Приложение
к постановлению МПА СНГ
от 27 ноября 2020 года № 51-24

Межпарламентская Ассамблея государств – участников Содружества Независимых Государств

РЕКОМЕНДАТЕЛЬНЫЕ ТИПОЛОГИИ НОВЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Развитие информационных технологий обусловило их применение в преступной деятельности. Анализ оперативной обстановки в области предупреждения, выявления и пресечения компьютерных преступлений свидетельствует о наличии устойчивой тенденции к изменению видов преступлений в сферах компьютерной информации и электронной коммерции в сегментах информационно-телекоммуникационной сети «Интернет»[1].

Неконкретность понятий и отсутствие единого подхода к терминологии, применяемой при осуществлении количественного учета и классификации новых способов совершения преступлений в сфере информационных технологий, осложняет определение реальной степени их угроз.

Предлагаемая типология преступлений дает возможность создать единый механизм учетно-аналитических операций при оценке состояния и динамики киберпреступности, а также обосновать практические рекомендации и определить пути сотрудничества в рассматриваемой сфере.

1. Способы совершения мошеннических действий с использованием сети Интернет, средств подвижной связи и систем дистанционного банковского обслуживания

Основную долю компьютерных инцидентов составляют распространение вредоносных программ, предназначенных для хищения учетных записей пользователей сети Интернет, и преступления, связанные с электронными платежными системами.

Способы совершения данных преступлений обусловлены особенностями их предмета и средств совершения: в преступных целях используется порядок осуществления банковских операций по переводу безналичных денежных средств, находящихся на счетах банковских платежных карт, с использованием средств мобильной связи, а также порядок оказания услуг подвижной (так называемой мобильной) связи операторами.

Мошеннические действия, в том числе с использованием мобильных средств связи, путем перевода денежных средств со счетов банковских карт потерпевших на счета третьих лиц в большинстве случаев совершаются в

[1] Далее — сеть Интернет.

отношении держателей банковских карт клиентов, подключенных к системам дистанционного банковского обслуживания.

Анализ материалов судебной практики позволяет классифицировать способы завладения денежными средствами, находящимися на счетах банковских карт, следующим образом.

1.1. Введение потерпевшего в заблуждение относительно целей перевода денежных средств путем совершения телефонных звонков или направления СМС-сообщений. Под влиянием заблуждения потерпевший самостоятельно переводит денежные средства со своего счета на счета третьих лиц через системы интернет-банкинга и мобильного банкинга, терминалы банков или иным способом.

1.1.1. Побуждение потерпевшего к переводу денежных средств со своего счета на счета третьих лиц путем сообщения ему по телефону или через СМС-сообщение ложных сведений о внезапно возникших у его близких родственников серьезных проблемах, связанных с несчастным случаем, дорожно-транспортным происшествием, причинением вреда здоровью третьих лиц, задержанием за хранение наркотических средств, совершением других преступлений либо с долговыми обязательствами, для незамедлительного решения которых срочно требуется определенная сумма денег.

При этом злоумышленники звонят или направляют СМС-сообщения потерпевшим по случайно подобранным номерам телефонов, как мобильных, так и стационарных, от имени их родственников, друзей, знакомых или сотрудников правоохранительных органов, указывают номер телефона или банковской карты, на который следует осуществить перевод, а также сумму денежных средств, которую необходимо перечислить. Во многих случаях мошенничество данным способом совершают лица, отбывающие наказание в местах лишения свободы.

1.1.2. Уведомление потерпевшего по телефону (в основном путем рассылки СМС-сообщений) о выпавшем ему крупном призе при розыгрыше лотереи и необходимости перевода определенной суммы денежных средств (якобы налоговых или иных платежей) на указанный номер телефона или платежного средства в качестве условия получения приза.

1.1.3. Направление потерпевшему (путем рассылки СМС-сообщений) ложного уведомления о зачислении на его банковский счет определенной суммы денежных средств, а через некоторое время — сообщения об ошибочном зачислении этой суммы с просьбой о ее возврате посредством перевода на указываемый номер телефона или банковской карты.

1.1.4. Осуществление звонков потерпевшим от имени оператора связи с предложением подключить новую услугу и набрать для этого под диктовку определенный код, который в действительности является комбинацией для перевода денежных средств со счета абонента на счет третьего лица.

