

**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:

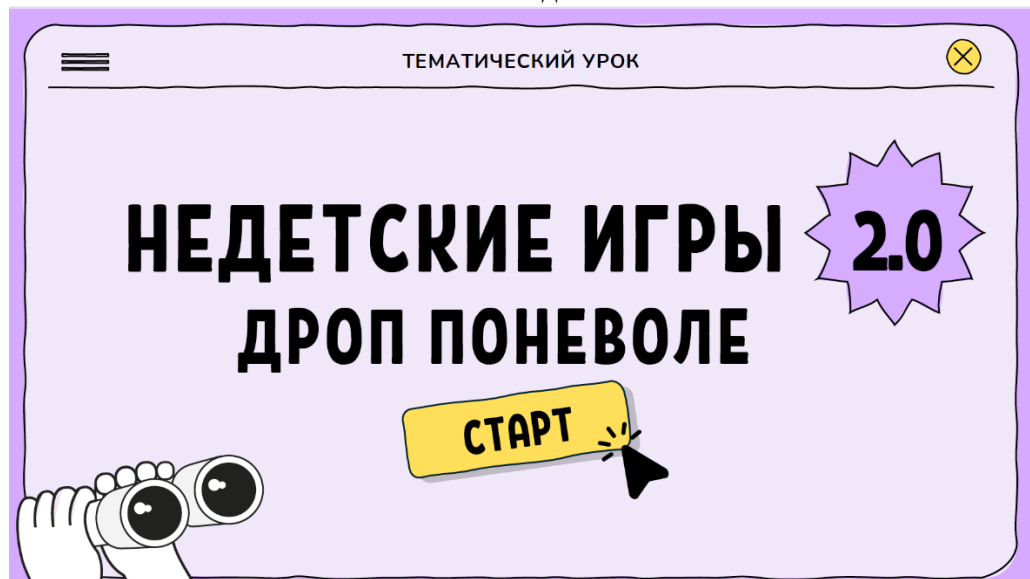
- заложить у обучающихся основы грамотного финансового поведения;
- сформировать у обучающихся представление о признаках ситуаций финансового мошенничества, а также признаках фишинговых и других мошеннических схем;
- научить обучающихся:
 - распознавать угрозу мошенничества и не совершать действий по 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)

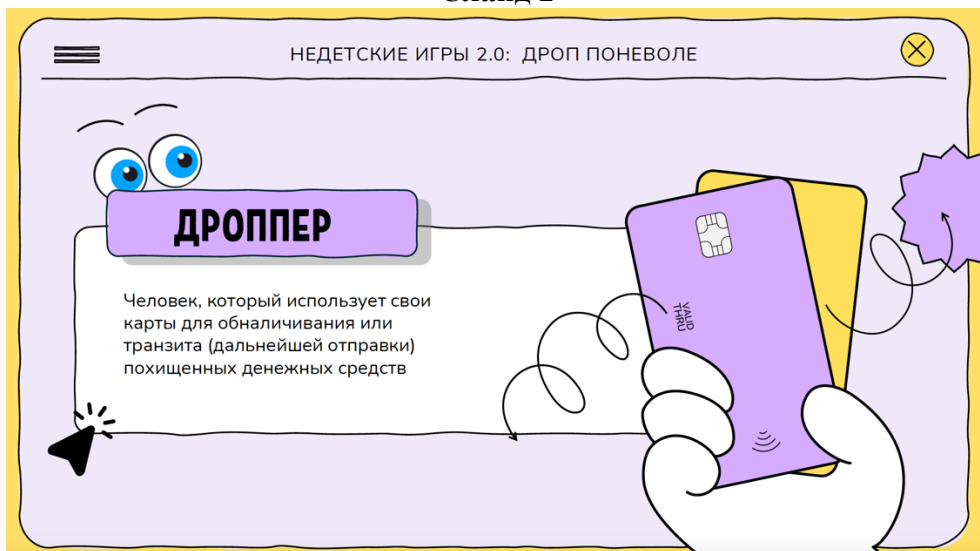
Комментарий для учителя

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 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». 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, аккумуляция крупных денежных сумм, с последующей покупкой криптовалюты;
- обналичивание, аккумуляция 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

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

«О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма»

115-ФЗ

Организация противодействия «отмывания» денежных средств, полученных незаконным путем, регламентируется 115-ФЗ («О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма»)



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.

