МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КАРАЧАЕВО-ЧЕРКЕССКОЙ РЕСПУБЛИКИ

369000, г. Черкесск, пл. Ленина. Тел. 26-60-96
http:// www. minobrkchr.ru,
e-mail:obrazovanie09@mail.ru

Руководителям муниципальных органов управления образованием

Руководителям негосударственных и подведомственных образовательных организаций

27.02.2024 № 1132
на №_____от _____

Министерство образования и науки Карачаево-Черкесской Республики информирует о проведении Федеральной службой по финансовому мониторингу Международной олимпиады по финансовой безопасности для обучающихся 8-10 классов (далее – Олимпиада).

Цель Олимпиады - повышение информационной, финансовой и правовой грамотности молодого поколения, поиск талантливой молодежи, стимулирование учебно-познавательной и научно-исследовательской деятельности в области финансовой безопасности.

В целях подготовки проведения Олимпиады необходимо организовать в срок до 15 марта 2024 г. проведение Всероссийского тематического урока «Финансовая безопасность» (далее – Урок), обеспечив максимальный охват участников.

С дополнительной информацией о проведении Урока можно познакомиться на сайте Международной Олимпиады по финансовой безопасности https://rosfinolymp.ru/ и на сайте образовательной платформы «Содружество» https://sodrujestvo.org/ru.

Этапы Олимпиады:

- Уроки по финансовой безопасности для школьников: 14 февраля – 15 марта 2024 года
- Пригласительный этап: 4 – 22 марта 2024 года
- Отборочный этап:

1-й тур: 3 апреля 2024 года

2-й тур: 17 апреля 2024 года

- Квалификационный этап: 2 – 6 сентября 2024 года
- Финальный этап: 30 сентября – 4 октября 2024 года

В целях формирования статистической отчетности необходимо представить информацию о проведении Урока по адресу электронной почты kubekova12@mail.ru в указанные сроки: 11 марта и 18 марта 2024 года по приложенной форме.

Приложение: в электронном виде.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 27F00040983052A2B9E09D9C695D5CBF
Владелец **Кравченко Инна Владимировна**
Действителен с 05.04.2023 по 28.06.2024

Министр И.В. Кравченко

Исп. Кубекова А.М.
Тел. (8782) 26-69-37

Приложение

Информация о ходе проведения Всероссийского урока
по финансовой безопасности

№ п/п	Наименование ОО	Количество проведенных уроков	Количество учеников, принявших участие в уроке	Примечание

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНПРОСВЕЩЕНИЯ РОССИИ)

Департамент государственной политики в сфере воспитания, дополнительного образования и детского отдыха

Каретный Ряд, д. 2, Москва, 127006
Тел. (495) 587-01-10, доб. 3400
Факс (495) 587-01-13
E-mail: d06@edu.gov.ru

14.02.2024 № 03-180

Руководителям органов исполнительной власти субъектов Российской Федерации, осуществляющих государственное управление в сфере образования

О проведении Всероссийского тематического урока «Финансовая безопасность»

Во исполнение указания Президента Российской Федерации от 26 января 2021 г. № Пр-103, распоряжения Правительства Российской Федерации от 24 сентября 2016 г. № 2015-р «Об утверждении перечня международных спортивных, культурных, научных и деловых массовых мероприятий и сроки пребывания в Российской Федерации иностранных граждан и лиц без гражданства в связи с участием в таких мероприятиях», а также Плана мероприятий («дорожной карты») по подготовке к проведению IV Международной Олимпиады по финансовой безопасности, утвержденного заместителем Министра науки и высшего образования Российской Федерации Д.В. Афанасьевым 20 декабря 2023 г., Федеральной службой по финансовому мониторингу совместно с Министерством просвещения Российской Федерации, другими заинтересованными органами государственной власти, научными и образовательными организациями в 2024 году организовано проведение Международной олимпиады по финансовой безопасности (далее – Олимпиада).

В целях подготовки проведения Олимпиады Департамент государственной политики и управления в сфере общего образования (далее – Департамент) рекомендует организовать в срок до 15 марта 2024 г. проведение Всероссийского тематического урока «Финансовая безопасность» (далее – Урок) согласно прилагаемым методическим материалам (приложения 1-3).

С дополнительной информацией о проведении Урока можно познакомиться на сайте Международной Олимпиады по финансовой безопасности https://rosfinolymp.ru/ и на сайте образовательной платформы «Содружество» https://sodrujestvo.org/ru.

Одновременно в целях формирования статистической отчетности по Уроку Департамент просит предоставить информацию о проведении Урока в Межрегиональные управления Росфинмониторинга, осуществляющие оперативное сопровождение соответствующих субъектов Российской Федерации по проведению Олимпиады, в срок до 15 апреля 2024 г. по формам согласно приложениям 4-5 к настоящему письму.

Приложение:

1. Методические рекомендации по подготовке и проведению Всероссийского тематического урока «Финансовая безопасность».
2. Презентация «Финансовая безопасность».
3. Рекомендации по работе с презентацией Всероссийского тематического урока «Финансовая безопасность».
4. Статистическая таблица о ходе проведения этапа «Урок по финансовой безопасности» Международной олимпиады по финансовой безопасности.
5. Статистическая таблица о количестве образовательных организаций и количестве учащихся школ.

Директор Департамента

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 1CCB9DF9694ED681BC3451BF4815B04BE339D54A
Владелец Благинин Алексей Геннадьевич
Действителен с 04.07.2023 по 26.09.2024
Подлинник электронного документа, подписанного электронной подписью, хранится в единой системе электронного документооборота Министерства просвещения Российской Федерации

А. Г. Благинин

Рахманкина Ю.Ю.
(495) 587-01-10, доб. 3264

НЕДЕТСКИЕ ИГРЫ

КАК НЕ СТАТЬ УЧАСТНИКОМ ФИНАНСОВЫХ ПРЕСТУПЛЕНИЙ

ТЕМАТИЧЕСКИЙ УРОК

СИТУАЦИЯ

21 ноября дома у 12-летней Вики зазвонил домашний телефон — на том конце провода кто-то сильно плакал. Школьнице показалось, что голос принадлежит её бабушке. После Вике сразу же позвонили на мобильник, неизвестный сказал, что бабулю сбила машина — она получила серьёзные травмы, на лечение которых нужно 600 тысяч рублей. Вика пообещала помочь: по инструкции от звонившего она подготовила полотенце, бумагу, постельное бельё, взяла у отца 50 тысяч и упаковала их так, чтобы было не видно, что внутри.

Вскоре к ней домой пришёл неизвестный мужчина — он был в спортивных штанах и с тёмной бородой. Вика отдала ему деньги, надеясь, что бабуля скоро поправится.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

...психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации.

МЕТОДЫ

обман или злоупотребление доверием

психологическое давление

манипулирование

СХЕМА СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

НЕОЖИДАННОСТЬ

ЭМОЦИИ

ПСИХОЛОГИЧЕСКОЕ ДАВЛЕНИЕ

АКТУАЛЬНАЯ ТЕМА

ЭМОЦИИ, КОТОРЫЕ ВЫЗЫВАЕТ ИНФОРМАЦИЯ ОТ МОШЕННИКОВ, БЫВАЮТ ДВУХ ВИДОВ:

ОТРИЦАТЕЛЬНЫЕ

СТРАХ, ПАНИКА

ЧУВСТВО СТЫДА

ПОЛОЖИТЕЛЬНЫЕ

РАДОСТЬ, НАДЕЖДА

ЖЕЛАНИЕ ПОЛУЧИТЬ ДЕНЬГИ

ТЕЛЕФОННОЕ И МОБИЛЬНОЕ МОШЕННИЧЕСТВО

КЕМ МОЖЕТ ПРЕДСТАВИТЬСЯ МОШЕННИК:

Службой безопасности банка, банковскими сотрудниками

Сотрудником правоохранительных органов

Друзьями

Родными

РАСПРОСТРАНЕННЫЕ АЛГОРИТМЫ МОШЕННИКОВ

Пять признаков того, что вам звонит мошенник

Звонок поздно вечером, ночью или рано утром в выходные

От вас требуют немедленных действий

Торопят и запугивают, давят на эмоции

Требуют сообщить конфиденциальную информацию: данные карты, ПИН-код или одноразовый пароль из СМС-сообщения

При отказе называть данные угрожают, что деньги с вашей карты прямо сейчас уйдут к мошенникам

ЗАБЛОКИРОВАНА БАНКОВСКАЯ КАРТА

Вам поступил звонок из банка или пришло сообщение о блокировании банковской карты или несанкционированных операциях со счетом. Не отвечайте и не перезванивайте. ЭТО МОШЕННИКИ. Обратитесь в банк, в полицию или к родственникам.

ВЫПЛАТА КОМПЕНСАЦИЙ

Вам позвонили или пришло СМС-сообщение с предложением получить выплату компенсаций за страхование, медобслуживание, коммунальные и прочие услуги, но для этого Вам необходимо перевести некую сумму в качестве комиссии. Будь осторожны, скорее всего, это ОБМАН.

ВЫИГРЫШ В ЛОТЕРЕЕ

Вам сообщили, что Вы выиграли приз, но для его получения необходимо оплатить налоги и перевести сумму денег на незнакомый Вам счет. НЕ торопитесь следовать инструкции! Проверьте информацию! Вполне возможно, что с Вами общаются МОШЕННИКИ.

ПЕРЕВОД ДЕНЕЖНЫХ СРЕДСТВ

Если для перевода Вам денежных средств на банковскую карту просят сообщить 3 цифры с оборота карты (код CVV), Вы столкнулись с мошенничеством. Никому не сообщайте трехзначный код проверки подлинности карты, а также пароль для списания средств.

СЛУЧАИ С РОДСТВЕННИКАМИ

Если Вам звонят и сообщают, что Ваш родственник попал в аварию, за решетку, в больницу или совершил ДТП, и теперь за него нужно внести залог, штраф – это ОБМАН.
Если Вам звонят и сообщают, что Вашего родственника похитили и за него необходимо заплатить выкуп, – СРОЧНО позвоните в полицию и этому родственнику.

СИТУАЦИЯ

21 ноября у 15-летнего школьника Пети зазвонил мобильный телефон. На том конце провода мошенник представился стримером. Он сообщил, что случайно выбрал Петю для участия в онлайн-стриме, готов оплатить ему билет в другой город для участия в стриме, но для этого ему потребуются фотографии паспорта Пети и его банковской карты или карты его родителей.

