1. Криминалистическая характеристика мошенничества с использованием информационно-коммуникационных технологий.
2. Проведение проверки по заявлениям о мошенничестве с использованием информационно-коммуникационных технологий.
3. Особенности расследования мошенничества с использованием информационно-коммуникационных технологий

1. Криминалистическая характеристика мошенничества с использованием информационно-коммуникационных технологий.

Данные криминалистической характеристики мошенничества, составляют наиболее важную информацию о способе хищения, которые создают основу для профилактики данного вида уголовно-наказуемых деяний, а в случае совершения - способствуют раскрытию и расследованию преступлений.

В криминалистической характеристике мошенничества с использованием сети Интернет особую значимость имеет раскрытие содержания способа совершения преступления.

Проанализировав наиболее распространенные пути завладения имуществом в сфере информационно-коммуникационных технологий, необходимо выделить три основных способа совершения данного вида преступлений, которые являются производными для всего разнообразия мошеннических действий в сфере информационно-коммуникационных технологий: с использованием сети Интернет и с использованием операторов связи, с использованием нейросети.

1.Завладение имуществом с использованием сети Интернет:

1.1. Под предлогом покупки товара, аренды, оказания услуг.

Фишинг – это вид интернет-мошенничества, при котором злоумышленники пытаются получить доступ к личной информации, такой как пароли, номера кредитных карт и другие конфиденциальные данные, путем выдачи себя за доверенное лицо или организацию.

Преступники, обладая навыками программирования, применяют специальные программы для скачивания программного кода веб-страниц использующихся для создания копий веб-сайтов. В этом случае мошеннику не понадобится помощь профессиональных программистов имеющих серьезные технические навыки и знание языков программирования HTML и CSS.

Мошенниками создается веб-сайт с регистрацией доменного имени, на котором расположен фиктивный популярный интернет-магазин по продаже различных популярных товаров по недорогой цене. Например «21 vek-off.by.», вместо «21 vek.by» или Mark Farmelle вместо Mark Formelle [30; 31].

Как правило, причиной дешевизны называют большую скидку по надуманному поводу, например распродажа либо «черная пятница» и т.п.

В данном случае мошенники прекрасно понимают, что покупатель всегда проявит интерес к нужному ему товару, стоимость которого значительно ниже той, по которой он реализуется в других магазинах. Продажа товара в данном магазине проводится только по предварительному безналичному расчету. Посетитель заходит на интернет-страницу и оформляет сделку – вносит предоплату за товар или услугу, уверенный в надежности известной компании, однако товар после оплаты к потребителю не поступает.

Фишинговая веб-страница может иметь сходство также и с разными сервисами: Kufar, Белпочта, Беларусбанк и т.д.

Потерпевший при переходе на вышеуказанную страницу вводит персональную информацию (реквизиты банковской карты, личный номер, пароль для входа в личный кабинет и т.п.) которая, после обработки позволяет преступнику совершить хищение денежных средств через дистанционную систему банковского обслуживания (Интернет-банкинг, мобильный банкинг) либо онлайн-сервисы [32; 33; 34, с. 106].

Для распространения ссылок на сайты используется спам в виде рассылок на электронную почту, в ходе обмена сообщениями в социальных

сетях, фиктивных объявлений от популярных интернет-магазинов либо онлайн-сервисов.

1.2. Под предлогом заработка.

Предложения различных видов удаленной работы.

Внесение страхового взноса. Потерпевший в сети Интернет находит объявление о выполнении работы по месту жительства или в других помещениях по выбору, но не в производственных помещениях работодателя, за вознаграждение с целью производства товаров или услуг, согласно указаниям работодателя. Перед началом работы мошенники просят потерпевшего внести страховой взнос и только тогда вышлют задание, обещая вернуть взнос после выполнения работы [35, с. 100].

Изготовление (сортировка, сборка, фасовка) товара из материалов заказчика. Соискателю на предложенную должность предлагают выкупить материалы для изготовления, оплатить часть расходов и после перевода денег мошенники прекращают общение.

Просмотр товаров в интернет-магазинах. Схема работает по принципу пирамиды: нового сотрудника просят внести на счет «работодателя» небольшую сумму денег, которая будет увеличиваться ежеминутно от числа просмотров товаров в интернет-магазинах. Чем больше человек вкладывает собственных средств, тем больше обещают доходность. Но вывести якобы «заработанные» деньги у потерпевшего не получится, поэтому он просто теряет свои средства.

Притворяясь потенциальными работодателями, мошенники часто получают от потерпевшего личную информацию (паспортные данные, номер страхового свидетельства государственного социального страхования и т.д.), которое затем используют для совершения преступлений [36; 37].

1.3. Под предлогом получения дохода.

Схема Памп и дамп (Pump and dump). Переводится как «накачка и сброс». Данная схема появилась еще в 30-е годы прошлого века. Биржевые маклеры по телефону продавали акции ранее неизвестных компаний, за что

получали хорошее вознаграждение. За счет высокого спроса цена акций значительно возрастала. Как только количество желающих купить акции заканчивалось, компания продавала акций на пике их стоимости, что влекло за собой обвал цены и убытки для акционеров. В это суть данного вида мошеннической схемы: при помощи различных манипуляций поднять цену на какой-либо актив, а затем дорого его продать.

В настоящее время данная схема работает не только с акциями, но и перешла на рынок **криптовалют.** Сейчас существует тысячи криптовалют многие из которых дешевы и имеют низкую капитализацию. Используя мессенджеры и социальные сети мошенники создают целевые группы для заработка денежных средств. Администраторы группы, размещая на канале новости, актуальную статистику, экспертные оценки, утечки инсайдерской информации и т.п. постепенно продвигают какую-либо криптовалюту не имеющую под собой ценности и потенциала. Перед основным ростом данной валюты происходит несколько пробных, цель которых посмотреть общее настроение держателей электронных денег и убедить их, а также иных участников группы купить либо продолжить покупку виртуальных денежных единиц. Как итог – получение огромной прибыли администраторами сообщества после продажи криптовалюты на пике ее роста и денежные потери для остальных участников целевой группы [38, с. 132].

Онлайн-казино. Фактически это интернет-площадка (сайт или специальная программа) позволяющая играть в Интернете в азартные игры. Привязка к сайту происходит через аккаунт, процесс развития происходит через стимулирующие бонусы и привилегии от количества внесенных денежных средств.

Для привлечения новых игроков и внесения ими депозитов продвигается реклама онлайн-казино: раскрутка через известных блоггеров, создание в социальных сетях аккаунтов людей, которые научились обыгрывать казино, создание в мессенджерах канала по сливу выигрышных схем, видеореклама на различных интернет-платформах и т.п.

