.

9. Укрепление социальных связей: развитие социальных связей внутри сообществ, способствующих укреплению их устойчивости для противодействия психологическим манипуляциям и повышения общего благополучия.

10. Сотрудничество и обмен информацией: установление партнерских отношений между государственными учреждениями, организациями частного сектора и международными организациями для обмена информацией об угрозах, передовым опытом и координации усилий по реагированию.

11. Законодательство и политика в области борьбы с кибертерроризмом: разработка законов, правил и политики, направленных на борьбу с кибертерроризмом и обеспечивающих правовую основу для расследования преступлений и наказания правонарушителей.

12. Реагирование на инциденты и восстановление: создание четко определенных протоколов (алгоритмов действий) и групп для эффективного реагирования на кибератаки, минимизации ущерба, восстановления услуг и расследования инцидентов.

13. Разработка и внедрение программ профессиональной подготовки специалистов по информационной безопасности: проведение регулярных программ обучения по кибербезопасности специалистов данной категории и организаций о потенциальных угрозах, безопасных методах и важности сообщения о подозрительных действиях.

Конкретные меры могут различаться в зависимости от контекста и возникающих уникальных проблем с учетом конкретной ситуации, с которыми сталкивается каждый гражданин, общество или государство.

Считаем необходимым рассмотреть несколько примеров, связанных с кибертерроризмом.

Одним из примеров кибертерроризма является атака Stuxnet. Stuxnet представлял собой сложный компьютерный червь, который атаковал **иранские** ядерные объекты в 2010 году. Он был разработан для нарушения и саботажа процесса обогащения урана путем использования уязвимостей в их системах промышленного контроля. Эта кибератака считается актом кибертерроризма, поскольку ее целью являлось причинение физического вреда и значительного ущерба критически важной инфраструктуре страны.

Атака с помощью программы-вымогателя WannaCry, затронувшая тысячи компьютеров по всему миру, а также взлом SonyPictures в 2014 году являются яркими примерами кибертеррористических инцидентов.

Кибератаку на SonyPictures в 2014 году предположительно осуществила Северная Корея. Эти инциденты демонстрируют явное негативное воздействие на критически важную инфраструктуру страны.

Теракт на Крымском мосту также является актом кибертерроризма. Крымский мост был подорван 17 июля 2023 г. двумя надводными беспилотными летательными аппаратами Украины, что нанесло существенный материальный ущерб, нарушив на некоторое время транспортное движение между Кубанью и Крымом. Также в результате данного теракта погибли супруги Кулик, а их несовершеннолетний ребенок в возрасте 14 лет получил серьезные ранения грудной клетки и закрытую черепно-мозговую травму.

Также хочется остановиться на дискуссии вокруг дерзкого террористического акта, связанного с подрывом «Северных потоков». 26 сентября 2022 г. был совершен подрыв «Северного потока», системы газопроводов, соединяющих Россию и Германию. Взрыв произошел на дне Балтийского моря (Борнхольмская котловина). Данная диверсия на газопроводах была совершена на фоне полномасштабного вторжения в Украину, на пике газового конфликта России и Евросоюза. В результате серии взрывов в исключительных экономических зонах Дании и Швеции были разрушены обе нити «Северного потока-1» и одна из двух нитей «Северного потока-2». На момент аварии прокачка газа по ним не велась: СП-1 был остановлен российской стороной, СП-2 так и не был запущен. В ходе осмотра мест происшествия и выяснения обстоятельств инцидента был установлен факт намеренного подрыва трубопроводов «Северного потока». Также было достоверно установлена осведомленность руководства Швеции и Дании о практикуемых погружениях в Балтийском море спецслужбами США на протяжении нескольких месяцев перед подрывами.

Официальные расследования датских, норвежских и немецких властей по состоянию на январь 2024 года не пришли к выводам об организаторе или исполнителях диверсий. Также стало известно, что в июне 2023 года боевые пловцы ВМС США, действуя под прикрытием широко-разрекламированных учений НАТО BALTOPS 22, установили взрывные устройства с дистанционным управлением, а спустя три месяца взорвали три из четырех труб «Северного Потока».

Информационный и психологический кибертерроризм подразумевает использование кибертехнологий для внушения чувства страха, создания паники и организации беспорядков среди отдельных лиц, организаций или обществ. Данное понятие включает в себя преднамеренное распространение вводящей в заблуждение или ложной информации, взлом компьютерных систем с целью манипулирования данными или кражи конфиденциальной информации, а также использование тактики психологического манипулирования с целью причинения вреда обществу или пропаганды террора. Цель состоит в том, чтобы использовать уязвимости в цифровых

системах и подрыв психологии пользователя для достижения политических, идеологических или личных целей. Данные целенаправленные действия можно квалифицировать как киберсаботаж.

Авторами данного пособия предпринята попытка представить своё понимание такого явления, как киберсаботаж (кибердиверсия).

Киберсаботаж (кибердиверсия) – это преднамеренное нарушение или разрушение компьютерных систем, сетей или цифровой инфраструктуры отдельными лицами или группами со злыми намерениями такими, как взлом, распространение вредоносного ПО, запуск распределенных атак типа «отказ в обслуживании» (DDoS) или подделка критически важных данных или систем. Целью кибердиверсии обычно является причинение ущерба, получение несанкционированного доступа, кража, модификация, искажение, уничтожение информации или срыв операций.

Кибертерроризм, по своей сути, является набором мер, способов и методов атаки на технические устройства, информационные сети с целью либо вывода атакуемого устройства (или сети) из строя, либо с целью получения конфиденциальной информации или материальной выгоды. К кибертерроризму, на наш взгляд, можно отнести и такой сегмент, как распространение фейков, пропаганда (контрпропаганда), кибербуллинг и прочие методы психологического воздействия на личность.

Фейк (от английского fake - подделка) – это подделка фактов, событий, обстановки, относящихся к чему-то, что не является подлинным или реальным. Зачастую, это обман или фальсификация информации, объектов или событий.

Все вышеперечисленное можно отнести именно к психологическим атакам через информационные технологии (ярким примером можно назвать распространение видеозаписи «Белых касок», группы «Синие киты» и прочие), а точнее – к информационному терроризму, а в зависимости от содержания фейка, в ряде случаев, можно отнести к информационному экстремизму.

В результате проведения оперативно-розыскных мероприятий, направленных на недопущение и предотвращение террористических актов, была получена информация в отношении гражданина Белоруссии, некоего «Н», который был взят на оперативный учет. В результате проведения вышеназванных мероприятий с применением специальных технических средств была установлена причастность разрабатываемого лица к ранее совершенным преступлениям по подрыву двух поездов в Северомуйском тоннеле БАМа на территории Бурятии, а также была предотвращена подготовка к другим террористическим актам.

В конце 2023 года сотрудниками ФСБ России данный гражданин Белоруссии был задержан. Подозреваемым оказался гражданин Белоруссии

1971 года рождения. Его задержали в Омской области. ТАСС и РИА Новости также опубликовали оперативную съемку ФСБ России: на видео подозреваемый признается, что действовал по заданию проживающего в Литве соотечественника, который работает на украинские спецслужбы. Из показаний задержанного следует, что взрывные устройства устанавливал он сам.

Инцидент на перегоне Итыкит-Окусикан в Бурятии произошел 29 ноября в 17:20 по московскому времени. Машинист услышал хлопок, после в одном из составов начался пожар, машинист и его помощник не пострадали, в результате взрыва были повреждены три вагона-цистерны, один из них выгорел полностью.

Вскоре сообщили, что на обходном пути взорвался еще один состав, загорелись шесть вагонов. Топливо разлилось на площади 150 кв. м, так же обошлось без пострадавших. 2 декабря движение поездов на перегоне Итыкит-Окусикан было полностью восстановлено.

В качестве противодействия планируемым террористическим актам сотрудниками правоохранительных органов осуществляются комплексные оперативно-розыскные мероприятия, направленные на своевременное выявление, пресечение, предотвращение, раскрытие и расследование современных видов преступлений, совершаемых с использованием возможностей информационно-коммуникационных сетей. Предлагаем рассмотреть несколько примеров.

Пример 1.

Совершенный 22 марта в городе Красногорске и шокирующий весь мир кровавый террористический акт – далеко не первая террористическая атака против нашей страны за последнее время. Проведенные российскими компетентными органами следственные действия указывают, что следы всех этих преступлений ведут на Украину. Другие варварские теракты с применением взрывных устройств стоили жизни журналистам Д.А. Дугиной и М.Ю. Фомину (В. Татарскому) привели к тяжелому ранению писателя Е.Н. Прилепина и смерти его водителя А.И. Шубина, гибели пяти человек в результате подрыва Крымского моста, ранениям 42 человек при взрыве в кафе Санкт-Петербурга. Убийствами и увечьями мирных граждан, в том числе детей, сопровождалась рейды террористической организации «Русский Добровольческий Корпус»¹⁰⁸. МИД России передал властям Украины требования о немедленном аресте и выдаче всех лиц, причастных к данным терактам. В числе этих требований – арест главы СБУ В. Малюка¹⁰⁹, цинично признавшего 25 марта организа-

¹⁰⁸ РДК – признан террористической организацией и запрещен на территории Российской Федерации.

¹⁰⁹ Василий Малюк внесен в перечень террористов и экстремистов Росфинмониторинга.

цию Украиной подрыва Крымского моста в октябре 2022 года и раскрывшего детали организации других терактов в Российской Федерации¹¹⁰.

3 апреля 2024 г. по настоятельной просьбе французской стороны состоялись телефонные переговоры Министерства обороны Российской Федерации генерала армии Сергея Шойгу с министром обороны Французской республики Себастьяном Лекофню. Министр обороны Франции выразил соболезнование в связи с терактом в концертном зале «Крокус Сити Холл» 22 марта 2024 г. При этом настоятельно пытался убедить в непричастности Украины и стран Запада к атаке террористов, перекладывая ответственность на ИГИЛ.

Сергей Шойгу подчеркнул, что начатое в связи с террористическим актом в «Крокус Сити Холле» расследование будет, безусловно, доведено до конца, а все виновные будут наказаны. Имеются сведения об украинском следе в организации теракта. «Киевский режим ничего не делает без одобрения западных кураторов. Рассчитываем, что в данном случае за этим не стоят французские спецслужбы», - заявил глава российского ведомства. Далее он уведомил, что в отношении заявлений Елисейского дворца об отправке Французского контингента на Украину, в случае их практической реализации, это создаст проблемы для самой Франции.

Пример 2.

При въезде на территорию Российской Федерации был обнаружен микроавтобус с прицепом, с европейскими номерами. В ходе осмотра микроавтобуса таможенной службой был обнаружен груз, доставляемый с Украины, сотни произведенных в Киеве икон: образа «Христа Спасителя», «Казанской Божьей Матери», - под которыми была спрятана взрывчатка чудовищной силы (гексоген). Мощность данного взрывчатого вещества в полтора раза больше мощности тротила. Масса изъятого взрывчатого вещества достаточна для подрыва пятиэтажного жилого дома. Впрочем, тот, кто пытался доставить в Россию взрывчатку за «святыми образами», явно планировал не один взрыв. В церковной утвари оперативники обнаружили целый арсенал детонаторов промышленного производства, способных подрывать бомбы дистанционно по звонку или сообщению в мессенджере.

В результате проведенных мероприятий сотрудниками ФТС, Росгвардии и ФСБ России из груза, следовавшего по маршруту Украина – Румыния – Венгрия – Словакия – Польша – Литва – Латвия – Россия, извлечено 27 закамуфлированных в иконы и готовых к применению самодельных взрывных устройств, 70 кг изготовленного промышленным способом пластичного взрывчатого вещества повышенной мощности, 91 электродетонатор и части выстрела к РПГ-7. Эти выстрелы от грана-

¹¹⁰ Заявление МИД России от 31 марта 2024 г.

томета были спрятаны в церковный подсвечник. На боеприпасе значилась цифра 10 в двойной окружности, маркированная военным заводом в Болгарии, чье оружие давно использует Украина. На коробке было указано название промежуточной точки - Черновцы.

Данная взрывчатка прибыла из Киева, затем, как установили в ФСБ России, - через пункт пропуска «Порубное» груз был переброшен в Румынию на склад приграничного города Фэлтичени. Очевидно, этим занимались украинские спецслужбы, которым не составило труда создать «коридор» на своей границе, однако и румынские пограничники без проблем пропустили машину, груженую бомбами, несмотря на жесткие правила досмотра, которые ввели после начала СВО. В Россию по замыслу преступников этот груз должен был доставить второй автомобиль. По словам водителя, на таможне между Румынией и Венгрией он без лишних вопросов оформил документы для въезда в единое экономическое пространство Евросоюза. Дальше повез иконы-бомбы по трассе, даже не пытаясь объехать пункт досмотра на польско-литовской границе. Латвийские пограничники также без проблем пропустили машину. В итоге смертоносный груз пересек шесть стран, проделав путь почти в две тысячи километров, не вызвал ни малейшего подозрения ни на одном из четырех контрольно-пропускных пунктов Европы. Водитель, у которого есть гражданство России и Украины, на допросе хотел указать, что спецслужбы Украины своевременно его не поставили в известность о содержании груза. По словам компетентных сотрудников, на границе при досмотре груза водитель сильно нервничал и пытался торопить таможенников, поэтому и вызвал подозрение.

В настоящее время оперативные сотрудники силовых структур Российской Федерации устанавливают круг лиц, причастных к подготовке и осуществлению в последующем террористических актов на территории Российской Федерации.

Проигрывая на фронте в зоне проведения СВО, Украина осуществляет военные действия, взрывая гражданские объекты и совершая обстрел мирного населения, а также террористические акты на территории России.

Установлена связь между украинскими националистами и боевиками, устроившими кровавую акцию в «Крокус Сите Холле», Киев готов на все ради своей цели, пытаясь дестабилизировать ситуацию в нашей стране. Иконы, с помощью которых украинские спецслужбы готовили новую террористическую атаку, - это планируемый «подарок», особенно в канун православной пасхи¹¹¹.

¹¹¹ Новостная лента ТВ.

Пример 3.

Сотрудниками ФСБ России в ходе проведения контртеррористической операции была получена оперативная информация в отношении группы лиц, прибывших из Средней Азии. Данные лица были взяты на оперативный учет, и в отношении фигурантов были проведены соответствующие оперативно-розыскные мероприятия.

В результате проведенных мероприятий выяснены все обстоятельства и установлены конкретные лица, которые планировали осуществить террористический акт на территории Донецкой Народной Республики. Далее в целях недопущения террористического акта организованная преступная террористическая группа, состоящая из шести человек, была обезврежена. У задержанных изъяли два самодельных взрывных устройства, готовых к применению, и ручные гранаты. По оперативным данным, деятельность преступной группы курировалась с украинской территории. После совершения преступлений в России боевики планировали выехать в Турцию и оттуда переправиться на Украину. Однако в результате своевременно полученной оперативно значимой информации был намечен план проведения оперативно-розыскных мероприятий, и в результате тесного взаимодействия структурных подразделений преступники были задержаны.

Пример 4.

Еще один террористический акт удалось предотвратить 11 апреля 2024 г. в Москве. По данным ФСБ России, его планировалось совершить в одной из московских синагог. Подозреваемый мужчина из Средней Азии при его задержании оказал вооруженное сопротивление и был ликвидирован. Чуть позже при обыске в его квартире были обнаружены готовые взрывные устройства и другие взрывчатые вещества.

