НЕДЕТСКИЕ ИГРЫ 2.0

КАК НЕ СТАТЬ УЧАСТНИКОМ ФИНАНСОВЫХ ПРЕСТУПЛЕНИЙ

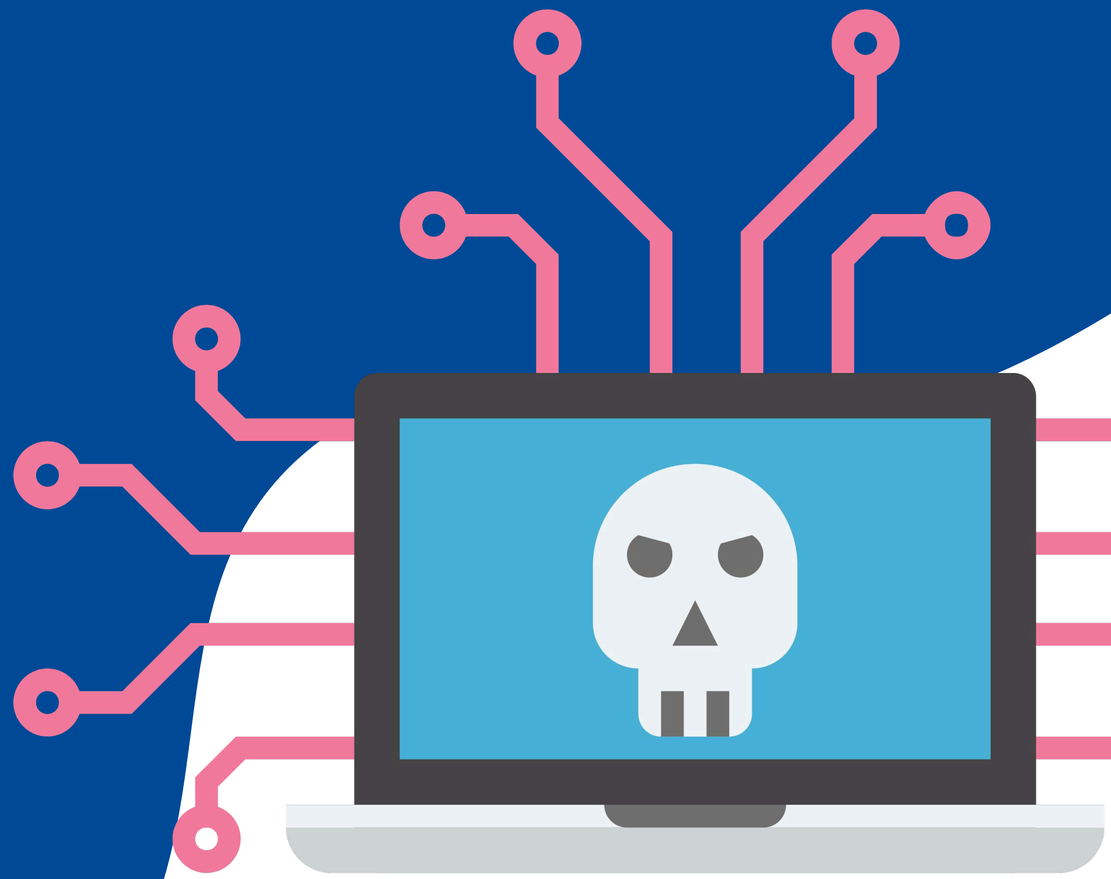
ТЕМАТИЧЕСКИЙ УРОК

ДРОППЕРЫ

это лица, которые используют свои карты для обналичивания или транзита (дальнейшей отправки) похищенных денежных средств

ПОПУЛЯРНЫЕ СПОСОБЫ ВЫВОДА ДЕНЕГ

1. перевод в криптовалюту сразу с карты потерпевшего, с т.е. так называемого «грязного» пластика
2. перевод в криптовалюту с «чистого пластика», т.е. взнос денежных средств на карты дропа, которая ранее не участвовала в сомнительных операциях
3. обналичивание, аккумулирование крупных денежных сумм, с последующей покупкой криптовалюты
4. обналичивание, аккумулирование крупных денежных сумм, с последующей покупкой валюты
5. обналичивание крупных денежных сумм, транспортировка в другой регион взнос на «чистый» пластик и далее межбанковские переводы



115-ФЗ

«О ПРОТИВОДЕЙСТВИИ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЁМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА»

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Согласно статистике, 80% хищений средств происходит дистанционно, более того ежегодно растет не только количество преступлений, но и объем похищенных средств

СИТУАЦИЯ

Людмила является активным клиентом одного из крупнейших федеральных банков страны, где имеет зарплатную карту, накопительный счет, вклад и другие банковские продукты. Людмила решила инвестировать накопившиеся сбережения в строящееся жилье. Ввиду современных трендов предполагалась цифровая сделка, то есть подписание ДДУ (договор долевого участия) с помощью УКЭП (усиленная квалифицированная электронная подпись), являющейся электронным аналогом рукописной подписи. Пока Людмила ожидала «выпуска» УКЭП, ей поступил звонок от «сотрудника» Госуслуг, который ей сообщил, что на ее имя было получено письмо. Злоумышленник уточнил, какой способ передачи письма наиболее удобен: посредством электронной почты или отправкой на домашний адрес, который к тому же был назван мошенником корректно. Людмила, не заподозрив подвоха, попросила направить письмо на адрес электронной почты (для ускорения процесса). Для этого «сотрудники» Госуслуг направили на ее телефон смс-код и попросили его продиктовать. Только через 10-15 минут, после того как смс-код был назван, женщина решила еще раз внимательно прочитать направленное ей сообщение и обнаружила, что в его содержании есть информация о смене пароля на портале Госуслуг. При попытке зайти в свой ЛК на Госуслугах она увидела, что доступ был уже более невозможен. Очевидно, что произошла смена пароля

Сотруднику одного из вузов города Москвы в Telegram пришло сообщение от ректора этого вуза о том, что в отношении образовательного учреждения проходит проверка со стороны правоохранительных органов в части распространения персональных данных. «Ректор» пояснил, что ранее сам он уже общался на данную тему и предупредил сотрудника о том, что скоро поступит звонок от представителя МВД. Далее, как было сказано ранее, с сотрудником связался представитель правоохранительных органов с сообщением о том, что от имени жертвы проводятся незаконные финансовые операции и для сохранности сбережений на время следствия необходимо перевести свои деньги на «специальный» счет

Самым лучшим вариантом противодействия такому виду мошенничества будет завершение контакта и связь с руководителем посредством городского или мобильного телефона по своей инициативе

СИТУАЦИЯ

Мужчине по имени Павел после рабочего дня раздался звонок с неизвестного мобильного номера. Павел как деловой человек, которому часто звонят по рабочим вопросам, ответил. Звонящий представился сотрудником мобильного оператора (при этом не уточнил, какого именно) и любезно сообщил о том, что если срок действия договора мобильной связи не продлить в тот же день, то сим-карта прекратит работу и данный номер продадут новому владельцу. Павел уточнил у «сотрудника» мобильного оператора, что нужно сделать для продления договора. Ему ответили, что договор можно продлить «прямо сейчас» в режиме телефонного звонка и никакие персональные данные не потребуются, поскольку они были переданы «ранее при оформлении сим-карты». Однако мошенники попросили продиктовать смс-код, который поступит на телефон. Так как Павел уже знал о подобных схемах, то он прервал разговор, положив трубку

1

Поступившее смс-сообщение якобы для продления договора на самом деле будет являться сбросом пароля для портала «Госуслуги» (о чем рассказано выше). Злоумышленники могут получить исчерпывающую информацию для дальнейших махинаций, например, для оформления кредитов в МФО (микрофинансовых организациях).

2

«Сотрудники» оператора для продления договора мобильной связи попросят ввести определенную комбинацию цифр на телефоне, что приведет к переадресации входящих вызовов и смс сообщений на мобильные телефоны мошенников и может дать им полный карт-бланш для смены паролей, в том числе в банковских приложениях.

ЗАПОМНИТЕ, ЧТО ОПЕРАТОРЫ СОТОВОЙ СВЯЗИ НИКОГДА НЕ БУДУТ ПРОСИТЬ ПРОДИКТОВАТЬ СМС-КОД И НИКОГДА НЕ ПОПРОСЯТ ПРОДИКТОВАТЬ ВАШИ ПАСПОРТНЫЕ ДАННЫЕ

СИТУАЦИЯ

Жертва получает анонимную доставку цветов или некого подарка, что вызывает приятное удивление. На следующий день жертве поступает звонок с сообщением от службы доставки, что курьер не отчитался за данную доставку установленным образом, и просьбой продиктовать «код подтверждения доставки»

Важно никогда не принимать от курьеров заказы, которые не были оформлены лично или о которых вы не уведомлены

СИТУАЦИЯ

Женщина из Москвы решила сдать свою квартиру в аренду. Для повышения стоимости она решила ее меблировать и приобрести шкаф на сервисе «Авито». Подобрав понравившуюся позицию, она связался с продавцом и договорилась о цене в размере 10 000 рублей. Он предложил ей самой заказать доставку, направив фишинговую ссылку на популярный сервис «Яндекс-доставка». Женщина прошла по ссылке (важно отметить, что страница сервиса выглядела, как ее оригинал), ввела нужный адрес доставки и данные своей банковской карты для оплаты. В этот момент с карты москвички была списана сумма 10 000 рублей, но на сайте произошел сбой, и сервис попросил ввести данные карты еще раз для возврата денежных средств. После повторного ввода данных с ее карты вновь была списана сумма в том же размере 10 000 рублей.

ОСНОВНОЕ ПРАВИЛО ФИНАНСОВОЙ БЕЗОПАСНОСТИ ДОСТАТОЧНО ПРОСТОЕ:

НЕ ОТВЕЧАТЬ НА ЗВОНКИ С НЕЗНАКОМЫХ НОМЕРОВ

Возможности искусственного интеллекта в реализации преступных схем

СОЗДАНИЕ ПОДДЕЛЬНОГО ВИДЕО

Создание дипфейка

Мошенники использовали технологии глубокого обучения для создания видео, имитирующего действия генерального директора компании. Они смогли сделать так, чтобы видео выглядело очень правдоподобно, используя открытые источники, такие как видеозаписи публичных выступлений и интервью генерального директора.

Обман

С помощью полученного дипфейка мошенники связались с одним из филиалов этой компании, представляясь генеральным директором. Они использовали видео, чтобы убедить сотрудников в том, что им необходимо сделать срочный перевод средств на «специальный счет».

Вымогательство

В результате манипуляций мошенников сотрудники филиала сделали перевод значительной суммы денег, полагая, что руководство компании действительно дало такое указание

Раскрытие мошенничества

Когда стало очевидно, что денежные средства не были переведены по легальным причинам, компания начала расследование. В ходе расследования было выяснено, что видео было фальшивым, и это привело к осознанию того, как технологические новшества могут быть использованы в преступных целях.

«ГЛУБОКОЕ ПОДДЕЛЫВАНИЕ ГОЛОСА» (VOICE SPOOFING)

ПРИМЕРЫ:

- создание подделки голоса
- фейковый звонок с просьбой о помощи
- вымогательство средств

СБОР ИНФОРМАЦИИ О КОМПАНИИ И/ИЛИ О ЧЕЛОВЕК ПЕРЕД «ВЗЛОМОМ»

- создание фальшивого профиля
- осуществление мошеннического запроса
- выполнение перевода
- раскрытие мошенничества

Обнаружение вредоносного ПО. Машинное обучение

ОБНАРУЖЕНИЕ ПО СИГНАТУРАМ

ГЕНЕРАЦИЯ ВРЕДОНОСНОГО КОДА

ИСПОЛЬЗОВАНИЕ МЕТОДОВ ИИ ДЛЯ АДАПТАЦИИ АТАК

АНАЛИЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ГЕНЕРАЦИЯ АТАКИ С ИСПОЛЬЗОВАНИЕМ ИИ

ФИЗИЧЕСКОЕ РАСПРОСТРАНЕНИЕ

ВАЖНО!

1. Активируйте многофакторную аутентификацию на всех значимых аккаунтах, таких как банковские приложения, портал «Госуслуги», личный кабинет Федеральной Налоговой Службы и другие.
2. Закройте доступ для посторонних лиц в социальных сетях, следите за цифровым следом, который вы оставляете в сети Интернет.
3. Критически относитесь ко всему, что видит и слышите.

ДРОППЕРЫ/ДРОПЫ: СВЯЗУЮЩЕЕ ЗВЕНО ПРЕСТУПНОЙ ЦЕПИ ФИНАНСОВЫХ МОШЕННИКОВ

Дропы являются соучастниками преступлений, которые могут быть классифицированы по статье 174 УК РФ Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем или по статье 159 УК РФ Мошенничество

Дропы – это подставные лица, которые задействованы в нелегальных схемах по выводу средств с банковских карт граждан. Стоит отметить, что дропы не являются организаторами преступлений, но являются их соучастниками, за что несут полную ответственность перед законом.

*По данным «Сбера», в дропперство вовлечено порядка **2 млн россиян** – это почти в два раза больше, чем в 2023 году. **Около 60%** – молодые люди до 24 лет, для которых характерно стремление к легкому заработку*

Примеры вербовки дропперов

Студент по имени Андрей хочет заработать денег в свободное время. На сайте по поиску работы ему подвернулась заманчивая вакансия со следующими требованиями: без опыта работы; удаленно; частичная занятность; высокий заработок за несколько часов в день; возраст 18+ и наличие карты любого банка.
Те, кто откликается на подобные вакансии, почти всегда становятся участникам мошеннических схем. Мошенники придумывают различные легенды, например, представляются крупной компанией, занимающейся поставками большого количества товаров из Китая. С учетом крупных сумм покупок и лимитами банков на ежемесячные переводы в компанию требуются люди, которые «отдадут» в аренду свою банковскую карту вместе с личным кабинетом для контроля поступления денег от «клиентов» за вознаграждение.

СИТУАЦИЯ

«КУРЬЕР НАЛИЧНОСТИ»

перемещение денежных средств от одного лица или бизнеса к другому, с целью избежать традиционных банковских методов или при наличии ограничений на вывод. объявление о такой работе размещается телефонными мошенниками, при этом будущему курьеру могут сообщать, что работа не связана с криминалом и он ничем не рискует.

ПРИМЕР

Нужны ответственные люди по всем городам РФ;
Работа курьером;
Забираем посылки от 100 тыс. руб.
Даем 7%, выплата сразу;
Вся «почва» для безопасного забора нала подготовлена!!!

ВАЖНО!

ст. 159 УК РФ. Наказание в этом случае предусмотрено вплоть до 10 лет лишения свободы

СИТУАЦИЯ

На ваш счет поступает перевод денег от незнакомого лица, далее вам поступает звонок с информацией, что денежный перевод был совершен ошибочно, и просьбой перевести деньги обратно. Однако в случае возврата по указанным незнакомцем реквизитам на самом деле деньги направляются третьему лицу – участнику преступной схемы. Таким образом, случайно, пойдя навстречу человеку, можно стать соучастником преступления по выводу денег.

В данном случае правильным решением будет обратиться в банк и только вместе с банковским сотрудником решать вопрос, каким образом деньги отправить обратно.

ЧЕРЕЗ СОЦИАЛЬНЫЕ СЕТИ И САЙТЫ ЗНАКОМСТВ

Через социальные сети обращается незнакомец с правдоподобной легендой, например, что у него есть родственник за границей, которому срочно нужно отправить деньги, а его банк такие переводы не проводит. Обычно мошенники предлагают это сделать за небольшую плату в зависимости от суммы предполагаемого перевода. Далее на счет жертвы поступают ворованные деньги, которые она перенаправляет дальше, становясь таким образом звеном в преступной цепочке.

ВОВЛЕЧЕНИЕ В ДИВЕРСИОННУЮ ДЕЯТЕЛЬНОСТЬ

Работа с уязвимыми группами – привлечение людей, испытывающих финансовые трудности

«Борьба за правое дело» - злоумышленники занимаются пропагандой через социальные сети, обещая участие в «правой войне»

Подрыв доверия к государству – мошенники призывают действовать против «несправедливой системы»

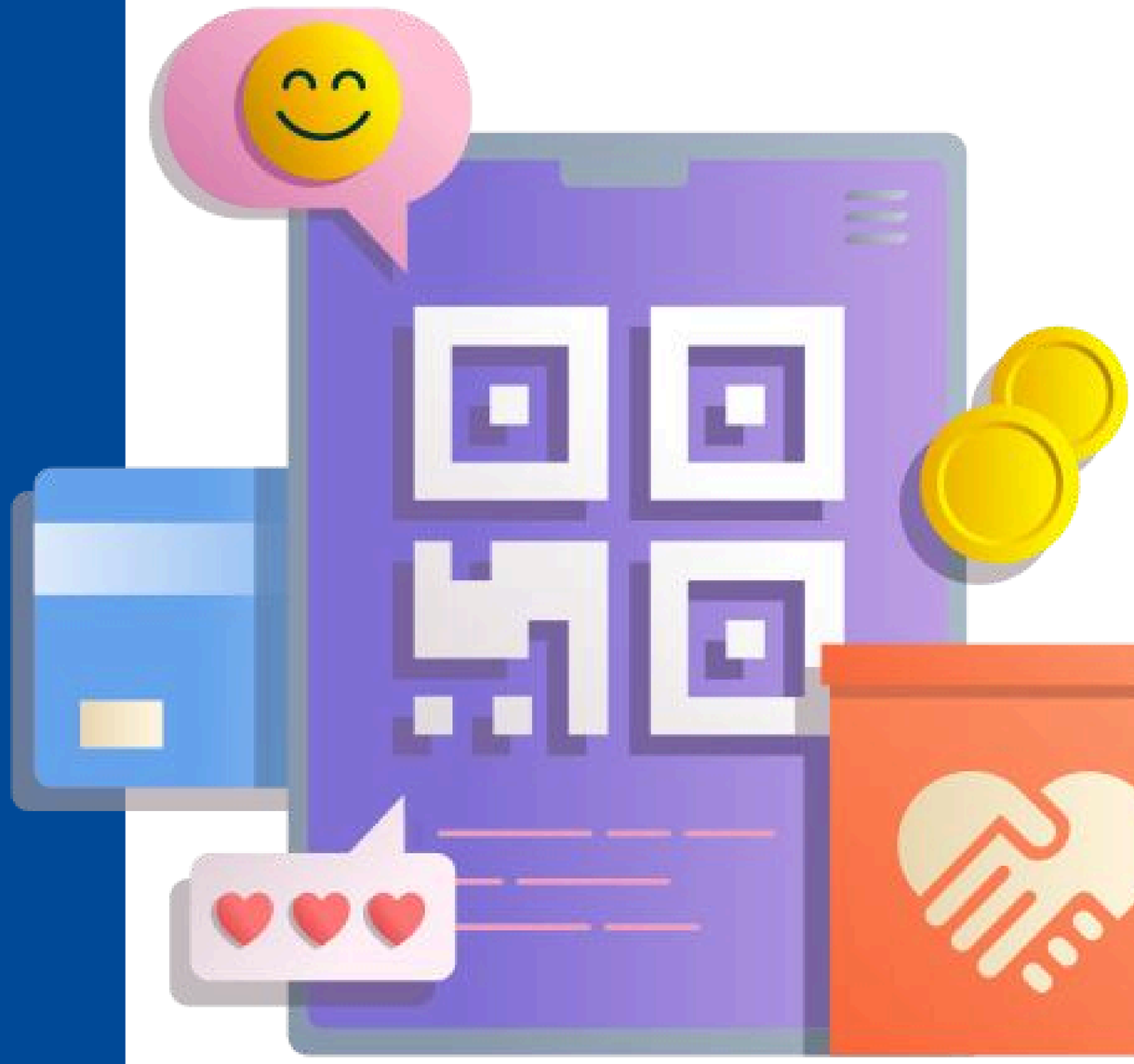
Обеспечение наркотиками – вербовщики делают людей зависимыми от наркотиков и склоняют их к диверсионным действиям

ВАЖНО!

За совершение диверсии наступает уголовная ответственность в виде лишения свободы на срок от 10 до 20 лет лишения свободы.

БЛАГОТВОРИТЕЛЬНЫЕ СБОРЫ ДЛЯ СВО/ПРИЮТ ДЛЯ ЖИВОТНЫХ/НА ОПЕРАЦИЮ

Мошенники создают благотворительный фонд, например, для помощи студентам вузов, попавшим с сложную жизненную ситуацию; и на счет созданного фонда те организации, которым необходимо легализовать преступные средства, перечисляют деньги



ОБМЕН КРИПТОВАЛЮТЫ НА РУБЛИ

ПРАВИЛА РАБОТЫ С КРИПТОВАЛЮТОЙ

- вести переписку через инфраструктуры p2p площадки
- совершать сделки с аккаунтами, которые давно зарегистрированы на площадке и имеют хорошую репутацию

ВАЖНО!

Важно помнить, что самые безопасные сделки проводятся на криптобиржах

ОБНАЛЬЩИКИ

*это дропы, которые **снимают со своей карты** преступные деньги и передают их мошенникам.*

ТРАНЗИТЧИКИ

*это дропы, которые **пересылают безналичным путем** преступные деньги по указанным мошенникам реквизитам.*

ЗАЛИВЩИКИ

*это дропы, которые получают наличные деньги от таких же дропов, **вносят их на свою карту** и пересылают дропам «транзитчикам».*

УНИВЕРСАЛЫ

*это дропы, которые могут выполнять **все вышеуказанные действия**.*

Важно отметить, что суровость наказания не зависит от того, знал ли дроп о том, что он делает, или нет

ПРАВИЛА БЕЗОПАСНОСТИ

- не откликайтесь на вакансии с легким заработком. когда обещается легкий и при этом высокий заработок, то это точно мошенническая схема
- потенциального работодателя проверяйте на предмет наличия отзывов в интернете
- никогда и никому не оставляйте данные своей банковской карты, тем более не передавайте ее третьим лицам (во многих банках передача карт третьим лицам запрещена)
- регулярно обновляйте пароли к своим банковским приложениям, личному кабинету портала «госуслуги» и прочим финансово значимым приложениям
- не переходите по ссылкам из неизвестных источников, во избежание взлома доступа к банковскому личному кабинету
- всегда повышайте свою финансовую грамотность – читайте новости о новых видах мошенничества, ведь «предупрежден – значит вооружен»
- если вас попросят вернуть случайный перевод денег, совершенный на ваше имя, не соглашайтесь на это, обратитесь с этим вопросом в ваш банк

Только тихо!
Всё об анонимности криптовалют

ВЫВОД СРЕДСТВ ИЗ КРИПТОВАЛЮТНЫХ ОБМЕННИКОВ И БИРЖ

Криптобиржи

это более сложная структура, которая предполагает регистрацию и часто необходимость пройти процедуру «Знай своего клиента». Ключевым отличием от криптообменников является возможность торговать на бирже своими активами, а не просто обменивать.