Существует два способа обмана: игра на свои деньги, игра на чужие деньги.

В игре на свои деньги потерпевший не понимает, что обыграть казино невозможно, так как все ставки и выигрыши по ним полностью контролируются администрацией сайта. Для того чтобы вывести выигрыш с депозита необходимо сделать определенное количество ставок, имеются и иные ограничения. Как правило человеку сначала позволяют немного выиграть для того чтобы подогреть интерес, но не всегда достаточно что бы вывести деньги из игры.

Дополнительно мошенники используют схему финансовой пирамиды, в которой проигравшимся игрокам для пополнения их депозита или начисления определенных бонусов предлагают привести в онлайн-казино новых клиентов.

В игре на чужие деньги мошенник, часто связанный с онлайн-казино за определенный процент от нахождения новых клиентов, выступает в качестве работодателя, находя жертву в социальных сетях, мессенджерах, по электронной почте, на специально созданном для обмана сайте. Далее мошенник делится четким алгоритмом действий по игре в онлайн-казино, который приносит стабильный доход. При этом, чтобы не испугать потерпевшего мошенник открывает аккаунт, сам оплачивает игровой взнос за жертву, обучает тонкостям игры и дает задание наиграть определенную сумму для чего рекомендует на какие сайты онлайн казино заходить и на каких игровых столах делать ставки. Когда жертва выигрывает заданную сумму, мошенник под различными предлогами отказывает в выплате. Потерпевший убедившись, что схема работает и проносит прибыль, вносит свои денежные средства для продолжения игры. В другом случае злоумышленник, отказывая в выплате, предлагает стать партнерами и внести потерпевшему часть своих денег на пробный счет для продолжения игры с общим банком [39, с. 138].

1.4. Под предлогом знакомства в социальных сетях.

Данный вид мошенничества играет на эмоциональной стороне жертвы, чтобы заставить **отдать ценные подарки, перевести деньги или личные данные.** Злоумышленник создает фейковые профили на легальных сайтах знакомств в Интернете. Как только потерпевший вступит в контакт с мошенником, тот выразит сильные любовные чувства за относительно короткий период времени и предложит перенести отношения с веб-сайта на телефон, электронную почту или мессенджеры, Преступник путем психологических приемов сделает все возможное, чтобы завоевать у жертвы доверие и дать почувствовать, что эти отношения на всю жизнь. Как только это произошло мошенник под различными предлогами (нужны деньги на авиабилет, чтобы приехать, болезнь родственника, финансовые трудности и т.п.) явно или скрытно попросит деньги или данные банковской карты [40].

В других случаях, после знакомства мошенник, как правило, женщина предлагает сходить в кино либо театр и рекомендует пройти по ссылке на сайт где продают билеты. Данный сайт является фишинговым. Потерпевший совершает покупку билет и с его карты списываются деньги, однако, на сайте возникает сообщение об ошибке и необходимости повторно провести операцию. Снова происходит покупка билетов, со счета повторно списываются деньги, но билеты не появляются, и приходит новое сообщение с извинениями за допущенную ошибку и просьбой снова предоставить данные банковской карты. В итоге деньги списываются в третий раз [41, с. 215].

1.5. Под предлогом блокировки системы компьютера.

Такая методика вымогательства основана:

на обратимой блокировке работы компьютера. Типовые примеры — Trojan.Win32.Agent.il (он же Trojan.Griven), Trojan.Win32.Krotten;

на шифрации или обратимом искажении данных пользователя. Наиболее известный пример — троян Gpcode.

Перечисленные операции выполняются на пораженном компьютере при помощи троянской программы, после чего пользователю предлагается

заплатить злоумышленнику некоторую сумму за «противоядие». Причем если в случае повреждений настроек операционной системы, как правило, можно без особых проблем восстановить работу компьютера, то в случае применения несимметричного шифрования требуются создание утилиты-дешифратора и подбор ключа для расшифровки файлов.

Троянская программа получила свое название от мифологического коня, с помощью которого обманом была захвачена Троя, так как она проникает в систему под видом какой-либо полезной программы. Трояны не самовоспроизводятся и не распространяются сами по себе.

С помощью программы Troyan.Winlock. после блокировки компьютера приходит сообщение от имени правоохранительных органов, что компьютер заблокирован за копирование либо просмотр видео с педофилией и т.п. Для разблокирования компьютера и не привлечения к ответственности потерпевшему предлагается перевести денежные средства на электронный кошелек [42, с. 67-68].

1.6. Под предлогом блокировки электронных кошельков.

Аналогично мошенничеству под предлогом блокировки системы компьютера, злоумышленники поступают при взломе электронных кошельков. Доступ к ним, как правило, получают через троянские либо вирусные программы.

1.7. Под предлогом победы в рекламном розыгрыше.

Мошенники используют различные предлоги: письмо, поступившее на электронную почту, текстовое сообщение в мессенджере, звонок на мобильный телефон, рекламное предложение в социальных сетях пройти тест и стать участником розыгрыша в связи с юбилеем известной компании, уведомление из онлайн-магазина на фейковую страницу которого был подписан гражданин.

Все предлоги ведут к одному – потерпевшему сообщается о победе в розыгрыше или лотерее. Однако, для того чтобы забрать приз победителю

предлагается заплатить некоторую комиссию за выдачу выигрыша (государственный налог, курьерские расходы, оплата за доставку и т.п.) для чего перевести деньги на указанный преступниками счет [44, с. 33].

Во многих мошенничествах с лотереями используются названия законных лотерейных организаций или иных известных компаний, которые не причастны к мошенничеству, но их узнаваемые названия являются хорошей маскировкой для преступников.

1.8. Под предлогом одолжить деньги с использованием социальных сетей или месенджеров (письмо от друга).

Один из самых популярных способов – просьба занять деньги со взломанных аккаунтов от имени владельца профиля. Обычно такие сообщения идут от близких друзей либо родственников. Войдя на взломанную страницу мошенники начинают вести переписку в сообщениях, располагая жертву к диалогу. Как только общение налаживается, под разными предлогами просят определенную сумму в долг [42, с. 67].

1.9. Под предлогом сбора денег для оказания материальной помощи.

Реализуется двумя путями. Первый - создание лже-сайтов благотворительных организаций для сбора денег на различные пожертвования с подменой банковских счетов организаций своими собственными.

Второй путь – создание сайта для помощи больным детям, жертвам террористических актов, природных катастроф и т.п. В Интернете распространяется фото с больным ребенком, рассказывается история, о том, что родители не могут оплатить дорогостоящую операцию и прилагается перечислить деньги на предлагаемый расчетный счет [24, с. 147].