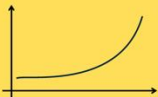

Слайд 5

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

80% хищений происходит дистанционно

ежегодно растет количество преступлений и объем похищенных средств



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

КЕЙС #1
(схема Госуслуги)

Людмила активный клиент крупного федерального банка, где имеет зарплатную карту, накопительный счет, вклад и другие банковские продукты.

Людмила решила инвестировать сбережения в строящееся жилье, 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, поступил звонок от «сотрудника» Госуслуг, сообщившего, что на ее имя пришло письмо. Злоумышленник уточнил, какой способ передачи письма наиболее удобен: посредством электронной почты или отправкой на домашний адрес, который 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. 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. Произошла смена пароля

Код подтверждения: 101001
Не сообщайте никому

Adobe Acrobat Reader Helper

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

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

КЕЙС #2

(схема Fake Boss)

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

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 довольно 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

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ



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

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

КЕЙС #3

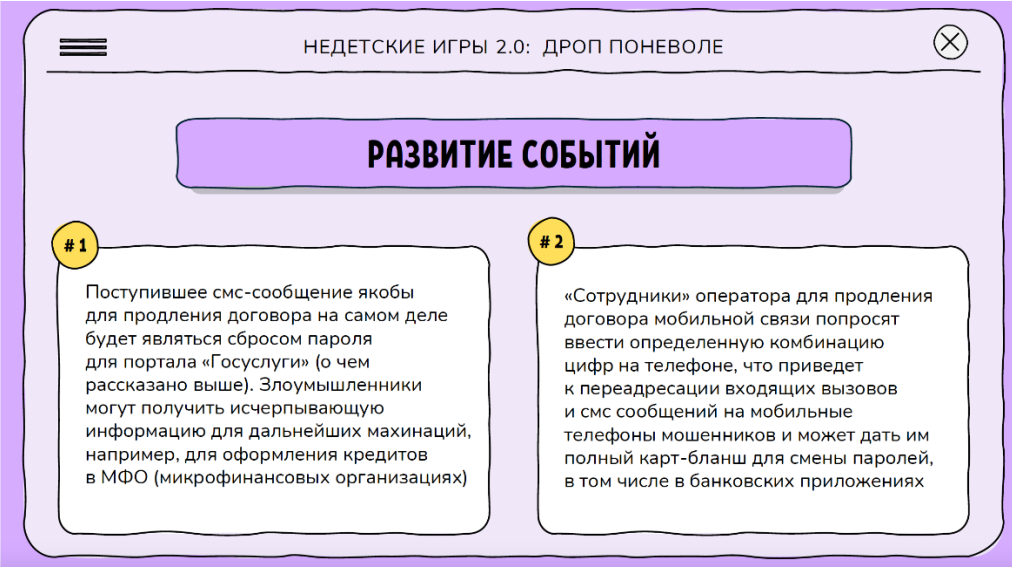
(схема Мобильный оператор)



Павлу поступил звонок с неизвестного мобильного номера. Ему часто звонят по рабочим вопросам, поэтому он ответил. Звонящий представился сотрудником мобильного оператора и сообщил, что если не продлить срок действия договора мобильной связи в тот же день, сим-карта прекратит работу и номер продадут новому владельцу. Павел уточнил, что нужно сделать для продления договора. Ему ответили, что договор можно продлить «прямо сейчас» в режиме звонка, персональные данные не потребуются, так как они были переданы «ранее при оформлении сим-карты». Но когда мошенники попросили продиктовать sms-код, который поступит на телефон, Павел прервал разговор, так как уже знал о подобных схемах

•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 усиления 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

