**Методические рекомендации**

по заполнению отдельных кодовых значений справочников, предусмотренных для отражения сведений об использовании при совершении преступлений информационно-телекоммуникационных технологий

1. Настоящие методические рекомендации разработаны на основе Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Положения о едином порядке регистрации уголовных дел и учета преступлений и Инструкции о порядке заполнения и представления учетных документов, утвержденных приказом Генеральной прокуратуры РФ, МВД РФ, МЧС РФ, Минюста РФ, ФСБ РФ, Министерства экономического развития и торговли РФ и Федеральной службы РФ по контролю за оборотом наркотиков от 29.12.2005 № 39/1070/1021/253/780/353/399 «О едином учете преступлений», в целях оказания практической помощи правоохранительным органам Чукотского автономного округа и обеспечения полного и достоверного отражения сведений об использовании при совершении преступлений информационно-телекоммуникационных технологий.

Рекомендации могут быть использованы также органами прокуратуры округа при проведении проверок полноты и достоверности статистических данных и изучении состояния первичного учета в сфере уголовно-правовой статистики.

1. Сведения о способе совершения преступления с использованием информационно-телекоммуникационных технологий формируются согласно справочнику 12 «Способ совершения преступления», отражаются в реквизитах 26 статистической карточки формы № 2, 33 карточки формы № 2.
2. Заполнение сведений о способе совершения преступления с использованием информационных технологий осуществляется на основании материалов уголовного дела, включая показания потерпевшего, свидетелей, подозреваемого (обвиняемого), данных технических средств и является обязательным по всем преступлениям при совершении которых используются информационно-телекоммуникационные технологии или по преступлениям в сфере компьютерной информации.
3. Данные положения методических рекомендаций также учитываются при заполнении документов первичного учета по материалам проверок сообщений о преступлениях, по которым приняты решения об отказе в возбуждении уголовных дел по нереабилитирующим основаниям.
4. При отражении в статистических карточках сведений о применении информационных технологий следует руководствоваться нижеприведенной таблицей:

| код | Наименование | Определение (в каких случаях подлежит заполнению) | Примеры |
| --- | --- | --- | --- |
| 049 | средств мобильной связи | В случае использования преступником средств сотовой (мобильной) связи, в том числе, при хищении денежных средств путем отправки SMS сообщений с использованием услуги «Мобильный Банк» | * Преступник совершает телефонный звонок, в ходе которого либо убеждают потерпевшего перевести денежные средства на счета преступников, либо выманивают у потерпевшего конфиденциальную информацию о его банковской карте, после чего совершают хищение денежных средств;
* преступник совершает звонок в дежурную часть УМВД и сообщают заведомо ложные сведения об акте терроризма;
* преступник на законных основаниях получают от потерпевшего телефон, после чего совершает хищение денежных путем отправки SMS сообщений с использованием услуги «Мобильный Банк».
 |
| 048 | сети Интернет | В случаях, если при совершении преступления злоумышленником используются возможности глобальной сети «Интернет»  | * Преступник по средствам электронной почты направляет письма в различные организации с заведомо ложными сообщениями об акте терроризма;
* злоумышленником создается поддельный сайт по продаже авиабилетов (различных товаров) при помощи которого совершаются хищение денежных средств;
* преступник получает доступ к банковским счетам потерпевшего в онлайн банке и похищают денежные средства.
 |
| 050 | неправомерное списание денежных средств со счетов банковских карт | В случае списания денежных средств с банковского счета потерпевшего без направления им в банк соответствующего распоряжения, в том числе, с использованием специализированного программного обеспечения или ввода конфиденциальной информации по карте. | * Неустановленное лицо с использованием вредоносного программного обеспечения получило доступ к онлайн банку потерпевшего и списало со счета его банковской карты денежные средства;
* неустановленное лицо получив конфиденциальную информацию о банковской карте потерпевшего похищает с нее денежные средства;
* лицо приобретает (в том числе незаконно) банковскую карту потерпевшего и в последующем путем оплаты товаров и услуг (снятия в банковских устройствах самообслуживания) похищает с нее денежные средства.
 |
| 086 | социальных сетей | При совершении преступления злоумышленниками используются онлайн платформы, созданные для общения, знакомства, создание социальных отношений между людьми, которые имеют схожие интересы, а также для развлечения и работы (Одноклассники, Вконтакте, Facebook, Instagram и т.д.). | * Преступник размещают в одной из социальных сетей объявление о сдаче в аренду квартиры (продажи имущества), получают предоплату, а услугу (товар) не предоставляет;
* неустановленное лицо с использованием социальной сети размещают информацию, порочащую честь и достоинство потерпевшего.