1.1.5. Сообщение потерпевшему заведомо ложных сведений (посредством телефонных звонков или СМС-сообщений от имени банка) о возникших технических или иных проблемах, препятствующих дальнейшему использованию им своей банковской карты, с предложением совершить для

устранения данных препятствий определенные операции по банковскому счету через системы интернет-банкинга, мобильного банкинга или терминал банка. Совершение потерпевшим, введенным в заблуждение, данных операций в действительности влечет перевод денежных средств со счета его банковской карты на счет третьего лица.

Такие действия производятся лицами, совершающими мошенничество, как правило, двумя способами. Первый способ заключается в направлении потерпевшему ложного уведомления посредством СМС-сообщения от имени банка о временной блокировке банковской карты с предложением навести справки по указанному номеру телефона.

Когда потерпевший звонит по данному номеру, мошенник, представившись сотрудником службы безопасности банка, объясняет причины блокировки карты попытками посторонних лиц получить информацию о реквизитах банковской карты или о банковском счете, сбоями в работе сервера банка либо иными надуманными обстоятельствами.

Затем злоумышленник, в зависимости от информации, предоставленной потерпевшим при ответах на поставленные вопросы, предлагает совершить определенные действия посредством интернет-банкинга, мобильного банкинга либо через ближайший банкомат. При этом потерпевшему сообщается о важности оперативного совершения данных действий, поскольку в противном случае якобы возникнет необходимость замены банковской карты, которая может затянуться на долгое время, и воспользоваться денежными средствами, хранящимися на карте, в течение этого периода будет невозможно.

Согласившись на выполнение ложной операции разблокировки карты, потерпевший, например, подходит к банкомату, звонит по сообщенному ему номеру телефона и, действуя по указанию, вставляет свою банковскую карту в банкомат, набирает на нем код доступа к карте, осведомляет мошенников об остатке денежных средств на ней. После этого он набирает под диктовку цифры, полагая, что вводит код для разблокировки карты, а в действительности переводит денежные средства со своей карты на банковскую карту или лицевые счета абонентских номеров сотовых операторов третьих лиц либо подключает услугу «Интернет-банк» или «Мобильный банк», позволяющую управлять счетом его банковской карты.

При этом потерпевшему становится известно по полученным чекам или поступающим СМС-уведомлениям об осуществлении им операции перевода денежных средств. Однако его убеждают, что переведенные денежные средства зарезервированы и в течение нескольких часов будут возвращены на счет, и предлагают ему не пользоваться картой до их поступления. Затем злоумышленники переводят поступившие денежные средства на банковские счета других лиц либо на счета до востребования через системы денежных переводов отдельных кредитных учреждений. Впоследствии лица, не осведомленные об истинном их происхождении этих денежных средств, за финансовое вознаграждение получают их в банке и передают незнакомым им лицам.

Используемые мошенниками для рассылки СМС-сообщений, разговоров с потерпевшими и перечисления денежных средств абонентские номера, как правило, оформляются ими на вымышленных лиц. Банковские карты, на которые перечисляются похищенные денежные средства, в основном принадлежат не имеющим отношения к мошенникам лицам, по просьбе или по собственной инициативе оформляющим их на свое имя и передающим полученные средства за денежное вознаграждение малознакомым или незнакомым лицам.

Второй способ состоит во введении держателя банковской карты (владельца счета) в заблуждение (в том числе с помощью методов социальной инженерии, т. е. с использованием познаний в области психологии) относительно сущности операций с целью получения информации, необходимой для несанкционированного доступа, либо принуждения потерпевшего совершить определенные действия.

Лица, совершающие мошенничество, при первом телефонном разговоре с потерпевшим выясняют, что абонентский номер его телефона подключен к системе дистанционного банковского обслуживания. Поводом к возникновению доверительных отношений может стать, например, то, что преступник представляется сотрудником службы социального обеспечения либо сотрудником банка, целью которого является перечисление потерпевшему дополнительной социальной выплаты и т. п.

Затем злоумышленники предлагают потерпевшему посредством данной системы совершить для разблокировки банковской карты операции якобы по временному резервированию денежных средств, находящихся на его банковском счете, а в действительности по переводу их на счета третьих лиц. Введенный в заблуждение держатель карты переводит, действуя по указанию мошенников, денежные средства на указанный ему счет банковской карты или абонентский номер, не сомневаясь, что переведенные им денежные средства в течение суток поступят обратно на его счет.