Криптообменники

Онлайн криптообменник предоставляет возможность быстрого обмена криптовалюты. Достаточно выбрать валюту, которую вы хотите продать, и валюту, которую хотите купить. После ввода своих данных вы получаете нужные средства на свой кошелек.

ОСНОВНЫЕ ТИПЫ ПРЕСТУПЛЕНИЙ С КРИПТОВАЛЮТАМИ

МОШЕННИЧЕСТВО

В Управление поступило обращение гражданки «М», денежные средства которой похитили преступники. С использованием одной из социальных сетей с гражданкой «М» связалась девушка, которая, используя методы социальной инженерии убедила «М» приобрести криптовалюту и инвестировать её на бирже «С». В ходе финансового расследования МРУ Росфинмониторинга по СКФО установило, что сайт биржи был подделкой, а криптовалюта, вложенная потерпевшей, выводилась преступниками на одну из известных криптобирж, обменивалась на стэйблкойны и в дальнейшем переводилась на анонимные криптокошельки

ПРОГРАММЫ-ВЫМОГАТЕЛИ (RANSOMWARE)

Одна из крупнейших атак осуществлена на компанию Colonial Pipeline. в 2021 году. Вымогатели потребовали оплату в биткойнах на сумму около 4,4 млн долларов. После получения выкупа преступники пытались скрыть свои средства, разбивая транзакции на мелкие части и переводя их через различные криптовалютные кошельки для запутывания следов

КИБЕРПРЕСТУПЛЕНИЯ И ВЗЛОМЫ

Наиболее известные случаи взлома криптовалютных бирж, такие как взлом Mt. Gox в 2014 году и взлом Bitfinex в 2016 году, привели к огромным потерям.

НАРКОТОРГОВЛЯ И ИНАЯ НЕЛЕГАЛЬНАЯ ТОРГОВЛЯ

В качестве примера можно привести платформу Hydra, деятельность которой была пресечена в 2022 году. По имеющимся данным Hydra контролировала более 90% незаконной торговли в даркнете, где за все товары и услуги, включая наркотики, оружие и поддельные документы, оплачивались криптовалютой

ФИНАНСИРОВАНИЕ ТЕРРОРИЗМА

Криптовалюты также используются для финансирования террористических организаций, так как они позволяют совершать анонимные переводы без необходимости использовать традиционные банковские системы.

ПРАВИЛА БЕЗОПАСНОСТИ

используйте двухфакторную аутентификацию

храните резервные копии в безопасных местах

используйте сложные пароли

желательно использовать отдельное устройство только для доступа к кошелькам

регулярно обновляйте программное обеспечение

позаботьтесь о защите своего устройства

не афишируйте в публичных местах наличие большого количества криптовалюты на ваших кошельках

МЕЖДУНАРОДНАЯ ОЛИМПИАДА ПО ФИНАНСОВОЙ БЕЗОПАСНОСТИ

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ФИНАНСОВОМУ МОНИТОРИНГУ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

РУДН

МУМЦФМ

ВЫСШАЯ ШКОЛА ЭКОНОМИКИ

ЦЕНТР МЕЖОЛИМПИАДНОЙ ПОДГОТОВКИ

содружество

Т БАНК

Альфа-Банк

Цели Олимпиады:

- повышение общей информационной, финансовой и правовой грамотности молодежи, формирование новой формы мышления и нового формата деятельности, выявление талантливых школьников и студентов в области финансовой безопасности;
- создание условий для индивидуальной образовательной траектории, содействие профессиональной ориентации школьников и студентов для формирования кадрового ресурса системы финансовой безопасности;
- стимулирование учебно-познавательной и научно-исследовательской деятельности школьников и студентов, развитие научных знаний в области финансовой безопасности.

Рекомендации по работе с презентацией
тематического урока на тему:
«НЕдетские игры 2.0: Дроп поневоле»

Цель урока – мотивировать обучающихся на выработку личной стратегии грамотного поведения в ситуациях растущих финансовых рисков и финансового мошенничества.

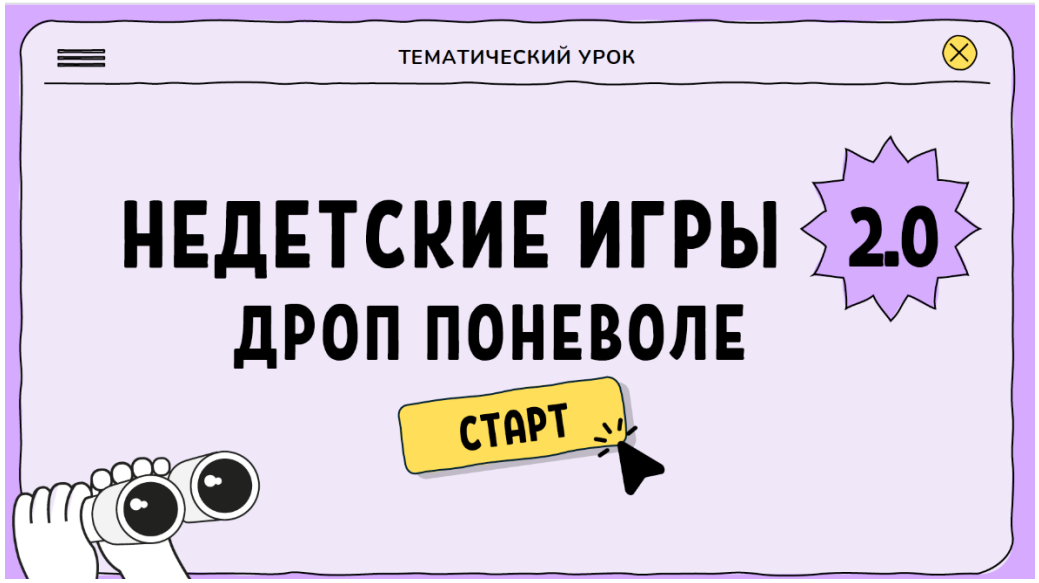
Задачи урока:

- заложить у обучающихся основы грамотного финансового поведения;
- сформировать у обучающихся представление о признаках ситуаций финансового мошенничества, а также признаках фишинговых и других мошеннических схем;
- научить обучающихся:

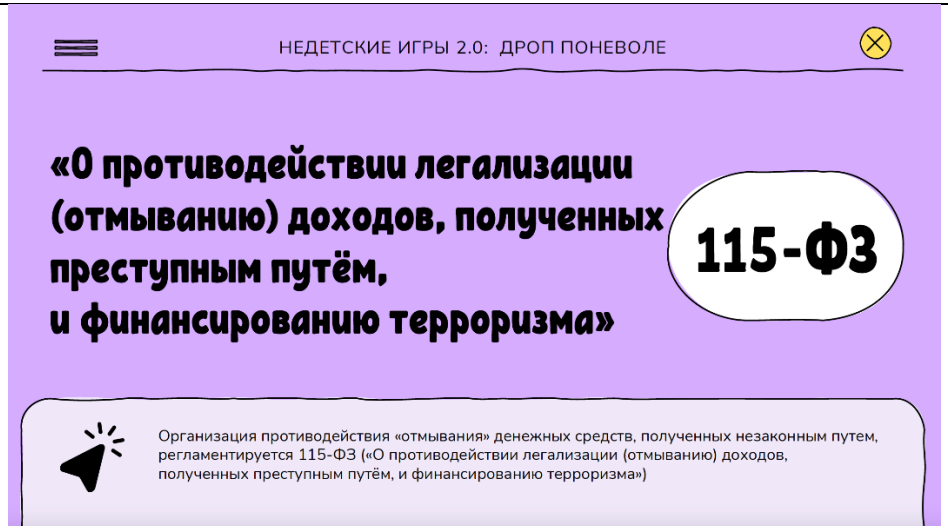
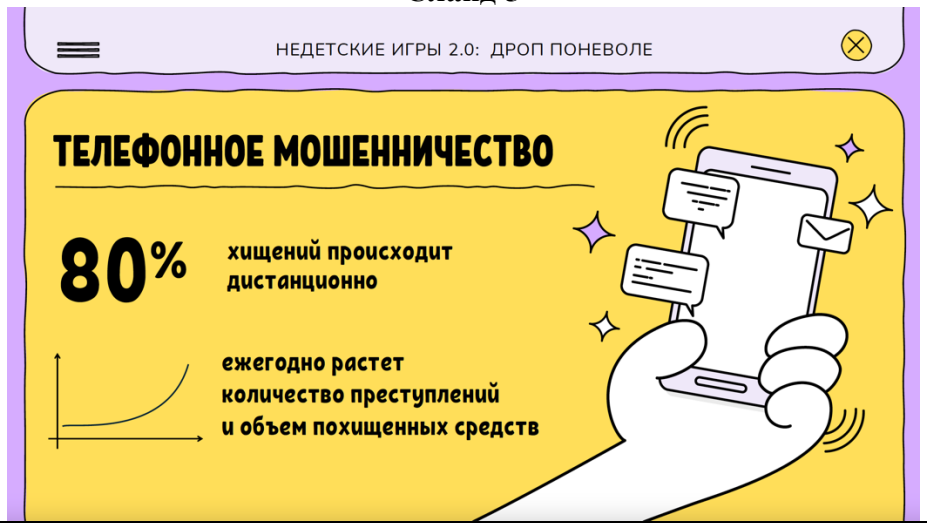
- распознавать угрозу мошенничества и не совершать действий по платежам и переводам в пользу мошенников;
- использовать алгоритмы действий в типичных ситуациях, связанных с возможным или уже совершенным финансовым мошенничеством;
- предпринимать меры предосторожности при использовании различных видов денег и проведении операций с ними;
- критически относиться к предложениям с признаками давления, манипулирования, мошеннических действий;

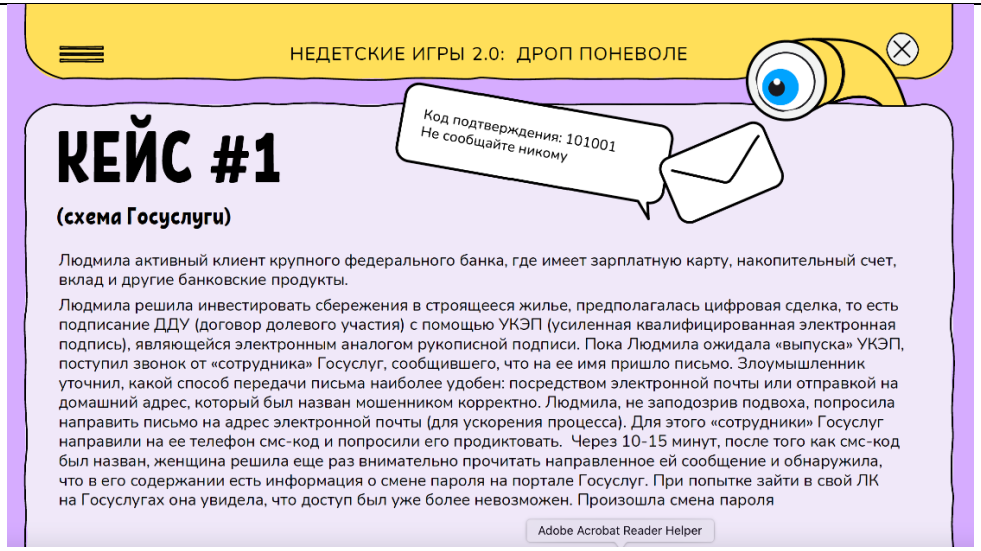
- понимать и осознавать, что за все финансовые решения ответственность несет собственник средств, даже если решения приняты под влиянием рекламы и под давлением мошенников.

Методический материал носит рекомендательный характер; преподаватель, принимая во внимание особенности обучающихся, может варьировать задания, их количество, менять этапы занятия.

Слайд (содержание слайда)	Комментарий для учителя
Слайд 1  	Согласно аналитическим данным ЦБ РФ по итогу 3 квартала 2024 года, основными инструментами, которые используют мошенники, по-прежнему остаются социальная инженерия, фишинговые атаки, однако лидирует по количеству преступлений телефонное мошенничество. Более того сегодняшнее время особо опасно, поскольку ввиду высоких процентных ставок по вкладам население не только размещает свои сбережения, которые находились дома «под подушкой», но и переводит свои средства с фондового рынка (рынка ценных бумаг) в денежный рынок (вклады). Это представляет для кибермошенников особых интерес не только с точки зрения социальной инженерии, но и с точки зрения компьютерных атак. В связи с этим мы должны следить за трендами мошенников, ведь «предупрежден значит вооружен». Однако у мошенников имеются проблемы с так называемым «отмыванием» денежных средств. Это означает, что киберпреступникам необходимо придать вид законного владения денежными средствами, которые были получены, например, в результате кибермошенничества. Для этих целей мошенники применяют различные «инструменты», например, привлекают к этому процессу так называемых дропперов.

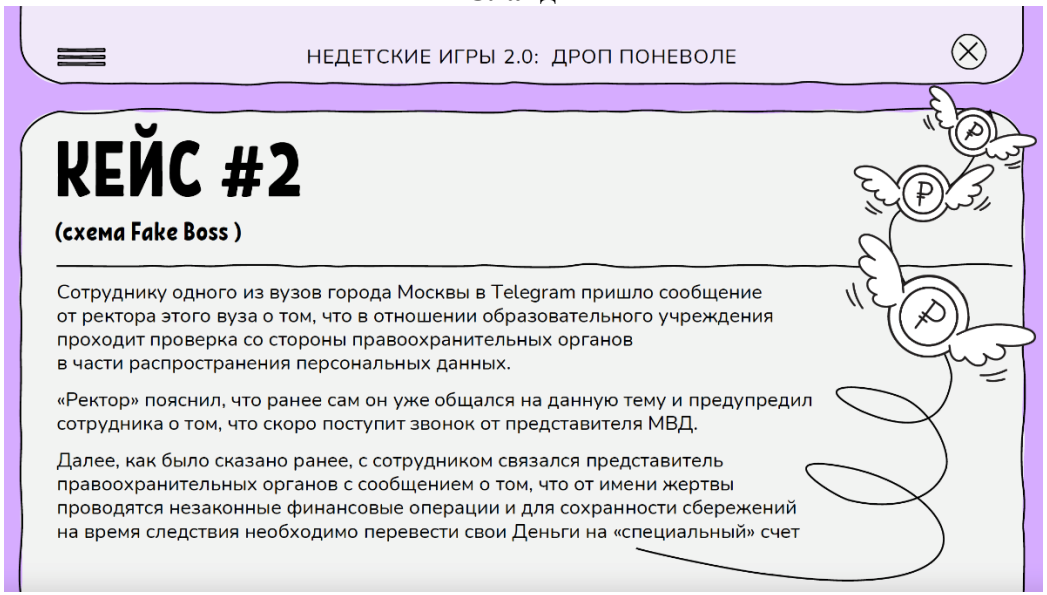
Слайд 2 	Дропперы – это лица, которые используют свои карты для обналичивания или транзита (дальнейшей отправки) похищенных денежных средств.
Слайд 3 	Согласно материалам различных банков наиболее популярными способами вывода похищенных денежных средств являются: - перевод в криптовалюту сразу с карты потерпевшего, с так называемого «грязного» пластика; - перевод в криптовалюту с «чистого пластика», т.е. взнос денежных средств на карты дропа, которая ранее не участвовала в сомнительных операциях; -обналичивание, аккумулирование крупных денежных сумм, с последующей покупкой криптовалюты; -обналичивание, аккумулирование крупных денежных сумм, с последующей покупкой валюты; -обналичивание крупных денежных сумм, транспортировка в другой регион взнос на «чистый» пластик и далее межбанковские переводы.
Слайд 4	Организация противодействия «отмывания» денежных

	средств, полученных незаконным путем, регламентируется 115-ФЗ («О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма»). Рассматриваемая в настоящем уроке тематика является особенно актуальной в современной жизни.
Слайд 5 	Не будет преувеличением сказать, что практически каждый россиянин сталкивался с телефонными мошенниками. Вопрос знаний в сфере киберпреступлений остается по-прежнему важным, его актуальность растет в геометрической прогрессии. Согласно статистике, 80% хищений средств происходит дистанционно, более того ежегодно растет не только количество преступлений, но и объем похищенных средств.
Слайд 6	***Схема телефонного мошенничества с использованием портала «Госуслуги»***



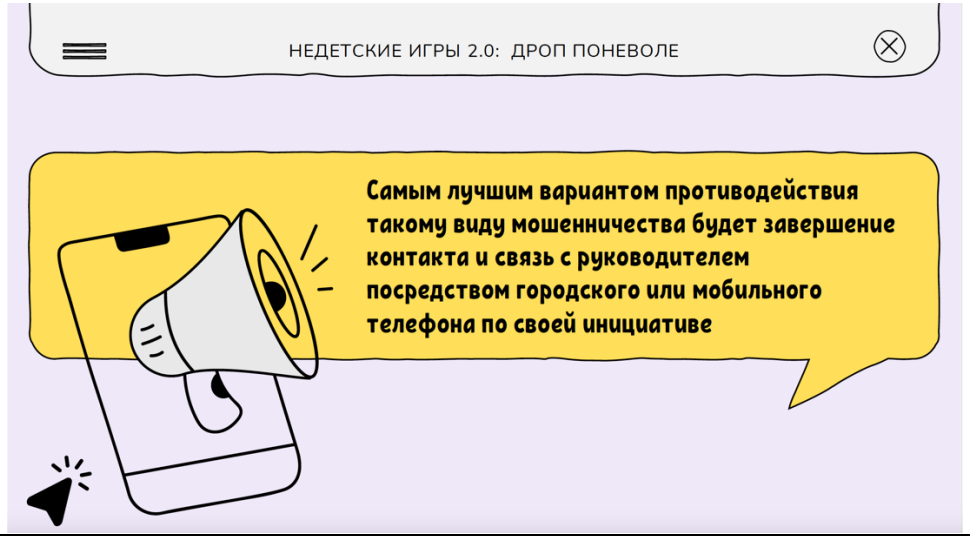
Злоумышленники стали активнее использовать портал «Госуслуги» в своих схемах. Ведь, получив доступ к «Госуслугам», мошенники получают самое главное: наши исчерпывающие персональные данные. Как известно, на портале имеются такие сведения, как паспортные данные, ИНН, СНИЛС, ОМС, водительское удостоверение и прочее. Самое безобидное, что могут сделать мошенники, – это продать наши персональные данные злоумышленникам, а также, например, оформить микрозайм, используя портал «Госуслуги» для подтверждения личности в некоторых МФО (микрофинансовых организациях).

В дополнение к уже широко известным схемам получения смс-кода, подтверждающего смену пароля, с помощью социальной инженерии появились несколько новых возможностей атак на контакты службы поддержки сервиса. Одним из последних методов является публикация фейковых номеров службы поддержки «Госуслуг». Для этого мошенники подделывают справочные сайты, публикуют на них фейковые номера служб поддержки «Госуслуг». Через них злоумышленники похищают доступ к аккаунтам пользователей портала, далее с помощью поискового продвижения добиваются их появления в ТОП-10 поисковых систем. Помимо этого, злоумышленники рассылают смс-сообщения о якобы неудачной попытке входа или взлома аккаунта и в них же указывают поддельный номер службы поддержки. Основная опасность для граждан здесь заключается в том, что они искренне верят, что действительно обратились в службу поддержки портала и готовы выполнять команды мошенников. Как мы видим, в отношении «жертвы» здесь были использованы методы «социальной инженерии», ведь злоумышленниками были названы ее «чувствительные» данные: ФИО, адрес электронной почты, адрес постоянной регистрации, да и в

	целом она ждала звонок по факту готовности УКЭП. Это привело к усыплению бдительности и потере доступа ЛК портала Госуслуг. Очевидным действием со стороны жертвы должна была быть верификация смс-сообщения перед озвучиванием смс-кода мошенникам. Кроме того, ***мы должны всегда помнить, что сотрудники портала «Госуслуг» никогда не звонят гражданам, тем более с мобильных номеров***
Слайд 7 	***Мошенничество по схеме Fake Boss*** Наряду с такими формами мошенничества, как взлом учетных записей на портале «Госуслуги», звонков от «сотрудников» ЦБ РФ, ФСБ, МВД, прокуратуры и других, также известна такая схема, как Fake Boss. Схема довольная проста: злоумышленники выдают себя за руководителя жертвы, пишут ей сообщение в наиболее популярных мессенджерах о необходимости переговорить с представителем «полиции», «профильного» ведомства или другим государственным органом. При дальнейшем взаимодействии с такими «представителями» это приведет к тому, что жертва перечислит свои денежные средства на так называемые специальные/безопасные счета. Алгоритм следующий: - создается либо фейковый аккаунт руководителя в мессенджере (при этом используется вся необходимая информация, размещённая на сайте организации, в которой работает жертва, например, государственные организации, в частности, образовательные учреждения: вузы, школы и т.д.), либо взламывается реальный аккаунт руководителя. - затем с этого аккаунта поступают сообщения сотруднику (жертве) организации, в которых «руководитель» организации уведомляет подчиненного о том, что ему поступит звонок от представителей государственных ведомств и будет необходимо сообщать достоверную

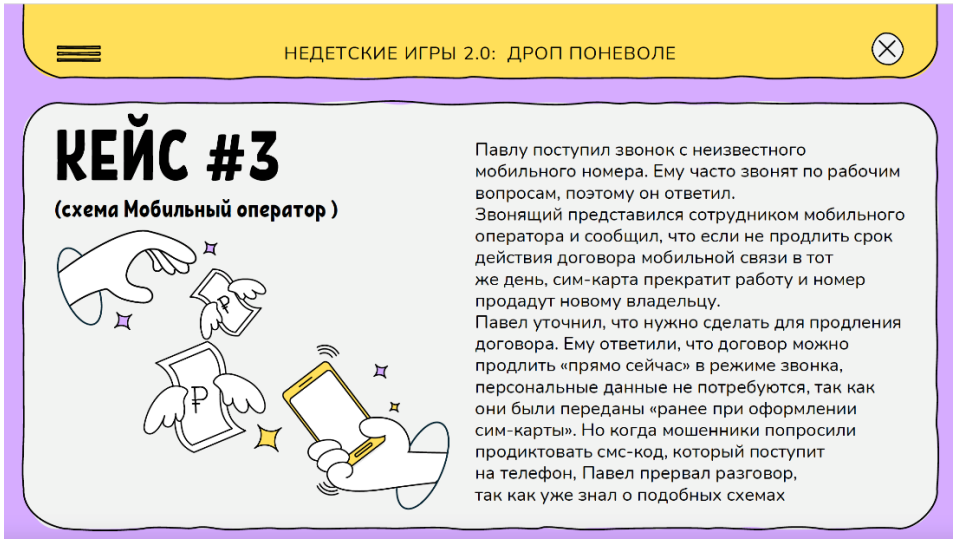
	информацию. Часто злоумышленник уверяет, что якобы он сам ранее общался с правоохранительными органами. Особое внимание «руководитель» уделяет конфиденциальности разговора, о котором никому нельзя говорить и что необходимо четко следовать инструкциям по телефону; - подготовленный к будущему разговору сотрудник теряет бдительность, что неминуемо приводит к финансовым потерям вследствие перевода своих денежных средств на «специальные счета». Таким образом, мошенниками часто проводится предварительная работа по подготовке жертвы, которая может занимать достаточно длительный период. Известны истории, в которых переписка с «руководителем» занимала несколько месяцев и содержала в себе поздравления с праздниками, рабочие вопросы, в которых было указание на конкретных лиц. От подвергшейся влиянию жертвы мошенники могут дополнительно потребовать взять максимально возможное количество кредитов в различных банках с последующим переводом полученных средств на «специальные счета». Кроме того, целью таких звонков может являться получение информации о других сотрудниках компании для использования в дальнейших атаках. Зачастую, чтобы влиться в доверие, мошенники направляют жертве сканированные копии документов от правоохранительных органов, которые очевидно являются поддельными.