 |
| 058 | расчетных (пластиковых) карт | При использовании для совершения преступления расчетных (пластиковых) карт, в том числе, при переводе на них похищенных денежных средств | * Преступник похищает банковскую карту потерпевшего и в последующем совершает хищение денежных средств путем оплаты товаров и услуг;
* преступник диктует номер банковской карты, на который потерпевший под воздействием обмана переводит денежные средства;
* преступник по средствам услуги мобильный банк переводит денежные средства со счета потерпевшего на счет своей банковской карты (банковской карты знакомого).
 |
| 087 | средств мгновенного обмена сообщениями (интернет-мессенджеров) | Если при совершении преступления используется специализированное программное обеспечение, предназначенное для обмена текстовыми сообщениями, фото, видео и иной информацией посредствам возможности сети Интернет (WhatsApp, Telegram, Viber и т.д.) | * Преступник размещает в одной из групп в мессенджере объявление о сдаче в аренду квартиры (продажи имущества), получают предоплату, а услугу (товар) не предоставляет;
* в ходе общения с потерпевшим при совершении мошеннических действий преступник использует один из мессенджеров;
* преступник размешает в одной из публичных групп в интернет мессенджере объявления о продаже наркотических средств (психотропных веществ), поддельных дипломов и т.д.
 |
| 091 | методов социальной инженерии | Код предусмотрен для отражения сведений об использовании преступником в отношении потерпевшего методов социальной инженерии.Под социальной инженерией понимается использование психологических методов, приемов и манипуляций с целью выманивания у потерпевшего конфиденциальной информации либо побуждения его к совершению иных действий в интересах злоумышленника. | * Побуждение указанным способом потерпевшего к установке на используемое им техническое устройство программ удалённого доступа;
* злоумышленник выманивает у потерпевшего реквизиты банковской карты, пин-код, пароль «мобильного банка», информацию содержащуюся в СМС-уведомлении, поступившей на телефонный номер потерпевшего, для тайного проникновения в систему дистанционного банковского обслуживания в обход системы безопасности;
* неустановленное лицо представившись сотрудником правоохранительных органов под предлогом «закрытия» уголовного дела в отношении близкого родственника понуждает потерпевшего перевести на счет злоумышленника денежные средства.
 |
| 094 | неправомерный доступ к компьютерной информации | Неправомерным считается доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты. | Преступник путем взлома логина и пароля потерпевшего получает неправомерный доступ к его электронной почте (личной странице в социальных сетях и д.р.) после чего использует ее для рассылки рекламных сообщений, совершения преступлений, представившись другим человеком, чтения личной переписки потерпевшего и т.д. |
| 072 | создание вредоносных компьютерных программ либо иной компьютерной информации | Создание программ представляет собой деятельность, направленную на разработку, подготовку программ, способных по своему функционалу несанкционированно уничтожать, блокировать, модифицировать, копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации. | Лицо разрабатывает программу для хищения денежных средств с банковского счета граждан для ее последующей реализации в сети «Интернет». |
| 055 | вредоносных компьютерных программ | Вредоносными компьютерными программами признаются программы способными по своему функционалу несанкционированно уничтожать, блокировать, модифицировать, копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации. | * Преступник размещает на сайте ссылку, при переходе на которую, потерпевший скачивает себе на телефон вредоносное программное обеспечение, с помощью которого у него похищают денежные средства;
* преступники рассылают SMS сообщение, содержащее ссылку на вредоносное программное обеспечение, блокирующее телефон пользователя.
 |
| 073 | распространение вредоносных компьютерных программ либо иной компьютерной информации | Под распространением вредоносных программ понимается предоставление доступа к ним любому постороннему лицу любым из возможных способов, включая продажу, прокат, бесплатную рассылку по электронной сети, то есть любые действия по предоставлению доступа к программе сетевым или иным способом. | * Лицо размещает в сети «Интернет» вредоносное программное обеспечение;
* лицо направило группе лиц вредоносное программное обеспечение по каналам электронной почты.
 |
| 089 | операции с цифровой валютой | Цифровой валютой признается совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам. | * Для продажи наркотических средств преступник использует криптовалютный кошелек на который получают денежные средства, полученные от реализации наркотических средств;
* злоумышленник использует криптовалютный кошелек для легализации денежных средств, полученных преступным путем.