Глава III

Особенности получения оперативно значимой информации сотрудниками оперативных подразделений и следственных органов в целях раскрытия преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет

3.1. Технологическая цепочка действий оперативных сотрудников и следователей, направленных на получение необходимой информации у сторонних компаний, организаций и учреждений

Сведения, запрашиваемые у операторов сотовой связи:

- паспортные данные владельца абонентского номера;
- детализация звонков за последние три месяца – эти сведения позволяют определить, сколько у мошенника сотовых аппаратов (IMEI), как часто он меняет абонентские номера, а также избавляется ли он от сим-карты после совершения мошеннических действий или же использует повторно;
- использованные для связи IMEI за последние три месяца;
- использованные для связи базовые станции за последние три месяца с указанием следующих технических характеристик: количество секторов (антенных блоков в месте установки), азимут направленности использованных антенных блоков и угол охватываемой ими территории;
- информация о входящих и исходящих платежах по лицевому счету абонентского номера;
- информация об IP-адресах, использованных для входа в личный кабинет сотового оператора по управлению данным номером. В большинстве случаев мошенник использует абонентские номера, зарегистрированные на подставных лиц, и все операции по управлению абонентским номером проводит через личный кабинет, тем самым оставляя «след» в виде своего IP-адреса;
- копия регистрационной формы – документ, который заполняет продавец сим-карты при ее регистрации. Помимо установочных данных в нем мы узнаем данные об адресе торговой точки, где сим-карта была реализована, а также данные продавца. К этому лицу у следствия должны возникнуть обоснованные вопросы.

Сведения, запрашиваемые по банковским картам и расчетным счетам.

По банковской карте:

- информация о паспортных данных владельца банковской карты;
- информация о движении денежных средств по банковской карте и местах их обналичивания за последние полгода с указанием точного времени проведения приходных и расходных операций, номера и коды транзакций и др. Проанализировав полученную информацию за последние полгода, возможно определить наиболее часто используемые банкоматы, которые, как показывает практика, находятся рядом с домом мошенника или местом частого посещения (работа, торговый центр, адрес родственников и т.д.), информацию о регулярно оплачиваемых абонентских номерах (личный номер, номер родственников или друзей); а также о торговых точках или интернет-магазинах, в которых совершались покупки. Каждый интернет-магазин предоставит информацию об адресе мошенника, на который почтовым переводом был отправлен приобретенный товар;
- информация об абонентских номерах, привязанных к данной банковской карте услугой «мобильного банкинга», где и каким образом они были подключены;
- информация об адресе офиса банка, в котором была открыта банковская карта;
- информация об IP-адресах, использованных для входа в онлайн-сервис по управлению данной банковской картой.

По расчетному счету необходимо запрашивать аналогичную информацию о банковских картах, открытых по данному расчетному счету.

Сведения, запрашиваемые по электронным кошелькам (ЮMoney, Яндекс. Деньги и др.):

- информация о паспортных данных владельца электронного кошелька;
- информация о способе и месте идентификации электронного кошелька;
- информация об абонентском номере, с использованием которого был создан электронный кошелек;
- информация об абонентских номерах, привязанных к электронному кошельку;
- информация о виртуальных банковских картах, которые были выпущены по данному электронному кошельку;

- информация о пластиковых картах, выпущенных по данному кошельку, способ их получения (адрес почтового отправления);
- информация о входящих и исходящих платежах по электронному кошельку с момента его регистрации;
- информация об IP-адресах, использованных для совершения денежных транзакций, а также администрирования электронного кошелька.

Сведения, запрашиваемые по сайтам объявлений («Авито», «Юла» и др.)

Если мошенник выступает как продавец:

- информация о лице, разместившем объявление о продаже (наименование товара) с абонентского номера (номер мошенника);
- установочные данные, использованные им для регистрации абонентского номера и электронной почты;
- использованные для создания и администрирования объявлений IP-адреса;
- аналогичная информация об иных объявлениях данного лица, созданная с использованием того же абонентского номера или электронной почты;
- аналогичная информация об иных объявлениях данного лица, установленных при анализе Cookie-файлов.

Если мошенник выступает как покупатель:

- информация об IP-адресах пользователей сайта, просматривавших объявление потерпевшего (номер объявления).

Сведения, запрашиваемые по социальным сетям:

- информация о пользователе страницы социальной сети (ссылка на страницу, например, <https://vk.com/id410077130>);
- установочные данные, использованные им для регистрации абонентского номера и электронной почты;
- IP-адреса, использованные для создания и доступа к странице за последние два месяца;
- аналогичная информация по иным страницам социальной сети «Вконтакте» данного пользователя, установленных при анализе Cookie-файлов (данный пункт не запрашивается в случае взлома страницы потерпевшего или страниц его друзей).

Сведения, запрашиваемые по доменному имени сайта:

- информация о паспортных данных регистратора доменного имени;
- информация об использованных для регистрации абонентских номерах и электронных почтах;
- информация о том, каким образом была произведена регистрация пользователя;
- информация об IP-адресах, использованных для регистрации доменного имени;
- информация об IP-адресах, использованных для входа в личный кабинет или панель управления для администрирования доменного имени;
- информация об оплате услуг регистрации и аренды доменного имени, с указанием полных реквизитов плательщика;
- аналогичная информация по иным доменным именам, зарегистрированным данным пользователем, установленным при анализе Cookie-файлов.

Сведения, запрашиваемые по арендуемому хостингу:

- информация о паспортных данных арендатора хостинга;
- информация об использованных для аренды абонентских номерах и электронных почтах;
- информация о том, каким образом была произведена регистрация пользователя;
- информация об IP-адресах, использованных для аренды хостинга;
- информация об IP-адресах, использованных для входа в личный кабинет или панель управления для администрирования хостинга;
- информация об оплате услуг аренды хостинга, с указанием полных реквизитов плательщика;
- аналогичная информация по иным хостингам, арендуемым данным пользователем, установленным при анализе Cookie-файлов.

Сведения, запрашиваемые у интернет-провайдера

С информацией о запрашиваемых сведениях можно ознакомиться в пункте 4.2 главы IV (Часть 2):

- информация о пользователе и адресе использованного оборудования, которому был выдан интересующий нас IP-адрес в интересующий нас промежуток времени.

Сведения, запрашиваемые по электронной почте:

- информация о паспортных данных владельца электронной почты;

- информация об использованных для регистрации абонентских номерах;
- информация об IP-адресах, использованных для доступа к электронной почте за максимально известный период;
- аналогичная информация по иным электронным почтам, зарегистрированным данным пользователем, установленным при анализе Cookie-файлов.

Сведения, запрашиваемые у провайдера SIP-телефонии:

- информация о паспортных данных владельца абонентского номера;
- информация об использованных для регистрации абонентских номерах, электронных почтах;
- информация о том, каким образом была произведена регистрация пользователя;
- информация об IP-адресах, использованных для регистрации абонентского номера;
- информация об IP-адресах, использованных для входа в личный кабинет, панель управления по администрированию данным абонентским номером;
- информация об IP-адресах, использованных для осуществления звонков;
- информация об абонентских номерах, использующих переадресацию входящих вызовов;
- информация о статистике звонков за интересующий период;
- информация об оплате услуг связи, с указанием полных реквизитов плательщика.

3.2. Схемы расследования наиболее распространённых преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет

Мошенничества через сайты объявлений.

Мошенник-продавец

Мошенник размещает на сайтах объявлений («Авито», «Юла», «Циан» и др.) информацию о продаже какого-либо товара, сдаче в аренду жилых помещений или же оказании тех или иных услуг, за которые в последующем получает предоплату, тем самым похищая деньги (см. рис. 26).



Рис. 26. Схема запросов сотовому оператору и в банк

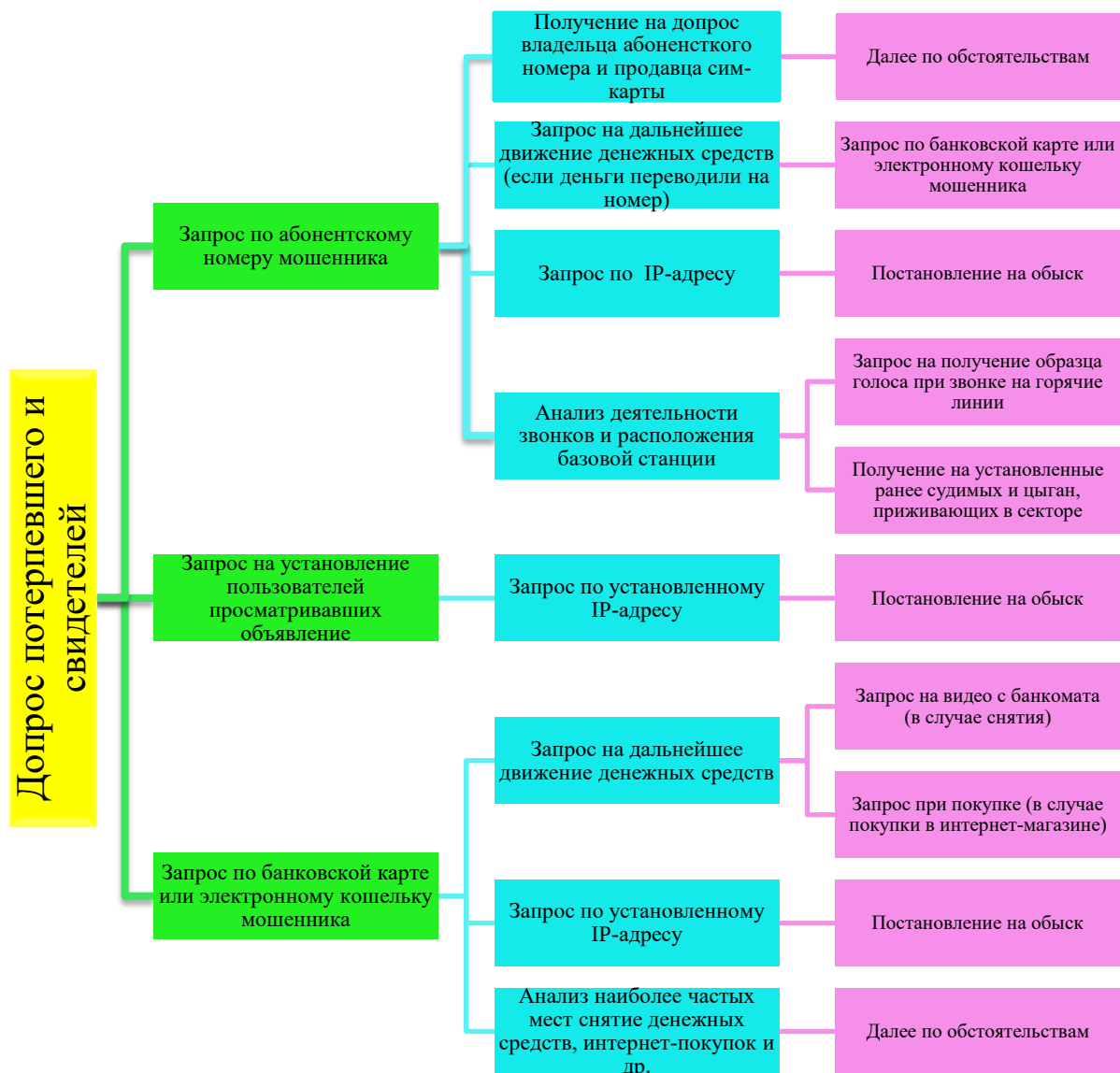


Рис. 27. Порядок действий сотрудника ОВД при раскрытии мошенничества через сайты объявлений (мошенник-продавец)

Мошенничества через сайты объявлений. Мошенник-покупатель

Мошенник звонит по объявлению потерпевшего, размещенному на сайте (Авито, Юла, Циан и др.), и говорит, что желает приобрести его товар и готов внести задаток, для чего просит продиктовать контрольные данные по банковской карте и поступивший код. Получив данные сведения, осуществляют перевод через онлайн-сервисы или покупку, или же мошенник просит подойти к банкомату и выполнить ряд комбинаций, подключая «Мобильный банк», и в последующем похищая денежные средства (см. рис. 28).

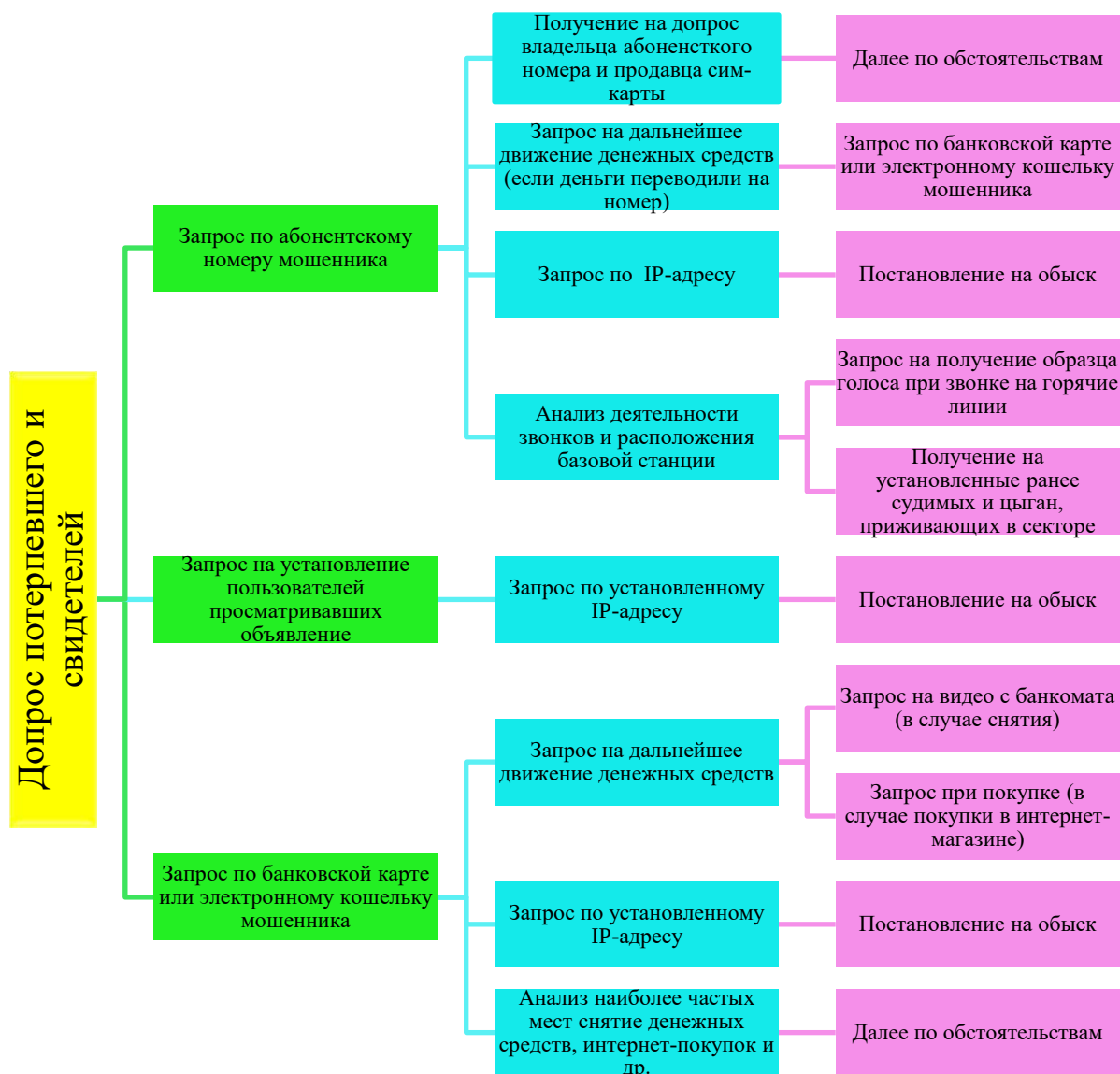


Рис. 28. Порядок действий сотрудника ОВД при раскрытии мошенничества через сайты объявлений (мошенник-покупатель)

Мошенничества через сайты объявлений. Мошенник-покупатель использует для введения в заблуждение ссылку, присланную потерпевшему

Преступник, непосредственно осуществляющий общение с потерпевшим, ищет объявление о продаже товара, создает ссылку путем движения по меню бота с возможностью создания простейшей страницы в сети с указанием номера объявления и данных о стоимости товара, а также адресе доставки, после чего в ходе переписки либо телефонного общения вводит в заблуждение потерпевшего и сообщает о том, что хочет приобрести товар. Далее направляет заранее подготовленную ссылку потерпевшему, который переходит по ней и видит данные своего товара и лейбл Ави-

то, Юла, скопированный с официального сайта, далее нажимает на кнопку «оплатить» и переходит на сервис «кард ту кард» какого-либо банка.