К разновидностям введения в заблуждение потерпевшего также следует отнести перевод средств со счета потерпевшего путем применения системы СМС-банкинга — технологии дистанционного банковского обслуживания посредством СМС-сообщений, в которой доступ к банковским счетам и операциям по банковским счетам предоставляется в любое время с использованием номера мобильного телефона клиента, предварительно зарегистрированного в банке. Эта технология, помимо «пассивного» СМС-оповещения о проведенных операциях и состоянии счета, позволяет осуществлять «активное» СМС-оповещение — отправку сообщений в ответ на получаемые от клиента СМС-запросы (например, о балансе банковской карты, предоставлении счета, мини-выписки или блокировке банковской карты), а также отправлять банку через сеть оператора подвижной связи команды на проведение операций с денежными средствами клиента банка (владельца сим-карты).

Мошенники также используют способ совершения операций по USSD-запросам[2]: предлагают потерпевшему набрать USSD-команду или отправить СМС на специальный номер банка для совершения перевода.

1.1.6. Вмешательство в функционирование средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей путем блокирования абонентского номера потерпевшего, восстановления его на дубликат сим-карты и перечисления денежных средств с банковского счета потерпевшего посредством системы мобильного банкинга на счета третьих лиц.

В некоторых случаях для получения дубликата сим-карты, установленной в телефоне потерпевшего, мошенники вступают в сговор с представителями оператора связи, работающими в офисах продаж и обслуживания клиентов. Иногда данные преступления совершаются представителями оператора связи самостоятельно.

Особенностью таких способов мошенничества является отсутствие непосредственного контакта лиц, их совершающих, с потерпевшими, поскольку последние вводятся в заблуждение и побуждаются к осуществлению определенных действий через средства дистанционной коммуникации.

1.2. Использование найденного, похищенного, приобретенного либо случайно оказавшегося у субъекта преступления чужого телефонного аппарата с абонентским номером владельца, подключенного к услуге «Мобильный банк»

Потерпевший, чей телефонный аппарат по тем или иным причинам выбыл из владения (утерян, похищен, продан вместе с сим-картой), своевременно не обращается в банк с просьбой отключить от его абонентского номера услугу «Мобильный банк», сам передает свой телефонный аппарат другому лицу во временное пользование или оставляет его без присмотра. Преступники, обнаружив при пользовании телефоном, что тот подключен к указанной услуге, совершают хищение денежных средств, находящихся на банковском счете потерпевшего.

1.3. Использование подключенного к услуге «Мобильный банк» абонентского номера, ранее принадлежавшего другому абоненту

Данный способ мошенничества заключается в использовании лицами, его совершающими, того обстоятельства, что потерпевший, осуществив замену абонентского номера, подключенного к услуге «Мобильный банк», не предупредил об этом кредитную организацию, а его абонентский номер впоследствии был перерегистрирован оператором связи на другое лицо. Обнаружив, что такой абонентский номер подключен к услуге «Мобильный банк», новый владелец номера посредством указанной услуги переводит

[2] USSD (Unstructured Supplementary Service Data) — стандартный сервис в сетях GSM, позволяющий организовать интерактивное взаимодействие между абонентом сети и сервисным приложением в режиме передачи коротких сообщений. Основное направление использования USSD-сервиса — предоставление абонентам возможности получать дополнительную информацию от приложений и управлять этими приложениями.

денежные средства потерпевшего на свой банковский счет или на счета третьих лиц.

2. Способы совершения хищений через вмешательство в функционирование средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей путем подделки электронных средств идентификации платежей, использования идентификационных данных банковских карт

Несанкционированное вмешательство в платежные системы — один из наиболее распространенных способов хищения денежных средств на территории государств — участников СНГ.

Основную долю (как по объему хищений, так и в количественном выражении) несанкционированных операций составляют CNP-транзакции (операции в сети Интернет).

Чаще всего хищение денежных средств физических и юридических лиц посредством так называемого карточного мошенничества совершается следующими способами.

2.1. Проведение банковских операций посредством несанкционированного доступа («хакерского взлома») к хранилищам данных и иной банковской информации

2.1.1. Хищение денежных средств путем доступа к идентификационным данным сотрудников кредитных организаций.