Слайд 8



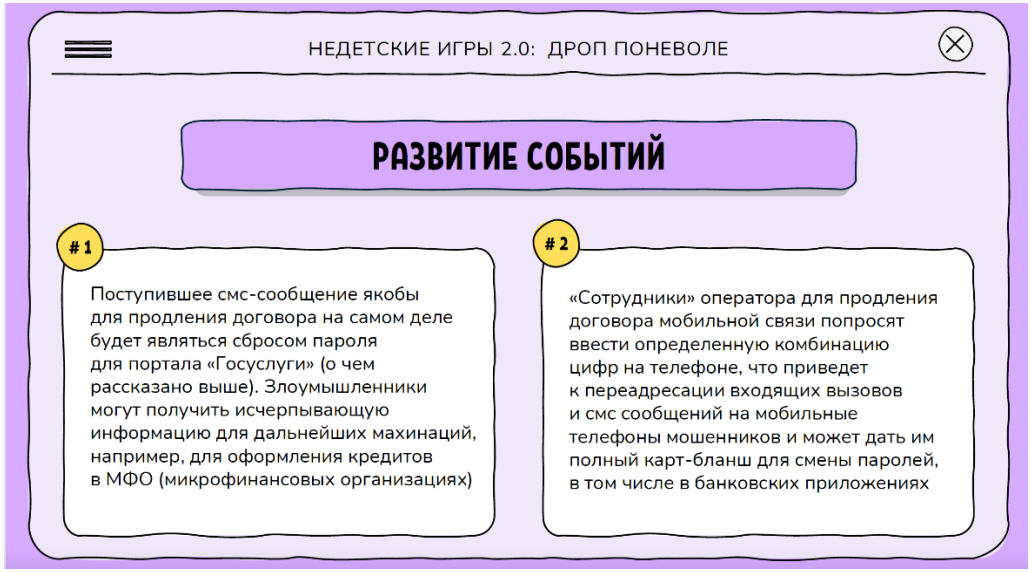
При данных видах атак рекомендуется проверять правильность номера или аккаунта, с которого звонят от имени руководителя. Также нужно обращать внимание, появляется ли в мессенджере уведомление «Добавить» и «Заблокировать». Если оно есть, то абонент отсутствует в списке ваших контактов

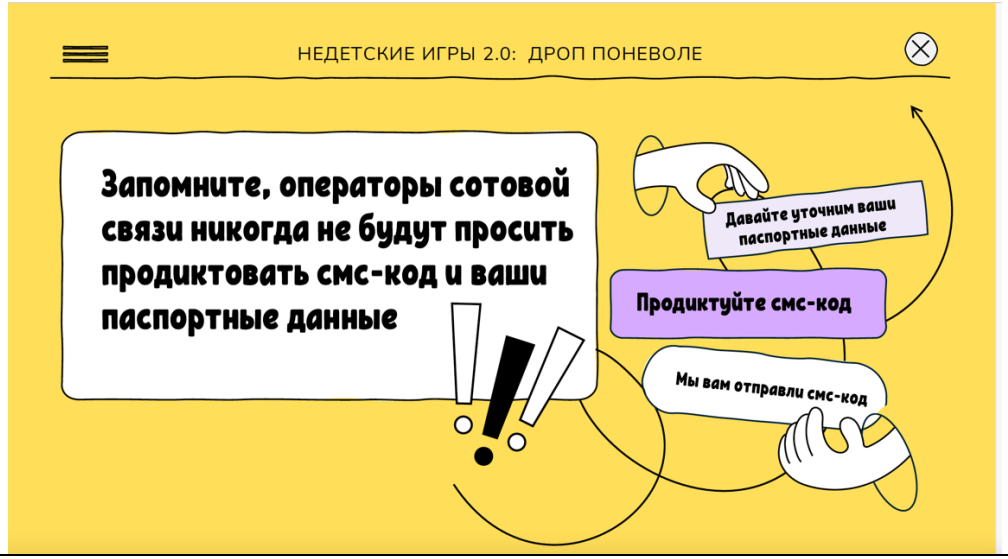
Слайд 9



• ***Звонок от оператора сотовой связи «У вас заканчивается срок действия договора»***

Данный вид телефонного мошенничества появился несколько лет назад и по-прежнему остается актуальным «инструментом» для злоумышленников. Якобы сотрудник колл-центра утверждает, что сим-карта абонента в ближайшее время не будет работать в связи с окончанием срока договора обслуживания мобильным оператором. Очевидно, что сегодня без связи оставаться никто не хочет, поэтому мошенники тут же «стелют красную дорожку», предлагая решение: прямо сейчас продлить договор и при этом для усыпления бдительности сообщают, что «никакие личные данные, в том числе паспортные называть будет не нужно», ведь они уже имеются в базе данных оператора связи. Не проинформированный о подобном роде мошенничестве гражданин, продолжая оставаться на связи со злоумышленником, рискует потерять свои деньги. Целью

	мошенников является тем или иным способом получить доступ к персональным данным для их использования в своих мошеннических схемах. Рассмотрим на примере, как это происходит.
Слайд 10  	Далее события могли развиваться по-разному Весьма нестандартный и неожиданный для неосведомленного человека вариант. В момент, когда «потерпевший» назвал мошенникам смс-код для восстановления доступа в ЛК портала «Госуслуги», они сразу же «раскрывают» карты и с насмешкой сообщают, что взломали аккаунт «Госуслуг». В этот момент растерянный человек, находясь в панике, начинает предпринимать быстрые и не всегда обдуманные действия, например, пытается восстановить доступ к порталу, используя механизм сброса пароля на официальном сайте. Однако злоумышленники уже авторизовались в ЛК гражданина и в строку контрольного вопроса для восстановления пароля вписали текст следующего содержания: «Ваша учетная запись временно заблокирована в связи с подозрительной активностью. Обратитесь по номеру +7 ***-***-**-** за более детальной информацией». Указанный номер принадлежит мошенникам, и сам потерпевший в паническом состоянии готов выполнять любые указания. Далее мошенниками прорабатываются различные схемы по хищению денег и персональных данных.

Слайд 11 	Стоит отметить, что вариации в данном виде мошеннической схемы могут быть разными, вместе с тем ***решение одно.*** Самое лучшее, что можно сделать в этой ситуации – это прервать разговор и перезвонить по номеру телефона, указанному на сайте мобильного оператора, если есть сомнения и вопросы.
Слайд 12 	Одним из новых сценариев мошенничества можно считать схему, связанную с доставкой цветов/товара. Схема работает следующим образом. В данном примере стоит отметить нестандартный ход мошенников: используется положительный, а не отрицательный стресс, к которому мы все уже привыкли. В данном случае жертва себя чувствует обязанным, в том числе и курьеру, который доставил подарок. Угрозой может быть не только финансовая потеря, но и здоровье, поскольку никто не знает, что может находиться в посылке, которую вы не заказывали.

Слайд 13

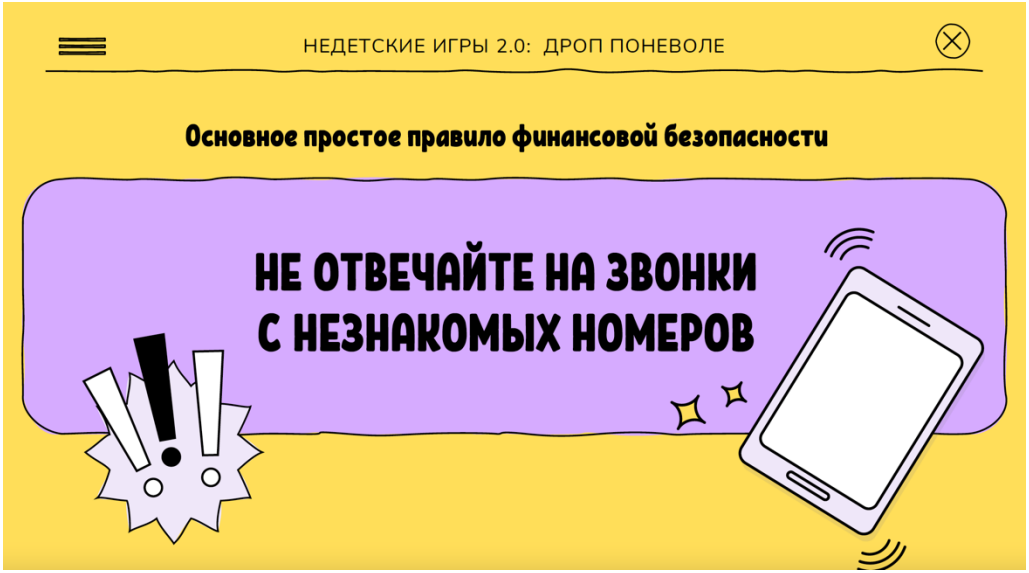
- ***Покупка/продажа товаров на «Авито»***

Схемы, применяемые мошенниками на сервисе «Авито», распространены и многим известны. Кроме того, сам сервис регулярно предупреждает своих клиентов о наиболее известных уловках, которые используют мошенники.

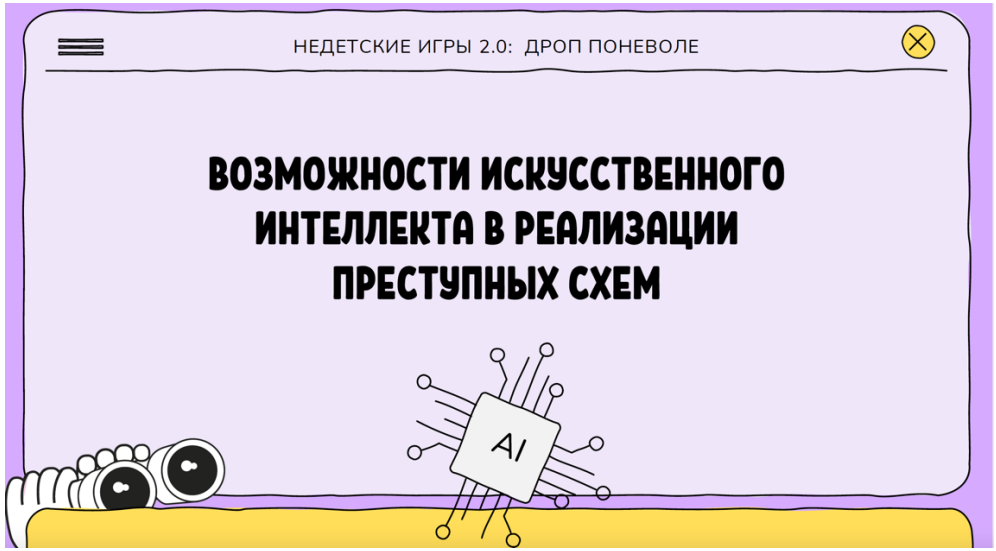
Рассмотрим одну из таких схем на примере.

Только в этот момент она догадалась, что имеет дело с мошенниками и обратилась в банк, выпустивший карту, где ей порекомендовали написать обращение в отделении полиции.

Данная ситуация демонстрирует, как работает фишинг (поддельный сайт). Основное грубое нарушение, которое было допущено женщиной, это переход по ссылке, которую ей направил «продавец» шкафа. После того, как жертва «попалась на крючок», очень сложно с него сорваться и в данном случае отличить настоящий сайт службы доставки от фейкового. **Самым правильным вариантом в данном случае и при работе в сети Интернет в целом является самостоятельный ввод нужного электронного адреса**, поскольку при переходе по ссылкам есть большой риск попасть на поддельные (фишинговые) сайты.

Слайд 14  	Все вышеприведенные примеры основаны на потере бдительности, отключении критического мышления, низком уровне финансовой грамотности, доверчивости. На том конце провода зачастую «работают» специально обученные, неглупые люди, в том числе психологи, финансисты, юристы. Прием, который используют мошенники, один и тот же – вывод жертвы из состояния спокойствия/равновесия под воздействием положительного или отрицательного стресса за счет передаваемой информации: либо произошло что-то «плохое» (например, «с вашего счета пытаются совершить перевод на сумму….»), либо что-то «хорошее» (например, «Ваш выигрыш составил….»). Ведь, когда мы находимся в подавленном или, наоборот, приподнятом настроении, мы не всегда можем принимать обдуманные решения, а мошенники всегда подталкивают нас на принятие моментальных решений. Конечно, мошенники используют разные информационные поводы, но их суть всегда одна: вовлечь нас в разговор и усыпить бдительность, поэтому важно владеть информацией о новых трендах мошенников.

Слайд 15

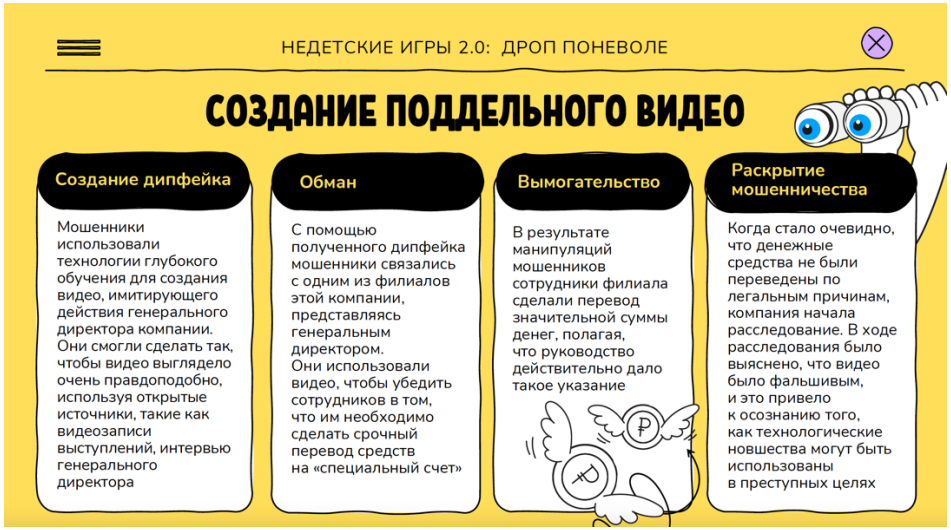


Злоумышленники для хищения денег стали чаще использовать новый инструмент обмана – дипфейк-технологии. С помощью нейросети мошенники создают реалистичное видеоизображение человека. Затем сгенерированный образ рассылают его друзьям или родным через мессенджеры или социальные сети. В этом фальшивом видеоролике виртуальный герой, голос которого иногда сложно отличить от голоса прототипа, рассказывает якобы о своей проблеме (болезнь, ДТП, увольнение) и просит перевести деньги на определенный счет. Иногда мошенники создают дипфейки работодателей, сотрудников государственных органов, известных личностей из той же сферы деятельности, в которой трудится их потенциальная жертва.

Для того, чтобы создать цифровую копию человека, злоумышленники используют фото и видео, а также запись голоса, полученные в основном в результате взлома его аккаунта в социальных сетях или мессенджерах.

Необходимо проявлять осторожность и «включать» критическое мышление при получении от своего знакомого голосового или видеосообщения с просьбой о финансовой помощи, ведь его аккаунт могли взломать злоумышленники. Иногда для рассылки таких сообщений мошенники создают поддельные страницы с именем и фото человека. Нельзя спешить переводить деньги. Необходимо обязательно сначала позвонить тому, от чьего имени поступило сообщение, и перепроверить информацию. Распознать дипфейк можно по неестественной монотонной речи собеседника, дефектам звука и видео, несвойственной мимике. Если возможности позвонить и убедиться, что человеку действительно нужна помощь, нет, задайте в сообщении личный вопрос, ответ на который знает только ваш знакомый.

Слайд 16



Один из реальных случаев использования технологии дипфейка для вымогательства денежных средств произошел в 2020 году, когда мошенники использовали алгоритмы дипфейка для создания поддельного видео с участием генерального директора одной из крупных компаний.

Основными этапами этого случая стали следующие моменты.

1. Создание дипфейка. Мошенники использовали технологии глубокого обучения для создания видео, имитирующего действия генерального директора компании. Они смогли сделать так, чтобы видео выглядело очень правдоподобно, используя открытые источники, такие как видеозаписи публичных выступлений и интервью генерального директора.

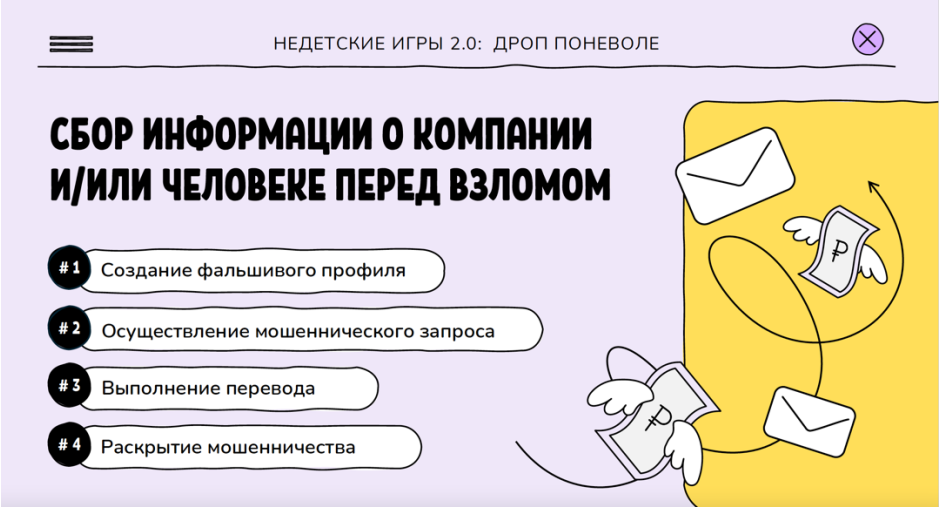
Обман. С помощью полученного дипфейка мошенники связались с одним из филиалов этой компании, представляясь генеральным директором. Они использовали видео, чтобы убедить сотрудников в том, что им необходимо сделать срочный перевод средств на «специальный счет».

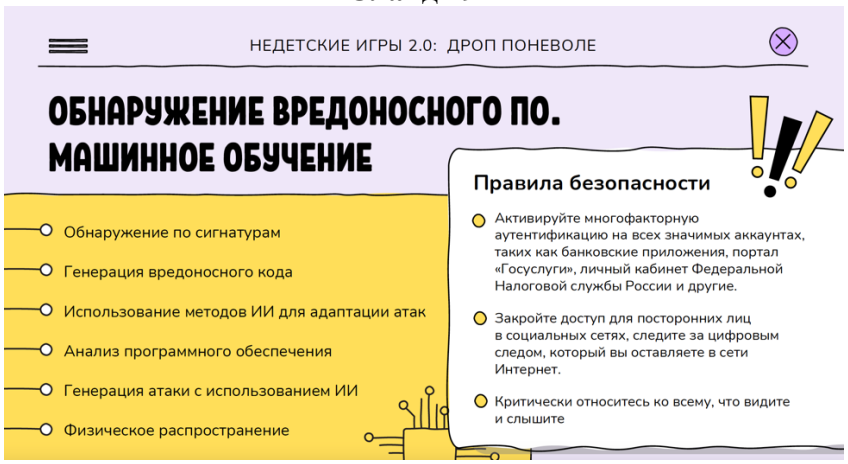
Вымогательство. В результате манипуляций мошенников сотрудники филиала сделали перевод значительной суммы денег, полагая, что руководство компании действительно дало такое указание.

Раскрытие мошенничества. Когда стало очевидно, что денежные средства не были переведены по легальным причинам, компания начала расследование. В ходе расследования было выяснено, что видео было фальшивым, и это привело к осознанию того, как технологические новшества могут быть использованы в преступных целях.