2. Завладение имуществом с использованием операторов телефонной связи:

2.1. От имени должностных лиц финансовых учреждений.

Звонок из банка. Преступники совершают звонок потерпевшему от имени сотрудников службы безопасности банка и сообщают, о том, что с его

банковской карточки неизвестные пытались снять денежные средства и подтверждает ли он перевод денег на другой счет. Далее в ходе беседы, используя психологические и социологические приемы, выясняют у потерпевшего сведения о наличии банковских платежных карточек (далее – БПК), сроках их действия, CVV (CVC)-кодах, паспортных данных, смс-кодах после чего совершают хищения денежных средств [45, с. 13].

Чтобы скрыть свое настоящее месторасположение, злоумышленники совершают их с помощью IP-телефонии (это мобильная телефонная связь, которая работает через сеть Интернет). Аббревиатура IP (Internet Protocol) расшифровывается как «межсетевой протокол». На его базе компьютеры и другие устройства распознают друг друга и безошибочно обмениваются голосовыми сообщениями. Фактически IP-телефония это специальные приложения для персональных электронных вычислительных машин (далее – ПЭВМ) и мобильных устройств для соединения и общения с абонентами стационарных телефонных сетей и мобильных устройств. С ее помощью можно совершать подмену любых номеров и осуществлять звонки либо с несуществующего номера либо от лица любого абонента [46, с. 204-205].

Кроме этого, преступники, используют мессенджеры Viber и WhatsApp в которых существует возможность использования виртуальных номеров. После регистрации таких номеров в мессенджерах, мошенники осуществляют звонки потерпевшим и под различными предлогами выманивают у них требуемые сведения.

В настоящее время разработаны различные телефонные системы «антифрод, которые позволяют отслеживать подмену номера при передаче вызова в сеть другого оператора. В Республике Беларусь компания А1 рекламирует «антифрод», который позволяет не только отслеживать поддельные номера, но и выявлять даже самые сложные схемы мошенничества на вебсайте и в мобильном приложении банка в режиме реального времени, еще до совершения транзакции.

2.2. От имени должностных лиц государственных органов.

Аналогичны преступлениям от имени должностных лиц финансовых учреждений. Мошенники под видом работников правоохранительных органов осуществляют звонки гражданам через мессенджеры под различными предлогами (попадание близкого человека в ДТП, помощь в поимке злоумышленников, контроль за транзакциями и т.п.). В последнее время общение потерпевшего с мошенником происходит по видеосвязи, где в качестве доказательств приводится обстановка «служебного кабинета», высылаются фотоизображения служебного удостоверения, подложные бланки о неразглашении полученной информации и т.п. [47, с. 358-359]

Цель общения – получение личных данных, сведений о банковской карте, паролях, а также получение кредитов для проведения оперативно-розыскных мероприятий с целью поимки злоумышленников, перевод денег на безопасную банковскую карту, установку вредоносного программного обеспечения на смартфоны либо персональные компьютеры.

Наряду с выделенными основными группами способов (исходя из анализа современной правоприменительной практики) прогнозируя возникновение новых способов, следует вести речь и о наличии в ближайшем будущем третьей группы.

Завладение имуществом с использованием нейросетей (искусственный интеллект).

Идеи создания искусственного интеллекта зародились в Соединенных Штатах Америки в средине прошлого века. Нейросети являются составной частью искусственного интеллекта, представляющих собой некие компьютерные модели, имитирующие деятельность человеческого головного мозга. Функционирование нейронных сетей основано на обработке и анализе Больших данных (Big data), на обмене информацией между множеством искусственных нейронов, которые находятся во взаимосвязи друг с другом, на постепенном обучении нейросети – адаптации к запросам пользователя [48, с 85].

Классической задачей для искусственных нейросетей является распознавание (классификация) образов – например, буквенно-цифровых символов (как в программе FineReader) или лиц людей (как при поиске фотографий в Google или Yandex), однако способность нейросетей к обучению сделала возможным выполнение ряда задач, одной из которых является моделирование [49, с. 46]. Умение нейросети автоматически обрабатывать изображения и речи и генерировать на их основе новый контент были взяты на вооружение преступниками при совершении мошенничеств.

Дипфейк (deepfake) – это технология, которая использует нейронные сети для создания фальшивых видео, где лица и голоса людей могут быть заменены на другие.

Замена лиц на фотографиях уже много лет является обычной практикой в Fhotoshop, создание дипфейковых роликов стало более поздней разработкой. Со временем технология усовершенствовалась до такой степени, что для создания убедительного дипфейка видео требуется небольшое количество фотографий либо вообще одна. Программа использует синтез человеческого изображения – объединяет несколько картинок, на которых человек запечатлен с разных ракурсов и с разным выражением лица, и делает из них видео. Анализируя фотографии, специальный алгоритм «учится» тому, как выглядит и может двигаться человек. Работают две нейросети. Первая генерирует образцы изображения, вторая – отвечает за то, чтобы отличать настоящие образцы от поддельных [50, с. 213]

Для создания дипфейка аудио, программе может потребоваться всего лишь пять секунд звука, чтобы успешно скопировать голос человека.

В настоящее время технологии дипфейка используются двумя способами. Первый рассчитан на конкретного человека. Осуществляется звонок подчинённому, имеющему возможность перевода денежных средств компании, якобы от его руководителя. Голос руководителя, сгенерированный

искусственным интеллектом, требует от подчиненного совершить платеж под каким-либо предлогом который и выполняет поручение.

Второй, начавший распространение, в том числе и на территории нашей страны, рассчитан на массовую аудиторию, реализуется в форме рекламы псевдоинвестиционных компаний, Для придания значимости и большей достоверности в распространяемой видеорекламе участвуют популярные политические и медийные личности, которые смонтированным голосом агитируют вкладывать денежные средства или криптовалюту под большие проценты [51].

В 2022 году в Беларуси зарегистрирован новый способ мошенничества с использованием нейросетей. *Неизвестные пытались выманить деньги у родственников человека, пропавшего без вести несколько лет назад. Злоумышленники потребовали выкуп за освобождение человека, в доказательство, прислав родственникам видеозапись с без вести пропавшим на которой он, как ни в чем не бывало, сидит на стуле. В ходе проверки установлено, что лицо жертвы было взято из фотографий о его поиске и при помощи нейросети внедрено в видеозапись [52].*

Как уже отмечалось выше, 3-й этап развития Интернет-мошенничества характеризуется **созданием и функционированием преступных групп, которые объединяют различные способы для достижения большей эффективности по обману граждан.**

Так, организация работы колл-центры, специализирующиеся на завладении имуществом с использованием операторов телефонной связи состоит из нескольких этапов:

организационные мероприятия: покупка либо кража баз данных потенциальных жертв (базы данных мобильных операторов, клиентов магазинов, банков и т.п.), осуществление дополнительного сбора сведений через Telegramm-боты.