	<p>мошенников является тем или иным способом получить доступ к персональным данным для их использования в своих мошеннических схемах.</p> <p>Рассмотрим на примере, как это происходит.</p>
<p style="text-align: center;">Слайд 10</p>  <p style="text-align: center;">РАЗВИТИЕ СОБЫТИЙ</p> <p>#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)</p> <p>#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</p>	<p>Далее события могли развиваться по-разному</p> <p>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 portalу, 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.</p>

Слайд 11

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

Запомните, операторы сотовой связи никогда не будут просить продиктовать смс-код и ваши паспортные данные

Давайте уточним ваши паспортные данные

Продуктуйте смс-код

Мы вам отправим смс-код

Слайд содержит иллюстрацию: рука держит карточку с текстом «Давайте уточним ваши паспортные данные», другая рука вводит код на телефоне. Надпись «Продуктуйте смс-код» указывает на процесс ввода кода. Сообщение «Мы вам отправим смс-код» приходит на телефон. В левом блоке три восклицательных знака подчеркивают предупреждение.

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

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

КЕЙС #4

(схема Доставка)

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

Слайд содержит иллюстрацию: злой персонаж с рогами и крыльями держит подарочную коробку. Рядом с ним мигает курсор мыши.

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

☰ НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ ☒

КЕЙС #5

(схема покупка/продажа на Авито)

Женщина из Москвы решила сдать свою квартиру в аренду. Для повышения стоимости она решила ее меблировать и приобрести шкаф на сервисе «Авито». Подобрал понравившийся, она связалась с продавцом, 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 10000 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



- **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 фэйкового.

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



НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ



Основное простое правило финансовой безопасности

**НЕ ОТВЕЧАЙТЕ НА ЗВОНКИ
С НЕЗНАКОМЫХ НОМЕРОВ**

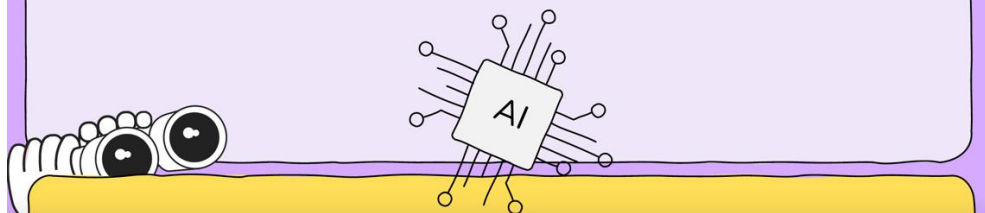


Все вышеприведенные примеры основаны на потере бдительности, отключении критического мышления, низком уровне финансовой грамотности, доверчивости. На том конце провода зачастую «работают» специально обученные, неглупые люди, в том числе психологи, финансисты, юристы. Прием, который используют мошенники, 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

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

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.

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

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

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 выступлений, 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 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

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

Слайд 17

☰ НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ ✕

ПОДДЕЛКА ГОЛОСА (VOICE SPOOFING)

ПРИМЕР:

- # 1 Создание подделки голоса
- # 2 Фейковый звонок с просьбой о помощи
- # 3 Вымогательство средств

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.

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 сослаться 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.*

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.

Слайд 18

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

СБОР ИНФОРМАЦИИ О КОМПАНИИ И/ЛИ ЧЕЛОВЕКЕ ПЕРЕД ВЗЛОМОМ

- #1 Создание фальшивого профиля
- #2 Осуществление мошеннического запроса
- #3 Выполнение перевода
- #4 Раскрытие мошенничества



Выполнение перевода. В результате этого мошеннического обращения сотрудник, выполняя указания СЕО, 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

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

ОБНАРУЖЕНИЕ ВРЕДНОСНОГО 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

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 видите и слышите

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

2 млн * россиян вовлечено в дропперство
Это почти в два раза больше, чем в 2023 году

60% * молодые люди до 24 лет
Для которых характерно стремление к легкому заработку

ДРОПЫ
Это подставные лица, задействованные 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