В некоторых случаях ссылка потерпевшему перенаправляется путем направления электронного письма на почтовый ящик, имитирующий название торговой площадки либо службы доставки. В данном случае необходимо направить запрос в службу, зарегистрировавшую электронный ящик с целью получения анкетных данных клиента, способов оплаты услуги, иных ящиках, зарегистрированных на данного клиента, IP-адресах администрирования в личном кабинете.

Не менее важной информация заключена в самой ссылке, которая состоит из доменного имени и набора цифр и букв, ведущих к адресу URL, то есть к IP-адресу хостинга, на котором находится информация. В случае, если доменное имя принадлежит российскому регистратору, необходимо направить запрос в данную организацию с целью получения информации (анкетные данные/способы оплаты, IP-адреса администрирования в личном кабинете). Полученная информация может способствовать установлению лица, создавшего Бот, который используется для совершения преступления (см. рис. 29).

Допрос потерпевшего, свидетеля		
Телефония: запрос оператору: 1. Данные клиента, с которым заключен договор о предоставлении услуг связи; 2. Детализация соединений абонентского номера на предмет установления IMEI-номера активации услуг мессенджера (в случае, если переписка велась в нем); 3. Способы оплаты абонентского номера за период активации мессенджера	Запрос в банк с целью получения информации вывода денежных средств: 1. Информация о движении денежных средств потерпевшего; 2. Информация об IP-адресе администрирования счета/карты/кошелек, на который переводились денежные средства; 3. Информация о движении денежных средств по карте/кошельку/счету	Запрос в компанию интернет-провайдера по ссылке: 1. Предварительно на сервисе Whois информация об организации регистраторе доменного имени и IP-адресе хостинга сервера, на котором расположена страница; 2. Информация об анкетных данных клиента, IP-адресах логирования и входа в личный кабинет, способов оплаты услуги, иных предоставляемых услугах клиенту

Рис. 29. Порядок действий сотрудника ОВД при раскрытии мошенничества через сайты объявлений (с подменой сайта объявлений)

Мошенничества со взломом страниц социальных сетей

Мошенник покупает в сети Интернет взлом страницы социальной сети («ВКонтакте», «Одноклассники», «ДругВокруг» и др.) или осуществляет его самостоятельно. В последующем пишет всем друзьям из списка сообщения мошеннического характера с просьбой занять денежные средства под различными предлогами: заболел родственник, не хватает на срочную покупку и т.д. (рис. 30).



Рис. 30. Порядок действий сотрудника ОВД при раскрытии мошенничества путем взлома страниц социальных сетей

Мошенничества, совершенные с использованием интернет-сайтов (интернет-магазинов)

Мошенник создает (или покупает) интернет-сайт по продаже товара различной тематики. Регистрирует несколько виртуальных номеров (8-800-..., 8-495-... и др.) у SIP-провайдера и указывает их на сайте в качестве контактов. В последующем принимает покупателей, получая от них денежные средства за покупку товара с сайта (см. рис. 31).

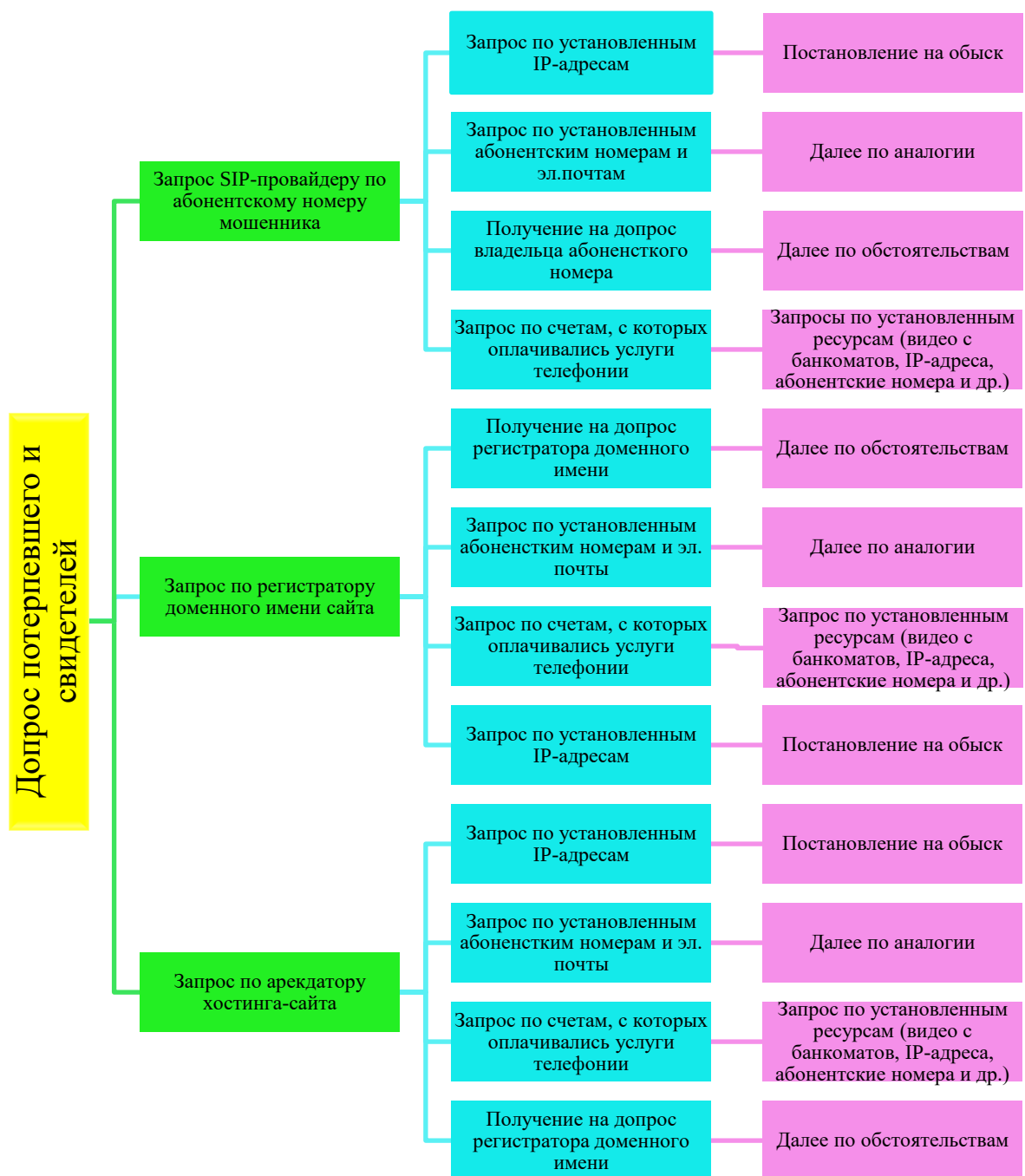


Рис. 31. Порядок действий сотрудника ОВД при раскрытии мошенничества с использованием интернет-сайтов

Мошенничество, совершенное под предлогом заказа банкета (или связь с курьером)

Мошенник звонит в организацию и говорит, что желает воспользоваться ее услугами по заказу банкета, заказу крупной партии товара или прочих услуг. Далее он сообщает адрес, где бы он хотел встретиться с представителем компании и спрашивает его телефон.

В последующем он связывается с представителем и просит последнего по пути пополнить счет абонентского номера (или банковской карты) на некоторую сумму (рис. 32).

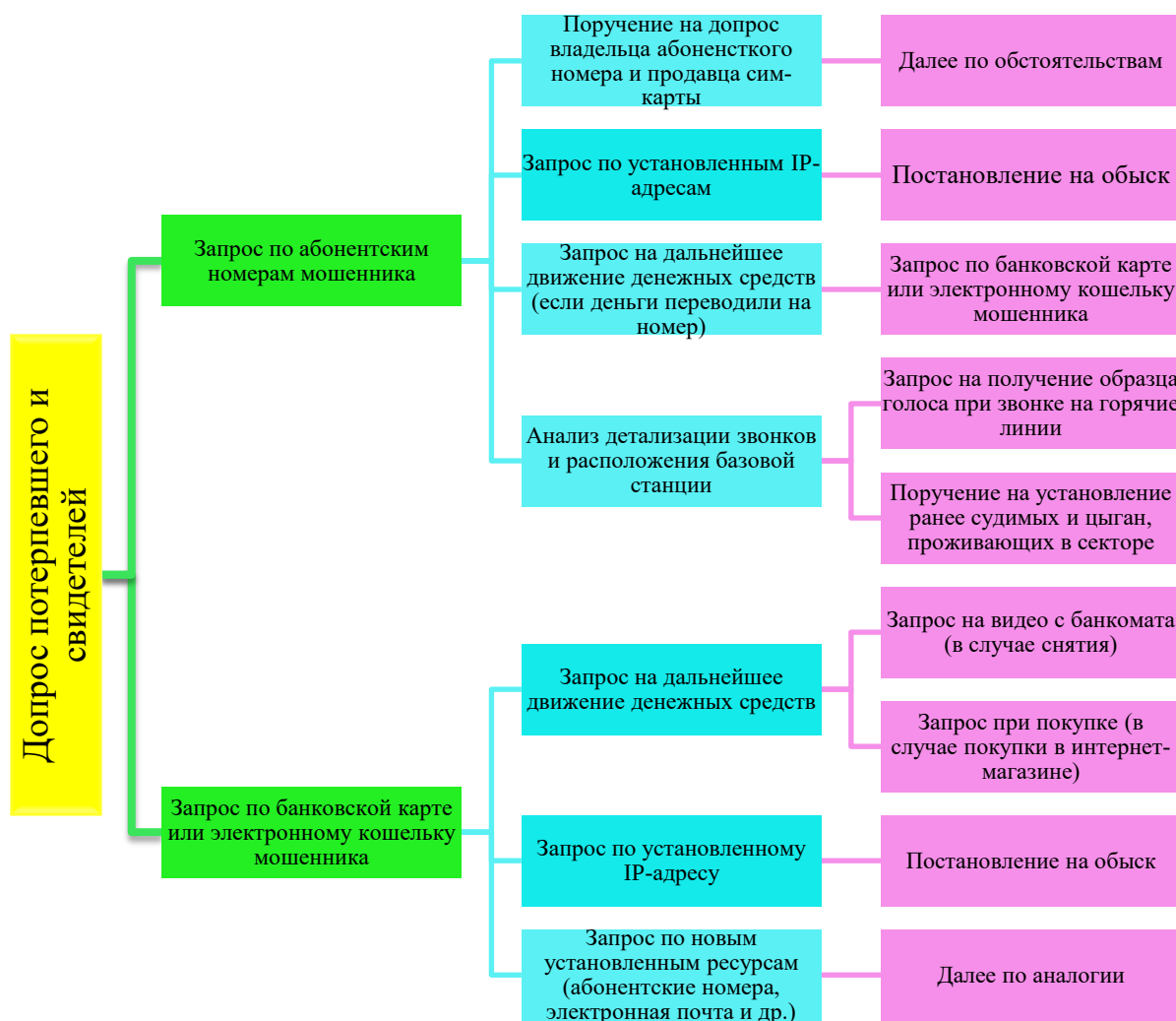


Рис. 32. Порядок действий сотрудника ОВД при раскрытии мошенничества, совершенного под предлогом заказа банкета

Мошенничество, совершенное под предлогом разблокировки банковской карты или предотвращения списания денежных средств

Мошенник осуществляет рассылку SMS-сообщений с текстом о списании денежных средств или блокировке банковской карты. В данном сообщении указывает свой другой абонентский номер (иногда

виртуальный 8-800-..., 8-495-... и др.), который может проинформировать о произошедшем. Потерпевший звонит по данному номеру, после чего мошенник либо просит сообщить контрольные данные банковской карты, либо просит подойти к банкомату (рис. 33).

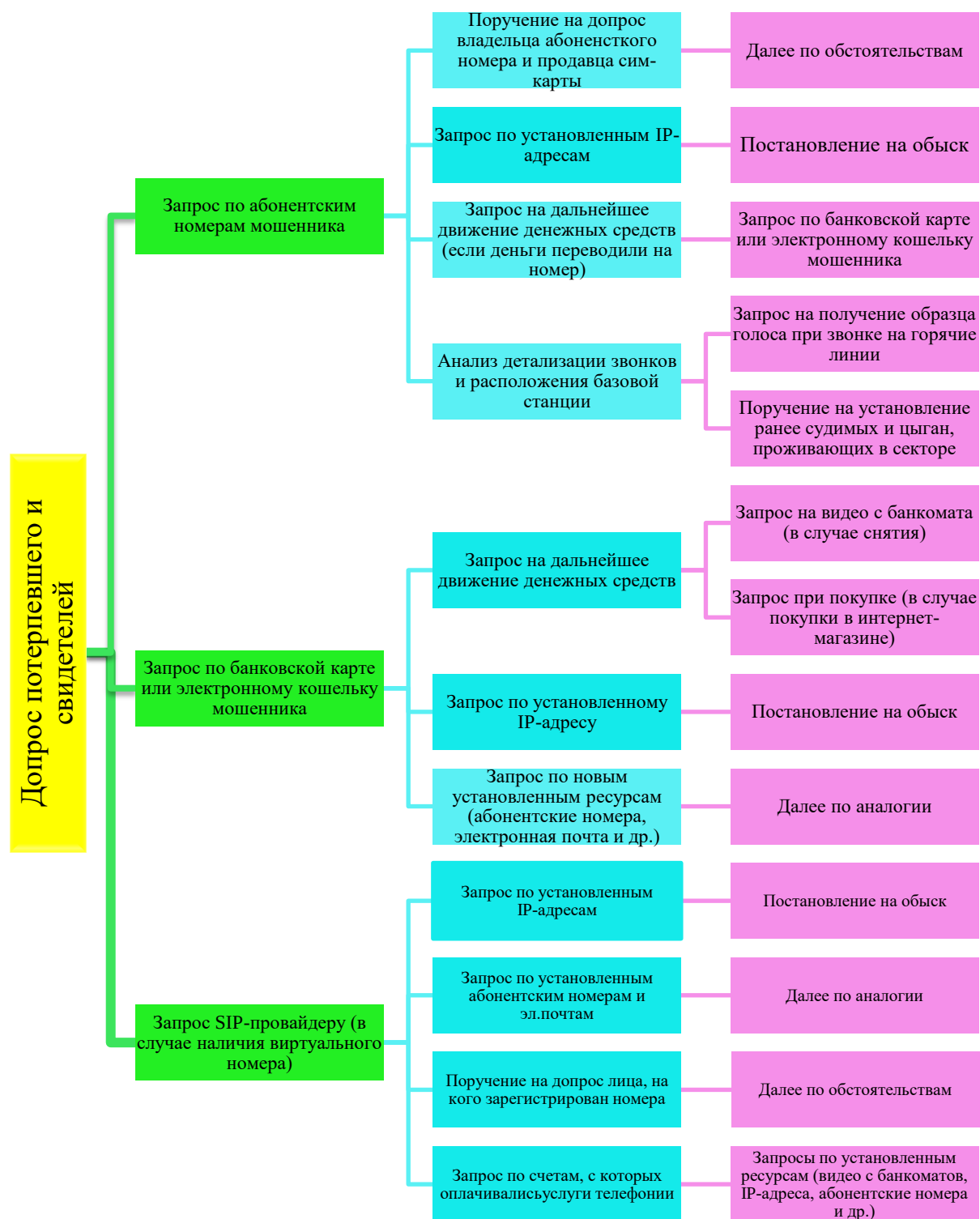


Рис. 33. Порядок действий сотрудника ОВД при раскрытии мошенничества под предлогом разблокировки банковской карты

Мошенничество, совершенное под предлогом помощи родственнику, попавшему в беду

На стационарный или абонентский номер потерпевшего звонит мошенник, который обращается под видом родственника («Привет, мама», «Привет, бабушка» и т.д.). Сообщает, что попал в ДТП и сбил человека, с кем-то подрался и т.д., а после передает трубку сотруднику полиции, который за отдельную плату предлагает «решить вопрос» об отказе в возбуждении уголовного дела (рис. 34).