Установление непосредственного контроля над компьютерными системами является распространенным способом совершения указанного вида преступлений. В таких случаях в зону риска попадают предприятия и организации, внутренняя сеть которых имеет точку доступа к сети Интернет. Злоумышленники, подобрав пароли к системе и получив полный контроль над ней, могут осуществлять шифрование данных либо похищение учетных данных. При этом оборудование жертвы без ее ведома на протяжении длительного времени может использоваться злоумышленниками в преступных целях (подбор паролей, рассылка нежелательных почтовых сообщений и т. п.).

2.1.2. Хищение и вымогательство денежных средств с помощью «банковских» вирусов.

Ввиду появления новых технологических решений по усовершенствованию средств противодействия бот-сетям[3] большая часть преступных групп, работающих против банков и их клиентов, отказывается от стандартных методов при распространении своих вредоносных программ-

[3] Бот-сеть, или ботнет, — компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами (автономным программным обеспечением). Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять определенные действия с использованием ресурсов зараженного компьютера. Обычно используется для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удаленной системе, атак на отказ в обслуживании (DoS- и DDoS-атаки).

троянов («троянских коней») в пользу спам-рассылок с возможностью автоматического цикла, например когда вредоносная программа перенаправляет интересующий трафик на другие серверы.

Вредоносные программы-трояны осуществляют не санкционированные пользователем действия: уничтожают, блокируют, модифицируют или копируют информацию, нарушают работу компьютеров или компьютерных сетей. В отличие от вирусов и червей, вредоносные программы-трояны не создают свои копии, не способны к самовоспроизведению.

В настоящее время наиболее распространенным способом использования вредоносных программ является отправление на персональный компьютер жертвы спам-сообщения, содержащего замаскированный загрузчик, который после исполнения загружает новую модификацию программы-трояна, загружающую в свою очередь компьютерного червя. После этого червь использует установленный на скомпрометированных устройствах почтовый клиент с целью рассылки спам-сообщений, к которым прикреплен вредоносный загрузчик. Червь отправляет спам-сообщения не контактам жертвы, а на адреса почты, полученные с сервера злоумышленников, а по окончании рассылки писем самоудаляется.

Участились случаи совершения хищений с использованием банковских троянов, которые способны вести электронный шпионаж за пользователем (копировать вводимые с клавиатуры данные, изображения экрана, список активных приложений и т. д.), похищать конфиденциальную информацию пользователей для доступа к системам онлайн-банкинга.

С целью сокрытия следов своей противоправной деятельности злоумышленники активно используют средства анонимизации (VPN, TOR, Proxy), шифрования интернет-трафика, компьютерной техники и личной переписки.

Большое распространение получили программы malware типа ransomware (иначе — «трояны-вымогатели») — вредоносное программное обеспечение, предназначенное для вымогательства. Их можно разделить на два основных типа — шифровальщики (cryptoransomware, крипторы) и блокировщики (blockers, блокеры). Шифровальщики, попадая в компьютер, шифруют ценные файлы (документы, фотографии, базы данных и т. п.) таким образом, что их нельзя открыть. За расшифровку мошенники требуют выкуп.

2.2. Способы получения учетных данных держателей банковских карт: пароля, логина, номера и кода проверки подлинности карты и т. д. (фишинг)

2.2.1. Получение путем обмана или иным неправомерным способом реквизитов банковской карты, идентификаторов ее держателя и последующее осуществление с использованием полученных данных и средств мобильной связи перевода денежных средств, находящихся на банковском счете потерпевшего, на счета третьих лиц.

Например, широко распространена рассылка от имени банка СМС-сообщений о блокировке банковской карты с указанием номера телефона для получения справок. Позвонившему на указанный номер потерпевшему

сообщается о произошедшем техническом сбое в работе компьютерной системы банка и предлагается для разблокировки или перерегистрации карты сообщить представителю банка номер и код карты либо пароли для ее использования.

Нередко мошенники получают идентификационные данные (номер и код проверки подлинности) банковской карты под предлогом необходимости этих сведений для осуществления перевода денежных средств на банковский счет потерпевшего, в частности в качестве оплаты за товар, объявление о продаже которого размещено в сети Интернет.

2.2.2. Получение учетных данных путем обмана потерпевшего в момент использования им платежной карты для осуществления операций через банкомат.