КИБЕРПРЕСТУПНОСТЬ И КИБЕРМОШЕННИЧЕСТВО

киберпреступность - любое противозаконное деяние, нарушающее права и свободы человека с помощью компьютерных систем и сетей.

ФИШИНГ

...вид мошенничества, при котором злоумышленники рассылают письма и пытаются обманом заставить получателей совершать различные действия

итоговая цель - получение доступа к финансам или личным данным обманутых пользователей.

темы и авторы писем:

- службы доставки
- маркетплейсы
- криптовалюта
- горячие новости
- лотереи
- дополнительный заработок и инвестиции
- туроператоры и отдых
- билеты на мероприятия
- подписки и онлайн-сервисы
- фото с вечеринки

ФИШИНГОВОЕ ПИСЬМО

— письмо, которое содержит вредоносное вложение, ссылку на мошеннический сайт или вредоносное программное обеспечение.

ПОДДЕЛЬНЫЕ САЙТЫ ИЛИ ПРИЛОЖЕНИЯ

ПРИЗНАКИ ПОТЕНЦИАЛЬНО ОПАСНОГО ИНТЕРНЕТ-МАГАЗИНА

НИЗКАЯ ЦЕНА

стоимость товаров в магазине мошенников зачастую существенно ниже, чем в других. Не следует поддаваться на слова "акция", "количество ограничено", "спешите купить" и т.д.

ОТСУТСТВИЕ КУРЬЕРСКОЙ ДОСТАВКИ И САМОВЫВОЗА

в этом случае нередко приходится вносить предоплату за услуги транспортной компании. Злоумышленники могут предоставить поддельные квитанции об отправке товара

ОТСУТСТВИЕ КОНТАКТНОЙ ИНФОРМАЦИИ И СВЕДЕНИЙ О ПРОДАВЦЕ

Если на сайте прописаны только форма обратной связи и мобильный телефон продавца, такой магазин может представлять опасность. Перед обращением сюда следует почитать отзывы в интернете.

ПОДТВЕРЖДЕНИЕ ЛИЧНОСТИ ПРОДАВЦА ПОСРЕДСТВОМ НАПРАВЛЕНИЯ ПОКУПАТЕЛЮ СКАНА ЕГО ПАСПОРТА

Документ, особенно отсканированный, легко подделать

НЕТОЧНОСТИ И НЕСООТВЕТСТВИЯ В ОПИСАНИИ ТОВАРОВ

Желательно почитать описания такого же товара на других сайтах.

ОТСУТСТВИЕ ИСТОРИИ У ПРОДАВЦА ИЛИ МАГАЗИНА

Потенциально опасными являются страницы, зарегистрированные пару дней назад

Схема обмана в онлайн-игре

сценарий:

1/4 вам приходит письмо, что вы «выиграли» приз в одной из игр;

2/4 вы нажимаете на ссылку для обмена со специальным ботом;

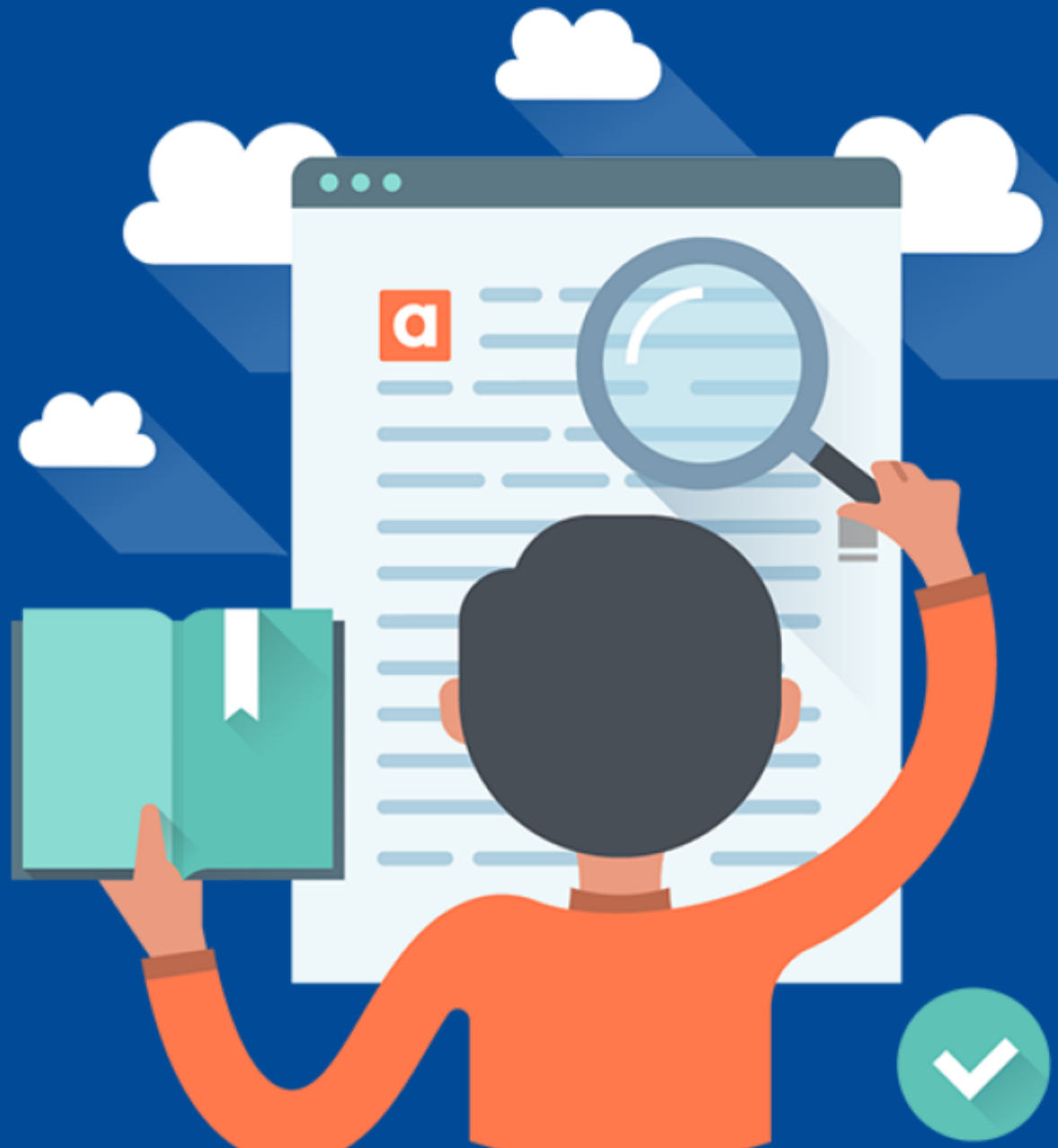
3/4 заходите в свой аккаунт на поддельном сайте;

4/4 отдаёте данные от аккаунта мошенникам.

ПРИМЕР

МОШЕННИЧЕСТВО В СОЦИАЛЬНЫХ СЕТЯХ И МЕССЕНДЖЕРАХ

- Переписка с мошенниками
- Взлом аккаунтов
- Цифровое клонирование
- Голосования
- Быстрый заработок
- Онлайн-пирамиды
- Инфоцыгане



СИТУАЦИЯ

К подростку в Telegram обратился неизвестный, представившись блогером. «Блогер» сообщил, что мальчик выиграл в конкурсе, и для получения награды ему необходимо взять телефон мамы и сделать скриншот экрана. Дальше подросток действовал по указаниям блогера-мошенника, однако не помнит, что именно делал. На следующий день после общения с «блогером» переписка автоматически удалилась, а со счета мамы мальчика исчезли 235 тысяч рублей.

СИТУАЦИЯ

Неизвестные лица создали телеграм-канал для любителей онлайн-шутера и предлагали делать ставки с обещанием заработать на турнирах по этой игре.

14-летний подросток сделал очень крупные ставки и перевел 100 тысяч рублей со счета своей мамы на Qiwi-кошелек и номера телефонов. В итоге он не получил никаких денег.

СИТУАЦИЯ

Молодой человек познакомился в соцсетях с девушкой и общался с ней две недели. Периодически она просила оплатить ей всякие недорогие «плюшки», чтобы они встретились – положить деньги на телефон, оплатить маникюр и т. д. И вот она пишет: «Я забронировала нам билеты в кино, сейчас тебе придет смс-ка с кодом для оплаты, можешь, пожалуйста, ее продиктовать, чтобы эти билеты оплатить».

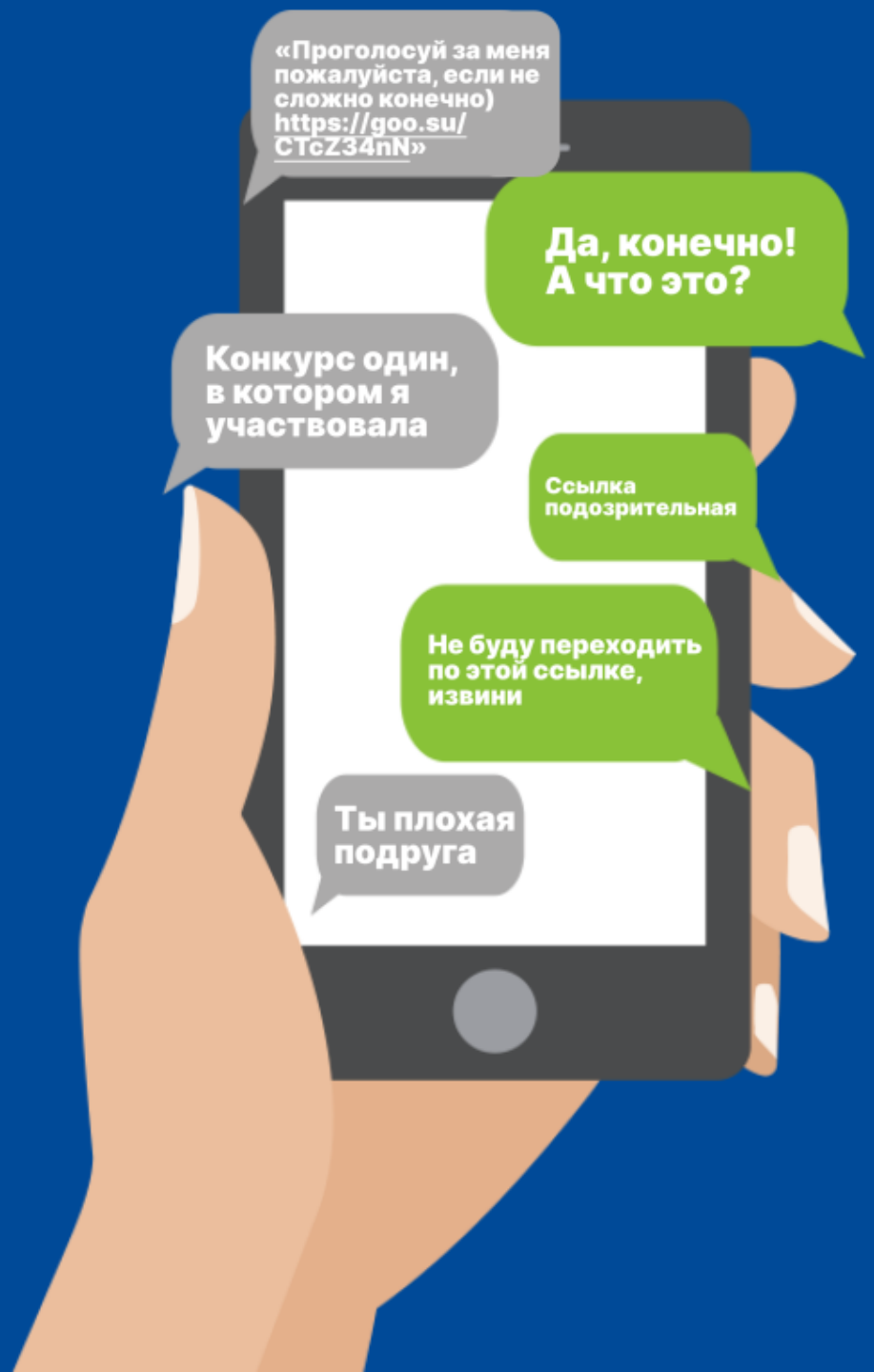
Парень продиктовал ей коды из СМС-сообщения. После этого с карточки списались все деньги, а девушка перестала отвечать на сообщения и звонки и удалила свой аккаунт.