На основном этапе, представляясь сотрудником банка или правоохранительных органов сотрудник колл-центра устанавливает контакт с

потерпевшим, согласно заранее разработанным сценариям с использованием методов социальной инженерии, получает информацию о его счетах. Ранее полученные сведения о жертве, создают у потерпевшего ощущение, что с ним действительно разговаривает должностное лицо. Если на счету жертвы имеется значительная сумма, то мошенники вынуждают ее обналичить денежные средства, при их отсутствии – пытаются подвести к необходимости взятия кредита у жертвы. Во время происходящего разговора мошенник запрашивает у потерпевшего максимальный набор данных по его банковским продуктам (счета, карты, баланс, операции) и с помощью конструктора фишинговых сайтов создает веб-страницу с поддельным личным кабинетом, скриншоты которых он может присылать потерпевшему.

В случае необходимости, сотрудник может соединить потерпевшего с одним из наиболее опытных сотрудников колл-центра с отработанными навыками убеждения, берущего на себя роль руководителя банка либо сотрудника правоохранительных органов, что позволяет преступникам создавать иллюзию, что только выполняя все инструкции он сможет избежать потери своих денежных средств.

Заключительный этап состоит из вывода денежных средств. Первоначально деньги потерпевшего попадают на счет к «дропу» – человеку, который используется для получения и дальнейшей отправки товаров и (или) денежных средств в другое государство либо предоставляет счет для проведения операций другими людьми [53, с. 357], после чего организуется обналичивание денег потерпевшего с дроперского счета и дальнейший их перевод на «чистые» счета либо криптокошельки.

Организационно, преступная группа скамеров (от англ. scam – мошенничество), работающая в сфере интернет-мошенничества, включает в себя:

организаторов, которые формируют преступную группу, поддерживают связь между ее участниками с помощью чата в мессенджерах,

регистрируют новые банковские счета, покупают новые абонентские номера, распределяют доходы между участниками группы [54, с. 101];

«кодеров» – участников организованной преступной группы скамеров, которые разрабатывают программные продукты для организации преступной деятельности скам-группы и автоматизации совершения хищений. Одним из таких продуктов являются телеграмм-боты, с появлением которых преступникам не нужно создавать фишинговые страницы, воркеру достаточно прислать в бот ссылку на нужный товар, после чего бот сам создает ссылки на страницы курьерской службы, оплату и возврат товара;

«прозвонщиков» - участников организованной преступной группы скамеров выступающих в роли «операторов» службы поддержки курьерских сервисов. Связавшись с жертвой по телефону или в мессенджерах, они предлагают оформить возврат денежных средств, однако при этом происходит повторное списание средств с банковской платежной карточки потерпевших. Прозвонщики» обладают хорошими навыками в социальной инженерии, готовы с ходу ответить на самые неожиданные вопросы сомневающихся покупателей;

воркеров – участников организованной преступной группы скамеров, в обязанности которого входит общение с потенциальными потерпевшими в целях убеждения последних перейти на фишинговую веб-страницу и указать там реквизиты БПК [53, с. 356];

«вбиверов» – участников организованной преступной группы скамеров, в обязанности которого входит быстрый перевод денежных средств с карт-счетов потерпевших на контролируемые преступниками банковские счета или электронные кошельки. [53, с. 355].

В настоящее время на территории Содружества Независимых Государств (СНГ) существует не менее 10 русскоязычных групп, работающих в сфере интернет-мошенничества (WinkyTeam, VendettaCorp., BruddaTeam, ForceTeam, TheEagleTeam и др.), жертвами которых становятся

граждане стран ближнего и дальнего зарубежья. Годовой доход таких преступных групп оценивается более чем в 5 млн долларов США [54, с. 101].

Главным управлением цифрового развития предварительного следствия Следственного комитета Республики Беларусь в январе 2024 года завершено расследование в отношении одного из руководителей крупнейшего транснационального скам-сообщества, работавшего по Беларуси.

Организованная преступная группа была создана в 2021 году. В ее состав входило более 700 участников из Украины, России, Беларуси и других русскоязычных стран. Скам-группа специализировалась на совершении хищений денежных средств с карт-счетов пользователей торговых онлайн-площадок с использованием «фишинговых» интернет-ресурсов, имитирующих такие площадки, сервисы служб доставки, платежные сервисы. С 2021 года по 2023 год участники данной группировки совершили значительное количество хищений путем «фишинга», только у белорусских граждан – более 6 000 хищений на сумму более 1,7 млн рублей.

Составленный «цифровой портрет» помог установить личность 17-летнего минчанина, который оказался «кодером» - ключевой фигурой транснационального скам-сообщества, разработчиком и администратором криминальных программных средств и интернет-ресурсов.

За свою работу молодой человек получал 5% от суммы всех денег, похищаемых скам-сообществом у белорусских граждан. За 1,5 года участия в преступной деятельности группировки до задержания он заработал более 90 000 рублей [55].

Личностью преступника обусловлены объект преступления, место, способ совершения и сокрытия преступления, его мотив, причины и условия, способствующие совершению уголовно-наказуемого деяния, следственные ситуации и т.д. Изучение поведения преступника, некоторых его особенностей и характерных черт может позволить продуктивно расследовать преступление.

Личность преступника необходимо охарактеризовать двумя типами признаков: общими и специальными.

К общим признакам, относятся: пол, возраст, профессия, образование, психологические особенности, отношение к общественным ценностям, и т. п.

Специальные признаки характеризуют личность конкретного преступника: мотив, способы совершения преступлений, наличие преступного опыта, судимость, навыки совершения преступления, наличие связей в преступной среде и т. д

Лица, использующие методы социальной инженерии в первую очередь обладают хорошими коммуникативными качествами, проявляют творческий подход при совершении преступления, любят риск[56, с. 117].

Злоумышленники, использующие вирусные программы, фишинговые сайты - это люди, как правило, с профильным образованием, наличием хороших технических навыков, обладают аналитическим складом ума и логическим мышлением, замкнуты, в реальной жизни некоммуникабельны, практически не имеют друзей.

Основной мотив злоумышленников это корысть, поэтому непосредственным предметом преступного посягательства, по мнению большинства исследователей являются:

1. Денежные средства, полученные преступниками путем предоставления услуг, продажи несуществующей продукции, оформления на фиктивную работу и иных способов;
2. Право на имущество потерпевшего (денежные средства потерпевшего, которые он перечисляет лжеблаготворительному фонду и т.п) ;
3. Какие-либо сведения личного характера (номер банковской карты, пароли к аккаунту и т.п., которые будут использованы при совершении иных преступлений [24, с. 146].