Мошенники обращаются к неосведомленному потерпевшему с просьбой проверить с помощью его карты, находящейся в картоприемнике банкомата, работу раздела «Интернет-обслуживание». Согласившись, потерпевший под диктовку проводит операции, завершающиеся распечаткой чека с полной информацией о его банковской карте, включая идентификатор и пароли для пользования системой интернет-банкинга, который попадает в распоряжение преступников.

2.2.3. Создание, распространение и использование вредоносных компьютерных программ, перенаправляющих потерпевших на ложный IP-адрес (pharming, фарминг).

Осуществляется с помощью вредоносного программного обеспечения, которое «перебрасывает» пользователя с запрошенных интернет-страниц на их мошеннические копии. В случаях с торгово-сервисными предприятиями по карте пользователя могут быть проведены мошеннические транзакции за не приобретаемые в действительности товары и услуги.

Например, мошенники осуществляют массовую рассылку СМС-сообщений, в которых предлагается скачать музыкальные или иные клипы, либо направляют ложные уведомления, в том числе от имени банков, с предложением установить для повышения уровня защиты своих персональных данных программу с сайта банка, ссылка на который приводится в сообщении. От имени банка жертвам может направляться письмо с указанием подтвердить правильность их реквизитов на специальном веб-сайте в связи с возникшими проблемами технического характера. Также злоумышленники могут сообщить клиенту банка, что он превысил максимально допустимую отсрочку платежа и его счет будет заблокирован, отметив необходимость для получения более подробной информации открыть прикрепленные документы.

2.2.4. Создание двойников сайтов по продаже авиабилетов и железнодорожных билетов, а также двойников сайтов финансовых организаций.

2.2.5. «Обход» используемой большинством банков двухфакторной аутентификации в системах интернет-банкинга с помощью СМС-сообщения.

Мобильное устройство жертвы заражается банковским трояном. После запуска пользователем подлинного банковского приложения на своем

смартфоне троян определяет, приложение какого банка используется, и перекрывает его интерфейс своим, показывая пользователю поддельный экран. Внешне поддельное приложение максимально похоже на настоящее. На поддельном экране пользователь вводит свои логин и пароль, а троян отправляет их злоумышленникам, которые таким образом получают возможность использовать эти данные для входа в банковское приложение. Затем злоумышленники инициализируют перевод денежных средств на свой счет. Системой дистанционного обслуживания на зараженный смартфон пользователя отправляется СМС-сообщение с одноразовым паролем, однако троян перехватывает пароль и пересылает его злоумышленникам. При этом пострадавший не видит СМС-сообщение и ни о чем не подозревает, пока не проверит список транзакций. Используя перехваченный одноразовый пароль, преступники подтверждают транзакцию и получают денежные средства.

2.3. Использование в банкоматах или POS-терминалах накладок и других устройств, копирующих данные магнитной полосы и запоминающих ПИН-код держателя (skimming, скимминг), в целях подделки карт (создания их копий)

Для реализации этого способа мошенники устанавливают на банкоматы считывающие устройства — скиммеры. На картридер устанавливаются рамки с магнитной головкой, считывающей информацию с магнитной полосы и записывающей электронные копии (дампы) карт на встроенную микросхему памяти. На клавиатуру приклеивается накладка, очень похожая на настоящую клавиатуру, которая запоминает нажатия клавиш и записывает их на встроенную микросхему. Кроме того, на банкомат может быть прикреплена миниатюрная видеокамера, которая сохраняет в модуле памяти либо передает на компьютер мошенника информацию о вводимом ПИН-коде.

Одним из вариантов такого способа считывания данных карты является установка на картридер, используемый для входа в помещение банка (в случае расположения банкоматов в закрытых помещениях, открывающихся посредством считывания карты), скимминговой накладки для считывания информации с карт входящих клиентов, а также ложной клавиатуры или накладки на клавиатуру. Дамп карты записывается на любую карточку с магнитной полосой, которая становится клоном карты пострадавшего и используется для доступа к его денежным средствам вместе с похищенным ПИН-кодом. Если ПИН-код мошенникам неизвестен, покупки совершаются с использованием поддельной банковской карты в магазинах по предварительному сговору с кассиром.

Мошенники нередко пересылают дампы карт для изготовления подделок и обналичивания в другие страны. Это делается с целью усложнения расследования и переноса ответственности за мошенничество на банки, поскольку при отсутствии в паспорте клиента отметки о пересечении границы банк не может возложить вину за несанкционированную операцию на владельца карты.