СИТУАЦИЯ

В начале октября 14-летней девочке в социальной сети пришло сообщение от ее знакомого. Он утверждал, что счета и деньги родителей школьницы в опасности. Все из-за того, что в интернете есть их персональные данные, которыми могут воспользоваться мошенники.

«Приятель» сразу же предложил решение проблемы. Он рассказал девочке, как спасти семейные сбережения. Школьница последовала совету. Взяла банковские карты родителей, которые лежали на пуфике в прихожей, сфотографировала их со всех сторон и отправила снимки знакомому.

В итоге со счетов взрослых пропали 280 тысяч рублей. Потерпевшие обратились в полицию. Установлено, что страницу знакомого девочки взломали, и от его лица с ней общались аферисты.


«Проголосуй за меня пожалуйста, если не сложно конечно) https://goo.su/CTcZ34nN»
Да, конечно! А что это?
Конкурс один, в котором я участвовала
Ссылка подозрительная
Не буду переходить по этой ссылке, извини
Ты плохая подруга

ФИШИНГ

МОШЕННИЧЕСКИЕ СХЕМЫ С БЫСТРЫМИ ЗАРАБОТКАМИ

- вложения в выгодные проекты
- просмотры видеороликов популярных блогеров
- оценка картинок и отелей
- голосование в рейтингах
- букмекерские ставки
- экономические онлайн-игры

БЕСПЛАТНЫЙ СЫР БЫВАЕТ ТОЛЬКО В МЫШЕЛОВКЕ

МОШЕННИЧЕСКАЯ СХЕМА «ТЫ ПЛАТИШЬ – ТЫ ВЫИГРЫВАЕШЬ»

ФИНАНСОВАЯ ПИРАМИДА

ПРИЗНАКИ:

- отсутствие геймплея
- сложная схема начисления дохода
- выплата средств за привлечение новых участников
- гарантия высокого дохода без всякого риска и агрессивная реклама в соцсетях

СХЕМА МОШЕННИЧЕСТВ С КРИПТОВАЛЮТАМИ И ICO

- скам-проекты (скам)
- проекты-пустышки
- rug n pull (раг пулл, дернуть коврик)
- классический фишинг

ДЕТИ – СОУЧАСТНИКИ ФИНАНСОВЫХ МОШЕННИКОВ

Соучастие в мошенничестве - оказание услуги курьера

«81-летняя пенсионерка обратилась в полицию после того, как 17-летний подросток забрал у нее 100 тысяч рублей.
Бабушка думала, что помогает внучке, которая якобы попала в ДТП и по телефону попросила деньги. Чтобы на молодую женщину не завели дело, пенсионерка не пожалела все свои сбережения, но позвонить родным додумалась только после ухода курьера.
Когда полиция задержала юношу, он рассказал, что в поисках подработки оставил заявку в группе с вакансиями в соцсетях. Вскоре ему предложили работу в инвестиционной компании: забирать деньги у клиентов и пересылать их через банкомат на определенные счета и получать процент от перечисленных денег. Юноша согласился, отправил "работодателю" свои паспортные данные и стал курьером.
Также он предложил подзаработать своему знакомому сверстнику. Они вместе отправились на "дело" в соседний город. И пока один следил за обстановкой на улице, второй забрал более 700 тысяч рублей у 12-летней девочки, поверившей, что ее мама попала в аварию и нуждается в дорогостоящем лечении.»

Соучастие в мошенничестве

ДРОППЕРЫ

- люди, которые помогают обналичивать и выводить деньги после совершения преступниками финансового преступления

“Подросток Петя хочет найти подработку в свободное время. На одном из сайтов по поиску работы Петя увидел объявление:
“Требуется сотрудник для удаленной работы с денежными переводами. Серьезный заработок за несколько часов в день. Трудоустройство без проверок и заполнения документов. Опыт работы не требуется. Гарантия высокого дохода. Требования: наличие карты любого банка РФ”

ВАЖНО!

ЛЮДИ, ОТКЛИКНУВШИЕСЯ НА ПОДОБНЫЕ ОБЪЯВЛЕНИЯ, ЧАСТО СТАНОВЯТСЯ УЧАСТНИКАМИ МОШЕННИЧЕСКИХ СХЕМ.

СХЕМЫ ВЕРБОВКИ ДРОППЕРОВ

1. Объявления в Интернете,социальных сетях и мессенджерах о быстром заработке, подработке, связанные сденежными переводами, обналичиванием, работой в ИТ-сфере

2. Звонки под видом правоохранительных органов о работе или помощи в поимке преступников

3. Случайный перевод денег на карту с просьбой вернуть

ВИДЫ ДРОППЕРОВ

разводные

неосведомленные о преступной схеме

действуют неосознанно, неумышленно и/или под воздействием мошенников

неразводные

осведомленные о преступной схеме

действуют добровольно и умышленно

ПОСЛЕДСТВИЯ ДЕЙСТВИЙ ДРОППЕРОВ

От мошенников могут поступать угрозы жизни дропперу и его близким, шантаж

Дроппер становится участником схем отмывания денежных средств, продажи оружия или наркотиков

Дроппера будут искать правоохранительные и налоговые органы, иные структуры

Дроппер станет фигурантом уголовного дела

Дроппер отвечает своим имуществом и деньгами, а также имуществом и деньгами родителей и опекунов

Придется выплачивать крупные суммы годами

Дроппер создает себе негативный финансовый рейтинг, подрывает свою репутацию

ОТВЕТСТВЕННОСТЬ ДЛЯ ДРОППЕРА

Штраф

Принудительные работы

Ограничение свободы

Лишение свободы

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ФИНАНСОВЫХ ПРЕСТУПЛЕНИЙ

- фальшивые документы
- поддельные картинки и иллюстрации
- фейковые новости и рассылки
- фишинг, мошеннические веб-сайты
- социальные боты и манипуляция в социальных сетях
- беседа (телефонная и в переписке)
- "клон" человека (deepfake)
- поддельные голосовые сообщения
- фальшивая регистрация в ChatGPT

Пользователи телеграма столкнулись с новым видом мошенничества - сначала преступники получают доступ к аккаунту, затем начинают писать потенциальным жертвам из числа списка контактов его владельца с просьбой перевести деньги. Историю о необходимости помощи преступники подкрепляют голосовым сообщением якобы от лица владельца аккаунта. Для аудиосообщения используются нарезки из его реальных старых голосовых сообщений.

Аудиосообщение дублируется в личную переписку и во все чаты, где состоит хозяин украденного аккаунта. Затем направляется фото банковской карты с именем и фамилией. Причем у пострадавшего собеседника имя и фамилия отличались в соцсетях от информации в паспорте, и мошенники использовали данные именно паспорта. Сумма, которую хотели заполучить преступники, составляла 200 тыс. руб.

СПОСОБЫ ЗАЩИТЫ ОТ ФИНАНСОВОГО МОШЕННИЧЕСТВА

ОБЩИЕ ПРАВИЛА ЗАЩИТЫ

- критическое восприятие любой ситуации
- незнакомец диктует порядок действий – это точно обман
- обещания быстрой прибыли — всегда тревожный знак
- переход по незнакомым и непроверенным ссылкам может привести к обману и потере денег
- нельзя говорить незнакомым лицам личные данные
- при любых сомнениях всегда нужно спрашивать совета у родных и друзей
- позвонить в полицию

ПРАВИЛА ЗАЩИТЫ ОТ МОШЕННИКОВ ПРИ ТЕЛЕФОННЫХ ЗВОНКАХ

- не отвечать и не перезванивать по неизвестным и сомнительным номерам
- обязательно самостоятельно позвонить близкому человеку /в банк / в организацию / в полицию, попросить у них помощи
- прервать разговор, если он касается финансовых вопросов
- никому никогда в разговоре не сообщать никакие данные банковской карты, коды подтверждения из СМС-сообщений

ПРАВИЛА ДЕЙСТВИЙ С БАНКОВСКИМИ КАРТАМИ И ПРИ РАСЧЕТНЫХ ОПЕРАЦИЯХ

- никому никогда не сообщать и не фотографировать никакие данные банковской карты, коды подтверждения из СМС-сообщений
- заблокировать карту, если она потерялась или пришло уведомление о совершенной без вас операции
- не верить подозрительным СМС-сообщениям с неизвестных номеров о карте
- оплачивать покупки только через официальные сайты магазинов и площадок: через переводы оплачивать покупки нельзя
- не давать незнакомцам в руки мобильный телефон с установленными банковскими приложениями
- обязательно самостоятельно позвонить близкому человеку /в банк / в организацию / в полицию, попросить у них помощи

ПРАВИЛА ДЕЙСТВИЙ В ИНТЕРНЕТЕ И В ПЕРЕПИСКЕ ДЛЯ ЗАЩИТЫ ОТ ФИШИНГА И КИБЕРМОШЕННИЧЕСТВА

- не верить информации о выигрышах и легком заработке
- не устанавливать неизвестные приложения, особенно по просьбе незнакомцев
- не переходить по неизвестным и странным ссылкам
- сверять официальные источники с полученной информацией, письмами и т.д.
- никому в переписке не сообщать никакие личные данные
- не вводить личные данные на подозрительных сайтах и в приложениях
- всегда проверять у настоящего близкого и друга (лучше позвонить) полученную информацию

ЗАЩИТА АККАУНТОВ И ТЕХНИЧЕСКИХ СРЕДСТВ

Подключить двухфакторную аутентификацию

Установить сложный пароль

Закрыть доступ посторонним к своему профилю

Обновлять антивирусное ПО

ПРАВИЛА ДЕЙСТВИЙ ПРИ ИНТЕРНЕТ-ПОКУПКАХ

ПРОВЕРЯТЬ ИНТЕРНЕТ-МАГАЗИН

НЕ ОБЩАТЬСЯ С ПРОДАВЦОМ В МЕССЕНДЖЕРАХ ВНЕ ТОРГОВОЙ ПЛОЩАДКИ

ОПЛАЧИВАТЬ ПОКУПКИ ТОЛЬКО ЧЕРЕЗ ОФИЦИАЛЬНЫЕ МАГАЗИНЫ, ПЛАТФОРМЫ И Т. Д.