Этот случай иллюстрирует, насколько опасной может быть технология дипфейков, особенно когда речь идет о

	финансовых махинациях и вымогательстве. Сложность в том, что такие технологии могут создавать высококачественные видео, которые трудно отличить от настоящих, что делает их идеальным инструментом для мошенников.
Слайд 17  	Один из реальных примеров использования технологий генерации человеческого голоса для вымогательства денежных средств связан с мошенничеством, которое получило название «подделывание голоса» (voice spoofing). **Пример такого вида мошенничества.** **Создание подделки голоса.** Мошенники использовали алгоритмы обработки звука и технологии глубокого обучения для имитации голоса руководителя компании. Они обучили модель на основе аудиозаписей настоящего голоса руководителя с публичных выступлений или телефонных звонков. **Фейковый звонок с просьбой о помощи.** После создания фейкового голоса мошенники позвонили на рабочий телефон одного из сотрудников компании, представляясь руководителем компании. Они использовали различные методы, чтобы подделать номер телефона, чтобы он выглядел законным и вызывал доверие. Во время звонка мошенник имитировал голос руководителя, утверждая, что компания попала в сложную финансовую ситуацию и очень срочно нужна помощь. Они могли ссылаться на срочные финансовые переводы, которые нужно было сделать немедленно для предотвращения больших убытков **Вымогательство средств.** Поскольку голос звучал правдоподобно и имел эмоциональный окрас, сотрудники поддались панике и немедленно выполнили перевод средств на указанный мошенниками счет, полагая, что это распоряжение их руководства. Подобные случаи показывают, как технологии генерации человеческого голоса могут быть использованы

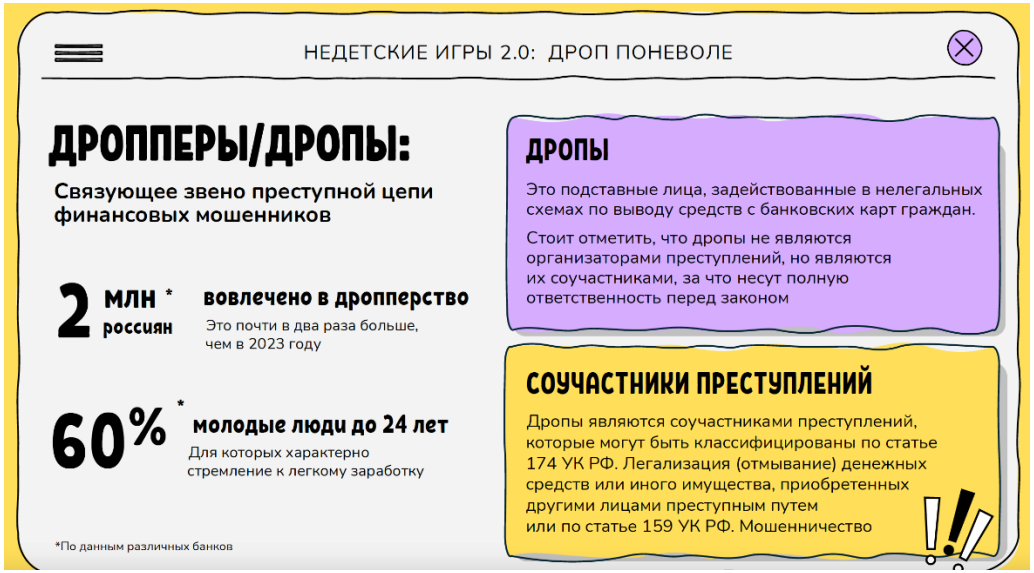
	для обмана и вымогательства. После таких инцидентов организации начинают пересматривать свои внутренние процедуры, чтобы предотвратить подобные мошенничества, включая обучение сотрудников по распознаванию подозрительных запросов, а также внедрение многофакторной аутентификации для финансовых операций. Эти примеры подчеркивают важность бдительности и осведомленности, поскольку ***технологии, использующие искусственный интеллект для создания подделок, становятся все более доступными и распространенными.***
Слайд 18 	Одним из случаев мошенничества на основе сбора всесторонней информации о деятельности одной из международных компаний является инцидент, связанный с так называемым «CEO Fraud». Для достижения своих целей мошенники использовали информацию, собранную из открытых источников и социальных сетей. **Создание фальшивого профиля.** Используя собранные данные, мошенники создали поддельный адрес электронной почты, который внешне казался легитимным. Они использовали адрес, схожий с настоящим, изменив всего одну букву или добавив поддомен (например, вместо ceo@company.com использовали ceo@company.co). **Осуществление мошеннического запроса.** Мошенник отправил электронное письмо одному из высокопоставленных сотрудников компании, входящих в состав ее руководства, представившись CEO компании. В письме он созвал «срочное собрание руководства компании» и попросил сделать трансферы денежных средств на «расходы, связанные с конфиденциальными сделками», которые, по его словам, должны были оставаться в тайне от других сотрудников. Письмо выглядело убедительным. Мошенник использовал правильный и характерный для CEO стиль общения и корпоративные термины.

	Выполнение перевода. В результате этого мошеннического обращения сотрудник, выполняя указания CEO, перевел значительную сумму денег на указанный мошенниками счет. Сделка проходила в сжатые сроки, что оказывало дополнительное психологическое давление на сотрудника. **Раскрытие мошенничества.** При анализе финансовой отчетности аудиторами были выявлены факты перевода денежных средств по подозрительным основаниям. При дальнейшем детальном анализе был установлен факт мошенничества и раскрыли всю цепочку действий злоумышленников. Этот случай подчеркивает важность проявления бдительности в вопросах кибербезопасности, особенно в отношении использования открытых данных для мошенничества. Многие компании вводят дополнительные меры безопасности, такие как многофакторная аутентификация, проверки на подлинность обращений высшего руководства, а также использование технологий искусственного интеллекта для распознавания подозрительных запросов.
Слайд 19 	Технологии искусственного интеллекта (ИИ) в области кибербезопасности включают как защиту, так и атаки. Обнаружение вредоносного ПО. Машинное обучение: Современные антивирусные и антишпионские программы используют алгоритмы машинного обучения для анализа поведения программ. Эти алгоритмы могут выявлять подозрительное поведение даже в новых, неизвестных образцах вредоносного ПО. Например, программа может отслеживать как приложение взаимодействует с файлами и сетью. Если оно пытается шифровать файлы или отправлять данные на неизвестные серверы, то считается подозрительным. **Обнаружение по сигнатурам.** Системы, использующие алгоритмы машинного обучения и глубокого

	машинного обучения, могут анализировать большой объем данных о сигнатурах вредоносного кода и сравнивать их с файлами, находящимися в системе. Эти технологии позволяют обнаруживать подобные угрозы. **Генерация вредоносного кода**. Группы мошенников могут использовать алгоритмы генерации кода, основанные на методах ИИ для создания новых версий вирусов и троянов. Например, генеративные модели, такие как GAN (Generative Adversarial Networks), могут использоваться для создания уникальных образцов вредоносного кода, которые с меньшей вероятностью могут быть обнаружены традиционными антивирусными программами. **Использование методов ИИ для адаптации атак**. Вредоносный код может использовать ИИ для анализа программных систем, которые он пытается атаковать. Например, при «взломе» веб-сайтов методы ИИ могут автоматически анализировать уязвимости системы даже без доступа к интернету путем изучения файлов конфигурации и настроек хостинга, которые могут быть доступны через локальный доступ. **Анализ программного обеспечения**. Злоумышленник может установить систему, использующую алгоритмы машинного обучения и/или нейросетевые алгоритмы на локальный компьютер, и использовать ее для анализа ПО, которое находится в сети или внешних носителях, чтобы выявить потенциальные уязвимости. **Генерация атаки с использованием ИИ**. На основе изученных уязвимостей методами ИИ можно сгенерировать исполняемый файл или скрипт. Такой скрипт может автоматически подстраивать свои действия в зависимости от программного окружения, к которому он попадает. **Физическое распространение**. Вредоносный код может быть загружен на устройства обычным способом

	(например, через USB-накопитель) и запущен для компрометации системы без необходимости подключения к интернету. Использование технологий ИИ для обеспечения кибербезопасности вызывает серьезные опасения и предстоящие вызовы. Защитные механизмы должны адаптироваться к новейшим угрозам, включая те, которые используют ИИ для создания вредоносного ПО. Правила безопасности!!! 1. Активируйте многофакторную аутентификацию на всех значимых аккаунтах, таких как банковские приложения, портал «Госуслуги», личный кабинет Федеральной Налоговой Службы России и другие. 2. Закройте доступ для посторонних лиц в социальных сетях, следите за цифровым следом, который вы оставляете в сети Интернет. 3. Критически относитесь ко всему, что видит и слышите

Слайд 20



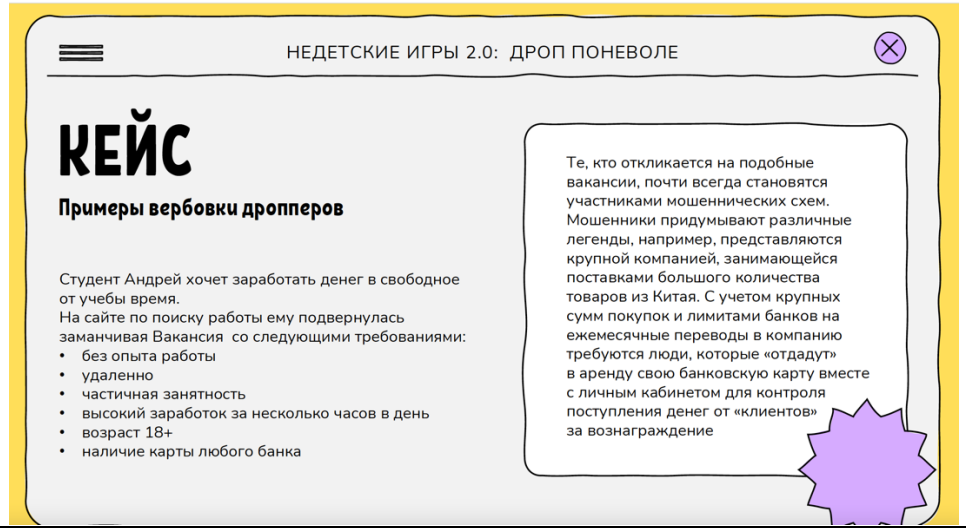
Дропперы/дропы: связующее звено преступной цепи финансовых мошенников

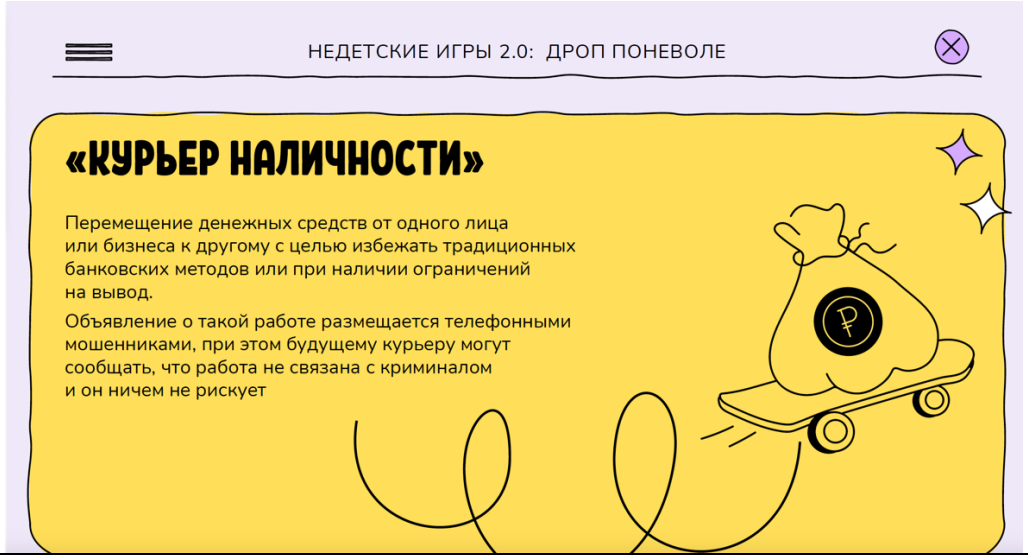
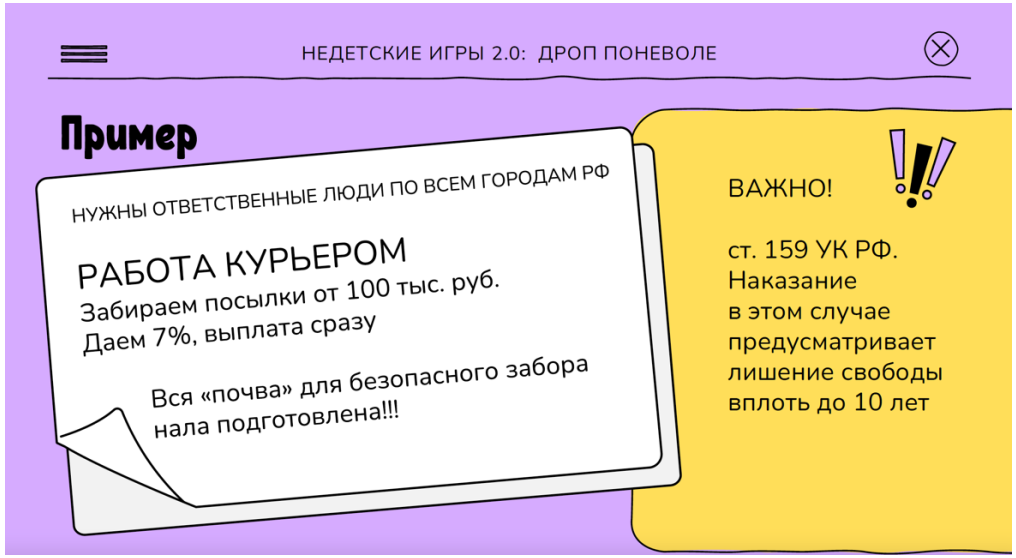
Ежегодно растет количество и суммы хищений средств у населения, в связи с этим растет и количество так называемых дропперов (от английского drop – «падать», «сбросить»). Дропы являются соучастниками преступлений, которые могут быть классифицированы по статье 174 УК РФ. Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем или по статье 159 УК РФ Мошенничество. МВД России разработало законопроект об уголовной ответственности для дропперов. Передачу зарегистрированных на себя электронных средств платежа или доступа к ним предложено определять как **преступление средней степени тяжести**, но, если преступление совершено **в составе организованной группы**, его квалифицируют как **тяжкое преступление**.

Дропы – это подставные лица, которые задействованы в нелегальных схемах по выводу средств с банковских карт граждан. Стоит отметить, что дропы не являются организаторами преступлений, но являются их соучастниками, за что несут полную ответственность перед законом.

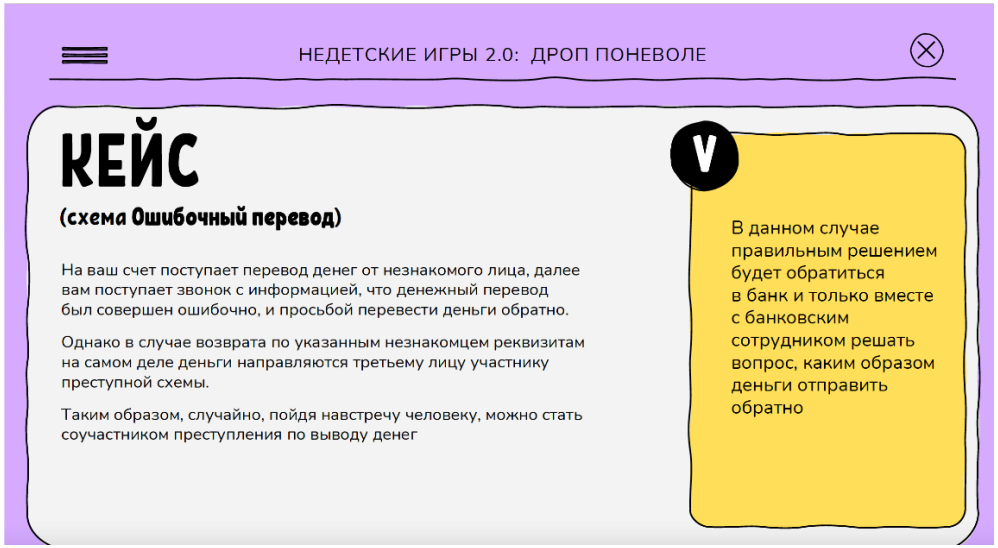
По сведениям ЦБ РФ, как правило, дропперами являются люди, нуждающиеся в деньгах: социально неблагополучные категории граждан, студенты или школьники, которым родители оформили карту с 14 лет.

Дропперы могут быть использованы злоумышленниками в разных качествах, к примеру, дроп может передать оформленную банковскую карту и онлайн-доступ к ней мошеннику, который далее самостоятельно пересылает деньги на другие счета с целью усложнить цепочку и «замыть» следы. В некоторых случая дроп

	получает на свои счета похищенные средства, обналичивает их и передает злоумышленникам. Известны случаи, когда дропы перевозят наличные средства в другие регионы страны и совершают иные противоправные действия. Формат работы дропа зависит от того, каким образом его вовлекли/завербовали в преступную схему. По данным «Сбера», в дропперство вовлечено порядка 2 млн россиян – это почти в два раза больше, чем в 2023 году. Около 60% – молодые люди до 24 лет, для которых характерно стремление к легкому заработку.
Слайд 21  	• ***Примеры вербовки дропперов*** *Под видом работодателя.* Принятие подобных предложений заканчивается вовлечением в преступные схемы молодых людей, которые не понимают, что они делают. Задачей мошенников является убеждение людей под разными легендами осуществлять переводы денег другим людям либо вовсе передать полный доступ к своему личному кабинету банка.

Слайд 22 	Еще один пример, который получил большое распространение – это подработка *«Курьером наличности».* По сведениям межрегионального управления Федеральной службы по финансовому мониторингу по СФО, мошенники активно распространяют информацию в социальных сетях о возможности подработки в качестве курьера.
Слайд 23 	*«Курьер наличности»* - перемещение денежных средств от одного лица или бизнеса к другому, с целью избежать традиционных банковских методов или при наличии ограничений на вывод. Объявление о такой работе размещается телефонными мошенниками, при этом будущему курьеру могут сообщать, что работа не связана с криминалом и он ничем не рискует. Рассмотрим реальный пример предложения о работе *«курьером наличных»:* Повторим еще раз, что подобные действия, в том числе и данное может классифицироваться как мошенничество по ст. 159 Наказание в этом случае предусмотрено вплоть **до 10 лет лишения свободы.** Мошенничество является умышленным преступлением, а курьеров чаще всего не посвящают в детали, говоря только о необходимости получения и перевода денежных средств (что деньги потерпевших людей об этом конечно же умалчивается).

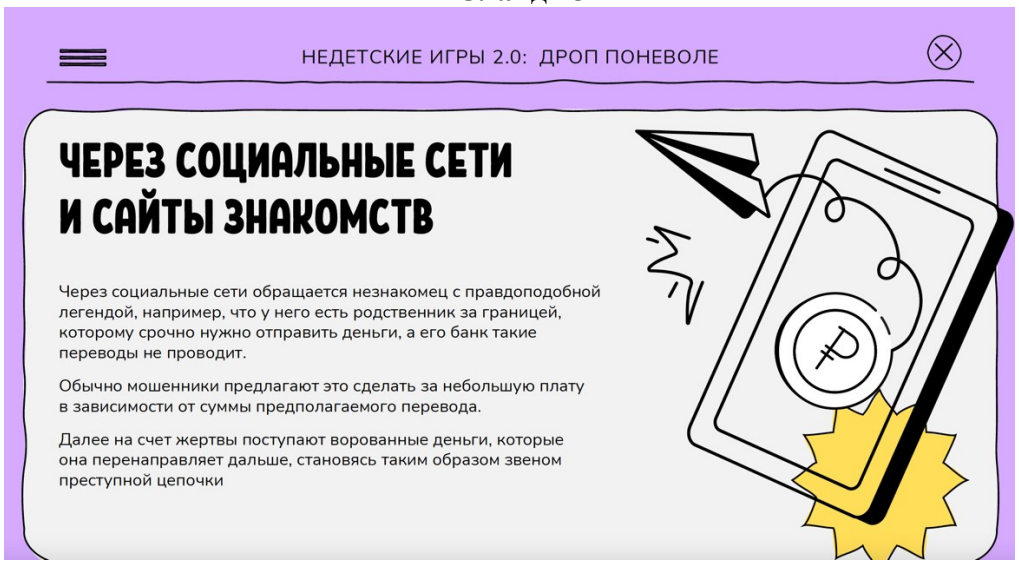
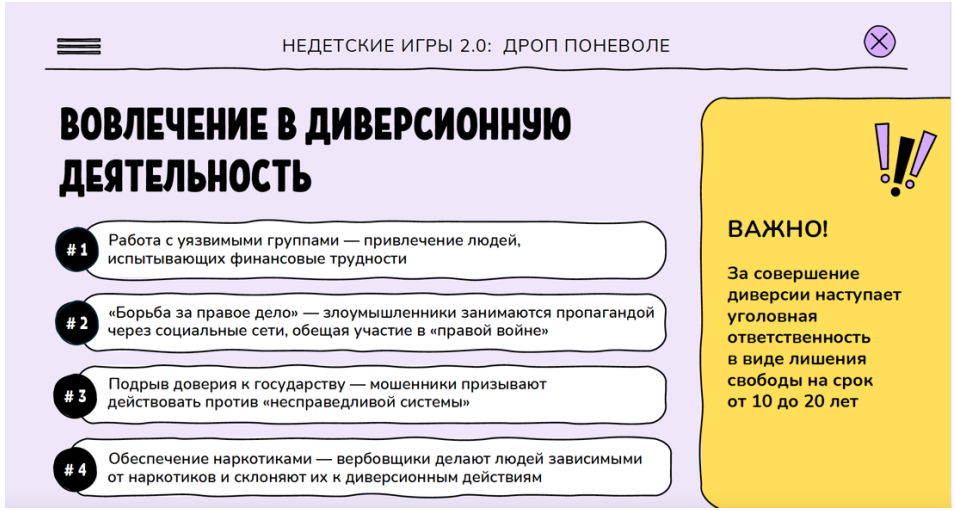
Слайд 24

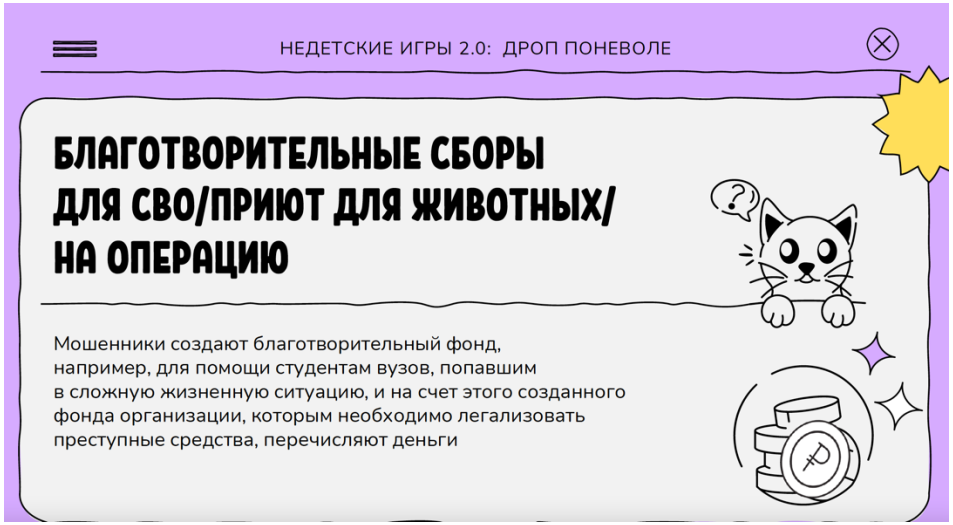


Под видом ошибившегося человека.