Скимминг сложный и затратный способ хищения, так как современное оборудование терминалов и банкоматов, как правило, не позволяет

устанавливать скимминговые устройства либо оснащено устройствами активного антискимминга.

2.4. Кража или использование утерянных карт

Одна из технологических разновидностей этого способа мошенничества — траппинг (trapping), т. е. захват карты в картридере с помощью специальных устройств. Мошенник вставляет в картридер терминала кусок пленки, надрезанный таким образом, что карта, попадая в прорезь, не возвращается владельцу, а остается в конверте, который впоследствии извлекается мошенником.

В тот момент, когда карта попадает в ловушку, злоумышленник оказывается рядом с потерпевшим и предлагает ему повторно ввести ПИН-код, мотивируя это тем, что с ним накануне произошла подобная ситуация и данная операция помогла вернуть карту. После дополнительных вводов ПИН-кода карта не возвращается. Мошенник советует жертве обратиться в банк и, после ее ухода, извлекает конверт из банкомата. В итоге у преступника оказывается банковская карта потерпевшего и информация о ПИН-коде.

3. Иные способы хищений и причинения имущественного ущерба посредством использования средств подвижной связи

3.1. Взимание повышенных сборов за телефонные звонки

Преступники присваивают обманным путем денежные средства клиентов компаний телефонной связи, совершающих звонки на зарубежные номера, за которые взимается повышенный сбор.

Схема мошенничества состоит в «сброшенных» звонках на номер телефона жертвы. Потерпевший, желая узнать, кто ему звонил, перезванивает по соответствующему номеру телефона, после этого с него взимается повышенный сбор за звонок на платный номер.

К этому способу следует отнести также отправку клиентам компаний телефонной связи текстовых сообщений с незнакомого номера. Если потерпевший отвечает на СМС из любопытства, с него взимается плата за СМС-сообщение по специальному тарифу.

3.2. Мошенничество на платформах бесплатных объявлений

Схема мошенничества заключается в размещении в сети Интернет бесплатных объявлений о продаже различных видов продукции по цене, которая в несколько раз ниже цены аналогичной продукции на рынке. При этом выставленный на продажу товар не имеет никаких технических или внешних недостатков, а заниженная цена объясняется его собственником срочной потребностью в денежных средствах.

Невозможность связаться с ними через указанные в объявлении контактные данные преступники объясняют тем, что находятся за пределами страны, предлагая альтернативные средства связи: адрес электронного почтового ящика, имена профилей в системах мгновенных сообщений, таких как WhatsApp, Viber, Telegram.

Во время переговоров, которые ведутся посредством альтернативных контактов, преступники под предлогом подтверждения реальности намерений просят покупателя перечислить аванс через различные международные системы денежных переводов. В некоторых случаях мошенники просят совершить такими способами дополнительные платежи, ссылаясь на различные надуманные причины (ремонт выставленного на продажу товара, отсутствие денег на счете мобильного телефона и т. д.). Получив деньги, преступники прекращают любые контакты с жертвой.

3.3. *Мошенничество в виде конкурса СМС-сообщений или теста на общие знания*

Как правило, преступники отправляют жертве текстовое сообщение, призывающее ее принять участие в конкурсе на получение ценного приза. Мошенники устанавливают крайне высокие тарифы на сообщения, которые отправляются потерпевшими и получаются ими. Первые вопросы делаются очень легкими, чтобы поощрить потерпевших к продолжению игры, а на последний вопрос или два последних вопроса очень сложно или даже невозможно ответить верно.

4. Использование информационных технологий для совершения преступлений в сфере незаконного оборота наркотических средств, психотропных веществ и их прекурсоров

Компьютерные сети и телекоммуникационные технологии весьма широко используются в сфере незаконного оборота наркотических средств.

Организованные группы наркоторговцев все чаще прибегают к бесконтактным способам сбыта наркотиков, широко используя при этом средства мобильной связи, интернет-ресурсы, электронные платежные системы.

Одной из тенденций последнего времени стала активизация нелегального производства синтетических наркотиков на территории стран Содружества Независимых Государств, что определяется их доступностью по цене и способу приобретения, в том числе через сеть Интернет.