СОУЧАСТНИКИ ПРЕСТУПЛЕНИЙ
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

*По данным различных банков

Дропперы/дроппы: 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 случаях дроп получает на свои счета похищенные средства, обналачивает 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

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

КЕЙС

Примеры вербовки дропперов

Студент Андрей хочет заработать денег в свободное от учебы время.
На сайте по поиску работы ему подвернулась заманчивая Вакансия со следующими требованиями:

- без опыта работы
- удаленно
- частичная занятость
- высокий заработок за несколько часов в день
- возраст 18+
- наличие карты любого банка

Те, кто откликается на подобные вакансии, почти всегда становятся участниками 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

- **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



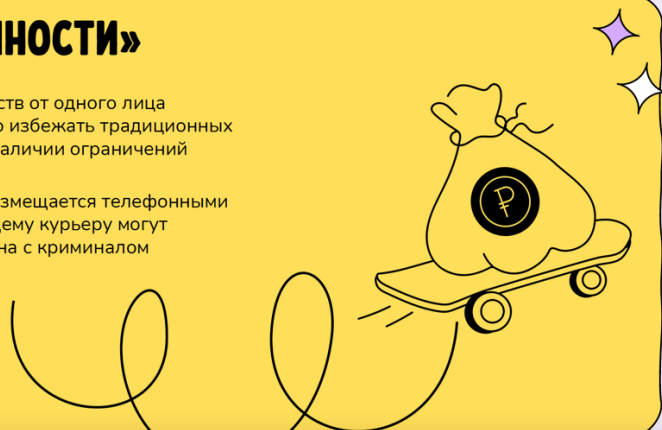
НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ



«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



Слайд 23



НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ



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
предусматривает
лишение свободы
вплоть до 10 лет

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*»:

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



НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ



КЕЙС

(схема Ошибочный перевод)

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

V

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

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

☰ НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ ☒

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 преступной цепочки



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


☰ НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ ☒

ВОВЛЕЧЕНИЕ В ДИВЕРСИОННУЮ ДЕЯТЕЛЬНОСТЬ

- #1 Работа с уязвимыми группами — привлечение людей, испытывающих финансовые трудности
- #2 «Борьба за правое дело» — злоумышленники занимаются пропагандой через социальные сети, обещая участие в «правой войне»
- #3 Подрыв доверия к государству — мошенники призывают действовать против «несправедливой системы»
- #4 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



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 стоит 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

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

БЛАГОТВОРИТЕЛЬНЫЕ СБОРЫ ДЛЯ СВО/ПРИУТ ДЛЯ ЖИВОТНЫХ/ НА ОПЕРАЦИЮ

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

The slide features a purple header with a hamburger menu icon on the left and a close button on the right. The main content is enclosed in a white rounded rectangle with a purple border. On the right side of the slide, there is a cartoon illustration of a white cat with black ears and whiskers, looking confused with a question mark above its head. Below the cat is a stack of three coins, with a single coin in front showing a ruble symbol (₽). There are also some decorative starburst and sparkle icons.

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


НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

ОБМЕН КРИПТОВАЛЮТЫ НА РУБЛИ

ПРАВИЛА РАБОТЫ С КРИПТОВАЛЮТОЙ

- #1 Ведите переписку через инфраструктуру p2p площадки
- #2 Совершайте сделки с аккаунтами, которые давно зарегистрированы на площадке и имеют хорошую репутацию

ВАЖНО!
Важно помнить, что самые безопасные сделки проводятся на криптобиржах



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.

Слайд 29

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

Дропов принято распределять на категории в соответствии с их действиями

Обнальщики	Транзитчики	Заливщики	Универсалы
Это дропы, которые снимают со своей карты преступные деньги и передают их мошенникам	Это дропы, которые пересылают безналичным путем преступные деньги по указанным мошенникам реквизитам	Это дропы, которые получают наличные деньги от других дропов, внося их на свою карту и пересылают дропам «транзитчикам»	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. Именно в этом большая опасность: дропом поневоле может стать каждый

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, внося 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

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

ПРАВИЛА БЕЗОПАСНОСТИ!!!