СОВЕТОВАТЬСЯ С РОДНЫМИ И БЛИЗКИМИ

ПРАВИЛА ДЕЙСТВИЙ В ИНТЕРНЕТЕ ОТ УГРОЗ, СВЯЗАННЫХ С ИИ

- Не вводить финансовую информацию в чат-ботах
- Проверять полученную информацию у реального человека, лучше ему позвонить
- Проверять данные на официальных ресурсах
- Задавать случайные вопросы

МЕЖДУНАРОДНАЯ ОЛИМПИАДА ПО ФИНАНСОВОЙ БЕЗОПАСНОСТИ

МЫ ЖДЕМ ИМЕННО ТЕБЯ!

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.

Участники: обучающиеся 8-10 классов / 1-3 курсы бакалавриата / 1-4 курсы специалитета / 1 курс магистратуры

Рекомендации по работе с презентацией
Всероссийского тематического урока на тему:
«НЕдетские игры: как не стать участником финансовых преступлений»

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

Задачи урока:

- заложить у обучающихся установки грамотного финансового поведения;
- сформировать у обучающихся представление о признаках ситуаций финансового мошенничества, о признаках фишинговых и других мошеннических сайтов.

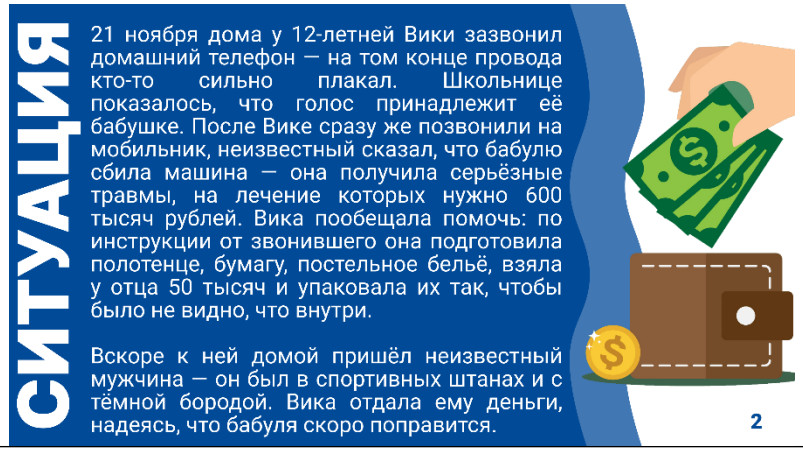
Научить обучающихся:

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

Дать понимание того, что за все финансовые решения отвечает собственник средств (своими деньгами), 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 **НЕдетские игры: как не стать участником финансовых преступлений** **Тематический урок**  	Согласно статистическим данным МВД России, в настоящее время молодые люди всё чаще становятся жертвами мошенников: пользуясь неопытностью и доверчивостью детей и подростков, злоумышленники крадут деньги с их карт и со счетов их родителей. При этом растет число обманутых жертв – подростков и детей до 14 лет. Для обмана используются телефонные звонки, мессенджеры, игры, призы и даже предложения о подработке. Такие мошеннические методы могут повлечь за собой несколько последствий: молодёжь становится жертвой финансовых мошенников или же становится их соучастником. Поэтому задача нашего урока - объяснить о подобных угрозах в реальной жизни, Интернете, социальных сетях и мессенджерах, научить самостоятельно определять мошенников по отличительным признакам и предпринимать определенные действия, чтобы не быть вовлеченными в мошеннические действия. Отдельно мы остановимся на мошеннических схемах с использованием искусственного интеллекта.
Слайд 2 **Ситуация** 21 ноября дома у 12-летней Вики зазвонил домашний телефон — на том конце провода кто-то сильно плакал. Школьнице показалось, что голос принадлежит её бабушке. После Вике сразу же позвонили на мобильник, неизвестный сказал, что бабулю сбила	**Задание:** 1. Изучите ситуацию, описанную на слайде. 2. Подумайте, какая схема мошенничества здесь была реализована? 3. На какую сумму был причинён ущерб и кому он был причинен – только девочке или ее семье? 4. Предположите, почему школьница поверила звонящему?

машина — она получила серьёзные травмы, на лечение которых нужно 600 тысяч рублей. Вика пообещала помочь: по инструкции от звонившего она подготовила полотенце, бумагу, постельное бельё, взяла у отца 50 тысяч (столько нашла) и упаковала их так, чтобы было не видно, что внутри. Вскоре к ней домой пришёл неизвестный мужчина — он был в спортивных штанах и с тёмной бородой. Вика отдала ему деньги, надеясь, что бабуля скоро поправится. 	**Предполагаемые ответы**: Это пример применения схемы телефонного мошенничества с несовершеннолетними. Ущерб в денежном выражении составил 50 тысяч рублей наличными, а также стоимость отданных вещей. Ущерб понесла семья девочки, так как было отдано имущество семьи. Школьница поверила звонящему, так как мошенники воздействовали на чувства и эмоции Вики – будто что что-то случилось с ее родным человеком. Кроме этого, мошенники попросили не только деньги, но и вещи для больницы, тем самым подтверждая придуманную ими ситуацию. В данном случае мошенники пользуются методами **социальной инженерии**. Социальная инженерия лежит в основе всех методов и видов кибермошенничества и телефонного мошенничества:
Слайд 3 **Социальная инженерия:** ...психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации. **Методы:** • Обман или злоупотребление доверием • Психологическое давление • Манипулирование	**Социальная инженерия** – это: ...психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации. Самым уязвимым звеном мошеннической цепочки все же остается человек, его реакции и эмоции. «Взломай» человека - взломаешь все остальное. Именно этим и пользуются мошенники. Поведение мошенника и жертвы в какой-то мере схожи. У мошенника есть две цели – обмануть и украсть. Психология жертвы – это особенности личности, которые позволяют ей попасться на уловку мошенника, плюс особая

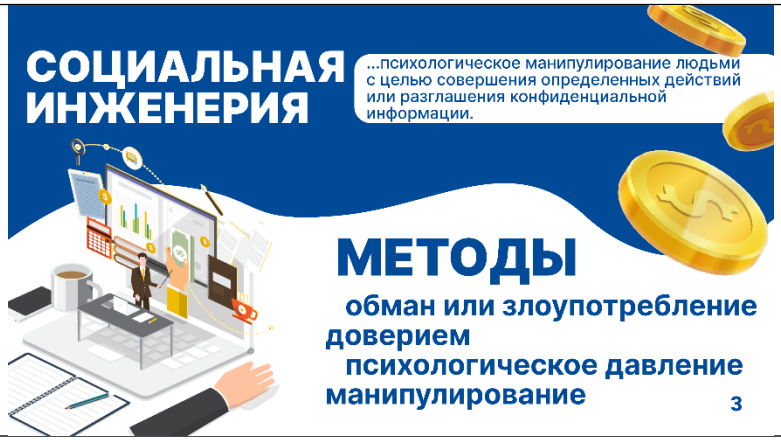
<table>
<tr>
<td> 
</td>
<td>социальная программа поведения. Например, кто-то хочет спасать мир, и тут получает СМС о том, что родственник в опасности. Кто-то боится сотрудников полиции, и ему звонят, представляясь полицейским.
Под влиянием социальной инженерии жертва добровольно расстается с деньгами или раскрывает личные и финансовые данные, которые нужны злоумышленникам для кражи средств</td>
</tr>
<tr>
<td>Слайд 4

Схема социальной инженерии

Эмоции, которые вызывает информация от мошенников, бывают двух видов:
1) отрицательные
➢ страх паника
➢ чувство стыда
2) положительные
➢ радость надежда
➢ желание получить деньги</td>
<td>Как работает этот метод:
1 этап — мошенники воздействуют на базовые эмоции (страх, радость, печаль, удивление, любопытство, злость, доверие, жадность), используя в том числе актуальные темы. Эти чувства выходят на первый план в любой стрессовой ситуации как защитный механизм человека, когда мы неожиданно слышим какую-то новость.

Эмоции, которые вызывает информация от мошенников, бывают двух видов:
1) отрицательные
➢ страх паника
➢ чувство стыда

Задание:
Привести пример фразы, которую может использовать мошенник, чтобы вызвать отрицательную эмоцию.
Предполагаемые ответы:
«С вашего счета списали все деньги»
«Ваш родственник попал в аварию и сбил человека»
«Вас беспокоит следователь Следственного комитета, ваша мама - участник уголовного дела о... коррупции или...»</td>
</tr>
</table>

2) положительные

- радость надежда
- желание получить деньги

Задание:

Привести пример фразы, которую может использовать мошенник, чтобы вызвать положительную эмоцию.

Предполагаемые ответы:

«Вы выиграли крупную сумму денег»

«Вам положены бонусы в игре».

2 этап — после активизации основных эмоций мошенники применяют определенные **психологические техники**, особенно успешно применяемые в устных и телефонных разговорах:

• Комплекс коротких вопросов, отработанный мошенниками сотни раз. Быстро отвечая на них, не перебивая мошенника, человек входит в состояние, близкое к трансу или гипнозу.

• Определенный тон голоса: официальный, либо вкрадчивый и доверительный, либо радостный и восторженный. Это усиливает эмоциональную реакцию жертвы.