 |
| 088 | электронных платежных систем | Под системой электронных платежей понимается система расчетов между финансовыми организациями, бизнес организациями и интернет пользователями при покупку-продаже товаров и услуг через Интернет | * Преступник предоставляет потерпевшему реквизиты «волшебного кошелька» при пополнении которого потерпевшему обещают удвоение денежных средств. После чего денежные средства не возвращаются, преступник перестает выходить на контакт.
 |
| 095 | операции с цифровыми финансовыми активами | Цифровыми финансовыми активами признаются цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов в порядке, установленном настоящим Федеральным законом, выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы. | * Преступник использует цифровой финансовый актив, через который легализует полученные преступным путем денежные средства;
* злоумышленник незаконным способом получает доступ к цифровым финансовым активам организации и при помощи мошеннических действий создает требование по передаче денежных средств в пользу третьих лиц.
 |
| 126 | сети Даркнет (теневой сети Интернет) | Код предусмотрен для отражения сведений об использовании преступником сети Даркнет (теневой сети Интернет), под которой понимается скрытая (одноранговая) сеть, соединения которой устанавливаются по типу p-2-p (peer-to-peer, децентрализованная сеть). | Преступник для приобретения наркотических средств заходит в Даркнет и на определенном сайте осуществляет их покупку с почтовой доставкой на территорию округа |
| 130 | бот-сетей (ботнет) | Код предусмотрен для отражения сведений об использовании преступником бот-сетей (ботнет), под которыми подразумевается компьютерная сеть, состоящая из узлов с запущенным однотипным централизовано управляемым вредоносным программным обеспечением. | С компьютера пользователя, зараженного специальной бот-программой осуществляется рассылка сообщений или DDos-атака. |
| 092 | SIP-телефонии | Код предусмотрен для отражения сведений об использовании преступником при совершении преступления технологии SIP-телефонии.Под SIP-телефонией понимается система звонков через сеть Интернет с использованием протокола IP на обычные телефонные сети передачи голосовой информации (подвижной или стационарной). В ряде случаев злоумышленники также используют технологию подмены виртуального номера в SIP-телефонии и потерпевшему поступает звонок, как бы с официального номера учреждения (банка, компании и т.п.). К примеру, такой номер, как правило, указан на оборотной стороне банковской пластиковой карты.  | Например, потерпевшему с номера (495) 955-15-21 позвонил неизвестный, который представился сотрудником банка и завладел обманным путем паролем «мобильного банка», после чего тайно похитил со счетов жертвы деньги путем перевода их на иные счета. На первый взгляд звонок потерпевшему был со стационарного телефона г. Москвы (код-495). Вместе с тем, телефонный номер принадлежит номерной емкости оператора связи, использующего SIP-телефонию, следовательно, звонок осуществлен с помощью Интернета, и злоумышленник мог находиться в любом месте, в том числе за пределами г. Москвы.  |
| 127 | фишингового (поддельного) сайта | Для совершения преступления злоумышленники создают в сети «Интернет» сайт похожий по своему написанию с официальным сайтом какой-либо компании (интернет-магазина и т.д.). После приобретения на нем товаров или услуг, они потерпевшему не отправляются, денежные средства за них не возвращают. | * Преступник создает сайт с названием Oz0n.ru (схожий с адресом интернет-магазина Ozon.ru) на котором осуществляются продажа товаров по цене значительно ниже остальных цен в Интернете. Через определенный промежуток времени сайт закрывается, товары потерпевшим не отправляются, денежные средства не возвращаются;
* преступник создают сайт схожий по написанию с сайтом популярной социальной сети, при регистрации на которой пользователь вводит свои установочные данные (пароли от электронной почты), которые в последующем использует злоумышленник;
* Преступник создает поддельный сайт по продажи товаров, при оплате которых потерпевший вводит реквизиты своей банковской карты, с которой в последующем похищаются денежные средства;
 |
| 128 | «программ-шифровальщиков» | Код предусмотрен для отражения сведений об использовании преступником «программ-шифровальщиков»,представляющих собой разновидность вредоносных программ, которые с помощью различных алгоритмов шифрования блокируют доступ пользователей к файлам на компьютере. | Потерпевший получает по электронной почте письмо, содержащее ссылку на вредоносное программное обеспечение, осуществляющее блокировку к файлам пользователя на компьютере. Для разблокировки потерпевшему следует отправить денежные средства на счета злоумышленников. |