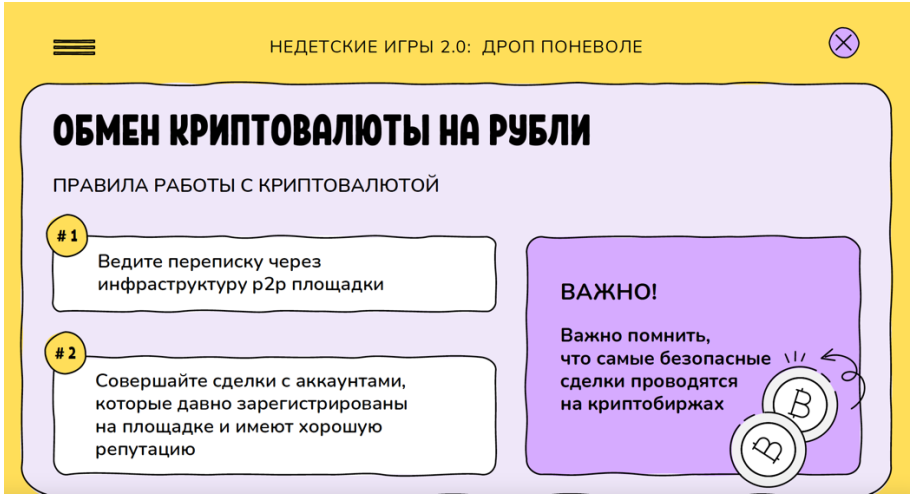
Подобная схема может реализована через пополнение номера телефона незнакомыми лицами, которые также связываются со своей «жертвой», сообщая, что произошла ошибка и просят перевести деньги «обратно», но по факту третьим лицам.

В данном случае правильным решением будет обратиться в банк и только вместе с банковским сотрудником решать вопрос, каким образом деньги отправить обратно.

Слайд 25  	*Через социальные сети и сайты знакомств* На сайте знакомств как правило, мошенники выбирают девушек с небольшим заработком и финансовыми обременениями. Они дарят небольшой подарок и предлагают приличные деньги за просьбу перевести через свой счет деньги другу, брату или маме нового знакомого, чтобы сэкономить на комиссии. После пары переводов «молодой человек» исчезает».
Слайд 26  	*Вовлечение в диверсионную деятельность.* Конечной целью данного «мероприятия» является дестабилизация экономической безопасности и обороноспособности государства. Привлечение людей в схему поджогов и террористических актов является серьезной угрозой безопасности общества. Рассмотрим способы вербовки. Что касается уголовной ответственности за соучастие в диверсионных действиях, то важно знать, что за диверсию привлекается любое вменяемое физическое лицо, достигшее 16-летнего возраста, и преследуется статьей 281 УК РФ. Также стоить отметить отдельно, что диверсионные действия квалифицируются как тяжкие преступления. За совершение диверсии наступает уголовная ответственность в виде лишения свободы на срок от 10 до 20

	лет лишения свободы.
Слайд 27  	*Благотворительные сборы для СВО/приют для животных/на операцию.* Рассмотрим пример «отмывания» денег на примере благотворительных фондов. Надо отметить, что данная схема не нова и существует продолжительное время. «Работает» она следующим образом: Далее для обналичивания денег со счета фонда привлекаются, например, «завербованные» студенты, которым якобы требуется материальная помощь, в связи с чем они обратились в тот самый благотворительный фонд. В результате на карту студента из фонда поступает сумма, которую он обналичивает в банкомате и отдает ее обратно мошенникам, оставляя себе малую часть. Таким образом, человек становится дроппером, то есть соучастником преступления, в котором доказать свою невиновность будет очень трудно.

Слайд 28



Обмен криптовалюты на рубли

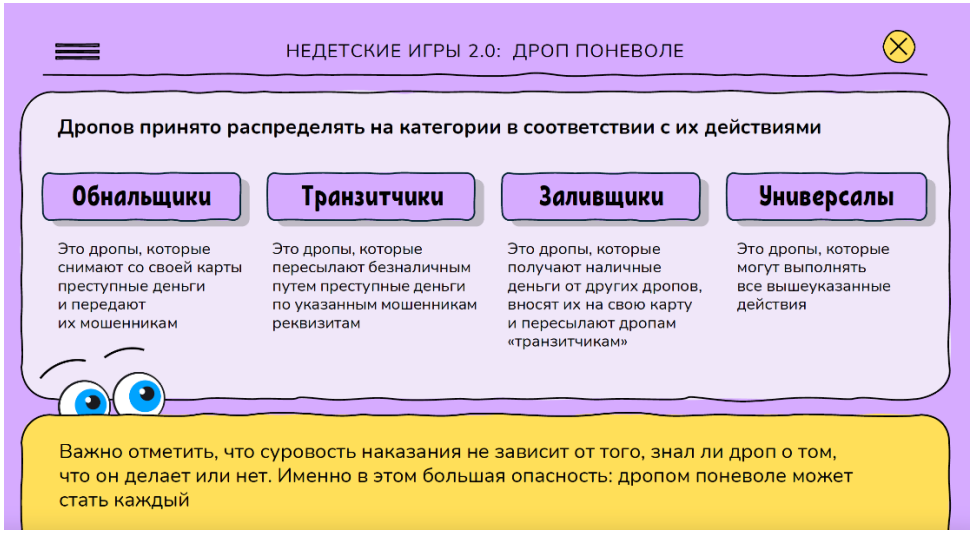
Одна из распространённых схем «обеления» преступных денег является покупка криптовалюты на p2p платформах. Множество инвесторов используют именно p2p площадки вместо криптобирж по причине низких комиссий, а также возможности удаленно купить криптовалюту. Именно этим и пользуются мошенники: они действительно покупают криптовалюту у продавцов, но делают это с целью легализации преступных доходов. В результате на счет продавца криптовалюты поступают похищенные денежные средства с карты дропа.

Соответствующие службы банков мониторят подобные сделки и блокируют счета не только дропа, но и продавца в рамках 115 ФЗ (О противодействии легализации(отмыванию) денежных средств, полученных преступным путем, и финансированию терроризма), более того, может быть возбуждено уголовное дело. Таким образом, можно случайно стать соучастником преступления.

Нужно отметить, что на 100% защитить себя от рисков получить себе на счет «грязные» деньги при проведении p2p сделок невозможно, однако можно снизить риски, соблюдая несколько рекомендаций: вести переписку через инфраструктуры p2p площадки, совершать сделки с аккаунтами, которые давно зарегистрированы на площадке и имеют хорошую репутацию.

P2p-сервисы ведут учет количества проведенных операций клиентами и показывают процент успеха. Чем эти показатели выше, тем больше доверия заслуживает трейдер. Важно помнить, что самые безопасные сделки проводятся на криптобиржах.

Слайд 29



Дропов принято распределять на категории в соответствии с их действиями:

Обнальщики – это дропы, которые снимают со своей карты преступные деньги и передают их мошенникам.

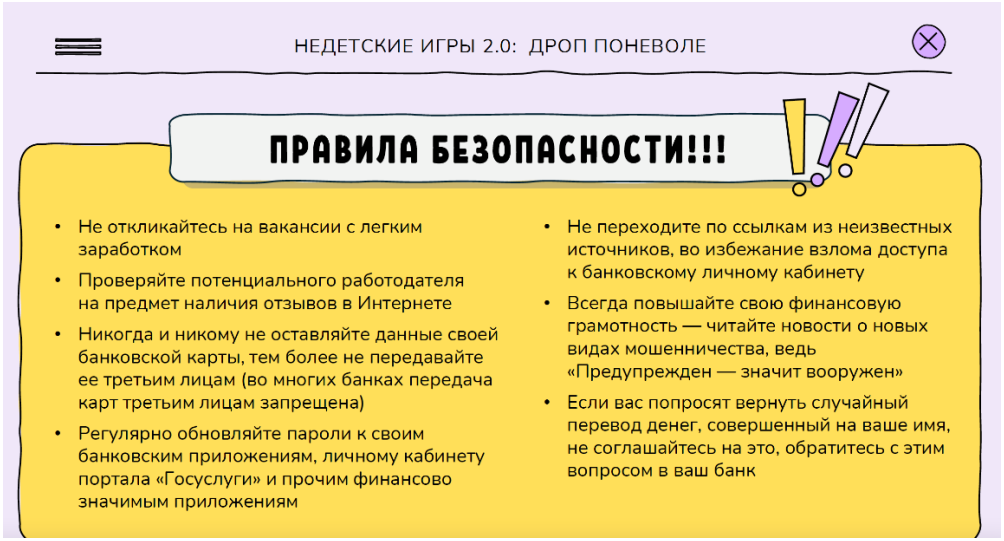
Транзитчики – это дропы, которые пересылают безналичным путем преступные деньги по указанным мошенникам реквизитам.

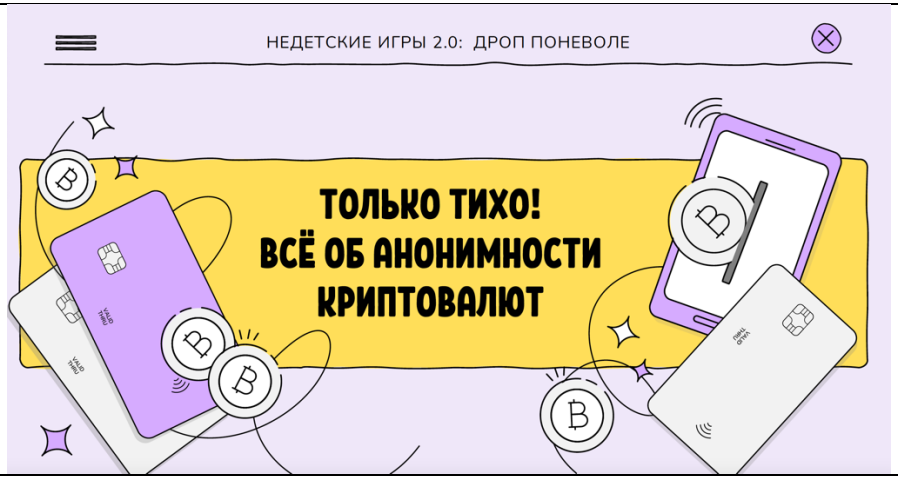
Заливщики **–** это дропы, которые получают наличные деньги от таких же дропов, вносят их на свою карту и пересылают дропам «транзитчикам».

Универсалы – это дропы, которые могут выполнять все вышеуказанные действия.

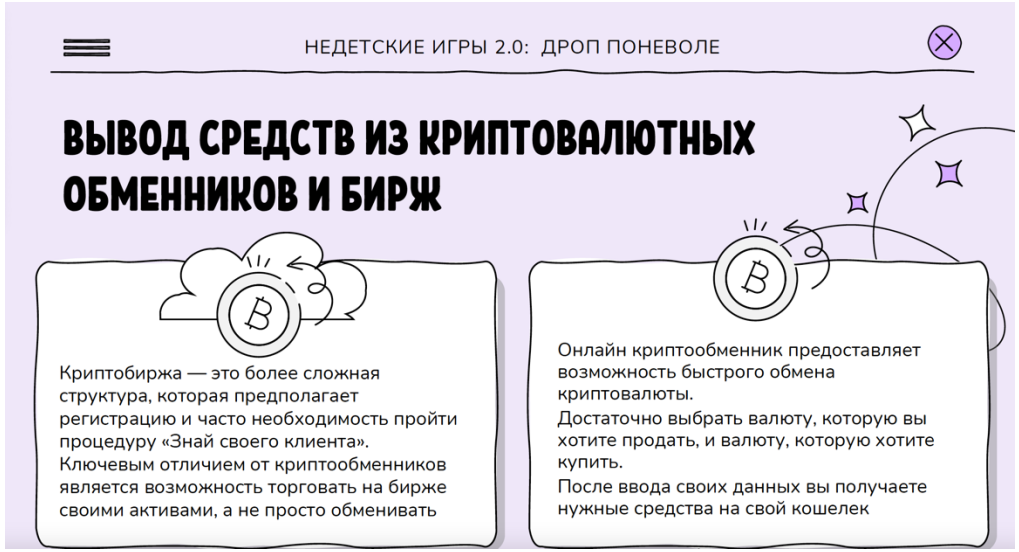
Помогать мошенникам «выводить» похищенные деньги – мероприятие неблагодарное. Действия дропперов могут попасть под уголовную статью 159 «Мошенничество» или 174 «Легализация денежных средств». При этом может быть назначен как немалый штраф, так и более суровое наказание – арест. В этом случае срок заключения в тюрьме может достигать 7 лет. Кроме того, в перспективе обеспечены минимальные шансы на обслуживание в том или ином банке, что в современной жизни практически невозможно.

Важно отметить, что суровость наказания не зависит от того, знал ли дроп о том, что он делает, или нет. Именно в этом большая опасность: дропом поневоле может стать каждый.

Слайд 30  	**Правила безопасности!!!** - не откликайтесь на вакансии с легким заработком; - потенциального работодателя проверяйте на предмет наличия отзывов в Интернете; - никогда и никому не оставляйте данные своей банковской карты, тем более не передавайте ее третьим лицам (во многих банках передача карт третьим лицам запрещена); - регулярно обновляйте пароли к своим банковским приложениям, личному кабинету портала «Госуслуги» и прочим финансово значимым приложениям; - если вас попросят вернуть случайный перевод денег, совершенный на ваше имя, не соглашайтесь на это, обратитесь с этим вопросом в ваш банк; - не переходите по ссылкам из неизвестных источников, во избежание взлома доступа к банковскому личному кабинету; - всегда повышайте свою финансовую грамотность – читайте новости о новых видах мошенничества, ведь «Предупрежден – значит вооружен».
Слайд 31	Например, такие криптовалюты, как Monero и Zcash, предоставляют инвесторам полную анонимность. Существуют криптокошельки, не требующие полной верификации его владельца, что также предоставляет анонимность инвесторам, чем охотно пользуются мошенники. В целом вся суть криптографии и блокчейна – это конфиденциальность, безопасность и децентрализация. Вместе с тем стоит отметить, что такие органы государственной власти, как Федеральная служба по финансовому мониторингу (Росфинмониторинг), Центральный Банк РФ и прочие, находятся в поиске инструментов, в том числе на техническом и законодательном уровнях, позволяющих взять под контроль

	операции цифровых активов. Одна из основных проблем правоохранительных органов при распутывании преступных схем заключается в использовании мошенниками подставных лиц – дропов, на чьи имена открываются криптокошельки. Поэтому соответствующие службы стараются установить связь подставного лица с реальными исполнителями мошеннических операций, но и это является трудной задачей, так как «отношения» между ними выстраиваются как правило дистанционно.

Слайд 32



Существует два основных, но не единственных метода по обмену криптовалюты: это использование криптобирж и криптообменников.

Криптообменники бывают двух видов: онлайн и офлайн.

Онлайн криптообменник предоставляет возможность быстрого обмена криптовалюты. Достаточно выбрать валюту, которую вы хотите продать, и валюту, которую хотите купить. После ввода своих данных вы получаете нужные средства на свой кошелек.

Офлайн вариант криптообменника подходит наилучшим образом для наличного обмена. То есть если нужно обменять криптовалюту на рубли или рубли на криптовалюту, то данный вариант будет самым приемлемым. Некоторые криптоомбенники позволяют проводить операции анонимно.

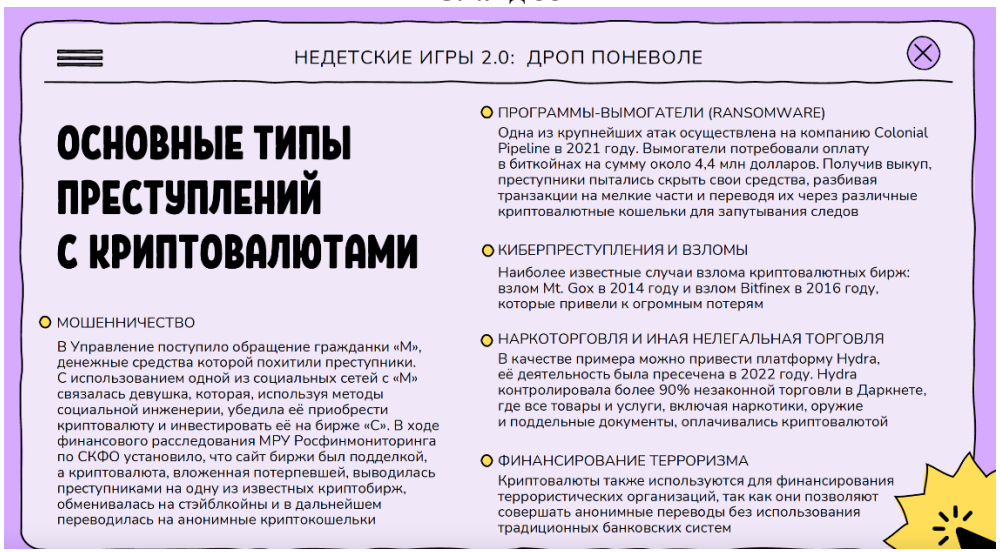
Криптобиржа – это более сложная структура, которая предполагает регистрацию и часто необходимость пройти процедуру «Знай своего клиента». Ключевым отличием от криптообменников является возможность торговать на бирже своими активами, а не просто обменивать.

С точки зрения рисков оба варианта являются рискованными, однако в случае использования криптобирж рисков становится меньше.

	По данным ЦБ, активность российских пользователей на рынке криптоактивов выросла за IV квартал 2023 – I квартал 2024 года. Об этом свидетельствует количество посещений сайтов крупнейших криптовалютных торговых площадок и объем потоков криптовалюты на биржах, который оценочно приходится на россиян. Криптовалют на рынке огромное множество, однако с точки зрения доходности мы рассмотрим наиболее популярную – биткоин. По данным РБК-Инвестиции за 2024 год, вложение в биткоин оказалось бы самым прибыльным, он принес бы инвестору доходность 146,35% в рублях. За это время курс биткоина вырос с 4 000 027 до 9 854 180 в рублевом эквиваленте. Конечно же, биткоин, как и другие криптовалюты, и в целом финансовые активы, очень волатилен, например, в ноябре 2021 года 1 биткоин стоил порядка 61 000 $, а в ноябре 2022 года уже 20 000$, то есть минус 300%. Вместе с ростом цены биткоина увеличивался и уровень его волатильности – с 23,4% в конце 3 квартала 2023 года до 80% в конце первого квартала 2024 года. Помимо этого, растут и риски в связи с возможными санкциями со стороны недружественных стран, что может привести к потере доступа к активам в случае их блокировки со стороны эмитентов криптовалют. Также нужно помнить, что чем выше доходность того или иного финансового актива, тем многократно выше и риски. Стоит помнить, что инвесторы покупают, например, биткоин потому, что он растет в цене, а в цене он растет потому как раз, что его покупают инвесторы, что приводит к замкнутому кругу, в котором можно как заработать, так и потерять свои средства. Сделки с криптовалютами сложно отследить, почти невозможно отменить транзакцию (сделку по купли-продаже

	актива). Следовательно, рискам в этом отношении подвержены оба участника сделки, если между ними нет надежного посредника. Стоит отметить, что даже мошеннические схемы на «этом рынке» отменить нельзя. Например, широко известен случай с «раздачей монет», где на фишинговом сайте от имени миллиардера Илона Маска сообщалось о несуществующей акции департамента Tesla по маркетингу, в ходе которой все поклонники марки могут получить криптовалюту. Для участия в акции необходимо выслать от 0,1 до 20 BTC (Bitcoin) или от 1 до 100 ETH (Ethereum) якобы для проверки, а обратно будет отправлено вдвое больше. На самом деле это была распространённая схема в блокчейне-сфере, и деньги возвращены доверчивым «инвесторам» не были.

Слайд 33



Разберем основные типы преступлений с криптовалютами:

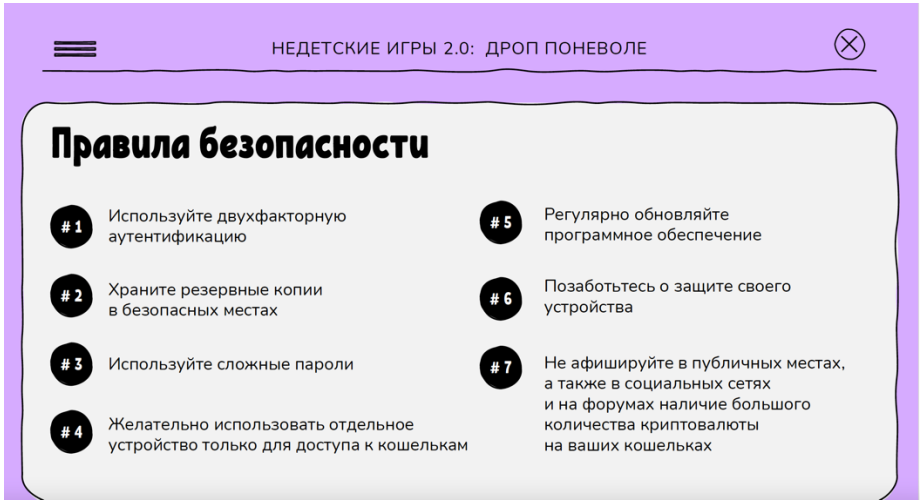
1. Мошенничество является одним из самых распространённых видов преступлений с цифровыми валютами. Злоумышленники создают фальшивые инвестиционные схемы, платформы для обмена криптовалюты или поддельные ICO (Initial Coin Offering). Пользователи вводятся в заблуждение и переводят свои средства, которые затем исчезают. В качестве примера можно привести финансовое расследование, которое проводило МРУ Росфинмониторинга по СКФО в 2022 году. В Управление поступило обращение гражданки «М», денежные средства которой похитили преступники. С использованием одной из социальных сетей с гражданкой «М» связалась девушка, которая, используя методы социальной инженерии, убедила «М» приобрести криптовалюту и инвестировать её на бирже «С». В ходе финансового расследования МРУ Росфинмониторинга по СКФО установило, что сайт биржи был подделкой, а криптовалюта, вложенная потерпевшей, выводилась преступниками на одну из известных криптобирж, обменивалась на стэйблкойны и в дальнейшем переводилась на анонимные криптокошельки.

Одна из крупнейших атак осуществлена на компанию Colonial Pipeline в 2021 году. Вымогатели потребовали оплату в биткойнах на сумму около 4,4 млн долларов. После получения выкупа преступники пытались скрыть свои средства, разбивая транзакции на мелкие части и переводя их через различные криптовалютные кошельки для запутывания следов.