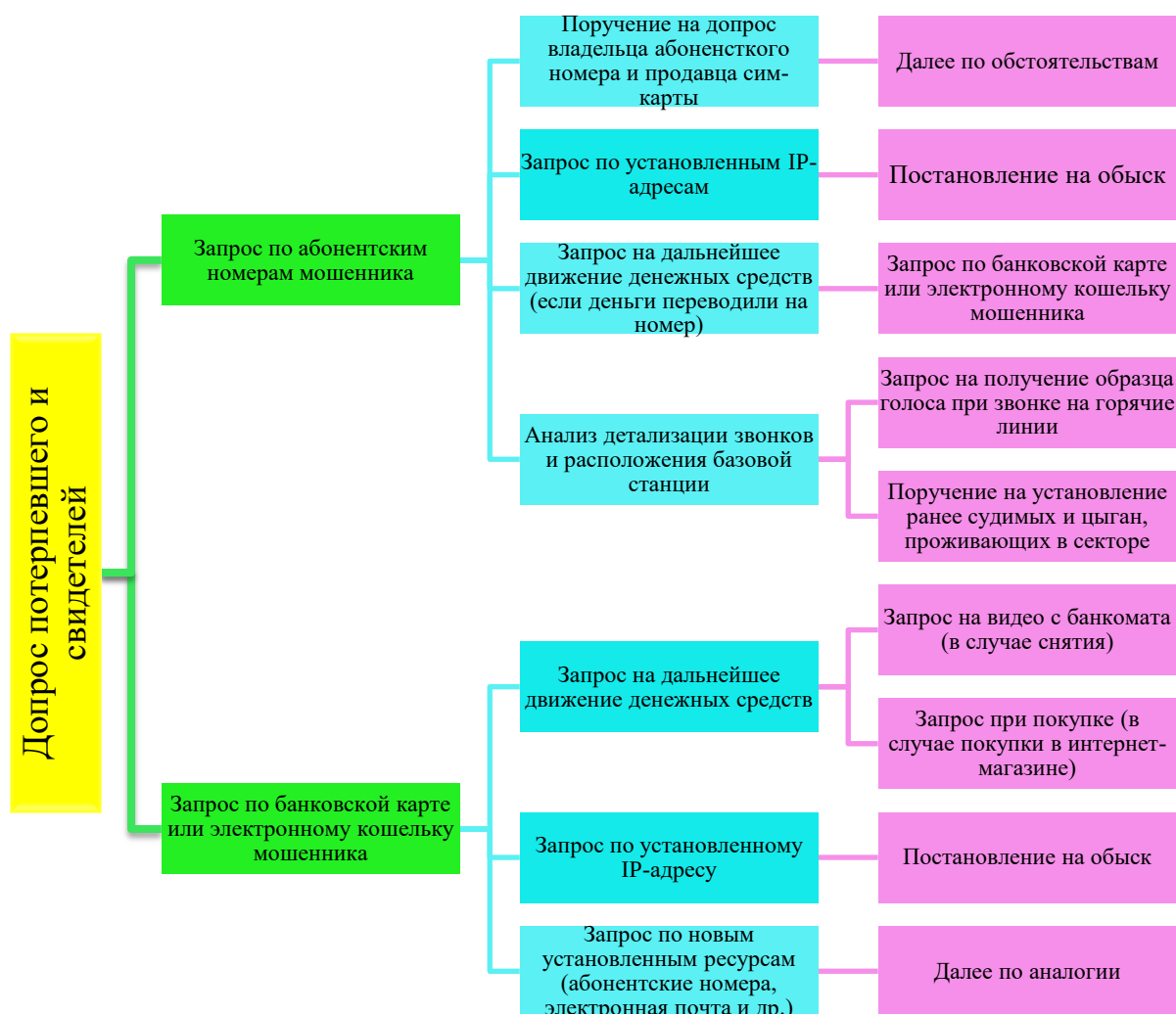


Рис. 34. Порядок действий сотрудника ОВД при раскрытии мошенничества, совершенного под предлогом помощи родственнику, попавшему в беду

Мошенничество, совершенное под предлогом компенсации за ранее приобретенные БАДы

На стационарный или абонентский номер потерпевшего звонит мошенник, который представляется сотрудником прокуратуры или правоохранительных органов. Он сообщает, что в настоящий момент задержана группа мошенников, продававших некачественные БАДы¹¹², и что потерпевшему положена компенсация. Однако для ее получения необходимо оплатить государственную пошлину или налоговый сбор (рис. 35).

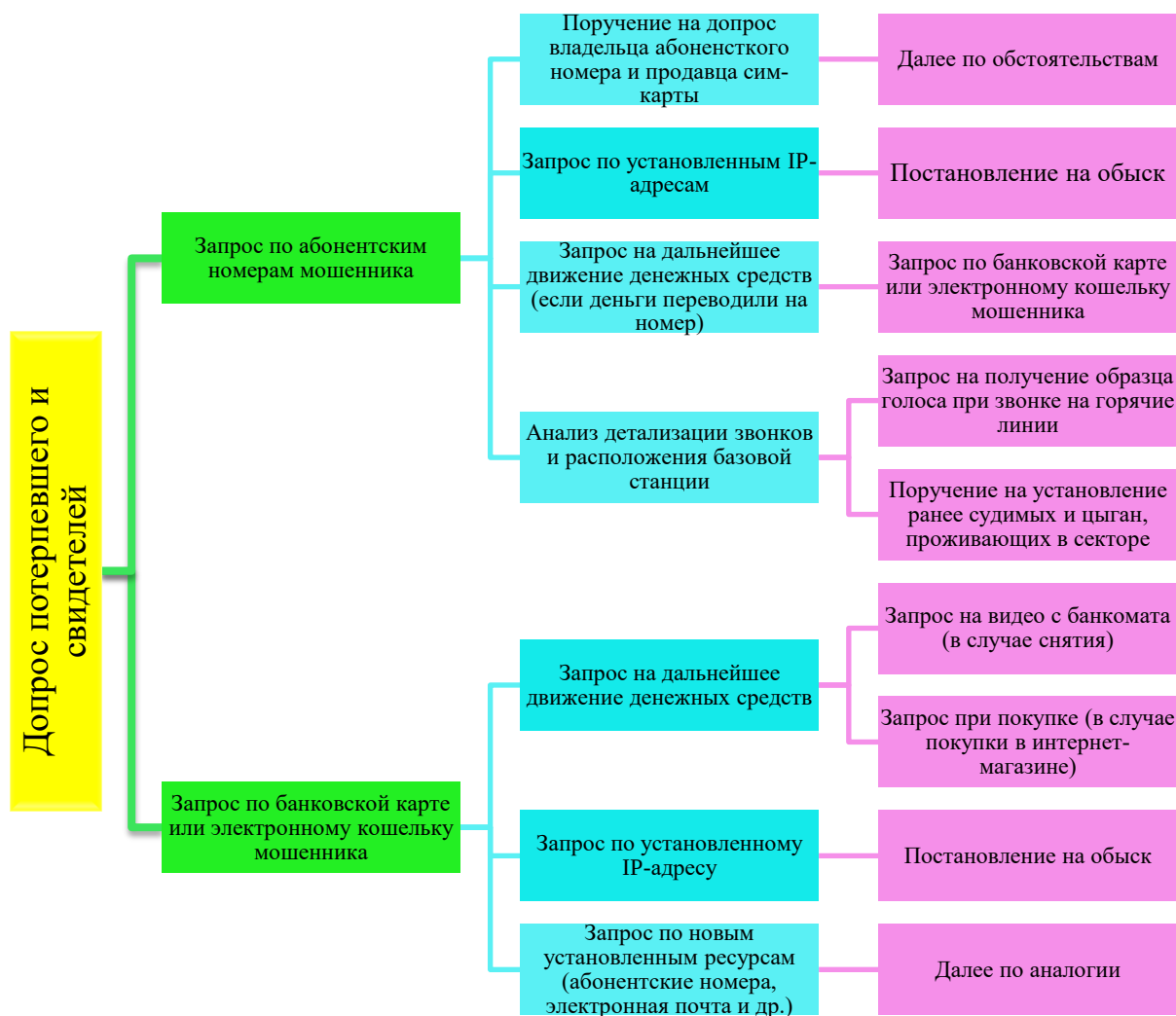


Рис. 35. Порядок действий сотрудника ОВД при раскрытии мошенничества, совершенного под предлогом компенсации за ранее приобретенные БАДы

¹¹²Биологические активные добавки и их композиции предназначены для непосредственного приема с пищей или введения в состав пищевых продуктов. БАД используется как дополнительный источник биологически активных веществ (пищевых волокон, витаминов, минеральных веществ, аминокислот) для ликвидации их дефицита в организме человека и оптимизации рационов питания. Стандартов по производству БАДов не существует, контроль их качества заключается лишь в оценке безопасности как пищевых продуктов.

Мошенничество, совершенное в современном информационном пространстве и сети Интернет с использованием вредоносных программ на ОС «Android»

Потерпевшему на сотовый телефон с операционной системой «Android» с неизвестного номера приходят SMS-сообщения с текстом: «Здравствуй, я по Вашему объявлению. Не интересует обмен с доплатой? Ссылка: www.avit.o.ru/FriZksk)» или SMS-сообщение с текстом: «Смотри, как мы здорово получились на этой фотографии. Ссылка www.bit.ly/ZreizE1eaAa)». Потерпевший проходит по данной ссылке, в результате чего загружает на свой телефон вирус (чаще всего используются вирусы под названием «Triada» и «Marcher»), предоставляющий злоумышленнику доступ к SMS-командам. В дальнейшем мошенник похищает деньги, путем направления сообщений на номер «900» (рис. 36).

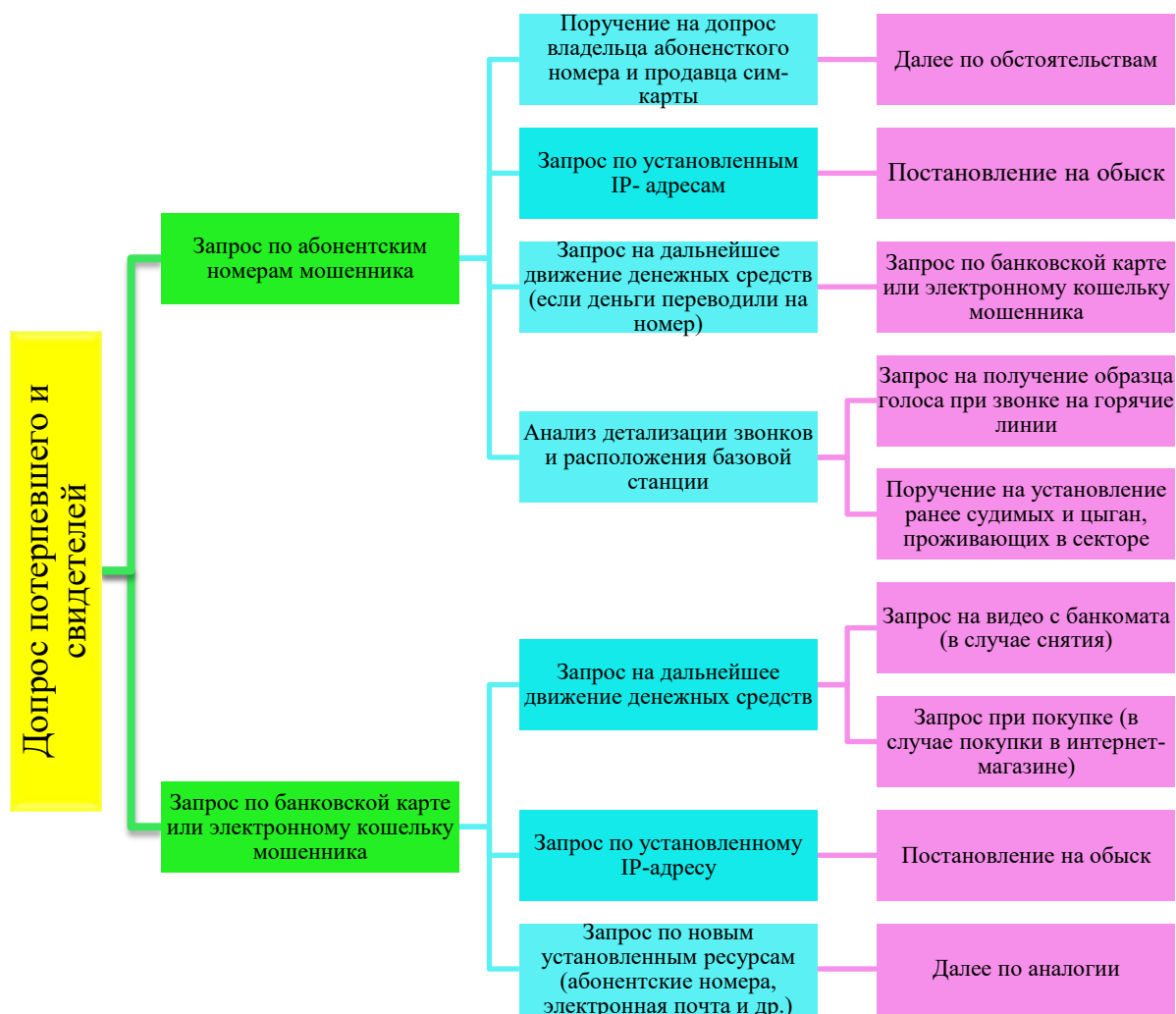


Рис. 36. Порядок действий сотрудника ОВД при раскрытии мошенничества, совершенного с использованием вредоносных программ на ОС «Android»

Мошенничество, совершенное с использованием социальных сетей (интернет-магазин «ВКонтакте»)

Мошенник создает страницу или группу в социальной сети, позиционирующую себя как интернет-магазин. В последующем принимает покупателей, получая от них денежные средства за покупку товара с сайта (см. рис. 37).