Основным способом распространения наркотиков является бесконтактный сбыт путем организации тайников-закладок и перевода денежных средств, включая криптовалюту, через различные платежные системы. С целью увеличения числа потребителей участники наркобизнеса все активнее используют сеть Интернет не только для рекламы наркотических средств и психотропных веществ, но и для анонимного осуществления оперативного поиска продавцов и покупателей, организации так называемого регионального маркетинга.

Организаторы торговли наркотиками активно используют ресурсы «темной сети» (DarkNet), или «глубокой паутины» (DeepWeb), которая обеспечивает анонимность, так как закрыта от поисковиков и отслеживания. Попасть в DarkNet можно через один из прокси-серверов, самый популярный из которых — сеть Tor (The Onion Router) и ее браузер (Tor Browser). Сайты сети Tor имеют доменное имя первого уровня onion.

Сайты наркоторговцев устроены по принципу обычных интернет-магазинов — в них можно оформить заказ, почитать отзывы и описание, поделиться мнением о качестве продукта и сервиса, связаться со службой поддержки. Оплата покупок возможна любыми способами: банковскими картами, через интернет-кошельки, криптовалютой (например, биткоинами).

DarkNet также используется организаторами и подстрекателями создания преступных групп для так называемого трудоустройства, в том числе вовлечения в свою деятельность «кладменов», которые делают закладки наркотиков, «гроверов», которые выращивают траву, химиков, которые производят ЛСД и экстази, курьеров, которые перевозят товар, «дропов», которые снимают деньги, трафаретчиков, которые пишут объявления на асфальте и заборах.

5. Использование информационных технологий с целью совершения преступлений против половой неприкосновенности несовершеннолетних, а также преступлений против здоровья населения и общественной нравственности

С развитием научно-технического прогресса сеть Интернет становится все более популярной среди детей и подростков. Растет количество времени, проводимого в ней несовершеннолетними. Одно из наиболее востребованных направлений использования Интернета — социальные сети, которые дают несовершеннолетним возможность общаться и обмениваться информацией с друзьями.

5.1. Преступления против половой неприкосновенности несовершеннолетних

Находясь в виртуальном пространстве, дети и подростки неизбежно сталкиваются с комплексом киберугроз, среди которых одной из наиболее опасных выступает угроза стать жертвой преступления против половой неприкосновенности, так как преступники, используя информационные технологии, получают возможность дистанционно связываться с несовершеннолетними, осуществлять в их отношении развратные действия.

Для обозначения действий совершеннолетнего лица, направленных на установление в Интернете доверительного контакта с ребенком с целью склонить его к вступлению в сексуальную связь, используется термин «кибергруминг», или «онлайн груминг»[4].

Типичный механизм кибергруминга заключается в том, что злоумышленник общается в сети Интернет с ребенком, выдавая себя за

[4] Термин «груминг» происходит от английского слова grooming — уход, забота. Суть этого метода — создание у несовершеннолетнего ощущения, что о нем заботятся, им искренне интересуются, чтобы способствовать возникновению психологической связи, завоевать доверие ребенка или подростка на основе его интересов. Этим понятием охватываются как действия, преследующие цель получения лицом, страдающим расстройством сексуального предпочтения (педофилией), сексуального удовлетворения, так и действия, направленные на вовлечение ребенка в коммерческую сексуальную эксплуатацию.

ровесника либо ребенка немного старше, знакомится в чате, на форуме или в социальной сети с жертвой, пытается установить с ней дружеские отношения и перейти на личную переписку.

Основные способы совершения преступлений против половой неприкосновенности и половой свободы несовершеннолетних:

1) участие в организации производства порнографической продукции (фото- и видеосъемка);
2) сбор из различных источников и распространение чужих «произведений»;
3) размещение на своих информационных ресурсах в сети Интернет ссылок на сайты, содержащие порнографические изображения несовершеннолетних (рекламирование).

5.2. Основные способы склонения несовершеннолетних к совершению самоубийства

Несмотря на успешное противодействие преступной деятельности лиц, занимавшихся склонением несовершеннолетних к самоубийствам, возникновение в сети Интернет «групп смерти» обладает высоким потенциалом опасности.

Выделяются следующие формы (способы) сетевого склонения к самоубийству:

1) размещение на информационном ресурсе сведений о способах совершения самоубийства;
2) размещение мультимедийных материалов (фото-, видео- и аудиоконтента, простых и креолизованных текстов);
3) онлайн-переписка.