Наиболее известные случаи взлома криптовалютных бирж, такие как взлом Mt. Gox в 2014 году и взлом Bitfinex в 2016 году, привели к огромным потерям.

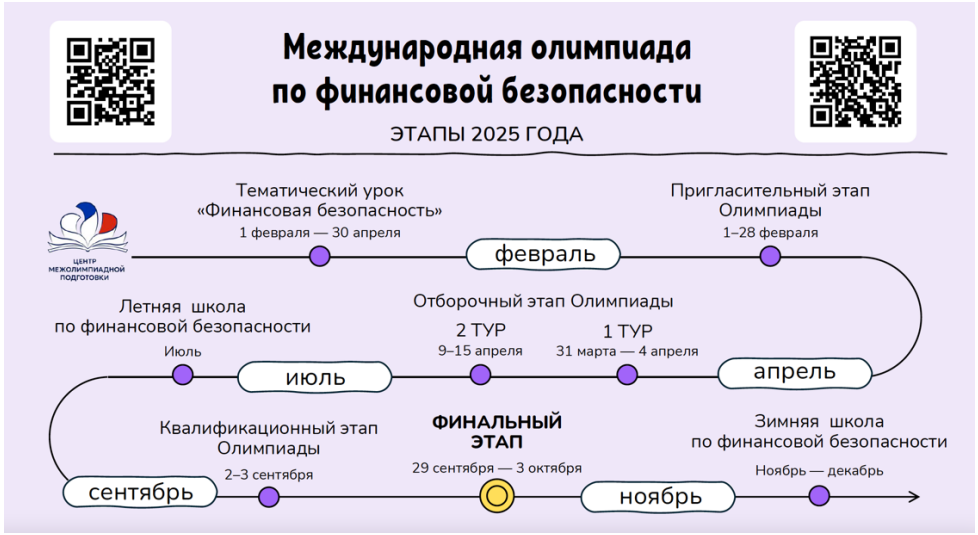
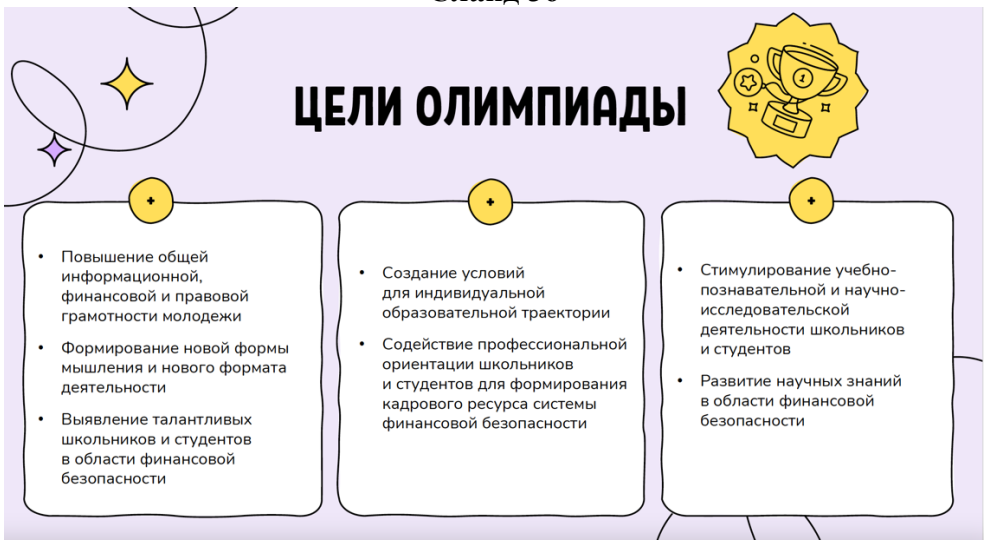
2. **Программы-вымогатели (ransomware)** — это один из наиболее распространённых видов кибератак, при которых злоумышленники шифруют данные на компьютерах жертвы и требуют выкуп, обычно в криптовалюте, для их восстановления. Этот тип атак особенно опасен, так как может парализовать работу компаний, больниц, государственных учреждений и других критически важных организаций. Деньги от жертв поступают в криптовалюте, после чего преступники используют сервисы «миксеры» (tumbler) для

Слайд 34



Правила безопасности

- Используйте двухфакторную аутентификацию. Если криптокошелек дает возможность, создайте «сид-фразу» для восстановления доступа в случае потери устройства или повреждения программного обеспечения.
- Храните резервные копии в безопасных местах, таких как сейфы, и не сохраняйте их в электронном виде (например, на компьютере или в облаке).
- Используйте сложные пароли.
- Желательно использовать отдельное устройство только для доступа к кошелькам.
- Регулярно обновляйте программное обеспечение.
- Не используйте публичные сети Wi-Fi.
- Позаботьтесь о защите своего устройства: устанавливайте пароли, биометрическую аутентификацию на своих устройствах.
- Не афишируйте в публичных местах, а также в социальных сетях и на форумах наличие большого количества криптовалюты на ваших кошельках.

Слайд 35  	Международная олимпиада по финансовой безопасности
Слайд 36  	Проведение Олимпиады направлено на популяризацию финансовой безопасности как нормы жизни, а также на формирование у молодежи нового типа мышления: от безопасности личности – к безопасности государства. В Олимпиаде принимают участие студенты бакалавриата (1–3 курс), специалитета (1–4 курс) и магистратуры (1 курс) вузов стран-участниц Олимпиады, а также школьники 8–10 классов российских школ. С учетом профиля Олимпиады («Финансовая безопасность») олимпиадные задания составлены на основе следующих программ: - для школьников – на основе программ общеобразовательных предметов: математика и информатика, обществознание, экономика; - для студентов – на основе основных образовательных программ высшего образования по направлениям подготовки:

	• юриспруденция; • математика, прикладная математика и информатика, прикладная математика, математика и компьютерные науки, фундаментальная информатика и информационные технологии, информатика и вычислительная техника, прикладная информатика, информационная безопасность, бизнес-информатика; • экономика, финансы и кредит, экономическая безопасность; • международные отношения, регионоведение. Победители и призеры Олимпиады получают преимущества при поступлении в вузы Международного сетевого института в сфере ПОД/ФТ на программы бакалавриата, магистратуры и аспирантуры в соответствии с льготами олимпиад I уровня, а также возможность стажироваться в Росфинмониторинге и других организациях. Олимпиада проходит в несколько этапов: − тематический урок "Финансовая безопасность"; − пригласительный этап; − отборочный этап; − квалификационный этап; − финальный этап.

Слайд 37	Международная олимпиада по финансовой безопасности
	

Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский университет дружбы народов имени Патриса Лумумбы»

Методические рекомендации по подготовке и проведению тематического урока на тему:

«НЕдетские игры 2.0: Дроп поневоле»

Москва, 2025

Оглавление

Аннотация

Методические рекомендации подготовлены в помощь педагогам образовательных организаций для проведения тематического урока, посвященного противодействию вовлечения молодых людей школьного возраста (8-11 классы) в финансовые преступления в качестве жертв и соучастников.

В методических рекомендациях предлагаются содержательные, методические и технологические подходы к проведению урока, раскрывается комплекс вопросов, связанных с организацией данного мероприятия. Предлагаемые материалы носят рекомендательный характер, поэтому преподаватель может провести одно или несколько занятий, опираясь на данные разработки, исходя из собственного опыта, учитывая возрастные особенности, уровень подготовки обучающихся, а также традиции региона.

Пояснительная записка

Финансовая грамотность молодежи способствует принятию ими грамотных решений, минимизирует финансовые риски и тем самым способствует повышению финансовой безопасности населения в целом. Низкий уровень финансовой грамотности может привести не только к банкротству, но и уязвимости к финансовым мошенничествам, чрезмерным долгам, социальным проблемам, а также к неграмотному планированию выхода на пенсию.

Согласно аналитическим данным ЦБ РФ по итогу 3 квартала 2024 года, основными инструментами, которые используют мошенники, по-прежнему остаются социальная инженерия, фишинговые атаки, однако лидирует по количеству преступлений телефонное мошенничество[11]. Более того

[1] Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств // ЦБ РФ. 09.12.2024. URL: https://cbr.ru/statistics/ib/review_3q_2024

сегодняшнее время особо опасно, поскольку ввиду высоких процентных ставок по вкладам население не только размещает свои сбережения, которые находились дома «под подушкой», но и переводит свои средства с фондового рынка (рынка ценных бумаг) в денежный рынок (вклады). Это представляет для кибермошенников особый интерес не только с точки зрения социальной инженерии, но и с точки зрения компьютерных атак. В связи с этим мы должны следить за трендами мошенников, ведь «предупрежден значит вооружен».

Внедрение современных цифровых технологий в различные сферы жизни и производства, упрощают нашу жизнь, но вместе с тем несут новые риски. Доступность информации и в первую очередь медиаконтента является основным источником пропаганды, мессенджеры используются для вербовки и координации преступной деятельности, цифровые валюты и электронные платежи применяются для отмывания денег и финансирования терроризма.

Еще одной уязвимостью является рынок криптовалюты и развивающиеся системы электронных платежей, которые активно используются для отмывания денежных средств. Новые механизмы финансовых операций активно прогрессируют и зачастую выходят за рамки контроля регуляторов (например ЦБ РФ), таким образом становятся инструментом финансирования преступной деятельности не только на территории Российской Федерации, но и во всем мире.

Существенную угрозу представляют многочисленные кол-центры, расположенные на территории недружественных государств, которые занимаются хищением денежных средств граждан и зачастую пытаются вынудить потерпевших совершить диверсионные действия. Эти центры неоднократно задействовались для массированных телефонных атак с сообщениями о готовящихся терактах.

С быстрым развитием электронных средств обмена и передачи данных все больше и больше преступлений совершается с применением высоких технологий.

Если говорить о цифрах, то, по сведениям ЦБ РФ, мошенники в III квартале 2024 года похитили у клиентов банков 9,3 млрд рублей, что в 1,9 раза больше показателя за II квартал (4,3 млрд рублей) и в 2,2 раза превышает средний показатель за предшествующие четыре квартала[2].

Согласно статистическим данным МВД, фиксируется ежегодный рост количества зарегистрированных преступлений с использованием информационно-телекоммуникационных технологий (ИТТ). За последние четыре года их число увеличилось на треть (+32,6%) с 510,4 тыс. в 2020 году до 677 тыс. в 2023 году. Органами внутренних дел РФ в 2023 году расследованы уголовные дела, возбужденные по фактам совершения 149,9 тыс. (+20%) посягательств данной категории, в период с января по июнь 2024 года – 82,3 тыс. (+1,9%) IT–деяний. В структуре ИТТ преступности в 2023 году преобладали дистанционные кражи и мошенничества, которые составили почти три четверти таких преступлений (70,2) %.

В январе-июне 2024 года число зарегистрированных ИТТ преступлений увеличилось на 15,8% и достигло 368,7 тыс.

Традиционные банковские инструменты используются злоумышленниками для осуществления вывода теневых денежных средств, полученных от совершения киберпреступлений, незаконной игорной деятельности (онлайн-казино), торговли наркотиками, оружием и другой противоправной деятельности. Указанные денежные средства проходят через большое количество счетов дропов, на которых смешиваются с легальным денежным оборотом, выводятся на криптобиржи или криптообменники для легализации или дальнейшего использования в противоправной деятельности.

[2]Объем похищенных мошенниками в РФ средств в III кв. вырос почти вдвое относительно II кв. // Интерфакс. 09.12.2024. URL: https://interfax.ru/russia/996734

Проблема куда серьезнее, чем может показаться на первый взгляд. Подобные угрозы отмечены не только в России и могут быть актуальны для стран СНГ.

Однако у мошенников есть проблемы с так называемым «отмыванием» денежных средств. Это означает, что злоумышленникам необходимо придать вид законного владения денежными средствами, которые были получены, например, в результате кибермошенничества. Для этих целей мошенники применяют различные «инструменты», например, привлекают к этому процессу так называемых дропперов. Дропперы – это лица, которые используют свои карты для обналичивания или транзита (дальнейшей отправки) похищенных денежных средств.

Согласно материалам расследования Сбера «Анализ системы вывода денежных средств, похищенных у граждан», наиболее популярными способами вывода похищенных денежных средств являются[3]:

- перевод в криптовалюту сразу с карты потерпевшего, с так называемого «грязного» пластика;

- перевод в криптовалюту с «чистого пластика», т.е. взнос денежных средств на карты дропа, которая ранее не участвовала в сомнительных операциях;

- обналичивание, аккумулирование крупных денежных сумм, с последующей покупкой криптовалюты;

- обналичивание, аккумулирование крупных денежных сумм, с последующей покупкой валюты;

- обналичивание крупных денежных сумм, транспортировка в другой регион взнос на «чистый» пластик и далее межбанковские переводы.

Также по сведениям МВД России в настоящее время сформировалась судебная практика по взысканию на основании исков граждан

[3] Анализ системы вывода денежных средств, похищенных у граждан // Сбер Банк. URL:https://www.sberbank.ru/ru/person/kibrary/investigations/analiz-sistemy_vyvoda_denezhnyh_sredstv

неосновательного обогащения с непосредственных владельцев счетов, на которые потерпевшие перечислили денежные средства.

Так, согласно положениям статьи 1102 Гражданского кодекса РФ, лицо, которое без установленных законом, иными правовыми актами или сделкой оснований приобрело или сберегло имущество за счет другого лица (потерпевшего), обязано возвратить последнему неосновательно приобретенное или сбереженное имущество (неосновательное обогащение). В ходе рассмотрения заявленных при указанных обстоятельствах исков ответчики – номинальные владельцы счетов доказательств наличия законных оснований для приобретения денежных средств представить не могут, в связи с чем суды выносят решения в пользу потерпевших. Более того, даже заявленные ими доводы о передаче данных о счете третьим лицам не рассматриваются как достаточное основание для отказа в удовлетворении иска, поскольку в этих случаях фактически подтверждается нарушение условий банковского обслуживания.

В настоящее время в ходе исковой работы в отношении владельцев счетов, на которые пострадавшими перечислялись денежные средства, в суды подано свыше 8,6 тыс. заявлений, из которых 2,9 тыс. рассмотрено и удовлетворено на сумму более 1 млрд. рублей.

Вышеуказанные данные свидетельствуют о том, что рассматриваемая в настоящем уроке тематика является особенно актуальной в современной жизни для каждого человека.

Цель урока – мотивировать обучающихся на выработку личной стратегии грамотного поведения в ситуациях растущих финансовых рисков и финансового мошенничества.

Задачи урока:

- заложить у обучающихся основы грамотного финансового поведения;

- сформировать у обучающихся представление о признаках ситуаций финансового мошенничества, а также признаках фишинговых и других мошеннических схем;
- научить обучающихся:

- распознавать угрозу мошенничества и не совершать действий по платежам и переводам в пользу мошенников;

- использовать алгоритмы действий в типичных ситуациях, связанных с возможным или уже совершенным финансовым мошенничеством;

- предпринимать меры предосторожности при использовании различных видов денег и проведении операций с ними;

- критически относиться к предложениям с признаками давления, манипулирования, мошеннических действий;

- понимать и осознавать, что за все финансовые решения ответственность несет собственник средств, даже если решения приняты под влиянием рекламы и под давлением мошенников.

Методические приемы:

- постановка проблемы (формулировка актуальной в современной жизни проблемы является важным аспектом привлечения внимания);
- обобщение (реальные примеры выявляют единый подход при реализации мошеннических схем);
- наглядная презентация (визуализация материала позволяет обучающимся законспектировать основные тезисы);
- мозговой штурм (при обсуждении кейсов обучающимся предлагается спрогнозировать развитие событий и самостоятельно определить правильные действия жертв мошенников);
- учебная дискуссия (рассуждение над поставленными проблемами создает благоприятную атмосферу для обмена личными опытом обучающихся);

- систематизация и классификация материала (четкое деление мошеннических схем и приемов на категории позволяет представить материал в запоминающемся формате).

Раздел 1. Современные инструменты телефонного мошенничества. Наиболее популярные схемы мошенничества

Не будет преувеличением сказать, что практически каждый россиянин сталкивался с телефонными мошенниками. Вопрос знаний в сфере киберпреступлений остается по-прежнему важным, его актуальность растет в геометрической прогрессии. Согласно статистике, 80% хищений средств происходит дистанционно, более того ежегодно растет не только количество преступлений, но и объем похищенных средств[4].

- ***Схема телефонного мошенничества с использованием портала «Госуслуги»***

Злоумышленники стали активнее использовать портал «Госуслуги» в своих схемах. Ведь, получив доступ к «Госуслугам», мошенники получают самое главное: наши исчерпывающие персональные данные. Как известно, на портале имеются такие сведения, как паспортные данные, ИНН, СНИЛС, ОМС, водительское удостоверение и прочее. Самое безобидное, что могут сделать мошенники, – это продать наши персональные данные злоумышленникам, а также, например, оформить микрозайм, используя портал «Госуслуги» для подтверждения личности в некоторых МФО (микрофинансовых организациях).

В дополнение к уже широко известным схемам получения смс-кода, подтверждающего смену пароля, с помощью социальной инженерии появились несколько новых возможностей атак на контакты службы поддержки сервиса. Одним из последних методов является публикация фейковых номеров службы поддержки «Госуслуг». Для этого мошенники подделывают справочные сайты, публикуют на них фейковые номера служб

[4]Кибермошенники за десять месяцев украли у россиян более 158 млрд рублей //Коммерсант.09.12.2024. URL: https://kommersant.ru/doc/7362381?ysclid=m4zytgdzed607797372

поддержки «Госуслуг». Через них злоумышленники похищают доступ к аккаунтам пользователей портала, далее с помощью поискового продвижения добиваются их появления в ТОП-10 поисковых систем. Помимо этого, злоумышленники рассылают смс-сообщения о якобы неудачной попытке входа или взлома аккаунта и в них же указывают поддельный номер службы поддержки. Основная опасность для граждан здесь заключается в том, что они искренне верят, что действительно обратились в службу поддержки портала и готовы выполнять команды мошенников.

Ярким примером может стать история, которая произошла с гражданкой из города Москвы: Людмила является активным клиентом одного из крупнейших федеральных банков страны, где имеет зарплатную карту, накопительный счет, вклад и другие банковские продукты. Людмила решила инвестировать накопившиеся сбережения в строящееся жилье.

Ввиду современных трендов предполагалась цифровая сделка, то есть подписание ДДУ (договор долевого участия) с помощью УКЭП (усиленная квалифицированная электронная подпись), являющейся электронным аналогом рукописной подписи. Пока Людмила ожидала «выпуска» УКЭП, ей поступил звонок от «сотрудника» Госуслуг, который ей сообщил, что на ее имя было получено письмо. Злоумышленник уточнил, какой способ передачи письма наиболее удобен: посредством электронной почты или отправкой на домашний адрес, который к тому же был назван мошенником корректно. Людмила, не заподозрив подвоха, попросила направить письмо на адрес электронной почты (для ускорения процесса). Для этого «сотрудники» Госуслуг направили на ее телефон смс-код и попросили его продиктовать. Только через 10-15 минут, после того как смс-код был назван, женщина решила еще раз внимательно прочитать направленное ей сообщение и обнаружила, что в его содержании есть информация о смене пароля на портале Госуслуг. При попытке зайти в свой ЛК на Госуслугах она увидела,

что доступ был уже более невозможен. Очевидно, что произошла смена пароля.

Как мы видим, в отношении «жертвы» здесь были использованы методы «социальной инженерии», ведь злоумышленниками были названы ее «чувствительные» данные: ФИО, адрес электронной почты, адрес постоянной регистрации, да и в целом она ждала звонок по факту готовности УКЭП. Это привело к усыплению бдительности и потере доступа ЛК портала Госуслуг. Очевидным действием со стороны жертвы должна была быть верификация смс-сообщения перед озвучиванием смс-кода мошенникам.

Кроме того, ***мы должны всегда помнить, что сотрудники портала «Госуслуг» никогда не звонят гражданам, тем более с мобильных номеров.***

- ***Мошенничество по схеме Fake Boss***

Наряду с такими формами мошенничества, как взлом учетных записей на портале «Госуслуги», звонков от «сотрудников» ЦБ РФ, ФСБ, МВД, прокуратуры и других, также известна такая схема, как Fake Boss. Схема довольная проста: злоумышленники выдают себя за руководителя жертвы, пишут ей сообщение в наиболее популярных мессенджерах о необходимости переговорить с представителем «полиции», «профильного» ведомства или другим государственным органом. При дальнейшем взаимодействии с такими «представителями» это приведет к тому, что жертва перечислит свои денежные средства на так называемые специальные/безопасные счета.

Алгоритм следующий:

- создается либо фейковый аккаунт руководителя в мессенджере (при этом используется вся необходимая информация, размещённая на сайте организации, в которой работает жертва, например, государственные организации, в частности, образовательные учреждения: вузы, школы и т.д.), либо взламывается реальный аккаунт руководителя.

- затем с этого аккаунта поступают сообщения сотруднику (жертве) организации, в которых «руководитель» организации уведомляет подчиненного о том, что ему поступит звонок от представителей государственных ведомств и будет необходимо сообщать достоверную информацию. Часто злоумышленник уверяет, что якобы он сам ранее общался с правоохранительными органами. Особое внимание «руководитель» уделяет конфиденциальности разговора, о котором никому нельзя говорить и что необходимо четко следовать инструкциям по телефону;

- подготовленный к будущему разговору сотрудник теряет бдительность, что неминуемо приводит к финансовым потерям вследствие перевода своих денежных средств на «специальные счета».

Рассмотрим реальную историю. Сотруднику одного из вузов города Москвы в Telegram пришло сообщение от ректора этого вуза о том, что в отношении образовательного учреждения проходит проверка со стороны правоохранительных органов в части распространения персональных данных. «Ректор» пояснил, что ранее сам он уже общался на данную тему и предупредил сотрудника о том, что скоро поступит звонок от представителя МВД. Далее, как было сказано ранее, с сотрудником связался представитель правоохранительных органов с сообщением о том, что от имени жертвы проводятся незаконные финансовые операции и для сохранности сбережений на время следствия необходимо перевести свои деньги на «специальный» счет.

Таким образом, мошенниками часто проводится предварительная работа по подготовке жертвы, которая может занимать достаточно длительный период. Известны истории, в которых переписка с «руководителем» занимала несколько месяцев и содержала в себе поздравления с праздниками, рабочие вопросы, в которых было указание на конкретных лиц. От подвергшейся влиянию жертвы мошенники могут дополнительно потребовать взять

максимально возможное количество кредитов в различных банках с последующим переводом полученных средств на «специальные счета».