• Поторапливание и ускорение событий, при котором жертва временно теряет способность к логике и анализу и выполняет инструкции мошенников.

• Угрозы, запугивание, ложные данные.

• Если человек попал в круговорот обмана, ему могут внушить, что вокруг все враги, никому не нужно верить и делиться, что же с вами происходит. Поэтому так сложно разубедить жертву, и она ничего не говорит своим близким и окружающим.

Использование данного метода и позволяет вовлекать несовершеннолетних в финансовые мошенничества.

Слайд 5

Телефонное и мобильное мошенничество

Кем может представиться мошенник:

- Службой безопасности банка, банковскими сотрудниками
- Сотрудником правоохранительных органов
- Родными
- Друзьями

Давайте рассмотрим более подробно формы мошенничества, в которые могут попадать несовершеннолетние. Первой и наиболее распространенной формой является ***Телефонное мошенничество.***

В данном случае совершается телефонный звонок потенциальной жертве (на городской или мобильный телефон, в том числе через мессенджеры) и применение различных техник манипуляции с целью заполучения денежных средств, иного имущества или личных данных.

Задание:

1. Назовите примеры того, кем могут представляться мошенники по телефону?

Предполагаемые ответы:

- *Служба безопасности Сбербанка*
- *Сотрудник Альфа банка*
- *Сотрудник Центрального банка*
- *Майор ФСБ*
- *Капитан полиции*
- *Старший следователь Следственного комитета*
- *Дочка, это я….*
- *Это Вася, папин друг….*

Задание:

2. Назовите примеры того, что говорят мошенники по телефону, представляясь службой безопасности, сотрудниками правоохранительных органов, родными и близкими?

Предполагаемые ответы:

«Ваша карта (счет) заблокирована»

«С вашей карты пытаются перевести деньги»

«К вашим счетам (счетам вашего отца) получили доступ злоумышленники и деньги нужно перевести на защищенный банковский счет...»

«По вашей карте выявлены подозрительные операции...»

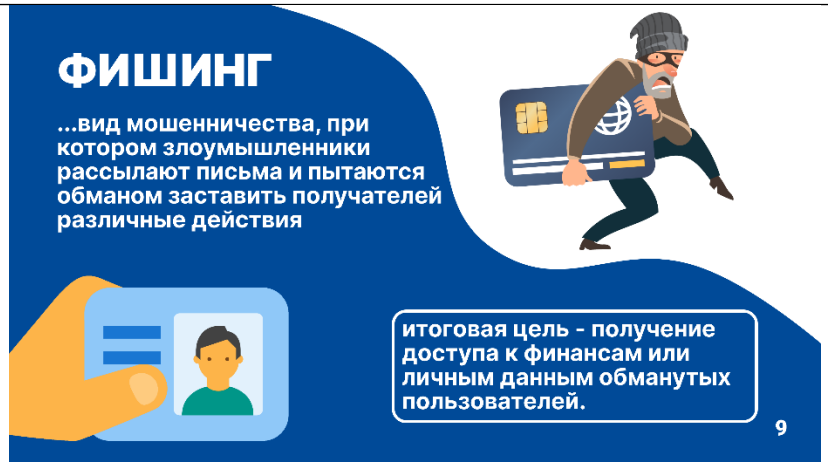
«На ваше имя пытаются взять кредит...»

«Ваш родственник сбил человека…»

	«По вашим поддельным документам кто-то пытается взять кредит на крупную сумму... Нам необходимо уточнить ее реквизиты….» *«Вы стали свидетелем по уголовному делу на вашего одноклассника…»* Если мошенник представляется родственником / другом / сыном знакомых, то обычно говорит: *«Наша бабушка попала в аварию, ей срочно нужны лекарства...»* *«Я сбил на машине ребенка, но уже договорился о взятке, срочно нужны деньги»* *«Ваш отец только что в результате ДТП сбил человека. Я готов помочь избежать наказания»*
Слайд 6 **Алгоритмы мошенников** 	В схемах с сотрудниками банков и правоохранительных органов злоумышленники предлагают решить проблему следующим способом и предлагают это своей жертве: • Вывести все деньги с банковских карт жертвы или ее родителей и перевести их на «безопасный» счет или на специальный счет в банке или в Центральном банке. • Исчерпать лимит кредитов по карте и перевести их на «безопасный» счет. Лжесотрудники банков или правоохранительных органов, органов государственной власти присылают своим жертвам фальшивые документы, сделанные через онлайн редакторы документов. Общение происходит в мессенджерах и в социальных сетях. На аватаре зачастую стоит значок банка или органа государственной власти (например, МВД). Часто в схеме участвует не один человек, и после звонка одного сотрудника происходит звонок другого сотрудника из другого ведомства, отдела и с другого номера. В схемах с использованием родственников и друзей часто мошенники сообщают, что родственник попал в больницу или

	аварию. Все это говорится быстро и с максимально достоверной актерской игрой, чтобы ввести потенциальную жертву в стресс и не дать мыслить рационально. Затем «чужой голос» просит отправить ему данные карты, сказать пин-код, собрать все деньги в доме, какие-либо предметы и сложить их в пакет. Злоумышленники отправляют курьера по адресу жертвы, чтобы забрать деньги. «Посылку» забирает специальный курьер. После чего и деньги и мошенники исчезают. Часто в схеме участвует не один человек.
Слайд 7 **Алгоритмы мошенников** **Ситуация:** 21 ноября у 15-летнего школьника Пети зазвонил мобильный телефон. На том конце провода мошенник представился стримером. Он сообщил, что случайно выбрал Петю для участия в онлайн-стриме, он готов оплатить ему билет в другой город для участия в стриме, но для этого, ему потребуются фотографии паспорта мальчика и фотография его банковской карты или его родителей. 	**Задание:** 1. Изучите ситуацию, описанную на слайде. 2. Какова была цель мошенника? 3. Как вы думаете, в какой момент стало понятно, что с девочкой говорит мошенник? **Предполагаемые ответы:** Мошенники выманивают данные банковских карт без участия курьеров и наличных денег. Получив данные карты (номер, CVV), они могут самостоятельно произвести мелкие финансовые операции без участия жертвы. Мальчику стоило остановить разговор в тот момент, когда его попросили прислать его личные данные. Признаками того, что позвонил или написал мошенник, могут быть следующие: • От вас требуют немедленных действий. • Торопят и запугивают, давят на эмоции, предлагают вознаграждение. • Требуют сообщить конфиденциальную информацию: данные карты, ПИН-код или одноразовый пароль из СМС. • Звонок поздно вечером, ночью или рано утром в выходные. • При отказе называть данные угрожают, что деньги с вашей карты прямо сейчас уйдут к мошенникам.

Слайд 8 **Киберпреступность и кибермошенничество** **Киберпреступность** - любое противозаконное деяние, нарушающее права и свободы человека с помощью компьютерных систем и сетей.  	Постепенная информатизация мира привела к появлению нового вида злодеев – кибермошенников. За время пандемии ковида многие сферы жизни перешли в онлайн, и киберпреступники (скамеры, черные шляпы, мошенники) также активизировали свою деятельность в интернете. Исследователи определяют киберпреступность как любое противозаконное деяние, нарушающее права и свободы человека с помощью компьютерных систем и сетей. Кибермошенничество - один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.). Оно реализуется в разных формах, о которых мы поговорим далее.
Слайд 9 **Фишинг** ...вид мошенничества, при котором злоумышленники рассылают письма и пытаются обманом заставить получателей различные действия Итоговая цель - получение доступа к финансам или личным данным обманутых пользователей.	**Фишинг** ...вид мошенничества, при котором злоумышленники рассылают письма и пытаются обманом заставить получателей совершить какое-то действие: • перейти по вредоносной ссылке • загрузить зараженное вложение • сообщить персональные данные и иную конфиденциальную информацию Итоговая цель мошенников чаще всего состоит в получении доступа к финансам обманутых пользователей.



Слайд 10

Фишинговое письмо — письмо, которое содержит вредоносное **вложение, ссылку** на мошеннический **сайт** или вредоносное программное обеспечение.

Темы и авторы писем:

- Службы доставки
- Маркетплейсы
- Криптовалюта
- Горячие новости
- Лотереи
- Дополнительный заработок и инвестиции
- Туроператоры и отдых
- Билеты на мероприятия
- Подписки и онлайн-сервисы
- Фото с вечеринки

Фишинговое письмо — письмо, которое содержит вредоносное вложение, ссылку на мошеннический сайт или вредоносное программное обеспечение.
Вирусные вредоносные программы нарушают работу системы на телефоне или компьютере, собирают данные, копируют или уничтожают файлы.
Какие уловки используют мошенники в таких письмах:

- Службы доставки
- Маркетплейсы
- Криптовалюта
- Горячие новости
- Лотереи
- Дополнительный заработок и инвестиции
- Туроператоры и отдых
- Билеты на мероприятия
- Подписки и онлайн-сервисы

Эти письма могут выглядеть как сообщения из вполне респектабельных источников: интернет-магазинов, банков, сервисов и пр.

Однако – это преступники, им интересны логины-пароли, которые могут использоваться для входа на разные сервисы, а также информация, содержащаяся в ноутбуках и компьютерах. Завладеть ею им помогают ***ссылки-ловушки***. Их направляют подросткам с предложением посмотреть интересные фотографии "с вечеринки или концерта", и при переходе по ссылке или при открытии файла на компьютер или телефон устанавливается вредоносное программное обеспечение.

Другим детям мошенники предлагают зарегистрироваться на специальных сайтах, чтобы участвовать в голосованиях, после чего телефон ребенка заражается вредоносными программами, и у мошенников появляется доступ к личной информации.

Слайд 11
Поддельные сайты или приложения
Фрод

Метод кибермошенничества в различных областях бизнеса с целью присвоения денежных средств называется **фрод**[1].