Вербовщики в «группы смерти» действуют в социальных сетях. После того как ребенок вступает в игру, кураторы подключают его к мессенджерам, позволяющим распространять мгновенные анонимные сообщения. В результате происходит активное влияние на несовершеннолетнего с целью склонения его к самоубийству.

6. Использование информационных технологий для совершения преступлений террористического и экстремистского характера

Роль сети Интернет в расширении пропаганды терроризма в наши дни очень велика. Информационные сети и сервисы являются удобным, эффективным средством и одновременно средой распространения экстремистской идеологии.

Одной из разновидностей терроризма является кибертерроризм, для которого свойственно использование преступниками в качестве средств достижения своих целей информационных технологий, специального программного обеспечения, предназначенного для несанкционированного проникновения в компьютерные системы.

Способы совершения кибертеррористических преступлений с учетом доктринальных позиций можно классифицировать следующим образом:

1) несанкционированное проникновение в атакуемую сеть или перехват управления сетью путем взлома, в том числе через подбор либо хищение идентификационных данных, позволяющих войти в систему (повысить пользовательские привилегии);
2) применение программного кода или последовательности команд, находящих и использующих уязвимости в программном обеспечении;
3) распространение компьютерных вирусов, которые модифицируют и уничтожают информацию или блокируют работу вычислительных систем;
4) введение в программу вирусов — логических бомб, программ, которые запускаются (срабатывают) при определенных условиях (временных или информационных) для осуществления вредоносных действий (как правило, несанкционированного доступа к информации, искажения или уничтожения данных);
5) использование «троянских коней», выполняющих передачу информации на удаленные компьютеры либо иные вредоносные действия без ведома владельца зараженной системы;
6) применение средств нарушения и подавления информационного обмена в сетях (в частности, нарушение функционирования серверов и сайтов путем применения DoS/DDoS-атак).

7. Поиск уязвимостей программного обеспечения в целях продажи третьим лицам и иные компьютерные преступления

Вышеописанные способы кибернападений террористической направленности свойственны атакам, совершаемым для демонстрации возможностей организованных преступных групп и хакеров-одиночек в целях поиска заказчиков (работодателей).

Существуют сервисы по поиску определенных уязвимостей в корпоративных сетях с последующей их продажей третьим лицам. Ведутся активные исследования программного обеспечения и сервисов операционных систем для выявления «угроз нулевого дня» — ошибок в программном обеспечении, приводящих к повышению пользовательских привилегий, о которых неизвестно даже разработчику[5].

«Угрозы нулевого дня» влекут за собой появление новых способов распространения вредоносного кода, что активно используется киберпреступниками для создания эффективного механизма заражения через программные продукты массового использования. Эксплуатация данных уязвимостей осуществляется через так называемые связки эксплойтов, реализующие удаленный доступ к операционной системе с последующей загрузкой вредоносного программного обеспечения.

[5] Происхождение термина «угроза нулевого дня» связано с тем обстоятельством, что об уязвимости программного обеспечения или атаке на него становится известно до момента выпуска производителем программного обеспечения, позволяющего исправить ошибки (т. е. уязвимость может быть использована на работающих копиях приложения без возможности защиты от нее).

Значительная часть «угроз нулевого дня» — это критические уязвимости, т. е. бреши, позволяющие злоумышленнику, имеющему готовый хакерский эксплойт, получить полный контроль над системой при условии отсутствия доступных исправлений программного обеспечения и антивирусных сигнатур. Обеспечение информационной безопасности особенно осложняет игнорирование пользователями необходимости установки исправлений даже после их выпуска, в особенности для программного обеспечения, не входящего в состав операционной системы.

Противодействие использованию информационных сетей преступными группами, специализирующимися на вымогательстве, мошенничестве, кражах, совершении преступлений в сфере компьютерной информации, а также защита важнейших информационных инфраструктур от кибератак имеют ключевое значение для внешней и внутренней безопасности как отдельных государств, так и СНГ в целом.

Решение этой задачи предполагает совместную работу правоохранительных и иных государственных органов, выстраивание сотрудничества и обмена информацией на национальном и межгосударственном уровне, а также разработку и реализацию комплекса нормативно-правовых и организационных мер по противодействию деятельности террористических и других преступных организаций и сообществ.

Приняты на пятьдесят первом
пленарном заседании
Межпарламентской Ассамблеи
государств — участников СНГ
(постановление № 51-24 от 27 ноября 2020 года)