Кроме того, целью таких звонков может являться получение информации о других сотрудниках компании для использования в дальнейших атаках. Зачастую, чтобы влиться в доверие, мошенники направляют жертве сканированные копии документов от правоохранительных органов, которые очевидно являются поддельными.

При данных видах атак рекомендуется проверять правильность номера или аккаунта, с которого звонят от имени руководителя. Также нужно обращать внимание, появляется ли в мессенджере уведомление «Добавить» и «Заблокировать». Если оно есть, то абонент отсутствует в списке ваших контактов. ***Самым лучшим вариантом противодействия такому виду мошенничества будет завершение контакта и связь с руководителем посредством городского или мобильного телефона по своей инициативе.***

- ***Звонок от оператора сотовой связи «У вас заканчивается срок действия договора»***

Данный вид телефонного мошенничества появился несколько лет назад и по-прежнему остается актуальным «инструментом» для злоумышленников. Якобы сотрудник колл-центра утверждает, что сим-карта абонента в ближайшее время не будет работать в связи с окончанием срока договора обслуживания мобильным оператором. Очевидно, что сегодня без связи оставаться никто не хочет, поэтому мошенники тут же «стелют красную дорожку», предлагая решение: прямо сейчас продлить договор и при этом для усыпления бдительности сообщают, что «никакие личные данные, в том числе паспортные называть будет не нужно», ведь они уже имеются в базе данных оператора связи. Не проинформированный о подобном роде мошенничестве гражданин, продолжая оставаться на связи со злоумышленником, рискует потерять свои деньги. Целью мошенников

является тем или иным способом получить доступ к персональным данным для их использования в своих мошеннических схемах.

Рассмотрим на примере, как это происходит. Мужчине по имени Павел после рабочего дня раздался звонок с неизвестного мобильного номера. Павел как деловой человек, которому часто звонят по рабочим вопросам, ответил. Звонящий представился сотрудником мобильного оператора (при этом не уточнил, какого именно) и любезно сообщил о том, что если срок действия договора мобильной связи не продлить в тот же день, то сим-карта прекратит работу и данный номер продадут новому владельцу. Павел уточнил у «сотрудника» мобильного оператора, что нужно сделать для продления договора. Ему ответили, что договор можно продлить «прямо сейчас» в режиме телефонного звонка и никакие персональные данные не потребуются, поскольку они были переданы «ранее при оформлении сим-карты». Однако мошенники попросили продиктовать смс-код, который поступит на телефон. Так как Павел уже знал о подобных схемах, то он прервал разговор, положив трубку.

Далее события могли развиваться по-разному.

1. Поступившее смс-сообщение якобы для продления договора на самом деле будет являться сбросом пароля для портала «Госуслуги» (о чем рассказано выше). Злоумышленники могут получить исчерпывающую информацию для дальнейших махинаций, например, для оформления кредитов в МФО (микрофинансовых организациях).

2. «Сотрудники» оператора для продления договора мобильной связи попросят ввести определенную комбинацию цифр на телефоне, что приведет к переадресации входящих вызовов и смс сообщений на мобильные телефоны мошенников и может дать им полный карт-бланш для смены паролей, в том числе в банковских приложениях.

3. Весьма нестандартный и неожиданный для неосведомленного человека вариант. В момент, когда «потерпевший» назвал мошенникам смс-код для восстановления доступа в ЛК портала «Госуслуги», они сразу же

«раскрывают» карты и с насмешкой сообщают, что взломали аккаунт «Госуслуг». В этот момент растерянный человек, находясь в панике, начинает предпринимать быстрые и не всегда обдуманные действия, например, пытается восстановить доступ к порталу, используя механизм сброса пароля на официальном сайте. Однако злоумышленники уже авторизовались в ЛК гражданина и в строку контрольного вопроса для восстановления пароля вписали текст следующего содержания: «Ваша учетная запись временно заблокирована в связи с подозрительной активностью. Обратитесь по номеру +7 ***-***-**-** за более детальной информацией». Указанный номер принадлежит мошенникам, и сам потерпевший в паническом состоянии готов выполнять любые указания. Далее мошенниками прорабатываются различные схемы по хищению денег и персональных данных.

Стоит отметить, что вариации в данном виде мошеннической схемы могут быть разными, вместе с тем ***решение одно – запомните, что операторы сотовой связи никогда не будут просить продиктовать смс-код и никогда не попросят продиктовать ваши паспортные данные***. Самое лучшее, что можно сделать в этой ситуации – это прервать разговор и перезвонить по номеру телефона, указанному на сайте мобильного оператора, если есть сомнения и вопросы.

- ***Звонок от курьера «Подтвердите доставку цветов/товара»***

Одним из новых сценариев мошенничества можно считать схему, связанную с доставкой цветов/товара. Схема работает следующим образом: жертва получает анонимную доставку цветов или некого подарка, что вызывает приятное удивление. На следующий день жертве поступает звонок с сообщением от службы доставки, что курьер не отчитался о данной доставке установленным образом, и просьбой продиктовать «код подтверждения доставки».

В данном примере стоит отметить нестандартный ход мошенников: используется положительный, а не отрицательный стресс, к которому мы все уже привыкли. В данном случае жертва себя чувствует обязанной, в том числе и курьеру, который доставил подарок.

Важно никогда не принимать от курьеров заказы, которые не были оформлены лично или о которых вы не уведомлены. Угрозой может быть не только финансовая потеря, но и здоровье, поскольку никто не знает, что может находиться в посылке, которую вы не заказывали.

- ***Покупка/продажа товаров на «Авито»***

Схемы, применяемые мошенниками на сервисе «Авито», распространены и многим известны. Кроме того, сам сервис регулярно предупреждает своих клиентов о наиболее известных уловках, которые используют мошенники.

Рассмотрим одну из таких схем на примере. Женщина из Москвы решила сдать свою квартиру в аренду. Для повышения стоимости она решила ее меблировать и приобрести шкаф на сервисе «Авито». Подобрав понравившуюся позицию, она связалась с продавцом и договорилась о цене в размере 10 000 рублей. Он предложил ей самой заказать доставку, направив фишинговую ссылку на популярный сервис «Яндекс-доставка». Женщина прошла по ссылке (важно отметить, что страница сервиса выглядела, как ее оригинал), ввела нужный адрес доставки и данные своей банковской карты для оплаты. В этот момент с карты москвички была списана сумма 10 000 рублей, но на сайте произошел сбой, и сервис попросил ввести данные карты еще раз для возврата денежных средств. После повторного ввода данных с ее карты вновь была списана сумма в том же размере 10 000 рублей. Только в этот момент она догадалась, что имеет дело с мошенниками и обратилась в банк, выпустивший карту, где ей порекомендовали написать обращение в отделении полиции.

Данная ситуация демонстрирует, как работает фишинг (поддельный сайт). Основное грубое нарушение, которое было допущено женщиной, это переход по ссылке, которую ей направил «продавец» шкафа. После того, как жертва «попалась на крючок», очень сложно с него сорваться и в данном случае отличить настоящий сайт службы доставки от фейкового. Самым правильным вариантом в данном случае и при работе в сети Интернет в целом является самостоятельный ввод нужного электронного адреса, поскольку при переходе по ссылкам есть большой риск попасть на поддельные (фишинговые) сайты.

Правила безопасности

Все вышеприведенные примеры основаны на потере бдительности, отключении критического мышления, низком уровне финансовой грамотности, доверчивости. На том конце провода зачастую «работают» специально обученные, неглупые люди, в том числе психологи, финансисты, юристы. Прием, который используют мошенники, один и тот же – вывод жертвы из состояния спокойствия/равновесия под воздействием положительного или отрицательного стресса за счет передаваемой информации: либо произошло что-то «плохое» (например, «с вашего счета пытаются совершить перевод на сумму….»), либо что-то «хорошее» (например, «Ваш выигрыш составил….»). Ведь, когда мы находимся в подавленном или, наоборот, приподнятом настроении, мы не всегда можем принимать обдуманные решения, а мошенники всегда подталкивают нас на принятие моментальных решений.

Основное правило финансовой безопасности достаточно простое: не отвечать на звонки с незнакомых номеров. Конечно, мошенники используют разные информационные поводы, но их суть всегда одна: вовлечь нас в разговор и усыпить бдительность, поэтому важно владеть информацией о новых трендах мошенников.

Раздел 2. Возможности искусственного интеллекта в реализации преступных схем

Злоумышленники для хищения денег стали чаще использовать новый инструмент обмана – дипфейк-технологии. С помощью нейросети мошенники создают реалистичное видеоизображение человека. Затем сгенерированный образ рассылают его друзьям или родным через мессенджеры или социальные сети. В этом фальшивом видеоролике виртуальный герой, голос которого иногда сложно отличить от голоса прототипа, рассказывает якобы о своей проблеме (болезнь, ДТП, увольнение) и просит перевести деньги на определенный счет. Иногда мошенники создают дипфейки работодателей, сотрудников государственных органов, известных личностей из той же сферы деятельности, в которой трудится их потенциальная жертва[5].

Для того, чтобы создать цифровую копию человека, злоумышленники используют фото и видео, а также запись голоса, полученные в основном в результате взлома его аккаунта в социальных сетях или мессенджерах.

Необходимо проявлять осторожность и «включать» критическое мышление при получении от своего знакомого голосового или видеосообщения с просьбой о финансовой помощи, ведь его аккаунт могли взломать злоумышленники. Иногда для рассылки таких сообщений мошенники создают поддельные страницы с именем и фото человека. Нельзя спешить переводить деньги. Необходимо обязательно сначала позвонить тому, от чьего имени поступило сообщение, и перепроверить информацию. Распознать дипфейк можно по неестественной монотонной речи собеседника, дефектам звука и видео, несвойственной мимике. Если возможности позвонить и убедиться, что человеку действительно нужна

[5] Мошенники обманывают людей с помощью дипфейков //ЦБ РФ.16.09.2024. URL:https://cbr.ru/information_security/pmp/15082024

помощь, нет, задайте в сообщении личный вопрос, ответ на который знает только ваш знакомый. Учитывая, как стремительно развиваются технологии в том числе в разработке дипфейков, отличить настоящего человека от его виртуальной копии будет не так просто.

По данным НИУ ВШЭ, в последние годы наблюдается значительный прогресс в качестве синтетически сгенерированного контента. Кроме того, регулярно появляются инструменты, с помощью которых обычный пользователь ПК может создать реалистичный поддельный контент.

За последние десятилетия было создано множество Интернет-ресурсов для реализации возможности делиться мультимедийным контентом с широкой аудиторией (например, социальные сети и форумы).

Создание поддельного видео

Один из реальных случаев использования технологии дипфейка для вымогательства денежных средств произошел в 2020 году, когда мошенники использовали алгоритмы дипфейка для создания поддельного видео с участием генерального директора одной из крупных компаний.

Основными этапами этого случая стали следующие моменты:

1. Создание дипфейка. Мошенники использовали технологии глубокого обучения для создания видео, имитирующего действия генерального директора компании. Они смогли сделать так, чтобы видео выглядело очень правдоподобно, используя открытые источники, такие как видеозаписи публичных выступлений и интервью генерального директора.

2. Обман. С помощью полученного дипфейка мошенники связались с одним из филиалов этой компании, представляясь генеральным директором. Они использовали видео, чтобы убедить сотрудников в том, что им необходимо сделать срочный перевод средств на «специальный счет».

3. Вымогательство. В результате манипуляций мошенников сотрудники филиала сделали перевод значительной суммы денег, полагая, что руководство компании действительно дало такое указание.

4. Раскрытие мошенничества. Когда стало очевидно, что денежные средства не были переведены по легальным причинам, компания начала расследование. В ходе расследования было выяснено, что видео было фальшивым, и это привело к осознанию того, как технологические новшества могут быть использованы в преступных целях.

Этот случай иллюстрирует, насколько опасной может быть технология дипфейков, особенно когда речь идет о финансовых махинациях и вымогательстве. Сложность в том, что такие технологии могут создавать высококачественные видео, которые трудно отличить от настоящих, что делает их идеальным инструментом для мошенников.

«Подделка голоса» (voice spoofing)

Один из реальных примеров использования технологий генерации человеческого голоса для вымогательства денежных средств связан с мошенничеством, которое получило название «глубокое подделывание голоса» (voice spoofing).

Пример такого вида мошенничества.

Создание подделки голоса. Мошенники использовали алгоритмы обработки звука и технологии глубокого обучения для имитации голоса руководителя компании. Они обучили модель на основе аудиозаписей настоящего голоса руководителя с публичных выступлений или телефонных звонков.

Фейковый звонок с просьбой о помощи. После создания фейкового голоса мошенники позвонили на рабочий телефон одного из сотрудников компании, представляясь руководителем компании. Они использовали различные методы, чтобы подделать номер телефона, чтобы он выглядел законным и вызывал доверие. Во время звонка мошенник имитировал голос руководителя, утверждая, что компания попала в сложную финансовую ситуацию и очень срочно нужна помощь. Они могли ссылаться на срочные

финансовые переводы, которые нужно было сделать немедленно для предотвращения больших убытков.

Вымогательство средств. Поскольку голос звучал правдоподобно и имел эмоциональный окрас, сотрудники поддались панике и немедленно выполнили перевод средств на указанный мошенниками счет, полагая, что это распоряжение их руководства.

Подобные случаи показывают, как технологии генерации человеческого голоса могут быть использованы для обмана и вымогательства. После таких инцидентов организации начинают пересматривать свои внутренние процедуры, чтобы предотвратить подобные мошенничества, включая обучение сотрудников по распознаванию подозрительных запросов, а также внедрение многофакторной аутентификации для финансовых операций.

Эти примеры подчеркивают важность бдительности и осведомленности, поскольку ***технологии, использующие искусственный интеллект для создания подделок, становятся все более доступными и распространенными.***

Сбор информации о компании и/или о человек перед «взломом»

Одним из случаев мошенничества на основе сбора всесторонней информации о деятельности одной из международных компаний является инцидент, связанный с так называемым «CEO Fraud». Для достижения своих целей мошенники использовали информацию, собранную из открытых источников и социальных сетей.

Сбор информации. Мошенники тщательно исследовали компанию через открытые источники, включая LinkedIn, Facebook и другие социальные сети. Они искали информацию о руководителе компании (Chief Executive Officer – CEO), его коллегах и внутренней структуре компании. Они смогли выяснить имена ключевых сотрудников, их должности и контактные данные.

Создание фальшивого профиля. Используя собранные данные, мошенники создали поддельный адрес электронной почты, который внешне казался легитимным. Они использовали адрес, схожий с настоящим, изменив всего одну букву или добавив поддомен (например, вместо ceo@company.com использовали ceo@company.co).

Осуществление мошеннического запроса. Мошенник отправил электронное письмо одному из высокопоставленных сотрудников компании, входящих в состав ее руководства, представившись CEO компании. В письме он созвал «срочное собрание руководства компании» и попросил сделать трансферы денежных средств на «расходы, связанные с конфиденциальными сделками», которые, по его словам, должны были оставаться в тайне от других сотрудников. Письмо выглядело убедительным. Мошенник использовал правильный и характерный для CEO стиль общения и корпоративные термины.

Выполнение перевода. В результате этого мошеннического обращения сотрудник, выполняя указания CEO, перевел значительную сумму денег на указанный мошенниками счет. Сделка проходила в сжатые сроки, что оказывало дополнительное психологическое давление на сотрудника.

Раскрытие мошенничества. При анализе финансовой отчетности аудиторами были выявлены факты перевода денежных средств по подозрительным основаниям. При дальнейшем детальном анализе был установлен факт мошенничества и раскрыли всю цепочку действий злоумышленников.

Этот случай подчеркивает важность проявления бдительности в вопросах кибербезопасности, особенно в отношении использования открытых данных для мошенничества. Многие компании вводят дополнительные меры безопасности, такие как многофакторная аутентификация, проверки на подлинность обращений высшего руководства, а также использование технологий искусственного интеллекта для распознавания подозрительных запросов.

Разработка вредоносного ПО, создание вирусов и вредоносных кодов без доступа к интернету для «взлома» веб-сайтов

Технологии искусственного интеллекта (ИИ) в области кибербезопасности включают как защиту, так и атаки.

Обнаружение вредоносного ПО. Машинное обучение: Современные антивирусные и антишпионские программы используют алгоритмы машинного обучения для анализа поведения программ. Эти алгоритмы могут выявлять подозрительное поведение даже в новых, неизвестных образцах вредоносного ПО. Например, программа может отслеживать как приложение взаимодействует с файлами и сетью. Если оно пытается шифровать файлы или отправлять данные на неизвестные серверы, то считается подозрительным.

Обнаружение по сигнатурам. Системы, использующие алгоритмы машинного обучения и глубокого машинного обучения, могут анализировать большой объем данных о сигнатурах вредоносного кода и сравнивать их с файлами, находящимися в системе. Эти технологии позволяют обнаруживать подобные угрозы.

Генерация вредоносного кода. Группы мошенников могут использовать алгоритмы генерации кода, основанные на методах ИИ для создания новых версий вирусов и троянов. Например, генеративные модели, такие как GAN (Generative Adversarial Networks), могут использоваться для создания уникальных образцов вредоносного кода, которые с меньшей вероятностью могут быть обнаружены традиционными антивирусными программами.

Использование методов ИИ для адаптации атак. Вредоносный код может использовать ИИ для анализа программных систем, которые он пытается атаковать. Например, при «взломе» веб-сайтов методы ИИ могут автоматически анализировать уязвимости системы даже без доступа к

интернету путем изучения файлов конфигурации и настроек хостинга, которые могут быть доступны через локальный доступ.

Анализ программного обеспечения. Злоумышленник может установить систему, использующую алгоритмы машинного обучения и/или нейросетевые алгоритмы на локальный компьютер, и использовать ее для анализа ПО, которое находится в сети или внешних носителях, чтобы выявить потенциальные уязвимости.

Генерация атаки с использованием ИИ. На основе изученных уязвимостей методами ИИ можно сгенерировать исполняемый файл или скрипт. Такой скрипт может автоматически подстраивать свои действия в зависимости от программного окружения, к которому он попадает.

Физическое распространение. Вредоносный код может быть загружен на устройства обычным способом (например, через USB-накопитель) и запущен для компрометации системы без необходимости подключения к интернету.

Использование технологий ИИ для обеспечения кибербезопасности вызывает серьезные опасения и предстоящие вызовы. Защитные механизмы должны адаптироваться к новейшим угрозам, включая те, которые используют ИИ для создания вредоносного ПО.

Правила безопасности

Активируйте многофакторную аутентификацию на всех значимых аккаунтах, таких как банковские приложения, портал «Госуслуги», личный кабинет Федеральной Налоговой Службы России и другие.

Закройте доступ для посторонних лиц в социальных сетях, следите за цифровым следом, который вы оставляете в сети Интернет.

Критически относитесь ко всему, что видит и слышите.

Раздел 3. Дропперы/дропы: связующее звено преступной цепи финансовых мошенников

Ежегодно растет количество и суммы хищений средств у населения, в связи с этим растет и количество так называемых дропперов (от английского drop – «падать», «сбросить»). Дропы являются соучастниками преступлений, которые могут быть классифицированы по статье 174 УК РФ. Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем или по статье 159 УК РФ Мошенничество. МВД России разработало законопроект об уголовной ответственности для дропперов. Передачу зарегистрированных на себя электронных средств платежа или доступа к ним предложено определять как преступление средней степени тяжести, но, если преступление совершено в составе организованной группы, его квалифицируют как тяжкое преступление.

Иными словами, дропы – это подставные лица, которые задействованы в нелегальных схемах по выводу средств с банковских карт граждан. Стоит отметить, что дропы не являются организаторами преступлений, но являются их соучастниками, за что несут полную ответственность перед законом.

По сведениям ЦБ РФ, как правило, дропперами являются люди, нуждающиеся в деньгах: социально неблагополучные категории граждан, студенты или школьники, которым родители оформили карту с 14 лет. По данным банков в дропперство вовлечено порядка 2 млн россиян – это почти в два раза больше, чем в 2023 году. Около 60% – молодые люди до 24 лет, для которых характерно стремление к легкому заработку. Дропперы могут быть использованы злоумышленниками в разных качествах, к примеру, дроп может передать оформленную банковскую карту и онлайн-доступ к ней мошеннику, который далее самостоятельно пересылает деньги на другие счета с целью усложнить цепочку и «замыть» следы. В некоторых случая дроп получает на свои счета похищенные средства, обналичивает их и

передает злоумышленникам. Известны случаи, когда дропы перевозят наличные средства в другие регионы страны и совершают иные противоправные действия. Формат работы дропа зависит от того, каким образом его вовлекли/завербовали в преступную схему.

- ***Примеры вербовки дропперов***

1. Под видом работодателя.

Студент Андрей хочет заработать денег в свободное время. На сайте по поиску работы ему подвернулась заманчивая вакансия со следующими требованиями: без опыта работы; удаленно; частичная занятность; высокий заработок за несколько часов в день; возраст 18+ и наличие карты любого банка.

Те, кто откликается на подобные вакансии, почти всегда становятся участникам мошеннических схем. Мошенники придумывают различные легенды, например, представляются крупной компанией, занимающейся поставками большого количества товаров из Китая. С учетом крупных сумм покупок и лимитами банков на ежемесячные переводы в компанию требуются люди, которые «отдадут» в аренду свою банковскую карту вместе с личным кабинетом для контроля поступления денег от «клиентов» за вознаграждение.

Принятие подобных предложений заканчивается вовлечением в преступные схемы молодых людей, которые не понимают, что они делают. Задачей мошенников является убеждение людей под разными легендами осуществлять переводы денег другим людям либо вовсе передать полный доступ к своему личному кабинета банка.

Еще один пример, который получил большое распространение – это подработка *«Курьером наличности».* По сведениям межрегионального управления Федеральной службы по финансовому мониторингу по СФО мошенники активно распространяют информацию в социальных сетях о возможности подработки в качестве курьера. *«Курьер наличности»* -

перемещение денежных средств от одного лица или бизнеса к другому, с целью избежать традиционных банковских методов или при наличии ограничений на вывод. Объявление о такой работе размещается телефонными мошенниками, при этом будущему курьеру могут сообщать, что работа не связана с криминалом и он ничем не рискует. Рассмотрим реальный пример предложения о работе *«курьером наличных»:*

- Нужны ответственные люди по всем городам РФ;
- Работа курьером;
- Забираем посылки от 100 тыс. руб.
- Даем 7%, выплата сразу;
- Вся «почва» для безопасного забора нала подготовлена!!!