- 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
- 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

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

НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ

ТОЛЬКО ТИХО! ВСЁ ОБ АНОНИМНОСТИ КРИПТОВАЛЮТ

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

	<p>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.</p>
--	---



ВЫВОД СРЕДСТВ ИЗ КРИПТОВАЛЮТНЫХ ОБМЕННИКОВ И БИРЖ



Криптовбиржа — 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



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

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 криптообменники позволяют проводить операции анонимно.

Криптовбиржа – 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 – биткойн. По данным РБК-Инвестиции за 2024 год, вложение в биткойн оказалось бы самым прибыльным, он принес бы инвестору доходность 146,35% в рублях. За это время курс биткойна вырос с 4 000 027 до 9 854 180 в рублевом эквиваленте.

Конечно же, биткойн, как и другие криптовалюты, и в целом финансовые активы, очень волатилен, например, в ноябре 2021 года 1 биткойн стоил порядка 61 000 \$, а в ноябре 2022 года уже 20 000\$, то есть минус 300%. Вместе с ростом цены биткойна 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, биткойн 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 купле-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.



ОСНОВНЫЕ ТИПЫ ПРЕСТУПЛЕНИЙ С КРИПТОВАЛЮТАМИ

МОШЕННИЧЕСТВО

В Управление поступило обращение гражданки «М», денежные средства которой похитили преступники. С использованием одной из социальных сетей с «М» связалась девушка, которая, используя методы социальной инженерии, убедилась её 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 стэйблкоины 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. Получив выкуп, 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: взлом Mt. Gox в 2014 году и взлом Bitfinex в 2016 году, которые привели к огромным потерям

НАРКОТОРГОВЛЯ И ИНАЯ НЕЛЕГАЛЬНАЯ ТОРГОВЛЯ

В качестве примера можно привести платформу Hydra, её деятельность была пресечена в 2022 году. Hydra контролировала более 90% незаконной торговли в Даркнете, где 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 использования традиционных банковских систем

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, убедилась «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 стэйблкоины 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 перемешивания средств и их дальнейшего вывода через многочисленные транзакции, снижая возможность отслеживания.

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.

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.

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.

Наркотоорговля и иная нелегальная торговля. Криптовалюты также используются в качестве средства оплаты за незаконные товары и услуги на «черном рынке». Платформы в «даркнете» (darknet) принимают криптовалюту за покупку наркотиков, оружия и других нелегальных товаров.

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.

Слайд 34

☰ НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ ☒

Правила безопасности

- #1 Используйте двухфакторную аутентификацию
- #2 Храните резервные копии в безопасных местах
- #3 Используйте сложные пароли
- #4 Желательно использовать отдельное устройство только для доступа к кошелькам
- #5 Регулярно обновляйте программное обеспечение
- #6 Позаботьтесь о защите своего устройства
- #7 Не афишируйте в публичных местах, а также в социальных сетях и на форумах наличие большого количества криптовалюты на ваших кошельках

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

ЭТАПЫ 2025 ГОДА



Международная олимпиада по финансовой безопасности

Слайд 36

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

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

☰ НЕДЕТСКИЕ ИГРЫ 2.0: ДРОП ПОНЕВОЛЕ ☒

ПАРТНЕРЫ

 ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ФИНАНСОВОМУ
МОНИТОРИНГУ

 МИНИСТЕРСТВО НАУКИ
И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

 МИНИСТЕРСТВО
ПРОСВЕЩЕНИЯ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

 МИНИСТЕРСТВО
ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

 РУДН

 ШКОЛА ЭКОНОМИКИ
И ЭНЕРГЕТИКИ

 МУМЦОМ

 ЦЕНТР
МЕЖОЛИМПИАДНОЙ
ПОДГОТОВКИ

 содружество

 ВТБ

 СБЕРБАНК

 Т БАНК

 Альфа Банк