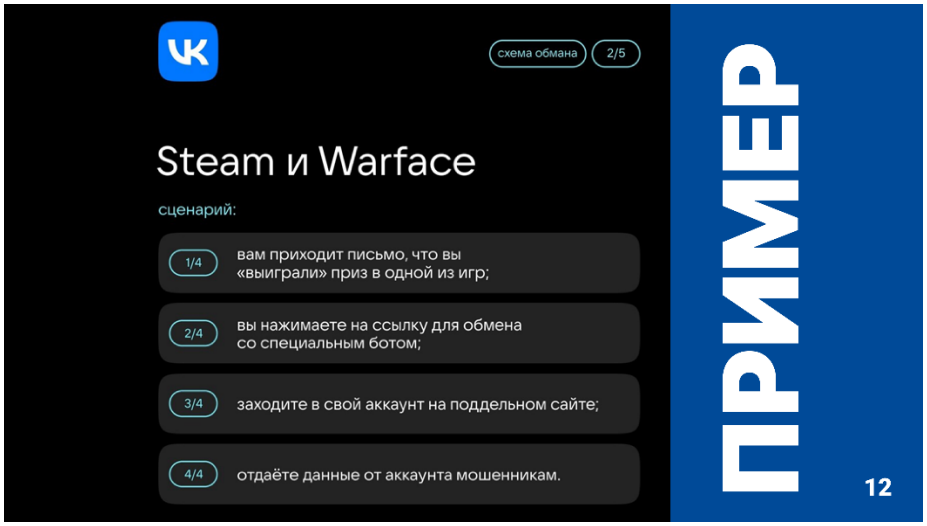
Мошенники могут создавать фишинговые сайты, предлагающие товары и услуги, например, компьютерную технику, *по более низким ценам.*

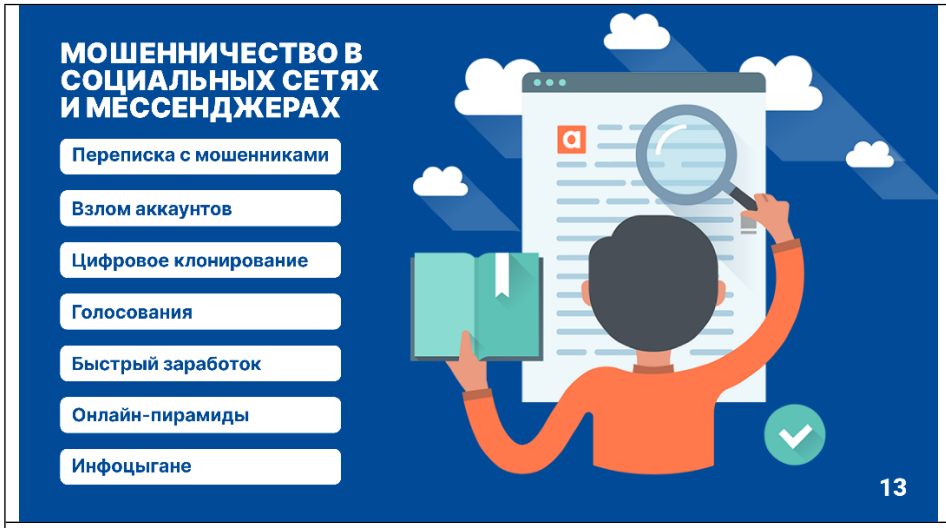
Существует много мошеннических сайтов, которые занимаются перепродажей внутриигровой валюты, графических оформлений (скинов) или предметов для компьютерных и телефонных игр.

После выбора товара или услуги и формы оплаты пользователя просят ввести реквизиты своей банковской карты (номер карты, CVV-код). После согласия осуществить оплату происходит передача реквизитов кредитной карты злоумышленникам, о чем пользователь даже и не догадывается.

Также мошенники научились подделывать, например, сайты банков, чтобы узнавать данные клиентов от их личного кабинета.

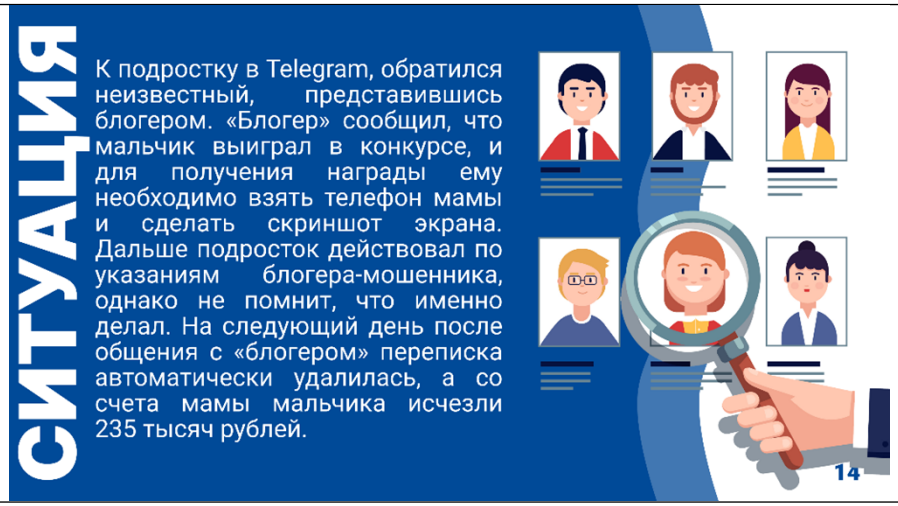
[1] https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov

Слайд 12 	В последнее время отдельной популярностью пользуются онлайн (мультиплеерные) игры, в которых за деньги можно повышать уровень игрока, покупать дополнительные возможности и переходить на более высокий игровой уровень. Игрокам приходится вводить данные банковских карт для оплаты этих улучшений или покупки внутриигровой валюты, и эти данные хранятся в персональном игровом аккаунте. Мошенники могут обманным путем попросить дать логин и пароль от аккаунта, предлагая «выгодную сделку», от которой трудно отказаться. Фишинговые игровые ресурсы также создаются для кражи аккаунтов у геймеров и последующего вымогательства денег в обмен на возвращение доступа. За персональные данные обещается солидный бонус в виде крупной суммы, золото по промокоду либо редкие скины. Дети и подростки не сразу могут понять, что оказались в сетях мошенников, однако результат остается один – мошенники крадут все деньги и персональные данные.
Слайд 13 **Мошенничество в социальных сетях и мессенджерах** o Переписка с мошенниками (социальная инженерия) o Взлом аккаунтов o Цифровое клонирование o Голосования o Быстрый заработок o Онлайн-пирамиды o Инфоцыгане	В последнее время мошенничество с использованием мессенджеров и социальных сетей все больше набирает обороты. Оно реализуется в различных формах: ○ Переписка с мошенниками (социальная инженерия) ○ Взлом аккаунтов ○ Цифровое клонирование ○ Голосования ○ Быстрый заработок ○ Онлайн-пирамиды ○ Инфоцыгане Мошенничество в социальных сетях и мессенджерах зачастую схоже с телефонным мошенничеством, но сначала может происходить переписка, а далее схема обмана может реализовываться различными способами – по телефону, через

<table>
<tr>
<td> 
</td>
<td>фишинг и тд. Самая популярная цель такого мошенничества – это махинация с банковскими картами, то есть получение данных карточки.</td>
</tr>
<tr>
<td>Слайд 14

Ситуация

К подростку в Telegram, обратился неизвестный, представившись блогером. «Блогер» сообщил, что мальчик выиграл в конкурсе, и для получения награды ему необходимо взять телефон мамы и сделать скриншот экрана. Дальше подросток действовал по указаниям блогера-мошенника, однако не помнит, что именно делал. На следующий день после общения с «блогером» переписка автоматически удалилась, а со счета мамы мальчика исчезли 235 тысяч рублей.</td>
<td>Задание:
1. Изучите ситуацию, описанную на слайде.
2. Как вы думаете, в какой момент стало понятно, что с мальчиком переписывается мошенник?
3. Почему мошенники попросили сфотографировать экран телефона родителей?
Предполагаемые ответы:
Стало понятно, что это мошенник тогда, когда блогер, во-первых, сам написал в Telegram – это подозрительное действие. Далее, когда мошенник попросил сделать определенные действия, связанные с чужим имущественном или данными.
Фото экрана было нужно мошенникам для того, чтобы посмотреть, какие приложения установлены на телефоне, и выяснить, приложением какого банка пользуется мама мальчика. Таким образом мошенники поняли, какое приложение для удаленного доступа можно установить, продиктовали ему, что сделать, и смогли украсть деньги.
Описанная схема – это один из популярных способов обмана - приходит сообщение, например, от имени популярного блогера о</td>
</tr>
</table>

<table>
<tr>
<td> 
</td>
<td>подарке или о потенциальном бонусе, для получения которого необходимо прислать реквизиты карты, на которую и поступит «заветный выигрыш». В таком состоянии дети и подростки отправляются данные своих карт или карт родителей, а также пароли или личные данные. Далее мошенник крадет все средства со счета карточки.</td>
</tr>
<tr>
<td>Слайд 15

Ситуация

Неизвестные лица создали телеграм-канал для любителей онлайн-шутера и предлагали делать ставки с обещанием заработать на турнирах по этой игре.
14-летний подросток сделал очень крупные ставки и перевел 100 тысяч рублей со счета своей мамы на Qiwi-кошелек и номера телефонов. В итоге он не получил никаких денег.</td>
<td>Рассмотрим пример, когда мошенники придумали аферу на основе популярной мобильной игры.
Задание:
1. Изучите ситуацию, описанную на слайде.
2. Какие признаки того, что данная схема - мошенническая?
Предполагаемые ответы:
В данном случае мошенники ловят игрока в игре, предлагая внутриигровую валюту, графические оформления (скины), предметы, делать ставки на турниры. Общение переходит в мессенджере, а не ведется через официальный ресурс (сайт, чат игры и прочее), что и является первым подозрительным признаком.
Дальше игрока просят делать ставки с реальными деньгами, что также является подозрительным признаком. Используется официальная оплата не через игровой аккаунт, а через сторонние кошельки и приложения, оплата в пользу частных лиц, что является подтверждающим признаком мошеннической операции.</td>
</tr>
</table>

<table>
<tr>
<td>


</td>
<td></td>
</tr>
<tr>
<td>

Слайд 16

Ситуация

Молодой человек познакомился в соцсетях с девушкой и общался с ней две недели. Периодически она просила просила оплатить ей всякие недорогие «*плюшки*», чтобы они встретились – положить деньги на телефон, купить ей комикс, оплатить маникюр и тд. И вот она пишет: «Я забронировала нам билеты в кино, сейчас тебе придет смс-ка с кодом для оплаты, можешь, пожалуйста, ее продиктовать, чтобы эти билеты оплатить».

Парень продиктовал ей коды из смс. После этого с карточки списались все деньги, а девушка перестала отвечать на сообщения и звонки и удалила свой аккаунт.

</td>
<td>

Задание:

1. Изучите ситуацию, описанную на слайде.
2. Какая мошенническая схема тут описана?
3. Какие признаки того, что описанная схема - мошенническая?
4. Какова цель мошенника?