Повторим еще раз, что подобные действия, в том числе и данное может классифицироваться как мошенничество по ст. 159 УК РФ. Наказание в этом случае предусмотрено вплоть **до 10 лет лишения свободы.**

Мошенничество является умышленным преступлением, а курьеров чаще всего не посвящают в детали, говоря только о необходимости получения и перевода денежных средств (что деньги потерпевших людей об этом конечно же умалчивается).

2. Под видом ошибившегося человека.

Очень распространенная схема: на ваш счет поступает перевод денег от незнакомого лица, далее вам поступает звонок с информацией, что денежный перевод был совершен ошибочно, и просьбой перевести деньги обратно. Однако в случае возврата по указанным незнакомцем реквизитам на самом деле деньги направляются третьему лицу – участнику преступной схемы. Таким образом, случайно, пойдя навстречу человеку, можно стать соучастником преступления по выводу денег.

В данном случае правильным решением будет обратиться в банк и только вместе с банковским сотрудником решать вопрос, каким образом деньги отправить обратно.

Подобная схема может реализована через пополнение номера телефона незнакомыми лицами, которые также связываются со своей «жертвой», сообщая, что произошла ошибка и просят перевести деньги «обратно», но по факту третьим лицам.

3. Через социальные сети и сайты знакомств.

Через социальные сети обращается незнакомец с правдоподобной легендой, например, что у него есть родственник за границей, которому срочно нужно отправить деньги, а его банк такие переводы не проводит. Обычно мошенники предлагают это сделать за небольшую плату в зависимости от суммы предполагаемого перевода. Далее на счет жертвы поступают ворованные деньги, которые она перенаправляет дальше, становясь таким образом звеном в преступной цепочке.

На сайте знакомств как правило, мошенники выбирают девушек с небольшим заработком и финансовыми обременениями. Они дарят небольшой подарок и предлагают приличные деньги за просьбу перевести через свой счет деньги другу, брату или маме нового знакомого, чтобы сэкономить на комиссии. После пары переводов «молодой человек» исчезает.

4. Вовлечение в диверсионную деятельность.

Конечной целью данного «мероприятия» является дестабилизация экономической безопасности и обороноспособности государства. Привлечение людей в схему поджогов и террористических актов является серьезной угрозой безопасности общества. Рассмотрим способы вербовки:

- Работа с уязвимыми группами – привлечение людей, испытывающих финансовые трудности;

- «Борьба за правое дело» - злоумышленники занимаются пропагандой через социальные сети, обещая участие в «правой войне»;
- Подрыв доверия к государству – мошенники призывают действовать против «несправедливой системы»;
- Обеспечение наркотиками – вербовщики делают людей зависимыми от наркотиков и склоняют их к диверсионным действиям.

Что касается уголовной ответственности за соучастие в диверсионных действиях, то важно знать, что за диверсию привлекается любое вменяемое физическое лицо, достигшее 16-летнего возраста, и преследуется статьей 281 УК РФ. Также стоить отметить отдельно, что диверсионные действия квалифицируются как тяжкие преступления. За совершение диверсии наступает уголовная ответственность в виде лишения свободы на срок от 10 до 20 лет лишения свободы.

5. Благотворительные сборы для СВО/приют для животных/на операцию.

Рассмотрим пример «отмывания» денег на примере благотворительных фондов. Надо отметить, что данная схема не нова и существует продолжительное время. «Работает» она следующим образом: мошенники создают благотворительный фонд, например, для помощи студентам вузов, попавшим в сложную жизненную ситуацию; и на счет созданного фонда те организации, которым необходимо легализовать преступные средства, перечисляют деньги. Далее для обналичивания денег со счета фонда привлекаются, например, «завербованные» студенты, которым якобы требуется материальная помощь, в связи с чем они обратились в тот самый благотворительный фонд. В результате на карту студента из фонда поступает сумма, которую он обналичивает в банкомате и отдает ее обратно мошенникам, оставляя себе малую часть. Таким образом, человек становится дроппером, то есть соучастником преступления, в котором доказать свою невиновность будет очень трудно.

6. Обмен криптовалюты на рубли.

Одна из распространённых схем «обеления» преступных денег является покупка криптовалюты на p2p платформах. Множество инвесторов используют именно p2p площадки вместо криптобирж по причине низких комиссий, а также возможности удаленно купить криптовалюту. Именно этим и пользуются мошенники: они действительно покупают криптовалюту у продавцов, но делают это с целью легализации преступных доходов. В результате на счет продавца криптовалюты поступают похищенные денежные средства с карты дропа.

Соответствующие службы банков мониторят подобные сделки и блокируют счета не только дропа, но и продавца в рамках 115 ФЗ (О противодействии легализации(отмыванию) денежных средств, полученных преступным путем, и финансированию терроризма), более того, может быть возбуждено уголовное дело. Таким образом, можно случайно стать соучастником преступления.

Нужно отметить, что на 100% защитить себя от рисков получить себе на счет «грязные» деньги при проведении p2p сделок невозможно, однако можно снизить риски, соблюдая несколько рекомендаций: вести переписку через инфраструктуру p2p площадки, совершать сделки с аккаунтами, которые давно зарегистрированы на площадке и имеют хорошую репутацию.

P2p-сервисы ведут учет количества проведенных операций клиентами и показывают процент успеха. Чем эти показатели выше, тем больше доверия заслуживает трейдер. Важно помнить, что самые безопасные сделки проводятся на криптобиржах.

Раздел 3.1. «Страшная реальность»: обнальщики, транзитчики, заливщики и универсалы

Дропов принято распределять на категории в соответствии с их действиями:

Обнальщики – это дропы, которые снимают со своей карты преступные деньги и передают их мошенникам.

Транзитчики – это дропы, которые пересылают безналичным путем преступные деньги по указанным мошенникам реквизитам.

Заливщики **–** это дропы, которые получают наличные деньги от таких же дропов, вносят их на свою карту и пересылают дропам «транзитчикам».

Универсалы – это дропы, которые могут выполнять все вышеуказанные действия.

- ***«Продолжительность жизни» дроппера, последствия и ответственность для дроппера.***

Помогать мошенникам «выводить» похищенные деньги – мероприятие неблагодарное. Действия дропперов могут попасть под уголовную статью 159 «Мошенничество» или 174 «Легализация денежных средств». При этом может быть назначен как немалый штраф, так и более суровое наказание – арест. В этом случае срок заключения в тюрьме может достигать 7 лет. Кроме того, в перспективе обеспечены минимальные шансы на обслуживание в том или ином банке, что в современной жизни практически невозможно.

Важно отметить, что суровость наказания не зависит от того, знал ли дроп о том, что он делает, или нет. Именно в этом большая опасность: дропом поневоле может стать каждый.

Правила безопасности

Как случайно не стать дропом?

- не откликайтесь на вакансии с легким заработком;

- проверяйте потенциального работодателя на предмет наличия отзывов в Интернете;

- никогда и никому не оставляйте данные своей банковской карты, тем более не передавайте ее третьим лицам (во многих банках передача карт третьим лицам запрещена);

- регулярно обновляйте пароли к своим банковским приложениям, личному кабинету портала «Госуслуги» и прочим финансово значимым приложениям;

- если вас попросят вернуть случайный перевод денег, совершенный на ваше имя, не соглашайтесь на это, обратитесь с этим вопросом в ваш банк;

- не переходите по ссылкам из неизвестных источников, во избежание взлома доступа к банковскому личному кабинету;

- всегда повышайте свою финансовую грамотность – читайте новости о новых видах мошенничества, ведь «Предупрежден – значит вооружен».

Раздел 4. Только тихо! Всё об анонимности криптовалют

- ***Вложения украденных средств в криптовалюту***

На сегодняшний день на рынке представлено более 9000 видов криптовалют, однако наиболее популярные среди них это Bitcoin и Etherium. Мошенники с целью легализации денежных средств покупают различные биткоины, что позволяет им скрыть конечного бенифициара (человека, в интересах которого совершаются действия; того, кто получит прибыль).

Отличительной особенностью таких цифровых активов, как криптовалюта, в отличие от банковских продуктов, является, так называемая, псевдоанонимность. Например, такие криптовалюты, как Monero и Zcash, предоставляют инвесторам полную анонимность. Существуют криптокошельки, не требующие полной верификации его владельца, что также предоставляет анонимность инвесторам, чем охотно пользуются мошенники. В целом вся суть криптографии и блокчейна – это конфиденциальность, безопасность и децентрализация.

Вместе с тем, стоит отметить, что такие органы государственной власти, как Федеральная служба по финансовому мониторингу (Росфинмониторинг), Центральный Банк РФ и прочие, находятся в поиске инструментов, в том числе на техническом и законодательном уровнях, позволяющих взять под контроль операции цифровых активов. Одна из основных проблем правоохранительных органов при распутывании преступных схем заключается в использовании мошенниками подставных лиц – дропов, на чьи имена открываются криптокошельки. Поэтому соответствующие службы стараются установить связь подставного лица с реальными исполнителями мошеннических операций, но и это является трудной задачей, так как «отношения» между ними выстраиваются как правило дистанционно.

- ***Вывод средств из криптовалютных обменников и бирж***

Существует два основных, но не единственных метода по обмену криптовалюты: это использование криптобирж и криптообменников.

Криптообменники бывают двух видов: онлайн и офлайн.

Онлайн криптообменник предоставляет возможность быстрого обмена криптовалюты. Достаточно выбрать валюту, которую вы хотите продать, и валюту, которую хотите купить. После ввода своих данных вы получаете нужные средства на свой кошелек.

Офлайн вариант криптообменника подходит наилучшим образом для наличного обмена. То есть если нужно обменять криптовалюту на рубли или рубли на криптовалюту, то данный вариант будет самым приемлемым. Некоторые криптоомбенники позволяют проводить операции анонимно.

Криптобиржа – это более сложная структура, которая предполагает регистрацию и часто необходимость пройти процедуру «Знай своего клиента». Ключевым отличием от криптообменников является возможность торговать на бирже своими активами, а не просто обменивать.

С точки зрения рисков оба варианта являются рискованными, однако в случае использования криптобирж рисков становится меньше.

- ***Статистическая информация о криптовалютных операциях, о доле мошеннических схем в общем обороте криптовалюты. Доходность криптовалюты. Риски «гореинвестора»***

По данным ЦБ, активность российских пользователей на рынке криптоактивов выросла за IV квартал 2023 – I квартал 2024 года. Об этом свидетельствует количество посещений сайтов крупнейших криптовалютных торговых площадок и объем потоков криптовалюты на биржах, который оценочно приходится на россиян[6].

[6] ЦБ оценил объем операций россиян в криптовалютах.//РБК Крипто. 24.05.2024. URL:https:// rbc.ru/crypto/news/665066579a794764c51aa31f

Криптовалют на рынке огромное множество, однако с точки зрения доходности мы рассмотрим наиболее популярную – биткоин. По данным РБК-Инвестиции за 2024 год, вложение в биткоин оказалось бы самым прибыльным, он принес бы инвестору доходность 146,35% в рублях. За это время курс биткоина вырос с 4 000 027 до 9 854 180 в рублевом эквиваленте.

Конечно же, биткоин, как и другие криптовалюты, и в целом финансовые активы, очень волатилен, например, в ноябре 2021 года 1 биткоин стоил порядка 61 000 $, а в ноябре 2022 года уже 20 000$, то есть минус 300%. Вместе с ростом цены биткоина увеличивался и уровень его волатильности – с 23,4% в конце 3 квартала 2023 года до 80% в конце первого квартала 2024 года. Помимо этого, растут и риски в связи с возможными санкциями со стороны недружественных стран, что может привести к потере доступа к активам в случае их блокировки со стороны эмитентов криптовалют.

Также нужно помнить, что чем выше доходность того или иного финансового актива, тем многократно выше и риски. Стоит помнить, что инвесторы покупают, например, биткоин потому, что он растет в цене, а в цене он растет потому как раз, что его покупают инвесторы, что приводит к замкнутому кругу, в котором можно как заработать, так и потерять свои средства.

Сделки с криптовалютами сложно отследить, почти невозможно отменить транзакцию (сделку по купли-продаже актива). Следовательно, рискам в этом отношении подвержены оба участника сделки, если между ними нет надежного посредника. Стоит отметить, что даже мошеннические схемы на «этом рынке» отменить нельзя. Например, широко известен случай с «раздачей монет», где на фишинговом сайте от имени миллиардера Илона Маска сообщалось о несуществующей акции департамента Tesla по маркетингу, в ходе которой все поклонники марки могут получить криптовалюту. Для участия в акции необходимо выслать от 0,1 до 20 BTC (Bitcoin) или от 1 до 100 ETH (Ethereum) якобы для проверки, а обратно

будет отправлено вдвое больше. На самом деле это была распространённая схема в блокчейне-сфере[7], и деньги возвращены доверчивым «инвесторам» не были.

Разберем основные типы преступлений с криптовалютами:

1. Мошенничество (Scams). Мошенничество является одним из самых распространённых видов преступлений с цифровыми валютами. Злоумышленники создают фальшивые инвестиционные схемы, платформы для обмена криптовалюты или поддельные ICO (Initial Coin Offering). Пользователи вводятся в заблуждение и переводят свои средства, которые затем исчезают.

В качестве примера можно привести финансовое расследование, которое проводило МРУ Росфинмониторинга по СКФО (далее - МРУ, Управление) в 2022 году. В Управление поступило обращение гражданки «М», денежные средства которой похитили преступники. С использованием одной из социальных сетей с гражданкой «М» связалась девушка, которая, используя методы социальной инженерии, убедила «М» приобрести криптовалюту и инвестировать её на бирже «С». В ходе финансового расследования МРУ Росфинмониторинга по СКФО установило, что сайт биржи был подделкой, а криптовалюта, вложенная потерпевшей, выводилась преступниками на одну из известных криптобирж, обменивалась на стэйблкойны и в дальнейшем переводилась на анонимные криптокошельки.

2. Программы-вымогатели (ransomware) — это один из наиболее распространённых видов кибератак, при которых злоумышленники шифруют данные на компьютерах жертвы и требуют выкуп, обычно в криптовалюте, для их восстановления.

---

[7] Илон Маск опять бесплатно раздает биткоины. На самом деле – это мошенники//РБК Крипто.06.07.2020 URL:https://www.rbc.ru/crypto/news/5f02c92a9a794757a240c661

Этот тип атак особенно опасен, так как может парализовать работу компаний, больниц, государственных учреждений и других критически важных организаций. Деньги от жертв поступают в криптовалюте, после чего преступники используют сервисы «миксеры» (tumbler) для перемешивания средств и их дальнейшего вывода через многочисленные транзакции, снижая возможность отслеживания.

Одна из крупнейших атак осуществлена на компанию Colonial Pipeline в 2021 году. Вымогатели потребовали оплату в биткойнах на сумму около 4,4 млн долларов. После получения выкупа преступники пытались скрыть свои средства, разбивая транзакции на мелкие части и переводя их через различные криптовалютные кошельки для запутывания следов.

В 2023 году выплаты по программам-вымогателям превысили отметку в 1 миллиард долларов, что стало наивысшим показателем за всю историю наблюдений. Хотя в 2022 году был зафиксирован спад объема выплат, общая тенденция с 2019 по 2023 годы указывает на то, что проблема программ-вымогателей продолжает усугубляться.

3.Киберпреступления и взломы. Хакеры часто нацеливаются на криптовалютные биржи и кошельки, чтобы украсть криптовалюту. Ряд хакерских атак нацелен на крупные биржи, что привело к утрате миллионов долларов. Наиболее известные случаи взлома криптовалютных бирж, такие как взлом Mt. Gox в 2014 году и взлом Bitfinex в 2016 году, привели к огромным потерям.

4.Наркоторговля и иная нелегальная торговля. Криптовалюты также используются в качестве средства оплаты незаконных товаров и услуг на «черном рынке». Платформы в «даркнете» (darknet) принимают криптовалюту за покупку наркотиков, оружия и других нелегальных товаров. В качестве примера можно привести платформу Hydra, деятельность которой была пресечена в 2022 году. По имеющимся данным Hydra контролировала более 90% незаконной торговли в даркнете, где за все товары и услуги,

включая наркотики, оружие и поддельные документы, оплачивались криптовалютой

5. Финансирование терроризма. Криптовалюты также используются для финансирования террористических организаций, так как они позволяют совершать анонимные переводы без необходимости использовать традиционные банковские системы. Международные террористические группы использовали криптовалюты для сбора средств через различные платформы, иногда через донаты или фальшивые благотворительные организации. При этом цифровые валюты могут использоваться в данной преступной деятельности сразу на нескольких этапах - как инструменты, обеспечивающие сбор, хранение финансовых средств для долгосрочных и краткосрочных целей террористических организаций и на этапе приобретения средств совершения террористического акта (поддельные документы, оружие и взрывчатка) в даркнете.

Указанные выше виды преступлений с использованием криптовалют продолжают эволюционировать, и с развитием технологий появляются новые схемы.

Правила безопасности

- Используйте двухфакторную аутентификацию. Если криптокошелек дает возможность, создайте «сид-фразу» для восстановления доступа в случае потери устройства или повреждения программного обеспечения.
- Храните резервные копии в безопасных местах, таких как сейфы, и не сохраняйте их в электронном виде (например, на компьютере или в облаке).
- Используйте сложные пароли.
- Желательно использовать отдельное устройство только для доступа к кошелькам.

- Регулярно обновляйте программное обеспечение.
- Не используйте публичные сети Wi-Fi.
- Позаботьтесь о защите своего устройства: устанавливайте пароли, биометрическую аутентификацию на своих устройствах.
- Не афишируйте в публичных местах, а также в социальных сетях и на форумах наличие большого количества криптовалюты на ваших кошельках.

Раздел 5. Международная олимпиада по финансовой безопасности

Проведение Олимпиады направлено на популяризацию финансовой безопасности как нормы жизни, а также на формирование у молодежи нового типа мышления: от безопасности личности – к безопасности государства.

В Олимпиаде принимают участие студенты бакалавриата (1–3 курс), специалитета (1–4 курс) и магистратуры (1 курс) вузов стран-участниц Олимпиады, а также школьники 8–10 классов российских школ.

С учетом профиля Олимпиады («Финансовая безопасность») олимпиадные задания составлены на основе следующих программ:

- для школьников – на основе программ общеобразовательных предметов: математика и информатика, обществознание, экономика;

- для студентов – на основе основных образовательных программ высшего образования по направлениям подготовки:

• юриспруденция;

• математика, прикладная математика и информатика, прикладная математика, математика и компьютерные науки, фундаментальная информатика и информационные технологии, информатика и вычислительная техника, прикладная информатика, информационная безопасность, бизнес-информатика;

• экономика, финансы и кредит, экономическая безопасность;

• международные отношения, регионоведение.

Победители и призеры Олимпиады получают преимущества при поступлении в вузы Международного сетевого института в сфере ПОД/ФТ на программы бакалавриата, магистратуры и аспирантуры в соответствии с льготами олимпиад I уровня, а также возможность стажироваться в Росфинмониторинге и других организациях.

Олимпиада проходит в несколько этапов:

− тематический урок «Финансовая безопасность»;

− пригласительный этап;

− отборочный этап;

− квалификационный этап;

− финальный этап.

Приложение № 1.

Глоссарий

Дроппер, дроп – это подставное физическое лицо, оформившее на себя средства платежей (банковские пластиковые карты, банковские счета, электронные кошельки, криптокошельки и пр.) и/или зарегистрировавшее себя в качестве индивидуального предпринимателя (МП) и/или директора и/или учредителя юридического лица без цели реального участия в предпринимательской деятельности с последующей передачей (сбытом) третьим лицам за денежное вознаграждение или иные материальные или нематериальные ценности электронных средств, предназначенных для управления своими средствами платежей и/или банковскими счетами и финансовой деятельностью оформленных на него организаций и/или индивидуального предпринимателя. К «дропам» также относятся физические лица, предоставившие свои персональные данные и документы для идентификации при проведении финансовых операций с наличными денежными средствами, принадлежащими третьим лицам и в их интересах.

ICO (Initial Coin Offering) – первичное размещение монет или первичное размещение токенов – форма привлечения инвестиций через выпуск и продажу инвесторам цифровых токенов за фиатные денежные средства или иные криптовалюты.

Инвестиции – денежные средства, ценные бумаги, иное имущество, в том числе имущественные права, иные права, имеющие денежную оценку, вкладываемые в объекты предпринимательской и (или) иной деятельности в целях получения прибыли и (или) достижения иного полезного эффекта.

Инвестор – лицо, осуществляющее инвестиции.

Криптовалюта – ***цифровая валюта*** – 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.

Крипторынок – Криптовалютный рынок – площадка, на которой торгуются криптовалюты.

Скам-проект (скам) – (от англ. scam — «мошенничество», «афера») - мошеннический инвестиционный проект, созданный для получения быстрой выгоды.

Социальная инженерия – это обман и манипуляции, заставляющие жертв делать то, чего они не должны (например, совершать электронные переводы средств, раскрывать учетные данные и прочее).

Сид-фраза (seed-фраза) — это **последовательность из 12, 18 или 24 слов**, которая служит главным инструментом для восстановления доступа к криптовалютному кошельку. Она представляет собой своего рода мастер-ключ, который предоставляет доступ к криптовалютному кошельку, его данным и средствам.

Приложение № 2.

Ресурсы

Материалы:

1. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств // ЦБ РФ. 09.12.2024. URL: https://cbr.ru/statistics/ib/review_3q_2024

2. Объем похищенных мошенниками в РФ средств в III кв. вырос почти вдвое относительно II кв. // Интерфакс. 09.12.2024. URL: https://interfax.ru/russia/996734

3. Анализ системы вывода денежных средств, похищенных у граждан // Сбер Банк. URL:https:// www.sberbank.ru/ru/person/kibrary/investigations/analiz-sistemy_vyvoda_denezhnyh_sredstv

4. Кибермошенники за десять месяцев украли у россиян более 158 млрд рублей //Коммерсант.09.12.2024. URL: https://kommersant.ru/doc/7362381?ysclid=m4zytgdzed607797372

5. Мошенники обманывают людей с помощью дипфейков //ЦБ РФ.16.09.2024. URL:https:// cbr.ru/information_security/pmp/15082024

6. ЦБ оценил объем операций россиян в криптовалютах.//РБК Крипто. 24.05.2024. URL:https:// rbc.ru/crypto/news/665066579a794764c51aa31f

7. Илон Маск опять бесплатно раздает биткоины. На самом деле – это мошенники //РБК Крипто.06.07.2020 URL:https:// www.rbc.ru/crypto/news/5f02c92a9a794757a240c661