Дудко Т.И. в своей статье «Криминологические особенности личности мошенника в сфере ICO» полагает, что для личности преступника

закономерно сочетание мотивов корысти и утверждения, а некоторым злоумышленникам присущи и игровые мотивы [57, с. 90-91].

Одним из элементов криминалистической характеристики мошенничеств с использованием информационно-коммуникационных технологий является личность потерпевшего.

По сравнению с другими преступлениями пожилые люди более уязвимы для мошенничества, что связано с медленной когнитивной обработкой информации и сильным чувством одиночества.

Также в группу риска входят как мужчины, так и женщины всех возрастов, которые часто используют возможности дистанционного обслуживания и купли-продажи посредством сети интернет.

Если рассматривать психологические характеристики личности, то факторами, влияющими на восприимчивость к интернет-мошенничеству являются люди с низким самоконтролем, так как они немедленно пытаются удовлетворить свои потребности, следуя инструкциям злоумышленника чтобы получить обещанное. Открытость и экстраверсия также увеличивают вероятность ответа на электронное письмо, полученное от неизвестного.

Более подвержены обману люди с эвристическим типом мышления, которое основано на интуиции. Личности с эвристическим мышлением неосознанно принимают решения, которые происходят на основании жизненного опыта, инстинктивных и интуитивных импульсов, так как эвристическое мышление во много зависит от эмоций, предубеждений и неосознанных стереотипов. Обман работает, так как фишинговая атака вводит жертву в заблуждение, заставляя интуитивно быстро, но неверно оценить полученную от преступника информацию.

Немаловажным элементом рассматриваемой криминалистической характеристики являются следы, которые были оставлены в ходе совершения преступления и механизм их образования.

Для мошенничеств в сфере информационно-коммуникационных технологий помимо идеальных и материальных следов также выделяют

виртуальные (цифровые) следы, находящиеся в памяти электронной техники.

Виртуальные следы – это отпечатки любых действий, совершенных в информационном пространстве цифровых (электронных) устройств, их систем и сетей.

Выделяются следующие виды виртуальных следов:

- на электронных устройствах, с помощью которых было совершено преступление: использовавшееся для неправомерного доступа программное обеспечение, сохраненные коды доступа, скопированная у потерпевшей стороны информация, тексты программ и т.п. Такие следы могут остаться в записях операционной системы, на электронных носителях, в аппаратно-программной конфигурации компьютерных средств и др.;

- на «транзитных» носителях информации, посредством которых лицо осуществляло связь с удаленными информационными системами или ресурсами: размещенная в сети информация, электронная переписка и др.;

- в подвергшейся воздействию компьютерной системе, в том числе, на электронных носителях: результаты неправомерного уничтожения, блокирования, модификации компьютерной информации, воздействия на средства защиты информации и несанкционированного доступа к компьютерной системе;

- на иных компьютерных средствах (компьютерах, органайзерах, мобильных телефонах, цифровых фотоаппаратах, видеокамерах, диктофонах, других носителях информации), непосредственно не участвовавших в совершении преступления, но содержащие имеющие значение для уголовного дела сведения.

3. В структуре криминалистической характеристики ключевым элементом является способ совершения мошенничества в сфере информационно – коммуникационных технологий. Анализ практики деятельности органов уголовного преследования Республики Беларусь в рамках изученных исторических этапов позволяет вести речь о двух группах

наиболее распространенных способов: с использованием возможностей сети Интернет, с использованием возможностей операторов телефонной связи.

К первой группе способов необходимо отнести:

завладение имуществом с использованием сети Интернет:

- под предлогом покупки товара, аренды, оказания услуг;

- под предлогом заработка;

- под предлогом получения дохода;

- под предлогом знакомства в социальных сетях;

- под предлогом блокировки системы компьютера;

- под предлогом блокировки электронных кошельков;

- под предлогом победы в рекламном розыгрыше;

- под предлогом одолжить деньги с использованием социальных сетей или месенджеров (письмо от друга);

- под предлогом сбора денег для оказания материальной помощи.

2. Ко второй группе способов необходимо отнести:

завладение имуществом с использованием операторов телефонной связи:

- от имени должностных лиц финансовых учреждений;

- от имени должностных лиц государственных органов.

На ряду с тем, что в настоящее время имеет место активное развитие нейросетей (искусственный интеллект) следует констатировать, что преступная среда будет использовать искусственный интеллект для завладения имуществом пользователей.

2 Проведение проверки по заявлениям о мошенничестве с использованием информационно-коммуникационных технологий.

Целью проведения доследственной проверки является установление наличия либо отсутствия в деянии признаков преступления. Она проводится лишь тогда, когда в действиях конкретно заподозренного лица необходимо установить признаки мошенничества. В случае если в его действиях имеют место признаки ст. 209 УК, то необходимо незамедлительно возбуждать уголовное дело и принимать меры к установлению и задержанию лица, его совершившего.

Исходя из структуры способа совершения мошенничества в сфере высоких технологий, необходимо выделить два основных алгоритма действий органа дознания по проверке заявлений граждан в стадии возбуждения уголовного дела:

- при завладении имуществом с использованием возможностей операторов телефонной связи;

- при завладении имуществом с использованием возможностей сети Интернет либо нейросетей.

В первом случае необходимо подробно опросить заявителя об обстоятельствах произошедшего, а также истребовать информацию:

- об абонентских номерах телефонов пострадавшего лица и лица, совершившего мошеннические действия;

- о номере IMEI устройства пострадавшего лица;

- об операторе связи, посредством которого осуществлялись переговоры с жертвой мошеннических действий;

- о детализации телефонных соединений за период общения пострадавшего лица и лица, совершившего мошеннические действия;

- от операторов мобильной связи УП А1 СООО «Мобильные ТелеСистемы», ЗАО «БеСТ»), РУП «Национальный центр обмена трафика», РУП «Белтелеком» и т.д. для установления личности абонента IP-телефонии

осуществлявшего звонок. От SIP-провайдера оказывающего данную услугу можно получить установочные данные владельца виртуального номера, информацию об иных номерах, арендованных им, реальный абонентский номер и адрес электронной почты, использованные мошенником IP-адреса которые он использовал для подключения к приложению (сайту) по работе с SIP-провайдерами, банковские карты и счета, и другую значимую информацию.

При проведении проверки по заявлениям о данных видах преступлений орган уголовного преследования сталкивается с проблемой установления данных соединения о прохождении вызова от абонента IP-телефонии или социальных сетей, использующего VPN-сервисы и адресное пространство операторов связи и интернет-провайдеров стран, не поддерживающих международное сотрудничество [60, с. 195].