| 129 | «фишинговых рассылок» | Код предусмотрен для отражения сведений об использовании преступником «фишинговых рассылок», под которыми понимается тактика рассылки мошеннических электронных писем, направленных на то, чтобы обманом заставить получателей активировать вредоносную ссылку или вложение. | Злоумышленник производит рассылку SMS сообщений, содержащих информацию о выигрыше потерпевшим денежного приза или выгодных предложений по инвестиции денежных средств в акции крупных компаний, после перехода по прилагаемой ссылке происходит заражение телефона вредоносным программным обеспечением. |
| 131 | DDoS-атак | Код предусмотрен для отражения сведений об использовании преступником DDoS-атак, представляющих собой распределенную атаку типа «отказ в обслуживании» с одновременным использованием большого числа атакующих компьютеров, целью которой, как правило, является воспрепятствование доступу легитимных пользователей к атакуемому ресурсу, частичное нарушение штатного функционирования информационной инфраструктуры и т.д. | На сайт потерпевшего одновременно с различных компьютеров осуществляется направление запросов, которые блокируют доступ остальных пользователей или затрудняют доступ к ним. |
| 132 | технологий «Дипфэйк» | Код предусмотрен для отражения сведений об использовании преступником технологий «Дипфэйк», под которыми подразумевается методика синтеза аудио или визуальной информации, основанная на искусственном интеллекте, с целью создания сравнимой с оригиналом копии аудио или видеоизображения. | Злоумышленник с использованием специального программного обеспечения подделывают голос звонившего и представившись знакомым (родственником) просит перевести денежные средства для решения проблем личного характера.  |
| 133 | специальных средств и техники, предназначенных для компрометации банковских устройств самообслуживания (банкоматов, терминалов) | В случаях использования преступником специальных устройств позволяющих считывать информацию о банковской карте (номер карты, ФИО владельца, CVV код и д.р.), размещаемых на банковских устройствах самообслуживания или блокирующих возврат банковской карты после проведения операций по ним.  | После проведения банковских операций на устройстве самообслуживания у потерпевшего происходит блокировка банковской карты. Во время звонка на заранее подготовленный злоумышленниками (приклеенный на банкомате) номер телефона потерпевшие сообщают преступникам Pin код от карты. В последующем злоумышленники извлекают банковскую карту и похищают с нее денежные средства. |
| 057 | компьютерной техники | В случае использования при совершении преступления специальной компьютерной техники. | * Злоумышленник похищает денежные средства из банкомата при помощи подключения к нему специальных устройств;
* преступник, получив физический доступ к серверной комнате организации с использованием заранее подготовленного носителя информации похищает хранящуюся на нем базу данных.
 |
| 134 | информационной инфраструктуры иностранного государства (или придание такого вида) | Код предусмотрен для отражения сведений об использовании преступником информационной инфраструктуры иностранного государства (или придание такого вида), под которой, в том числе понимаются зарубежные серверы (услуги хостинг-провайдеров, интернет-провайдеров, почтовых серверов), доменные зоны, телефонные сети и т.д. | Преступник рассылают сообщения о заведомо ложном акте терроризма с почтового адреса иностранного государства. |
| 135 | информационной инфраструктуры стран-участников СНГ (или придание такого вида) | Код предусмотрен для отражения сведений об использовании преступником информационной инфраструктуры стран-участников СНГ (или придание такого вида), под которой в том числе понимаются серверы стран-участников СНГ (услуги хостинг-провайдеров, интернет-провайдеров, почтовых серверов), доменные зоны, телефонные сети и т.д. | Преступники рассылают сообщения о заведомо ложном акте терроризма с почтового адреса страны СНГ. |
| 059 | программных средств | При использовании злоумышленниками для совершения преступления специального программного обеспечения | * Злоумышленник при помощи специального программного обеспечения получает доступ к мобильному телефону потерпевшего;
* преступник получают несанкционированный доступ к сайту государственного органа при помощи специального программного обеспечения;
* злоумышленник при помощи мобильного приложения, предоставляющего доступ к онлайн банкингу, похищает денежные средства потерпевшего.
 |
| 060 | фиктивных электронных платежей | При использовании преступниками поддельных адресов платежных систем, через которые потерпевшие переводят денежные средства на счета злоумышленников, либо через которые происходит компрометация конфиденциальной информации банковской карты или реквизитов доступа к онлайн кошельку потерпевшего | * На адрес электронной почты приходит письмо о необходимости смены пароля к онлайн кошельку Yandex Money. Прикрепленная к письму ссылка отсылает на мошеннический сайт внешне схожий с сайтом Yandex Money. После введения конфиденциальной информации с онлайн кошелька происходит хищение денежных средств.
 |

1. В случаях, если в процессе расследования уголовного дела устанавливаются ранее неизвестные сведения, указанные реквизиты подлежат корректировке.