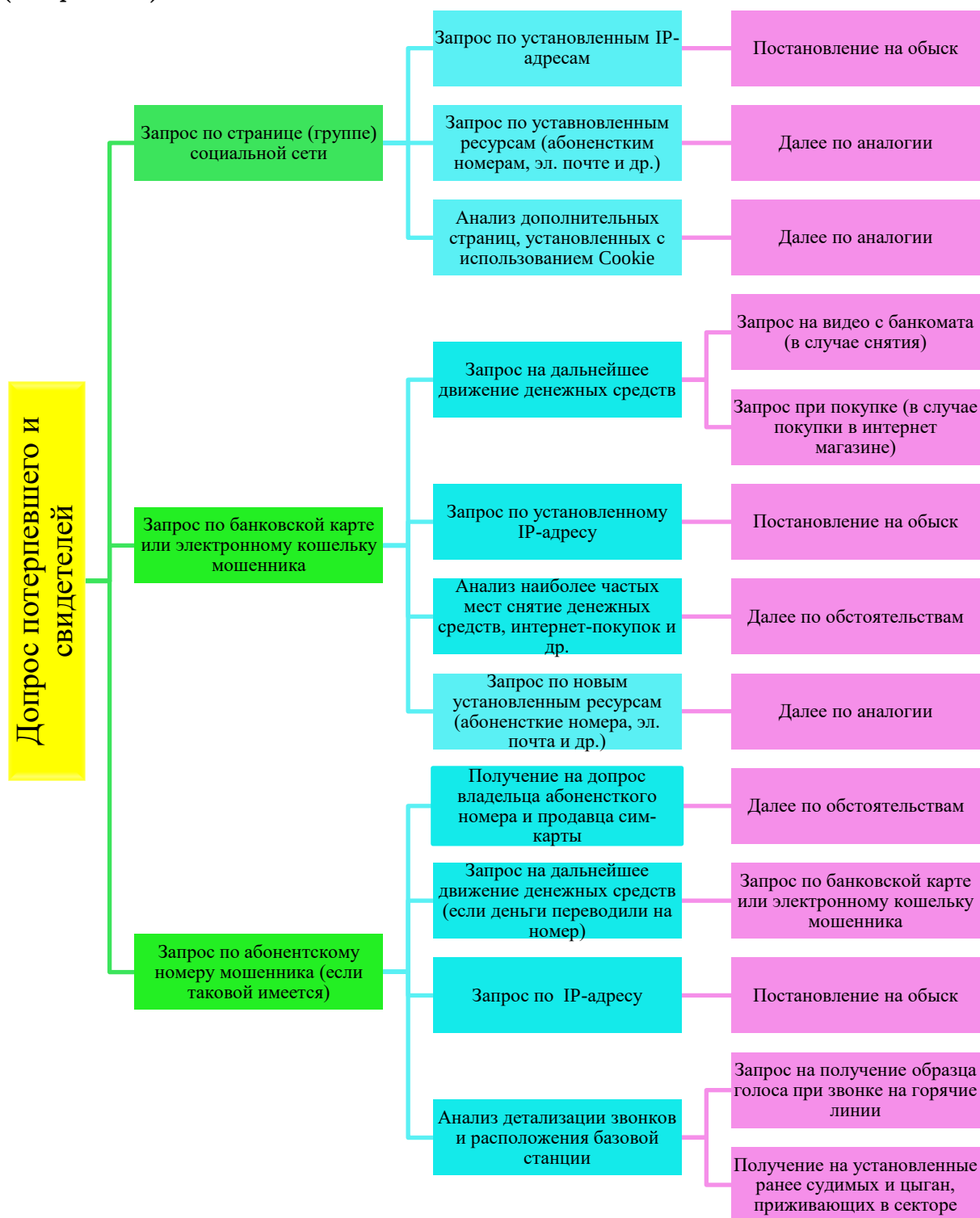


Рис. 37. Порядок действий сотрудника ОВД при раскрытии мошенничества, совершенного с использованием социальных сетей

Раскрытие преступления, совершенного от лица сотрудников банка, сообщающих о проведении сомнительных операций

Исходя из имеющегося опыта, очевидно, что звонки мошенников, осуществляются из колл-центров, находящихся в большинстве случаев на территории стран ближнего зарубежья и других, прилегающих к ним территориях. Это не значит, что установить преступников и задержать соучастников мы не можем.

Кроме информации о передвижении денежных средств со счетов потерпевших, имея знания об абонентских номерах, которые на настоящий момент могут подменить преступники, становится возможным только лишь тогда, когда заранее известно о номере, с которого они звонят. Это, скорее всего, подмененный номер либо IP-телефония, либо абонентский номер оператора сотовой связи. Кроме того, большое значение имеет способ оплаты абонентского номера преступниками. Данная информация отсутствует в соответствующих отделах подразделений специальных технических мероприятий органов внутренних дел и ее надо запрашивать либо от следственных органов в рамках уголовного дела, либо путем получения разрешения на проведение ОРМ «Наведение справок».

В настоящее время большое значение имеет информация об устройстве и IP-адресе входа в банк-онлайн потерпевшего, если такой факт имел место. Данная информация непосредственно ведет нас к лицам, осуществляющим звонки потерпевшим, то есть к «звонарям».

Таким образом, работа должна проводиться по трем направлениям: телефония, движение похищенных денежных средств, устройства (IP, абонентские номера, IMEI-мобильных устройств), с помощью которых переводили денежные средства со счета на счет (см. рис. 38).

Допрос потерпевшего				
Телефония		Вывод денежных средств		
Запрос сотовому оператору:	Запрос сотовому оператору:	Запрос в банк:	Запрос в банк:	Запрос в банк:
Абонентский номер потерпевшего; Транк номер операции; Абонентский номер звонившего	Абонентский номер преступника; Информация о лице, на чье имя зарегистрирован абонентский номер; Способы оплаты абонентского номера; IP-адреса логирования во время звонка (в случае, если звонок осуществляется с IP-телефонии)	Карта/счет/кошелек потерпевшего; Информация о дате, времени и сервисе, с помощью которого похитили денежные средства; Информация об IP-адресе входа в онлайн-банк; Информация об IP-адреса технических характеристиках устройства, с помощью которого вошли в личный кабинет	Обслуживающий сервис с целью получения информации: Информация об IP-адресе устройства, с помощью которого проводилась операция; Информация о карте/кошельке, куда были переведены средства	Карта преступника; Информация о дальнейшем движении денежных средств (адреса банкоматов снятия, время операции и адрес снятия); Информация об IP-адресе входа в онлайн-банк; Информация о технических характеристиках устройства, с помощью которого вошли в личный кабинет; Информация об абонентском номере, подключенном к карте

Рис. 38. Порядок действий сотрудника ОВД при раскрытии мошенничества, совершенного от лица сотрудников банка, сообщающих о проведении сомнительных операций

Мошенничество, совершенное с использованием разветвленной сети нелегальных узлов связи

В ходе проведения оперативно-розыскных мероприятий, направленных на раскрытие преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет, в тесном взаимодействии с сотрудниками ФСБ России была разоблачена разветвленная сеть нелегальных узлов связи, которая действовала в 13 регионах России. Тысячи иностранных номеров телефонные мошенники маскировали под российские, обзванивали пострадавших, главным образом пенсионеров, и убеждали их отдавать свои сбережения.

Телефонные мошенники отправляли сообщения на различные номера и предлагали будущим потенциальным жертвам заработать деньги. Сообщения направлялись от имени арбитражных специалистов, деятельность которых заключалась в обороте криптовалюты. Несостоявшийся криптовалютный трейдер¹¹³ был взят с поличным. В Казани, в результате проведения специальной операции столичной полицией, отследившей онлайн-переводы телефонных мошенников, была изъята банковская карта, на которой находилась часть похищенных денег в размере 1 млн. рублей. Деньги похитили у одной жительницы столичного района Марфино. Схема была классическая: сначала был осуществлен звонок, якобы из поликлиники, в процессе которого были получены все необходимые данные потерпевшего. Затем состоялся звонок уже от имени сотрудников полиции. Потом был получен доступ к мобильному банку потерпевшей женщины и переведены с ее счета 2 млн. рублей. Сообщника из г. Казани, который должен был покупать криптовалюту, использовали в темную через систему нелегальных автоматических «col-центров».

В ходе проведения оперативно-розыскных мероприятий и следственных действий в съемных квартирах было обнаружено и изъято оборудование, называемое «СИМ БОКСЫ» - мобильные АТС, в реальном времени подменяющие телефонные номера, с которых звонили мошенники из Украины на российские номера телефонов. В функции жителя из Казани входила своевременная замена сим-карт, когда приходили сведения на их замену. Задержано 26 операторов нелегальных АТС, изъято 8000 сим-карт, номера которых проходят по сотням нераскрытых преступлений, по которым возбуждены уголовные дела. Одним из потерпевших был профессор МГУ в возрасте 79 лет Александр Демидов, который пояснил, что ему начали звонить от имени сотрудников ФСБ России и в состоявшихся беседах известили профессора, что с его счетов перечислялись террористу денежные суммы в размере 300 тыс. рублей. Профессору мошенники предложили снять все имеющиеся на его

¹¹³ Трейдер – торговец, человек, который занимается покупкой и продажей финансовых активов (акций, валют, облигаций, криптовалют, деривативов и т.д.) с целью получения прибыли. Основная деятельность трейдера заключается в спекуляции на финансовых рынках, т.е. в покупке активов по низкой цене и их последующей продаже по более высокой или наоборот – продажа по высокой цене с последующей покупкой по более низкой цене. Трейдеры могут работать сами на себя или обслуживать клиентов, например, в банках. Профессиональные трейдеры обязательно имеют лицензию, которая позволяет заключать им сделки напрямую через биржу.

счетах денежные средства и передать на проверку. Мужчина отдал водителю такси 460 тыс. рублей. При реализации плана спецоперации по задержанию мошенников все члены, входившие в организованную преступную группу, были задержаны (рис. 39).

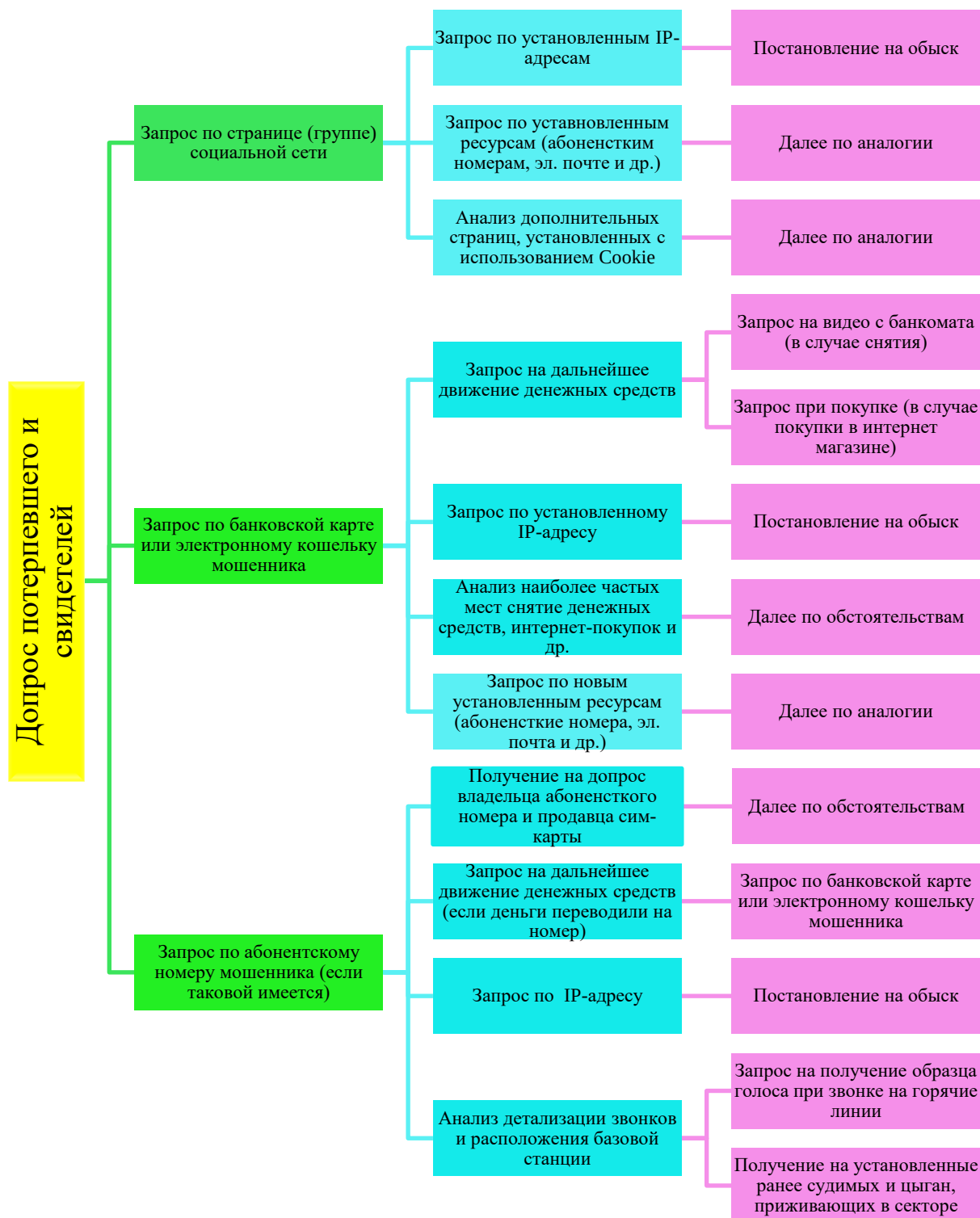


Рис. 39. Порядок действий сотрудника ОВД при раскрытии мошенничества, совершенного в современном информационном пространстве с использованием разветвленной сети нелегальных узлов связи

Мошенничество, совершенное в современном информационном пространстве с использованием различных мессенджеров

Предлагаем рассмотреть пример, именуемый «Поздравление с открыткой». Эксперты по кибербезопасности предупреждают о новом виде мошенничества. Изображения, например, в виде милого котика и других различных видов животных, автомашин и т.п. на деле могут оказаться «троянским конем», в котором вшиты, так называемые фишинговые ссылки. Одно нажатие, и все данные банковской карты, госуслуг могут оказаться в руках мошенников. При этом они могут действовать от лица родственников, близких людей, друзей, знакомых. Не стоит также открывать архивы: под их видом злоумышленники рассылают вредоносное программное обеспечение. Необходимо быть осторожным и предупредить близких!¹¹⁴ (см. рис. 40).

¹¹⁴ Новостная лента ТВ «Россия 1» от 27 сентября 2024 г.