Провести осмотр мобильного телефона потерпевшего, с целью обнаружения номеров, с которых поступали телефонные соединения, в случае если потерпевшим осуществлялись аудиозаписи разговоров либо преступник в ходе общения отправлял голосовые сообщения [61, с. 64].

Запросы в банковские учреждения направляются:

на получение информации о банковской карте (банковском счете) потерпевшего, его полном номере и данных владельца, сведения о совершенных отправителем транзакциях с указанием точного времени проведения приходных и расходных операций, номера и коды транзакций[62, с. 58];

сведения о бенефициаре, его данных, совершенных транзакциях;

запрос на предоставление записей с камер видеонаблюдения в случае обналичивания денежных средств в банкоматах банка.

Во втором случае, при завладении имуществом с использованием возможностей сети Интернет либо нейросетей, необходимо:

опросить потерпевшего об обстоятельствах произошедшего;

направить запрос о предоставлении подробной информации об интернет-сайте или веб-странице сайта хостинг-провайдеру на сервере, которого размещен сайт и регистратору зарегистрировавшего доменное имя данного сайта;

направить запросы об установлении электронных адресов интересующих почтовых ящиков, о предоставлении сведений относительно распространения вредоносной программы, аналогичной той, с использованием которой был заблокирован компьютер потерпевшего.

Запросы в банковские учреждения направляются:

на получение информации о банковской карте (банковском счете) потерпевшего, его полном номере и данных владельца, сведения о совершенных отправителем транзакциях с указанием точного времени проведения приходных и расходных операций, номера и коды транзакций;

сведения о бенефициаре, его данных, совершенных транзакциях;

запрос на предоставление записей с камер видеонаблюдения в случае обналичивания денежных средств в банкоматах банка.

запросы об установлении сведений в отношении пользователей электронных кошельков, при наличии фактов перечисления на них денег.

Согласно с ч.2 ст. 173 УПК до возбуждения уголовного дела может проводиться осмотр компьютерной информации, который является основным процессуальным действием по получению доказательств при совершении мошенничества с использованием сети Интернет либо нейросетей [63]. В зависимости от способа совершения преступления органом дознания может производиться осмотр объявления на различных торговых площадках, осмотр мессенджера (Viber, Telegram, WhatsApp и т.п.) в мобильном устройстве потерпевшего, осмотр фишингового ресурса ;

Подводя итог изложенному необходимо констатировать, что проверка заявления о мошенничестве, совершенном в сфере высоких технологий, организуется органом дознания с учетом особенностей двух сфер

деятельности лиц, совершающих обман либо злоупотребление доверием граждан:

- с использованием возможностей операторов телефонной связи;
- с использованием возможностей сети Интернет либо нейросетей.

3. Особенности расследования мошенничества с использованием информационно-коммуникационных технологий

Анализ практики свидетельствует, что в аспекте рассматриваемой проблемы следует вести речь о трех ситуациях с позиции наличия у органа уголовного преследования доказательственной информации об обстоятельствах, устанавливающих все, либо отдельные признаки состава мошенничества, совершенного в сфере высоких технологий – благоприятная, неблагоприятная, условно – благоприятная.

Считаем, что на их формирование будет влиять ряд факторов:

– наличие первоначальной информация, полученной из заявления о совершенном преступлении (событии преступления и лицах, причастных к нему);

– условия получения данной информации (гласно – доказательства; негласно – оперативные данные);

– имеющиеся в распоряжении органа уголовного преследования силы и средства для дальнейшей организации процесса расследования и использования полученных данных для установления обстоятельств, подлежащих доказыванию;

– наличие противодействия расследованию, как со стороны участников уголовного процесса, так и иных лиц (внутреннее; внешнее);

– иные факторы, влияющие на успешное установление обстоятельств, подлежащих доказыванию по уголовному делу.

Полагаем целесообразным дать краткую характеристику выделенных следственных ситуаций.

Благоприятная – известен способ совершения мошенничества, обнаружены виртуальные следы, известны сведения о субъекте преступления, однако его местонахождение не установлено.

Данная следственная ситуация подразумевает исследование полученной информации о подозреваемом, его проверку на причастность к совершению аналогичных преступлений, установление его местонахождения и задержания, наличие возможных соучастников преступления.

Условно-благоприятная – известен способ совершения мошенничества, обнаружены виртуальные следы, есть сведения, указывающие на возможную причастность определенного лица.

В данной ситуации планирование расследования направлено на дальнейший сбор доказательств, установление свидетелей преступления, взаимодействие с органом дознания по планированию и проведению следственных действий и оперативно-розыскных мероприятий направленных на установления обстоятельств совершенного мошенничества, причастности предполагаемого лица к преступлению.

Неблагоприятная – известен способ совершения мошенничества, виртуальные следы не обнаружены, сведений о преступнике, совершившем мошенничество в сфере высоких технологий не имеется.

Расследование преступления в сложившейся ситуации направлено на выявление следов преступления и сбор доказательств с привлечением технико-криминалистических средств и специалистов, обладающих специальными познаниями в области информационных технологий для последующего доказывания вины подозреваемого в случае его установления.

Резюмируя изложенное констатируем, что на первоначальном этапе расследования мошенничества в сфере высоких технологий складываются три наиболее распространенные следственные ситуации содержание которых обусловлено наличием полученных доказательств об отдельных элементах состава расследуемого деяния.

На первоначальном этапе расследования мошенничества одним из основных источников доказательств, позволяющих установить обстоятельства совершения преступления являются показания потерпевшего, который является, как правило, единственным человеком, который может сообщить сведения об отдельных обстоятельствах совершения преступления.

Допрос данного участника уголовного процесса представляет собой процесс передачи информации о расследуемом событии или связанных с ним обстоятельствах и лицах. Эта информация поступает к допрашиваемому в момент восприятия им тех или иных явлений или предметов, запоминается и затем при допросе воспроизводится и передается следователю [68, с. 600].

Допрос потерпевшего по делам рассматриваемой категории необходимо производить в наиболее кратчайшие сроки после возбуждения уголовного дела, так как со временем в человеческой памяти могут стираться важные детали происшествия.

При подготовке к допросу сотруднику органа уголовного преследования нужно представлять, какую именно информацию он намерен получить у потерпевшего, поэтому основной особенностью допроса потерпевшего по делам о мошенничествах в сфере высоких технологий является обязательность владения следователем, лицом, производящим дознание, прокурором специальными познаниями в области информационных технологий.