Предполагаемые ответы:

В данном примере рассмотрена схема обмана при знакомствах в сети - это еще одна сторона кибермошенничества с молодыми людьми.

Подозрение на мошенничество должно возникнуть, когда появляются странные предложения. В первую очередь, финансового характера.

Главной целью мошенников, орудующих по такой схеме, является получение персональных данных потенциальной жертвы и доступа к ее счетам.

Можно привести более простой пример, парень знакомится с девушкой онлайн, она предлагает провести время и назначает первое свидание в конкретном месте - в театре, на концерте. Она присылает ссылку на покупку билетов, сайт фейковый (поддельный) – тут работает схема фишинга. Жертва теряет все деньги с карты.

</td>
</tr>
</table>

<table>
<tr>
<td>СИТУАЦИЯ
Молодой человек познакомился в соцсетях с девушкой и общался с ней две недели. Периодически она просила оплатить ей всякие недорогие «плюшки», чтобы они встретились – положить деньги на телефон, оплатить маникюр и т. д. И вот она пишет: «Я забронировала нам билеты в кино, сейчас тебе придет смс-ка с кодом для оплаты, можешь, пожалуйста, ее продиктовать, чтобы эти билеты оплатить».
Парень продиктовал ей коды из смс. После этого с карточки списались все деньги, а девушка перестала отвечать на сообщения и звонки и удалила свой аккаунт
 
</td>
<td></td>
</tr>
<tr>
<td>Слайд 17
Ситуация
В начале октября 14-летней девочке в социальной сети пришло сообщение от ее знакомого. Он утверждал, что счета и деньги родителей школьницы в опасности. Все из-за того, что в интернете есть их персональные данные, которыми могут воспользоваться мошенники.
«Приятель» сразу же предложил решение проблемы. Он рассказал девочке, как спасти семейные сбережения. Школьница последовала совету. Взяла банковские карты родителей, которые лежали на пуфике в прихожей, сфотографировала их со всех сторон и отправила снимки знакомому.
В итоге со счетов взрослых пропали 280 тысяч рублей. Потерпевшие обратились в полицию. Установлено, что страницу знакомого девочки взломали, и от его лица с ней общались аферисты.</td>
<td>Задание:
1. Изучите ситуацию, описанную на слайде.
2. Какая мошенническая схема тут описана?
3. Какие действия совершил мошенник, чтобы ему поверили?

Предполагаемые ответы:
Данный пример – это использование или захват фейковой учётной записи в социальной сети.
Мошенники взламывают чужие аккаунты, создают цифровых двойников каких-то знакомых лиц или других людей.
Нередко дети и подростки становятся объектами обмана от имени своих «друзей / знакомых», просящих в долг на пару дней или оказавшихся в «трудной жизненной ситуации».

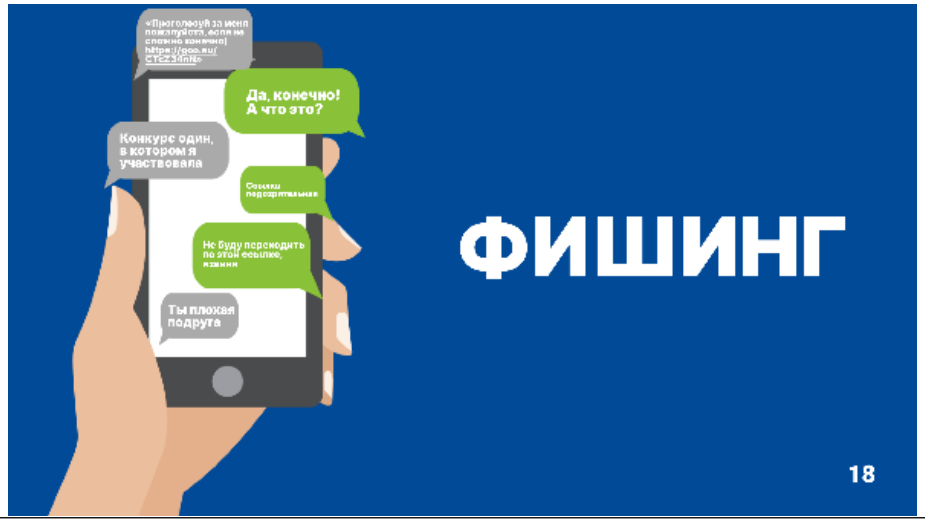
Кроме рассмотренных нами ситуаций, мошенники с фейковых (поддельных) аккаунтов, иногда подделывая страницы взрослых людей, знакомых ребенку, входят к нему в доверие, налаживают контакт.</td>
</tr>
</table>

Пока идет общение в соцсети, злоумышленники пытаются узнать у детей и подростков всевозможные подробности жизни семьи: где работают родители, когда бывают дома, с кем общаются, что покупают, куда ездят, как зовут членов семьи, какие машины у мамы и папы. Действуют не в лоб, вопросы задают аккуратно, издалека, тем самым незаметно получая нужную информацию.

Потом они умело используют эту информацию. Зная имена и детали чужой семейной жизни, звонят родителям детей и подростков, их родственникам, оперируя информацией, которая вызывает доверие у потенциальных жертв и притупляет их бдительность. Далее мошенник всеми возможными способами пытается завладеть денежными средствами жертвы.

В данном случае, получив от ребенка информацию, мошенник позвонит какой-нибудь бабушке и сообщит не просто, что «ваша дочь попала в аварию», а он называет эту дочь по имени, знает марку автомобиля, имена ее друзей и родственников, место работы.

Слайд 18



Кроме этого, часто приходят сообщения от друга или знакомого с различными просьбами: проголосовать, поставить лайк, дать денег в долг, купить билет и прочее.

Ссылка, отправляемая злоумышленниками, сделана при помощи сервиса для сокращения ссылок. Этот инструмент часто применяется, когда отправитель не хочет, чтобы реальный адрес сайта бросался в глаза.

На сайте злоумышленника, указав номер телефона, вы тут же получите код подтверждения, с помощью которого у вас «угонят» учётную запись. В данном случае можно квалифицировать данную схему как фишинг.

Слайд 19

Мошеннические схемы с быстрыми заработками

- вложения в выгодные проекты
- просмотры видеороликов популярных блогеров
- оценка картинок и отелей
- голосование в рейтингах
- букмекерские ставки
- экономические онлайн-игры

В Интернете или мессенджерах постоянно предлагают быстрый заработок или вложение денег в якобы выгодные проекты. Популярные схемы для детей и подростков – это деньги за просмотры видеороликов популярных блогеров, оценку картинок и отелей, голосование в рейтингах.

Реклама быстрого заработка, как правило, обещает высокий доход при минимальной трате времени.

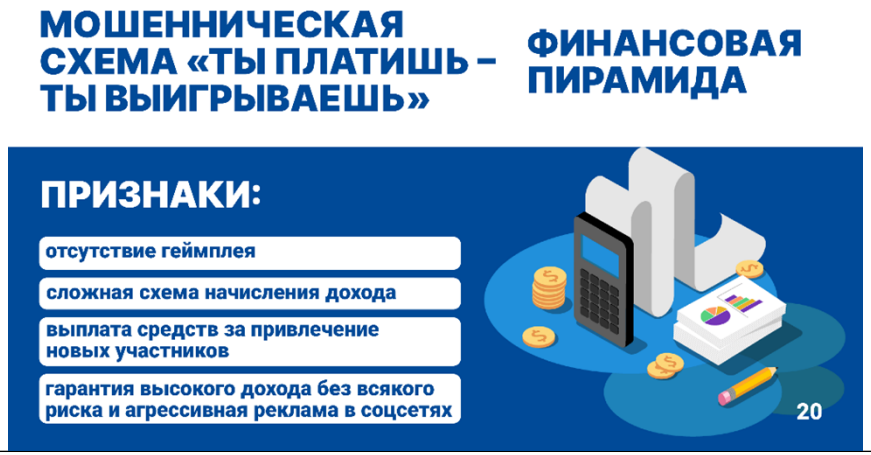
Более взрослым подросткам преступники рекламируют быстрые заработки с помощью букмекерских ставок на своих ресурсах.

Задание

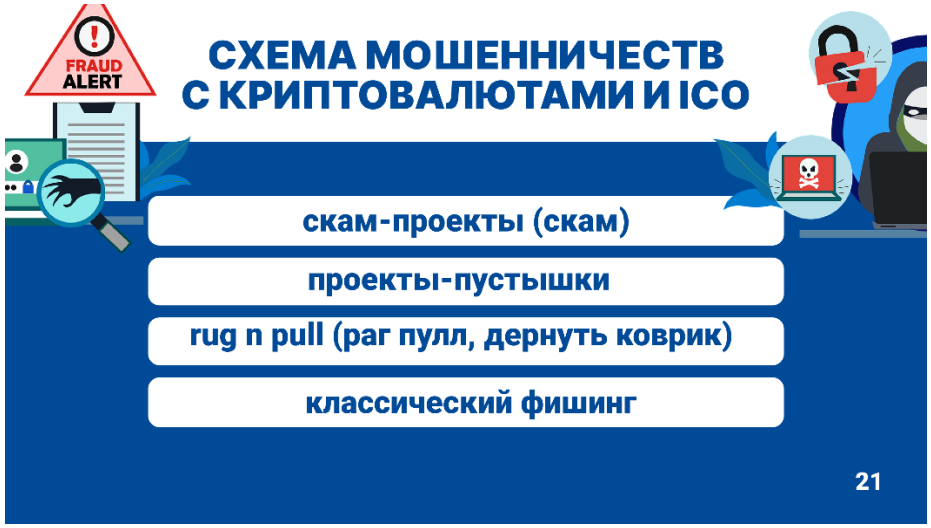
Подумайте, какую схему предлагает мошенник жертве, чтобы та потеряла деньги или личные данные?

Предполагаемые ответы:

- Перед началом "работы" ***мошенник отправляет ссылку и просит ввести банковские данные карты*** (своей или родителя), а также код из СМС-уведомления, объяснив, что по этим реквизитам в дальнейшем будет оплачивать услугу, или необходимо предварительно заплатить налог. После ввода СМС все средства со счета жертвы или ее родителей списываются.
- Мошенники убеждают людей ***оплатить текущие расходы (например, составление анкет, налоги) или оплатить какие-то услуги.***
- Мошенники показывают якобы успешные проекты, в которые можно вложить деньги или сделать ставки. Для вывода якобы заработка подростков ***просят оплатить комиссию***. В итоге деньги вместе с данными карты оказываются в руках киберпреступников.
- Мошенники, показывая вымышленные графики прибыли, убеждают жертву ***перевести как можно больше денег*** для выгодного инвестирования.