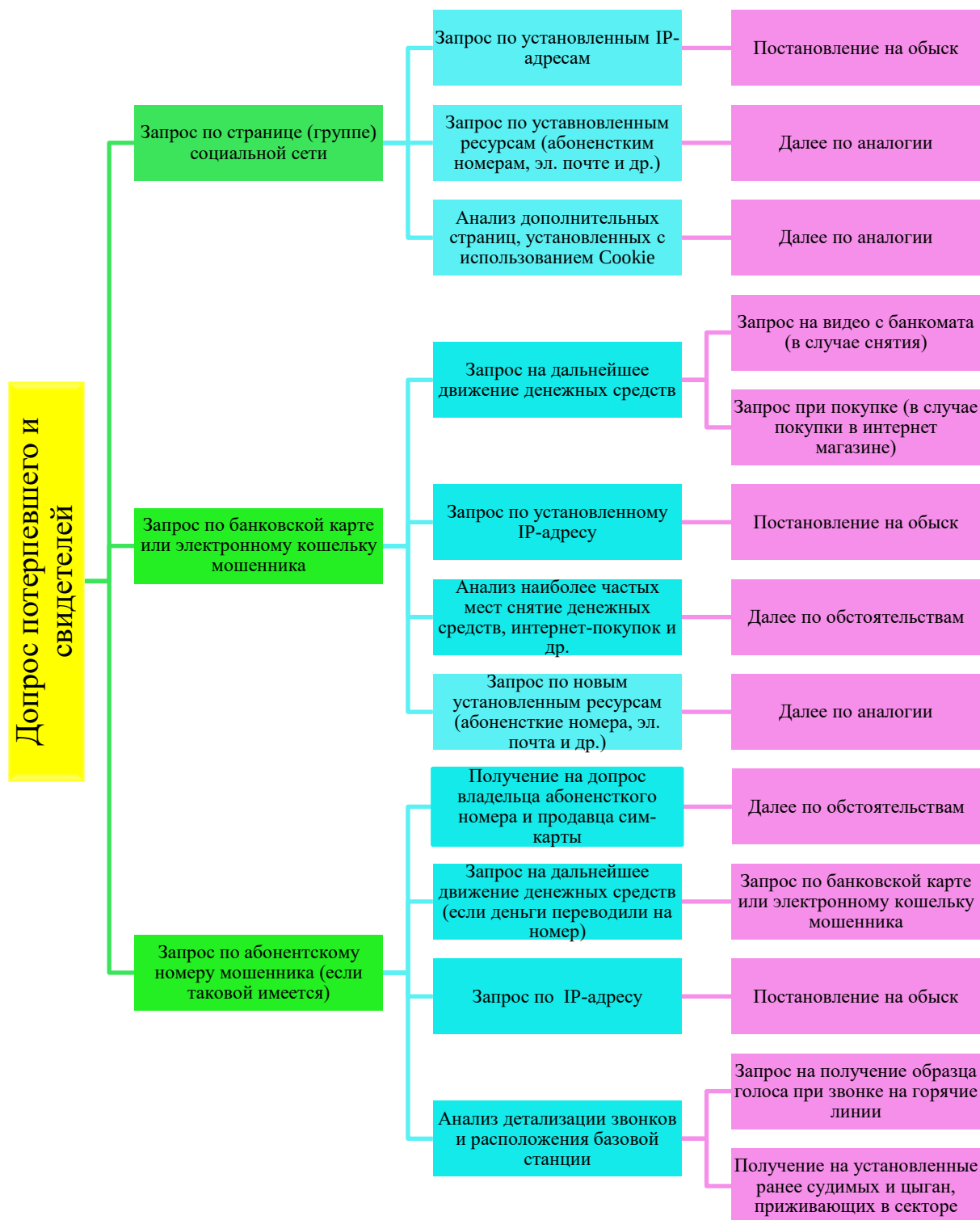


Рис. 40. Порядок действий сотрудника ОВД при раскрытии мошенничества, совершенного в современно информационном пространстве в сети Интернет с использованием различных мессенджеров

Мошенничество, совершенное в современном информационном пространстве в сети Интернет с использованием искусственного интеллекта

На Алтае зарегистрирован первый в истории случай мошенничества с помощью искусственного интеллекта. Злоумышленники, подделав голос и видео жительницы города Барнаула, смогли украсть деньги ее знакомых, используя фразу: «Мне просто оплату сейчас сделать нужно, а у меня карта на сутки заблокирована, если что, я завтра к обеду смогу вернуть».

Такие сообщения получили десятки контактов жителей Барнаула от имени Марины Василенко. Это ее голос. Хотя девушка ничего не отправляла. Пять человек откликнулись на просьбу. На неизвестную карту жители отправили более 100 тыс. рублей. По словам Марины Василенко, первой позвонила ее подруга и сообщила: «Я тебе отправила деньги. Ты получила их?» Марина поняла, что мошенники взломали ее телеграмм-аккаунт. Мошенники, используя видео и голосовые сообщения Марины Василенко, оставленные ранее в различных мессенджерах, с помощью искусственного интеллекта создали новые, с нужным им текстом. Давние друзья и родственники ничего не заподозрили, ведь слышали знакомый голос, так еще и получили видео-сообщения от девушки. Марина написала заявление в полицию. В Алтайском крае зарегистрирован первый в истории случай мошенничества с использованием нейросетей. Ученые говорят: «Раньше, чтобы подделать голос и создать дипфейк, то есть портрет человека с чужим лицом, потребовалось бы несколько дней, сегодня это займет не больше минуты, причем распознать человека и лжесообщение практически невозможно. Все упирается только в два параметра. Если у злоумышленника есть время и деньги, можно сделать любой дипфейк, который пройдет почти любые проверки. Недолгий поиск нейросети в Интернете, обычная фотография, которую можно скачать из социальных сетей человека и пару минут ожидания».

Сейчас на подходе, как минимум, три нейросети, которые умеют генерировать видео просто по описанию. Им вообще не нужно ничего реального. В этих случаях необходимо перезвонить абоненту, от имени которого ведется разговор, а если возможности позвонить нет, то в этом случае необходимо в сообщении задать личный вопрос, ответ на который знает потерпевший и тот, кто обращается с просьбой о заёме денежных средств. Поможет только звонок человеку, от имени которого просят занять денежную сумму. Далее необходимо проверить видео-сообщение на предмет монотонной речи собеседника, неестественной мимики. Нужно быть бдительным при получении обычных текстовых сообщений.

Эти схемы давно уже всем известны, но, к сожалению, в современном информационном пространстве хорошо работают. В 2024 году жители Алтайского края действиями мошенников в сфере информационно-коммуникационных технологий от такого вида мошенничества потеряли свыше миллиарда рублей¹¹⁵ (см. рис. 41).

¹¹⁵ Новостная лента ТВ «Россия 1» от 30 сентября 2024 г.

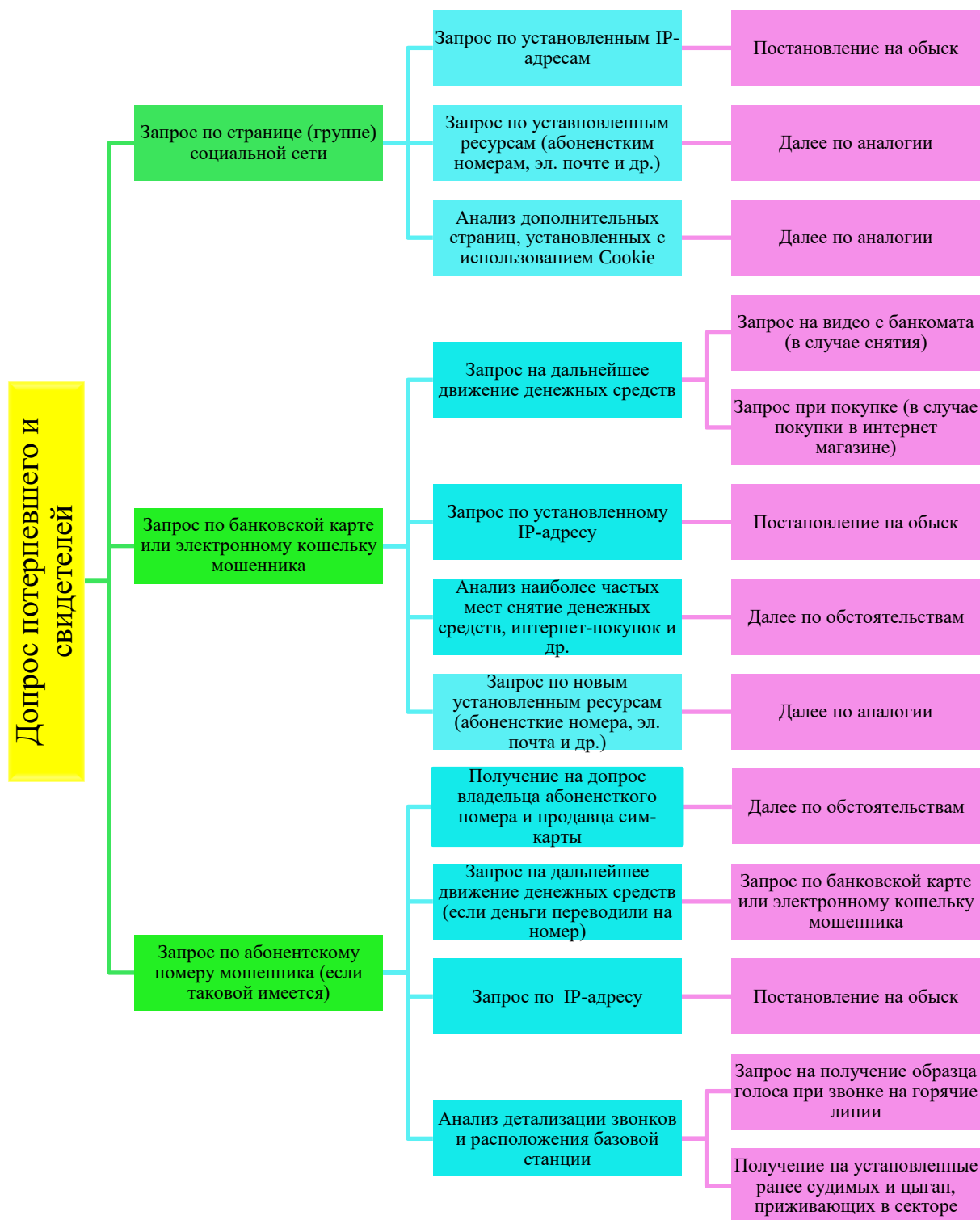


Рис. 41. Порядок действий сотрудника ОВД при раскрытии мошенничества, совершенного в современном информационном пространстве с использованием искусственного интеллекта

Мошенничество, совершенное в современном информационном пространстве в сети Интернет с использованием QR-кода

В настоящее время преступники стали использовать новый вид такого мошенничества, как сканирование QR-кода. При этом законопослушные граждане, используя современные виды платежей в торговых сетях и др. общественных местах, в целях экономии времени часто осуществляют взаиморасчёт с использованием предоставляемого отсканированного QR-кода.

Покупатели и другие граждане не подозревают, что данный вид платежа может предоставить доступ к их личным данным. В предоставленный QR-код мошенники заранее внедряют вредоносную программу, при помощи которой злодеи получают доступ к управлению не только денежными средствами пользователя, но и другой, принадлежащей ему, личной цифровой информацией.

За доли секунды телефон может загрузить вредоносную программу, предоставляя злодею доступ к личным данным, сообщениям, контактам, к микрофону, камере и даже местоположению. QR-код – быстрый отклик, по сути, это тип привычного нам штрих-кода, но он может содержать гораздо большую информацию по сравнению с предыдущей версией. При сканировании QR-кода он быстро расшифровывает информацию. Телефон на автомате выполняет любое действие, закодированное в шаблоне, например, открыть сайт, загрузить приложение и отправить платеж. Это хитрый способ обойти защиту телефона (мобильного устройства), так как пользователь добровольно отсканировал код и открыл мошеннику «дверь». Пагубность заключается в том, что пользователь не будет подозревать, что в его мобильное устройство заложена вредоносная программа.

При сканировании QR-кода может возникнуть и следующая ситуация. В нашей повседневной жизни мы часто прибегаем к фотографии и хотим запечатлеть важные события, однако при фотографировании мы можем случайно захватить вредоносный QR-код, размещенный мошенником заранее на том или ином стенде, стене, фотообоях и т.д.

В связи с этим, чтобы не попасться на уловку злоумышленников, необходимо правильно оценить возникшую жизненную ситуацию и лучше всего не использовать QR-код (см. рис. 42).

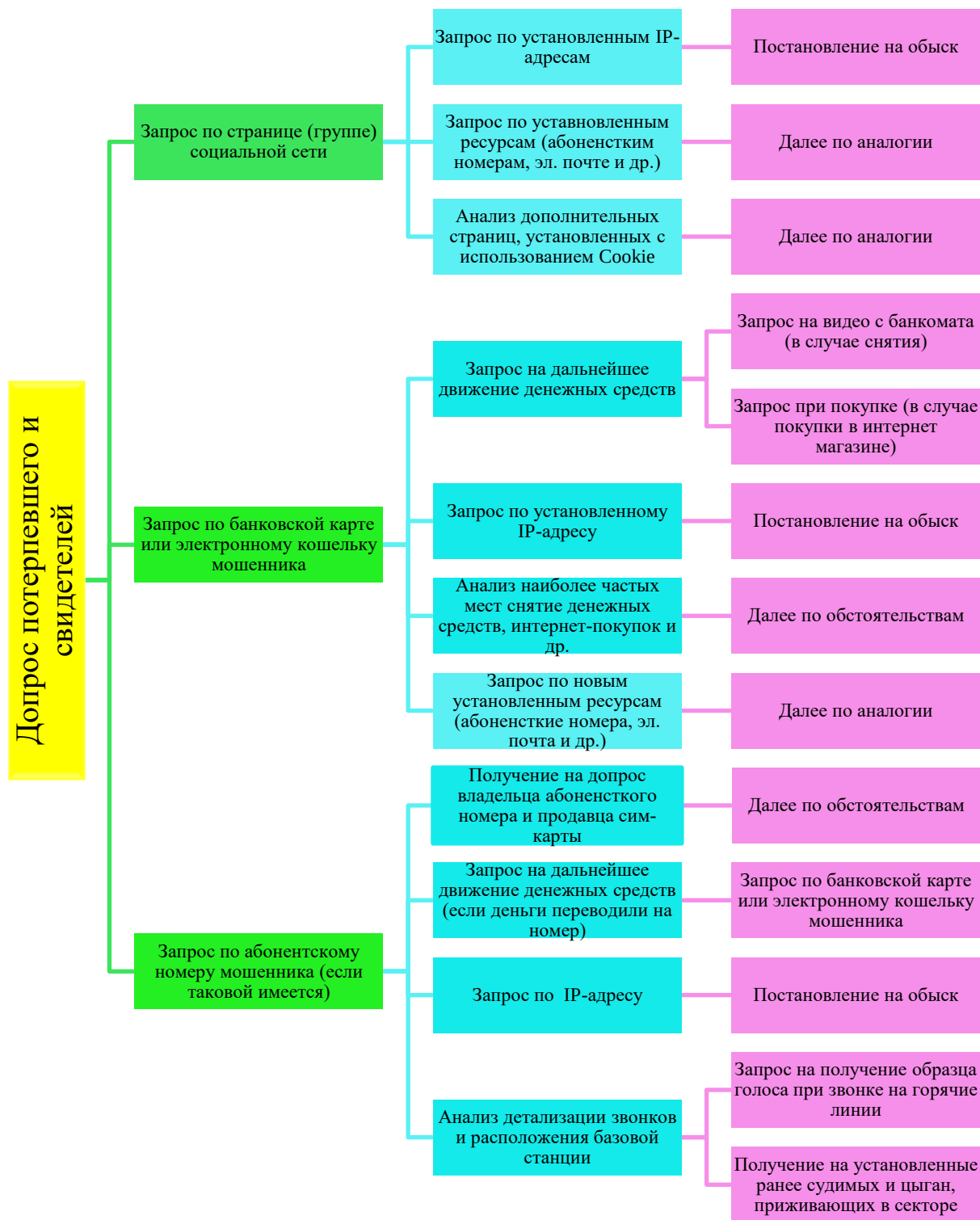


Рис. 42. Порядок действий сотрудника ОВД при раскрытии мошенничества, совершенного в современном информационном пространстве в сети Интернет с использованием QR-кода

Раскрытие преступления, связанного с получением крупной взятки в криптовалюте с использованием современного информационного пространства в сети Интернет

Балашихинский городской суд вынес приговор по делу о получении следователем крупной взятки в криптовалюте. На скамье подсудимых оказался бывший руководитель следственного отдела СКР по Тверскому району г. Москвы Марат Тамбиев. Его обвиняли в получении крупнейшей в истории России взятки больше 7 млрд. рублей. Несколько лет назад в производстве бывшей подчиненной Тамбиева М. следователя Кристины Лиховенко находилось уголовное дело в отношении группировки хакеров.