На этапе подготовки к допросу необходимо ознакомиться с информацией о функционировании электронных кошельков, осуществлении банковских операций через Интернет и мобильные приложения, об особенностях использования специализированных сайтов и интернетмагазинов, а также получить иную информацию в зависимости от индивидуальных особенностей совершенного преступления [69, с. 161].

Следователю также нужно брать в расчет объективные и субъективные факторы, препятствующие достоверному восприятию потерпевшим событий

преступления. В большинстве случаев, потерпевшие имеют поверхностные представления о современных интернет-ресурсах и банковских операциях, не всегда понимают, какие они совершили действия с помощью ЭВМ или мобильного телефона, повлекшие хищение принадлежащих им денежных средств, по этой причине их показания могут носить искаженный характер. Также потерпевшие из-за неловкости, что их позволили обмануть могут умышленно предоставлять неверную информацию или сглаживать некоторые обстоятельства произошедшего.

Способ мошеннических действий определяет предмет допроса потерпевшего.

При расследовании уголовных дел о хищениях имущества путем использования сети Интернет у потерпевшего необходимо выяснить следующее:

- сведения о сайте, где было опубликовано объявление о продаже товара либо предоставлении услуги («Куфар.by», «Одноклассники», «Белагропромбанк», специализированные интернет-магазины и т.д.);

- полная информация и контактные данные, указанные в тексте объявления;

- совершались ли ранее потерпевшим покупки на данной интернет-площадке;

- как был найден фишинговый сайт;

- обстоятельства переговоров либо переписки с продавцом;

- как осуществлялась покупка товара;

- через какую платежную систему проходила оплата;

- по какой причине принял решение внести предоплату за товар;

- получил ли потерпевший товар, если да то каким способом;

- если товар был передан курьером, то запомнил ли он его приметы;

- когда потерпевший обнаружил, что качество вещи либо сама вещь не соответствует заявленным в объявлении, связывался ли он после этого с продавцом некачественного товара;

- осталась ли у потерпевшего переписка с продавцом либо запись телефонных переговоров.

При расследовании уголовных дел о завладении имуществом с использованием операторов телефонной связи у потерпевшего необходимо выяснить:

- сведения о дате и времени звонка, где в это время находился потерпевший, количество звонков, с каким числом подозреваемых в преступлении он общался, что о них известно, какую обстановку видел потерпевший при видеозвонке, как представлялся преступник, содержание разговора, описание речи, имеется ли южнорусский или украинский акцент, голос картавый, шепелявый, молодой, старый и т.п., наличие фона при разговоре, качество связи (помехи, пропадание слышимости, разговор прерывался, хорошо или плохо был слышен голос и др.);

- возможность опознания преступника по голосу, предоставление голоса звонившего на мобильный телефон в случае записи разговора потерпевшим [69, с. 161; 70, с. 200-201];

- все обстоятельства, при которых потерпевший перевел свои деньги злоумышленнику. Абонентский номер сим-карты, привязанный к банковскому счету, реквизиты банковской карты, электронного кошелька или абонентский номер сотового телефона, на которые были переведены денежные средства мошенникам. Сумма денежных средств находившихся на счете, количество денег списанных со счета, материальный ущерб причиненный потерпевшему.

В ходе допроса следователю необходимо использовать имеющиеся в уголовном деле документы (выписка движения денежных средств по счету, детализация звонков на телефон потерпевшего, и т.д.), что позволит предельно точно восстановить обстоятельства произошедшего.

Таким образом, результаты, полученные при проведении допроса потерпевшего, позволяют выстраивать версии и планировать дальнейшие

действия необходимые для расследования уголовного дела и установления обстоятельств произошедшего.

Осмотр является самостоятельным следственным действием. Он представляет собой непосредственное обнаружение и исследование объектов, имеющих значение для уголовного дела, их признаков, свойств, состояния и взаиморасположения [68, с. 551]. .

Указом № 269 Президента Республики Беларусь «О мерах по противодействию несанкционированным платежным операциям».

2.1 Осмотр объявления на сервисе kufar.by. С участием потерпевшего произвести осмотр размещенного им на интернет-площадке объявления и зафиксировать url-адрес объявления (полный путь к странице объявления), после чего с согласия потерпевшего войти в его профиль и просмотреть количество лиц, осуществивших просмотр объявления и абонентского номера продавца (Профиль/Мои объявления).

Пример: *С участием Ивановой И.И. осуществлен поиск размещенного ею объявления на сайте kufar.by. Установлено, что данное объявление с заголовком «Коляска детская» размещено по адресу: kufar.by/item/99476584. Содержание веб-страницы с объявлением распечатано (Приложение 1). Затем с участием Ивановой И.И. и с ее согласия путем введения предоставленных данных авторизации (логин и пароль) осуществлен вход в ее профиль пользователя, из которого просмотрена статистика по данному объявлению: объявление просмотрено 17 раз, абонентский номер просмотрен 1 раз. Страница объявления из профиля распечатана (Приложение 2).*

2.2 Осмотр мессенджера (Viber, Telegram, WhatsApp) в мобильном устройстве или компьютере потерпевшего. С согласия потерпевшего и с его участием произвести осмотр принадлежащего ему мобильного устройства или компьютера с установленным в нем приложением соответствующего мессенджера и отражением информации об аккаунте пользователя, с которым осуществлена переписка, а также содержания самой переписки. Данную информацию целесообразно сохранить в виде таблицы скриншотов, являющейся приложением к протоколу осмотра. В протоколе осмотра необходимо отразить такие значимые данные, как имя пользователя, абонентский номер, гиперссылка на фишинговый ресурс.

Пример: *С участием Ивановой И.И. и с ее согласия осуществлен осмотр представленного ею смартфона «Samsung SM-1673». При этом осуществлен вход в приложение Viber, в котором просмотрен чат с пользователем «Николай». Скриншот информации о пользователе «Николай» распечатан (Приложение 3). Переписка с пользователем «Николай» распечатана в виде таблицы скриншотов (Приложение 4). В ходе осмотра переписки выявлена следующая значимая информация:*

- аккаунт пользователя «Николай» зарегистрирован с абонентского номера +380992738402;

- пользователем Николай отправлено сообщение со ссылкой на веб-страницу https://ibank-asb.com/sms.

2.3 Осмотр сведений о переводах денежных средств, осуществленных преступником. Для оперативного получения информации о дате, времени, сумме похищенных денежных средств и направлении их перечисления, необходимо принять меры по осмотру соответствующих источников информации, доступных потерпевшему: мобильный банкинг, интернет-банкинг, sms-сообщения о произведенных платежах (с распечаткой скриншотов).

Пример: *Затем произведен вход в приложение «Сообщения», после чего сделаны скриншоты 3 входящих sms-сообщений от сервиса ОАО «Приорбанк», которые распечатаны в виде таблицы скриншотов (Приложение 5).*

2.4 Осмотр фишингового ресурса. В отдельных случаях отправленные потерпевшему сообщения со ссылками на фишинговые веб-страницы после совершения преступления удаляются или подменяются. В этом случае необходимо произвести поиск соответствующей страницы в истории (журнале) браузера устройства потерпевшего.

Если к моменту производства процессуального действия доступ к веб-странице удален или ограничен, следует открыть и распечатать веб-страницу, открывающуюся по фишинговой ссылке.

Если фишинговая страница сохранилась, следует осуществить переход на нее, после чего произвести все действия, предусмотренные формами фишингового сайта, то есть повторить ранее произведенные потерпевшим действия, приведшие к компрометации данных его банковской карты или банковского счета (следует вводить в соответствующие поля форм ***произвольные реквизиты, в том числе вместо поступившего sms-сообщения указывать вымышленный набор цифр или символов***).

Следует учитывать, что большинство фишинговых сервисов использует проверку на корректность 16-значного номера банковской карты по последней контрольной цифре. Для подбора корректного

номера банковской карты и иных произвольных данных для ввода на страницах фишингового сайта разработан специальный скрипт (программа), прилагаемый к настоящим рекомендациям в виде файла **БПК-генератор.html.** Открывать данный файл желательно браузером Google Chrome, инструкция по пользованию приведена внутри файла.

Доказательственное значение имеют не только внешний вид и видимое содержание веб-страниц, но и их **исходный код**. Поэтому каждую открытую страницу необходимо:

1) распечатать в качестве приложения к протоколу осмотра. Если на веб-странице предусмотрен ввод данных, распечатать ее в первоначальном виде и после ввода данных;

2) сохранить исходный код веб-страницы ***(см. приложение 1)***. Фишинговая веб-страница является средством совершения преступления и одновременно содержит уникальные характеристики, которые могут способствовать установлению ее разработчика, свидетельствовать о связи с иными преступлениями. При необходимости исходный код может быть осмотрен с участием специалиста в области веб-программирования либо направлен на компьютерно-техническую экспертизу. При анализе кода может быть выявлена важная следственная информация: ссылки на внутренние и внешние файлы; комментарии разработчика; фрагменты кода, указывающие на особенности функционирования веб-ресурса.

Пример: *На компьютере следователя создана директория (папка) «ibank-asb.com» для сохранения файлов с исходным кодом веб-страниц. Доступ к исходному коду страниц с последующим его копированием осуществлялся с использованием опции браузера Google Chrome, активируемой комбинацией клавиш Cntrl+Shift+I. Исходный код каждой веб-страницы скопирован в текстовый файл, который сохранен с именем, соответствующим имени веб-страницы.*

Посредством браузера Google Chrome осуществлен переход на веб-страницу https://ibank-asb.com/sms. Страница распечатана (Приложение 6). Исходный код страницы сохранен в виде файла с именем «sms». В поле «Введите номер телефона» введен абонентский номер +375333990832, после чего страница повторно распечатана (Приложение 7). Осуществлено нажатие кнопки «получить смс-код». На указанный абонентский номер (телефон РОСК) поступил sms-код «12123».

Загрузилась страница https://ibank-asb.com/sms-kod. Страница распечатана (Приложение 8). Исходный код страницы сохранен в виде файла с именем «sms-kod». В поле «Введите SMS-Kod» введен код «23232», после чего страница повторно распечатана (Приложение 9). Осуществлено нажатие кнопки «Отправить».

Загрузилась страница https://ibank-asb.com/card. Страница распечатана (Приложение 10). Исходный код страницы сохранен в виде

файла с именем «card». В поле «Введите номер банковской карты» введен номер «2673 2342 1242 1235»; в поле «Имя и фамилия (как на карте)» введено: «VASYA VASILYEV»; в поле «Трехзначный код» введено «555», после чего страница повторно распечатана (Приложение 11). Осуществлено нажатие кнопки «Отправить».

Загрузилась страница https://ibank-asb.com/error. Страница распечатана (Приложение 12). Исходный код страницы сохранен в виде файла с именем «error».

По окончании осмотра директория «ibank-asb.com» с сохраненными в нее файлами записана на CD-R-диск, который затем помещен в бумажный конверт, который наклеен на лист формата А4 с пояснительной надписью: «CD-R-диск к протоколу осмотра от 23.07.2020» и опечатан бумажной биркой с оттиском печати №13 «Для документов» УСК по Брестской области с подписью следователя.

2.5 Осмотр голосового сообщения. Если преступник в ходе общения с потерпевшим отправлял голосовые сообщения или осуществлял голосовую связь с потерпевшим и последним велась аудиозапись данного разговора, в ходе осмотра (выемки) скопировать и записать на CD-R-диск аудиофайлы речи злоумышленника. Запись необходимо осмотреть и приобщить диск к уголовному делу в качестве вещественного доказательства.

АЛГОРИТМ
сохранения исходного кода веб-страницы

Предварительно создается новая директория (папка), которой присваивается имя сайта. Например, если открытая нами веб-страница имеет адрес https://kufar-pay.by/order, то созданная директория должна иметь имя «kufar-pay.by». Если пути к веб-страницам имеют многоуровневую структуру, создаются вложенные директории. Например, если осматриваются страницы https://kufar-pay.by/products/131231 и https://kufar-pay.by/orders/131231, то создается директория «kufar-pay.by», внутри которой создаются директории «products» и «orders» и файлы сохраняются в соответствующие директории, повторяя структуру нахождения соответствующих веб-страниц на сайте.

1. В браузере Google Chrome[1] загрузить необходимую веб-страницу и нажать комбинацию клавиш Ctrl+Shift+I.
2. В открывшемся правом фрейме выбрать вкладку «Elements».

[1] В большинстве мобильных версий браузеров отсутствует функция просмотра исходного кода страницы.

3. В одной из верхних строк выделить кликом мыши строку, начинающуюся <html. Нажать правую кнопку мыши.

4. В появившемся меню выбрать пункт «Copy».

5. В появившемся под-меню выбрать пункт «Copy outerHTML». Это действие копирует исходный код страницы в буфер обмена.

6. Открываем текстовый редактор «Блокнот», вставляем туда текст.

7. Сохраняем созданный текстовый файл с тем же именем, которое имеет веб-страница (Например, если страница имеет адрес https://kufar-pay.by/orders/payment/id3384949, сохраняем ее с именем «id3384949» в папке «payment», созданной внутри директории «orders», которая в свою очередь создана в директории «kufar-pay.by»).