Преступники организовали в Даркнете, по сути, маркетплейс по торговле личными данными. Организованная преступная группа располагала большими денежными средствами. Узнав об этом, Тамбиев М., по версии обвинения, вступил в преступный сговор с членами организованной преступной группы и стал с ними вести торги. Предложил киберферистам меру пресечения в виде «домашнего ареста» вместо нахождения в СИЗО. За данную услугу злоумышленники щедро отблагодарили Тамбиева М., а именно: передали Тамбиеву М. пароли от криптокошельков, на которых и хранились миллиарды. С целью недопущения разоблачения должностного преступления в получении взятки бывший следователь Тамбиев М. хранил данную информацию в ноутбук в папке под названием «Пенсия».

После совершения сделки между начальником следственного отдела и членами организованной преступной группы хакеры сообщили о совершенном должностном преступлении Тамбиевым М. сотрудникам ФСБ России. В результате полученной оперативно значимой информации в отношении Тамбиева М. были проведены оперативно-розыскные мероприятия. В процессе наблюдения за Тамбиевым М. выяснилось, что он часто посещал «Кальянную» в центре г. Москвы. В процессе документирования его преступной деятельности было установлено получение взятки в особо крупном размере в виде криптовалюты. Тамбиева М. задержали с поличным, в момент получения очередной взятки от адвоката хакеров. В процессе документирования преступной деятельности Тамбиева М. было установлено, что он действовал не один, а с подчиненной, следователем Лиховенко К., с которой Тамбиев М. успел поделиться своим миллиардным состоянием.

Следователи сумели доказать, как минимум, десять эпизодов получения взяток. Нажитое преступным путем, а именно: приобретенные квартиры, машины, мотоцикл – конфискованы в доход государства по решению суда. Во время расследования уголовного дела миллиарды биткоинов, находившихся в Интернет-пространстве, официально обратили в доход государства.

«Фемида» приговорила бывшего следователя Лиховенко К. к девяти годам лишения свободы, а начальник следственного отдела СКР по Тверскому району г. Москвы Тамбиев М. осужден к 16 годам лишения свободы с отбыванием срока наказания в колонии строго режима, с назначением штрафа в 500 млн. рублей и обязанностью вернуть государству 7 млрд. рублей (см. рис. 43).

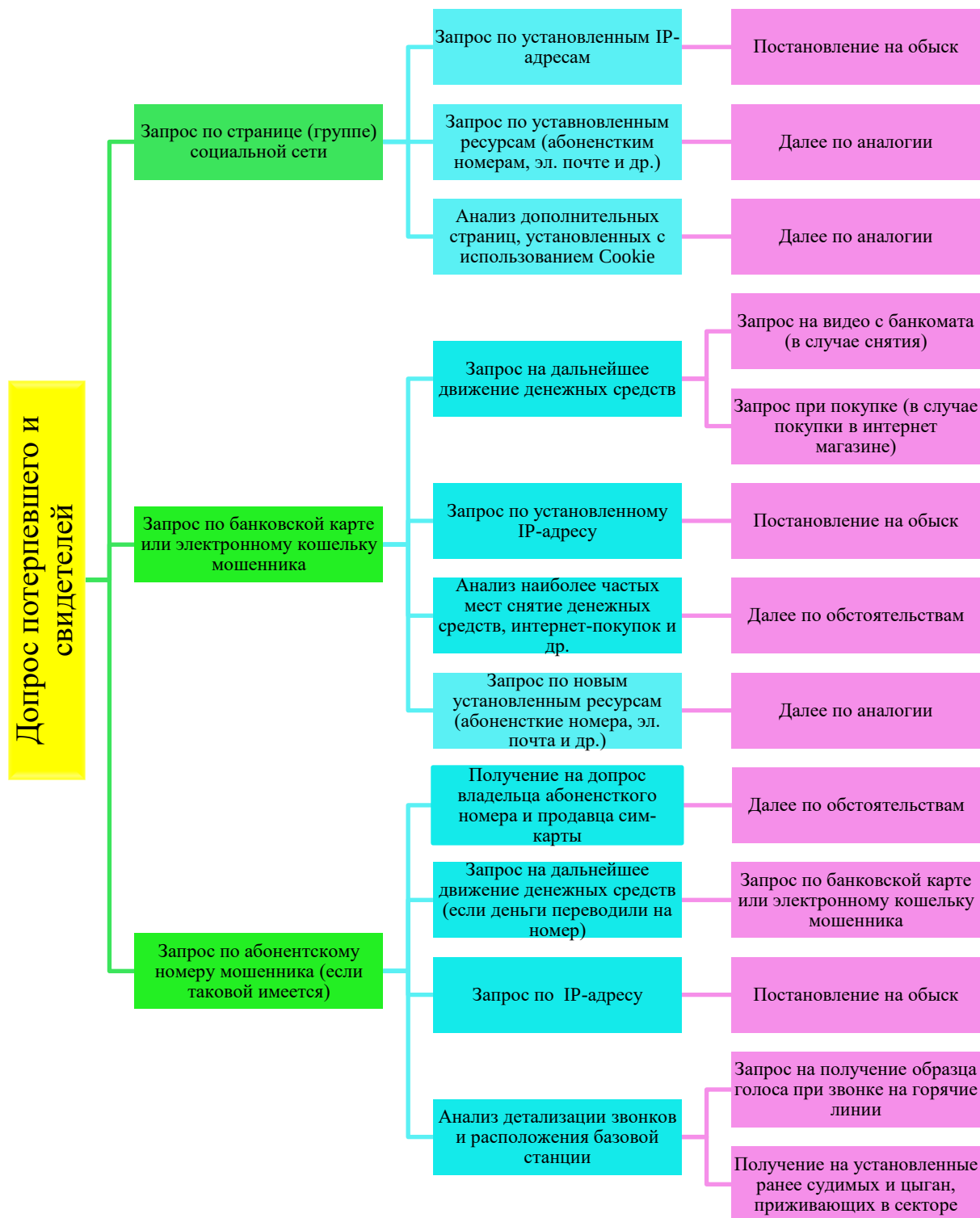


Рис. 43. Порядок действий сотрудника ОВД при раскрытии преступлений, связанных с криптовалютой, в современном информационном пространстве с использованием сети Интернет

Раскрытие преступления в сфере медицины, совершенного в современном информационном пространстве с использованием сети Интернет организованной преступной группой

В Москве обезвредили организованную преступную группу, которая совершала мошеннические действия с целью оказания медицинской помощи. В результате полученной оперативно значимой информации о данных преступных деяниях был намечен план оперативно-розыскных мероприятий, проводимых в тесном взаимодействии сотрудников ФСБ России и МВД России. В процессе документирования преступной деятельности была установлена роль каждого участника, а результаты собранного материала послужили основой для задержания подозреваемых.

Как выяснилось, аферисты пользовались лицензией на оказание частной медицинской помощи на дому, а свои услуги они рекламировали в современном информационном пространстве с использованием сети Интернет. На улице Смирновской они незаконно открыли псевдополиклинику и реабилитационный центр, куда отправляли пациентов, страдающих алкогольной и наркотической зависимостью. После госпитализации пациентов в лжемедицинское учреждение их родственникам сообщали, что больные находятся в крайне тяжелом состоянии, и им необходимо срочное дорогостоящее лечение. Поверив мошенникам, граждане переводили денежные средства на банковские счета, указанные мошенниками. По предварительным подсчетам, общий ущерб превышал миллионы рублей. По данным фактам было возбуждено восемь уголовных дел по статье «Мошенничество». В результате отлаженного взаимодействия ФСБ России и МВД России все члены организованной преступной группы были задержаны: пятеро подозреваемых арестованы, а один находится под подпиской о невыезде (см. рис. 44).

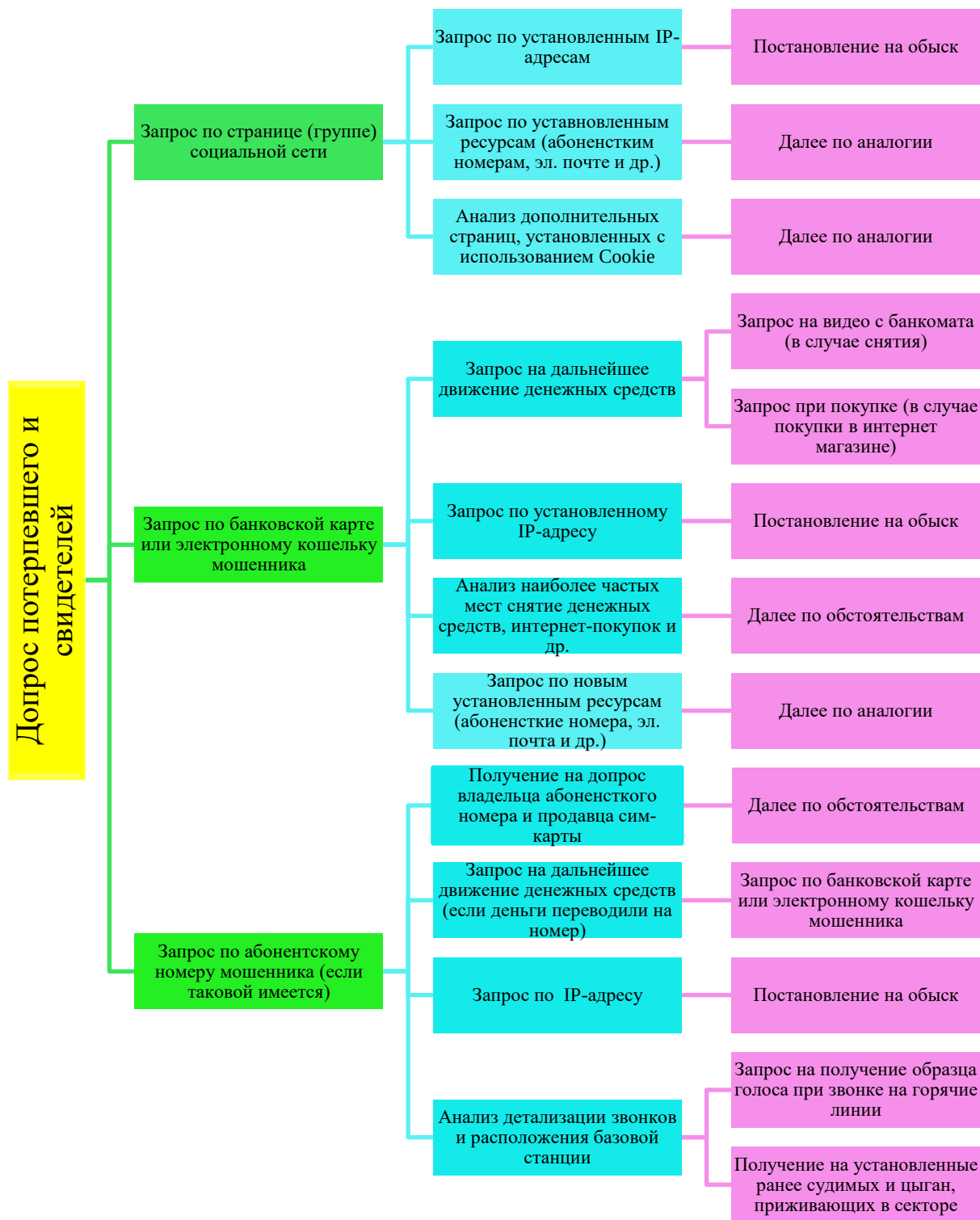


Рис. 44. Порядок действий сотрудника ОВД при раскрытии преступлений в современном информационном пространстве с использованием сети Интернет, связанных со сферой медицины

Предотвращение попыток совершения актов терроризма, подготовленных украинскими спецслужбами в современном информационном пространстве с использованием сети Интернет

С начала проведения специальной военной операции сотрудники СБУ активно используют возможности современного информационного пространства, и через социальные сети они ведут поиск лиц, враждебно настроенных и не согласных с политикой, проводимой руководством Российской Федерации. Сотрудники спецслужб Украины, устанавливая таких граждан, через социальные сети ведут с ними психологическую обработку, направленную на последующее осуществление вербовочных манипуляций с целью дальнейшего их использования для проведения преступлений экстремистской направленности и террористического характера.

Так, в Ярославской области сотрудниками ФСБ России предотвращен террористический акт, планируемый на одном из оборонных предприятий. Задержан гражданин России, которого ранее завербовали через социальные сети, а именно через мессенджер «Телеграмм». Он получил от заказчиков предполагаемого преступления мешок с токсичным веществом. Данный гражданин должен был отравить сотрудников военного завода. При желании осуществить террористический акт способом отравления преступник был задержан с поличным. Его преступные действия выражались в следующем: он должен был забрать мешок с ядовитым веществом из тайника. На допросе он дал показания о том, что в **социальных сетях** выражал свое недовольство проведением СВО. В связи с чем, в декабре 2024 года в сети «Телеграмм» на него вышел представитель Украины под ником «великий воин корпуса», задержанному за денежное вознаграждение было предложено совершить террористический акт.

Мужчина, по указанию своих украинских кураторов, должен был залить в воздуховоды машин, принадлежащих работникам оборонного предприятия Ярославской области, ядовитую жидкость. Сначала им была проведена рекогносцировка местности, автопарковки, и сведения об этом он отправил своему куратору, за что получил 10 тыс. рублей. Далее ему подготовили и прислали мешок с ядовитым веществом, указав координаты тайника через социальные сети. После задержания данного гражданина изъятый мешок с ядовитым веществом был отправлен на соответствующее исследование.

В результате проведенного исследования изъятого вещества установлено, что попадание паров данного яда в верхние дыхательные пути человека может произвести острый ожог слизистой, с возможным

развитием асфиксии с летальным исходом. При попадании на кожу могут возникать острые ожоги, язвы или рубцы.

Предлагаем рассмотреть очередной эпизод украинского государственного терроризма с применением яда на территории Краснодарского края.

В Ростове-на-Дону суд рассмотрел уголовное дело в отношении уроженца Мелитополя Егора Семенова, который свою вину полностью признал. На видеозаписи отчетливо видно, как он покупает напитки, в которые позже нальет отраву. К спиртному прилагался еще и торт. Е. Семенов сам доставил отравленные напитки и торт в ресторан, где летчики отмечали 20-летие выпуска из Армавирского высшего военного авиационного училища, якобы от сослуживца, который не смог приехать. Собравшиеся на праздник успели только разрезать торт, дальше сработала интуиция, и все, что привез странный курьер, отдали на экспертизу. За массовые убийства российских офицеров киевские наниматели пообещали Е. Семенову 400 тыс. рублей, но денег он так и не получил.

Следующий пример подготовки террористического акта в современном информационном пространстве с использованием сети Интернет. В Санкт-Петербурге завербованные главным управлением разведки Украины граждане планировали отправить на фронт посылку с отравленными крупами, кашами, зерном, мукой, сахаром, растворимым кофе. После добавления яда преступники искусно запечатывали упаковки в подпольной лаборатории. Оказавшись в зоне СВО, все это наверняка попало бы не только на столы военнослужащих, но и мирного населения. У организаторов преступлений была одна цель – уничтожить как можно больше населения Российского государства. Сотрудниками ФСБ России своевременно была получена оперативно значимая информация, которая в результате отработки способствовала предотвращению террористических актов. В процессе проведения оперативно-розыскных мероприятий был установлен гараж, в котором располагалась подпольная лаборатория, где осуществлялась преступная деятельность, выраженная в производстве ядохимикатов для последующего их использования в совершении террористических актов на территории Российской Федерации. В данном гараже при производстве обыска было обнаружено более 20 кг. ядовитого вещества.

Из вышесказанного можно сделать вывод о том, что в тесном взаимодействии спецслужб Украины и стран Североатлантического альянса избрана тактика «неизбирательных убийств множества случайных людей» способом использования отравляющих веществ, производство

которых ведется в западных странах. Достаточно вспомнить, как сотрудниками ФСБ России в феврале 2024 года предотвращен террористический акт в Запорожье при изъятии у граждан Украины препаратов, разработанных в США, которые применяют для создания химического оружия. С точки зрения спецслужб Украины, это абсолютно «нормальные» методы борьбы с врагом. За время проведения специальной военной операции сотрудники СБУ поняли, что, с точки зрения террора, руки у них развязаны, и соответственно в этом случае метод совершения убийства для сотрудников спецслужб западных стран не играет никакой роли. Конечно, сотрудники СБУ и других стран Североатлантического альянса потенциального убийцу тщательно подвергают психологической обработки, практически его зомбируют и превращают в послушного «робота», действующего по команде и выполняющего любое поручение без раздумывания. Украинские спецслужбы занимаются подбором граждан - будущих жертв, которые имеют ненавистнические взгляды по отношению к России, а где-то заинтересовывают людей и на материальных проблемах, но чаще всего и на том, и другом сразу. Финал между тем для всех завербованных граждан спецслужбами СБУ и стран западного альянса один: после выполнения части задуманного преступного задания или совершения преступления исполнителей просто ликвидируют. Необходимо отметить, что только по ст. 205 УК РФ «Террористический акт» преступнику грозит лишение свободы до 20 лет, а если рассматривать ситуацию, как в случае с армавирским отравителем, и в обвинении будет фигурировать госизмена, то и вовсе грозит пожизненное заключение (см. рис. 45).

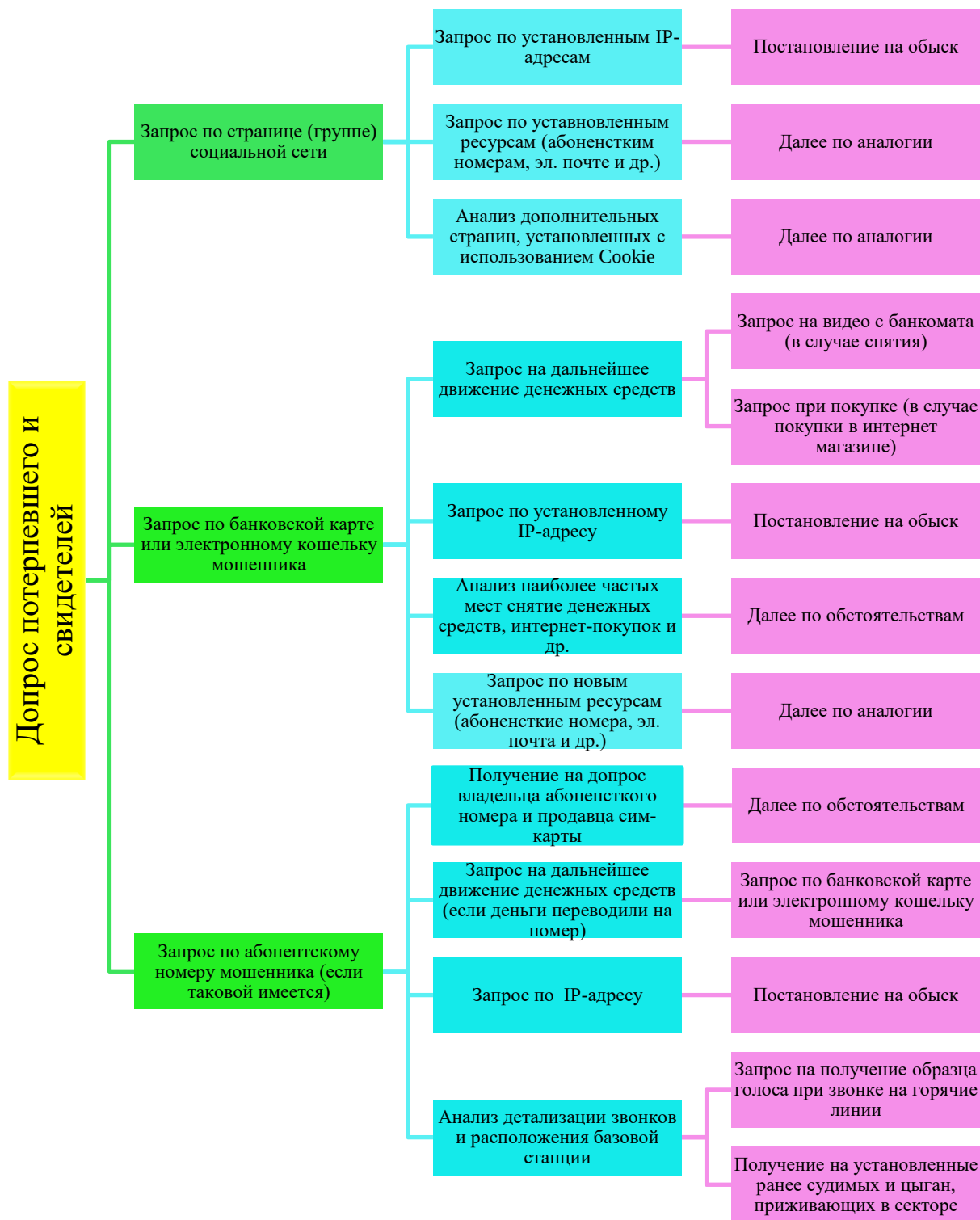


Рис. 45. Порядок действий сотрудника ОВД при предотвращении попыток совершения актов терроризма, подготовленных украинскими спецслужбами в современном информационном пространстве с использованием сети Интернет

Раскрытие преступлений, совершенных кибермошенниками в современном информационном пространстве с использованием сети Интернет и новых методов обмана

Раскрывая тему данного вопроса, авторы научно-практического пособия проанализировали ситуации, складывающиеся между мошенниками и потерпевшими и в целом криминогенную обстановку. Лишь после этого нами был сделан вывод о том, что не всегда необходимо верить содержанию информации, поступающей по телефону от родственников, друзей и даже близких людей. Всегда необходимо такую информацию подвергать тщательному анализу, так как в условиях с учетом возможностей IT-технологий кибермошенники легко могут при помощи искусственного интеллекта создать голос Вашего родственника, друга или близкого человека.

В одном из своих интервью, посвященном новым методам обмана, которые используют кибермошенники, вице-премьер Правительства Российской Федерации Дмитрий Григоренко обсудил подробности с обозревателем Наилей Аскер-заде¹¹⁶. Ключевой фразой было то, что кибермошенники для осуществления своих преступных целей идут на любые уловки, чтобы выманить деньги у доверчивых граждан. По мнению Дмитрия Григоренко, в настоящее время не стоит доверять даже близким родственникам. С помощью современных информационных технологий мошенники подделывают голоса родных и близких. Абонент слышит голос не мошенника, а поддельный голос родного человека, как обычно, это голоса мамы, папы, родного человека, близких людей, кому люди доверяют, абсолютно не сложно сделать фейк - подделку голоса любого человека, главное записать оригинальный голос. После этого мошенники пытаются узнать пароль к личному кабинету в банке либо к госуслугам, а потом пробуют оформить кредиты. В таких внезапно возникших ситуациях Дмитрий Григоренко рекомендует, прежде чем делиться конфиденциальными данными, все же необходимо перезвонить родственникам на их личные номера и уточнить информацию.

После выявленных многократных вышеназванных мошеннических манипуляций, направленных на завладение конфиденциальной информацией, и последующих денежных хищений Правительство Российской Федерации приняло ряд законопроектов, одним из которых является законодательный запрет на звонки госучреждений и госорганов, маркетплейсов, банков через мессенжеры. После чего ведомства или финансовые организации уже не совершают звонки через мессенжеры, но граждане об этом не знают. В 2025 году такая норма прописана на законодательном уровне.

¹¹⁶ Новостная лента ТВ «Россия 1» от 26 февраля 2025 г.

Кроме того, государство обязало маркировать все звонки, которые осуществляются от имени организаций, банков, госучреждений, медицинских учреждений. В этом случае у абонентов будет высвечиваться не номер телефона цифрами, а название организации. Естественно, если происходит звонок от неизвестного абонента, т.е. высвечивается цифрами неизвестный номер телефона, то в таком случае лицо, которому звонят, должно понимать, что, вероятнее всего, ему звонит мошенник.

В качестве предупредительной меры используется установка определенного временного интервала (тайминга) на получение нового пароля в случае его изменения на госуслугах. У большинства граждан на сервисе существует двухфакторная аутентификация. При смене пароля необходимо направлять подтверждение через смс-сообщение. Второе сообщение будет приходить с интервалом 10-15 минут, чтобы было время для обдумывания и понимания происходящего. К нашему сожалению, объемы хищений пока только растут. В 2024 году рост превысил 74 %. Мошенники похитили со счетов россиян 27,5 млрд. рублей. Это рекордный показатель за все время ведения статистики. Размер возмещения причиненного материального вреда законопослушным пользователям ничтожно мал: менее 10%.

Далее Дмитрий Григоренко пояснил, что за последние годы в Российской Федерации использование Интернет-трафика выросло на 20-30%. Сегодня 85% территории страны обеспечено доступом к Интернету. В среднем мировой показатель использования Интернет-трафика составляет 65-70%. По итогам прошлого года наша страна заняла 12 место по цене фиксированного Интернета среди 223 стран (см. рис. 46).

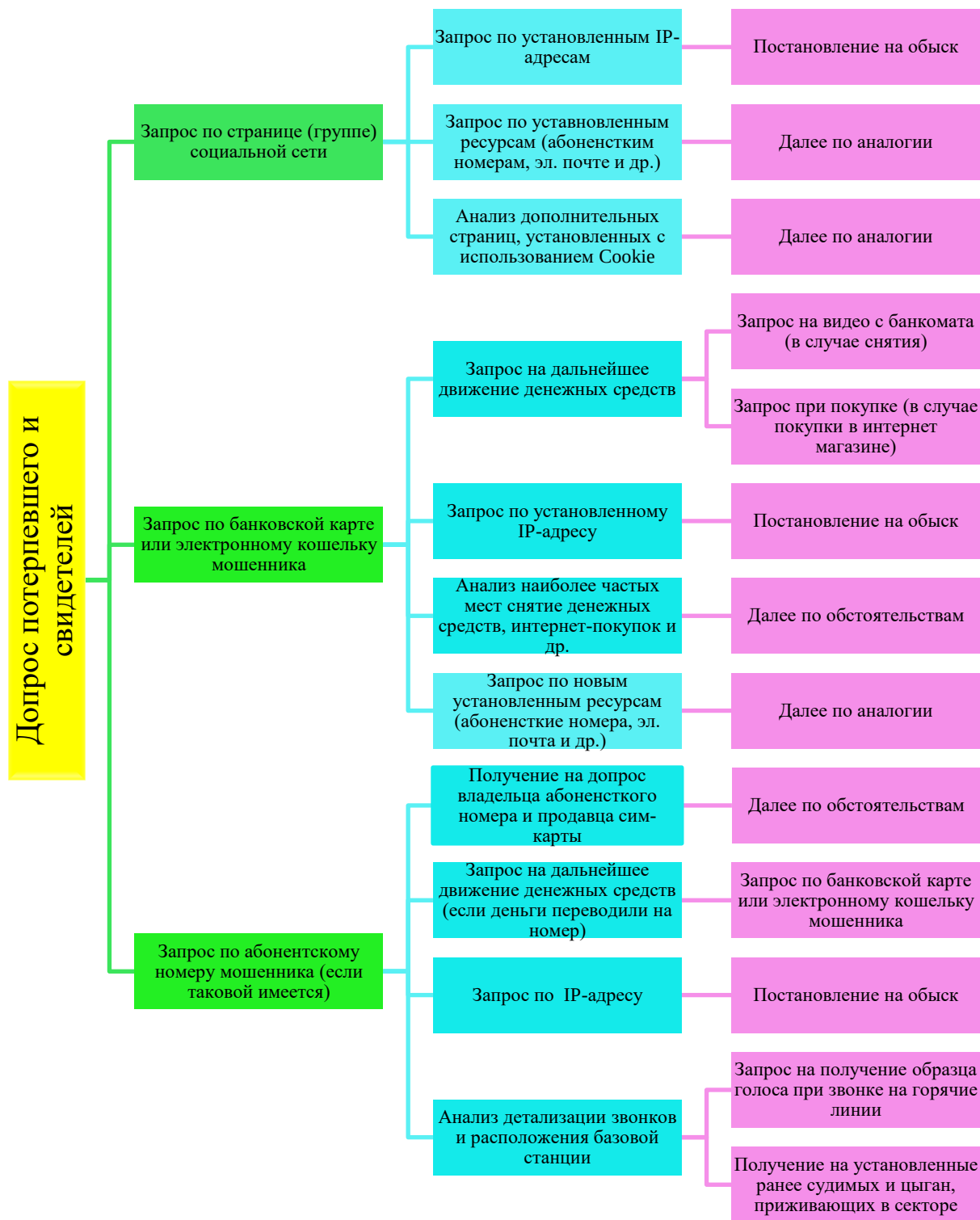


Рис. 46. Раскрытие преступлений, совершенных кибермошенниками в современном информационном пространстве с использованием сети Интернет и новых методов обмана

ОГЛАВЛЕНИЕ

	Стр.
Глоссарий.....	2
Введение	22
Глава I. Уголовно-правовая и криминалистическая характеристика преступлений, совершаемых в сфере телекоммуникаций и компьютерной информации	52
Глава II. Раскрытие преступлений, совершаемых в сфере телекоммуникаций и компьютерной информации.....	82
2.1. Вредоносные программы и компьютерные вирусы.....	82
2.2. Выявление и раскрытие преступлений, связанных с вредоносными компьютерными программами.....	108
2.3. Особенности производства отдельных следственных действий при расследовании преступлений в сфере телекоммуникаций и компьютерной информации	118
2.4. Особенности взаимодействия сотрудников оперативных подразделений ОВД с подразделениями СМ ОВД при раскрытии преступлений в ходе производства ОРМ и следственных действий	128
2.5. Некоторые виды преступлений, совершаемые в информационно-коммуникационных сетях.....	137
2.6. Преступления, совершаемые с блокчейном.....	161
2.7. Преступления террористического характера и экстремистской направленности, совершаемые с использованием сферы телекоммуникаций и компьютерной информации	175
2.8. Основные направления совершенствования системы противодействия кибертерроризму в деятельности органов внутренних дел Российской Федерации	201

Глава III. Особенности получения оперативно значимой информации сотрудниками оперативных подразделений и следственных органов в целях раскрытия преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет	215
3.1. Технологическая цепочка действий оперативных сотрудников и следователей, направленных на получение необходимой информации у сторонних компаний, организаций и учреждений	215
3.2. Схемы расследования наиболее распространённых преступлений, совершаемых в современном информационном пространстве с использованием сети Интернет	219

Научное издание

Литвинов Михаил Юрьевич,
кандидат технических наук
Алескеров Вагиф Исмаилович,
кандидат юридических наук, доцент

**ПРОТИВОДЕЙСТВИЕ
СОВРЕМЕННЫМ ВИДАМ ПРЕСТУПЛЕНИЙ,
СОВЕРШАЕМЫХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

Часть 1

Редактирование О.Н. Колокольчикова
Техническое редактирование Е.В. Бухарина

Подписано в печать 30.06.2026.
Формат 60х84 1/16. Объем 11,3 усл.-изд. л.
Тираж 100 экз. Заказ 09/26. Цена договорная.

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

142007, Московская обл., г. Домодедово, микрорайон Авиационный,
ул. Пихтовая, д. 3.