Слайд 20 **Мошенническая схема «Ты платишь – ты выигрываешь»** Финансовая пирамида **Признаки:** • Отсутствие геймплея • Выплата средств за привлечение новых участников • Сложная схема начисления дохода • Гарантия высокого дохода без всякого риска и агрессивная реклама в соцсетях 	В сети появились финансовые пирамиды под видом новых бизнес-игр. Особенностью таких проектов является отсутствие соревновательного элемента. Основные признаки финансовой пирамиды: • Отсутствие геймплея - отсутствие соревновательного элемента, рутинные и повторяющиеся действия. Чем проще механика, тем больше вероятность мошеннической схемы. • Выплата средств за привлечение новых участников. Если требуется привлекать новых игроков, это признак мошеннической схемы. • Сложная схема начисления дохода. Если получение дохода очень сложное, требуется множество действий, есть какая-то формула начисления дохода, скорее всего, цель этого – запутать игрока. • Гарантия высокого дохода без всякого риска и агрессивная реклама в соцсетях. Если реклама игры очень агрессивная, обещания заработка без риска, то, скорее всего, это мошенническая схема.
Слайд 21 **Схема мошенничеств с криптовалютами и ICO** **Скам-проекты (скам)** • Проекты-пустышки • Rug n Pull (раг пулл, дернуть коврик) • Pump and dump (Накачка и сброс)	Одним из самых популярных видов мошенничества в последние годы стали махинации с криптовалютами, в частности, со сбором средств на запуск различных проектов в сфере блокчейн, а также краудфандинд (коллективный сбор средств) на различные новые проекты (будь то создание новой игры, перевод книги и прочее). Люди вкладывают средства, а результатов нет, вложенные

- Классический фишинг



деньги исчезают. Такие мошеннические проекты называются **скам-проектами (скамом).**

Пример реализации такой схемы.

Злоумышленники презентуют на специальных сайтах якобы хороший проект, на реализацию которого требовались средства. Для этого используется так называемое поддельное ICO (Initial Coin Offering - первичное размещение ***токенов*** (монет)). Это формат сбора средств на развитие проектов в сфере криптовалют. Прикрываясь этим инструментом, мошенники продают фальшивую криптовалюту за биткоин или эфириум, которые имеют реальную стоимость (чтобы их купить – надо заплатить реальные (фиатные) деньги).

После нескольких раундов сбора средств «новаторы» (мошенники) пропадали без вести вместе с собранными средствами. При этом отследить их было практически невозможно, т.к. всеми собранными средствами можно распоряжаться анонимно.

Вторая схема мошенников с криптовалютами — это **Rug n Pull (раг пулл, дернуть коврик)** [2]. Смысл схемы заключается в выпуске токенов, большую часть которых оставляют себе мошенники, и лишь небольшая часть монет распределяется среди «инвесторов».

Важная характеристика возможного «вытягивания коврика» — монета, стремительно дорожающая в течение нескольких часов. После пампа (искусственного взлета) курса токена мошенники распродают все свои монеты и выводят средства, а обычные пользователи остаются с ненужными им токенами, которые обесцениваются почти на 100%. Такой токен невозможно продать (он становится неликвидным).

В 2023 году мошенники украли по такой схеме свыше $32 млн у приблизительно 42 000 пользователей[3].

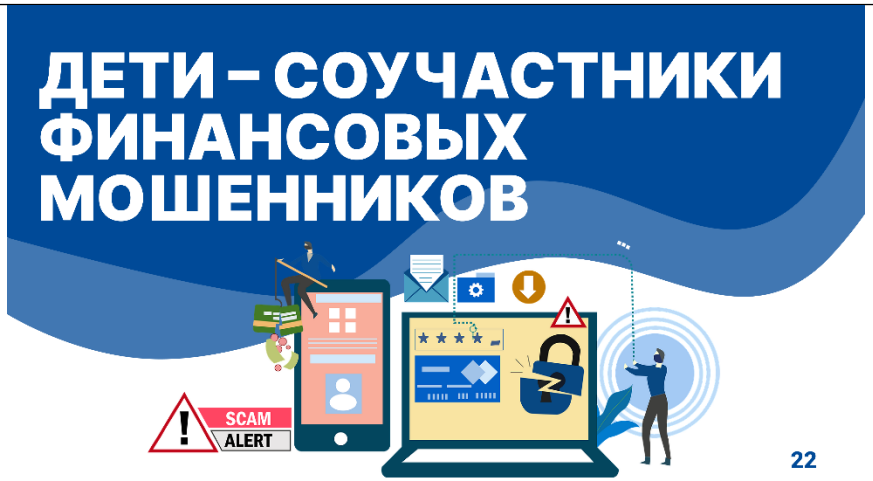
[2]Что такое скам в криптовалюте // Banki.ru. URL: https://www.banki.ru/news/daytheme/?id=10979400 https://www.banki.ru/news/daytheme/?id=10979400

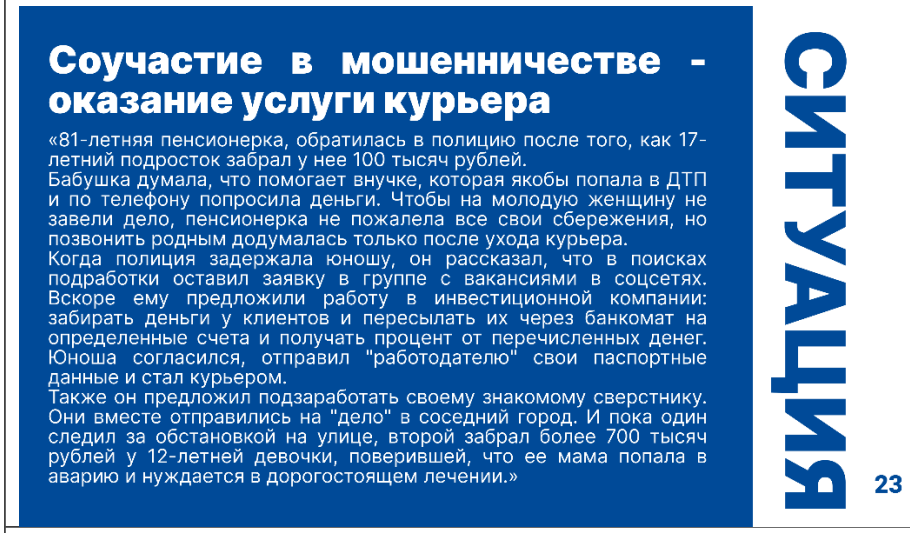
[3] Эксперты выявили автоматизированную скам-схему на $32 млн. URL: https://forklog.com/news/eksperty-vyyavili-avtomatizirovannuyu-skam-shemu-na-32-mln

	Третья схема мошенников с криптовалютами - **Pump and dump (Накачка и сброс)**[4] **-** вид скама, при котором создается ложный ажиотаж, хайп вокруг монеты. Мошенники создают или покупают по низкой и выгодной для них цене токены (обычно сомнительные). Далее с помощью различных чатов, новостных постов создается мнимый ажиотаж. Используются шумиха и дезинформация для создания ложного интереса к монетам, не имеющим известной и непосредственной ценности. Люди, не умеющие проводить грамотный анализ криптовалют, начинают закупаться монетами. Приходит волна таких покупок и стоимость токена начинает сильно расти. Когда цена достигает своего пика, а дезинформация вызывает покупательский ажиотаж, мошенники и влиятельные инвесторы «сбрасывают» все свои криптовалюты, обналичивая их с огромной прибылью. В результате распродажи цена монеты опустится значительно ниже первоначальной, и их невозможно будет продать[5]. Поэтому перед началом вложения реальных средств в различные проекты для начала надо изучить рынок криптовалют и создателей проекта более детально. Не следует покупать токены, которые не понимаете.
Слайд 22 **Дети – соучастники финансовых мошенников**	Вместе с тем, не всегда дети и подростки становятся лишь жертвами финансовых мошенников, так как злоумышленники вовлекают их в свою преступную деятельность. Подростки и молодежь часто ищут подработку в интернете. Этим пользуются мошенники, заманивая несовершеннолетних в свои преступные сети. Опасными схемами заработка можно назвать те, когда подросткам предлагают за процент или вознаграждение быть

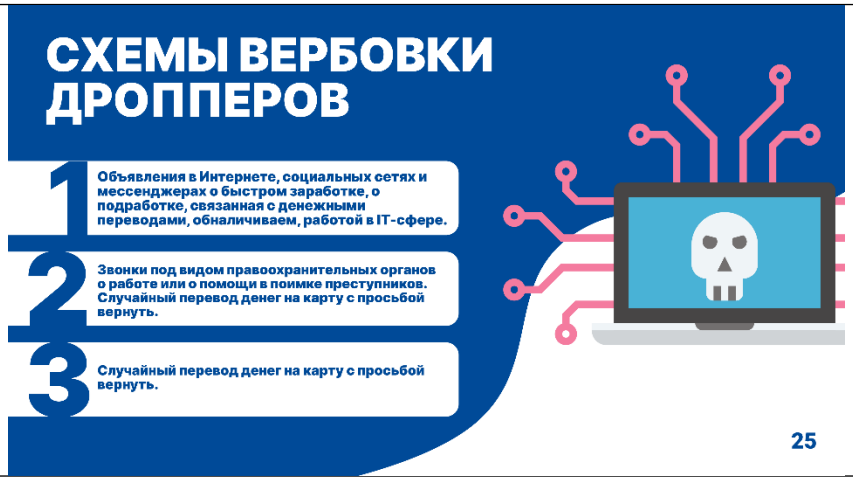
[4] Как вас могут скамнуть в щитках? Все виды скама в DEFI в одной статье. URL: https://vc.ru/u/2548531-nikita-slimkobag/927300-kak-vas-mogut-skamnut-v-shchitkah-vse-vidy-skama-v-defi-v-odnoy-state

[5] Как уберечься от мошенничества при “накачке” и “сбросе” криптовалют URL: https://bit.team/blog/ru/kak-uberechsya-ot-moshennichestva-pri-nakachke-i-sbrose-kriptovalyut/

	посредниками или курьерами при передаче или снятии денег, заработанных нелегальным путем. В таких случаях дети и подростки становятся пособниками или соучастниками в совершении преступления.
Слайд 23 **Соучастие в мошенничестве - оказание услуги курьера** **Ситуация** *«81-летняя пенсионерка, обратилась в полицию после того, как 17-летний подросток забрал у нее 100 тысяч рублей.* *Бабушка думала, что помогает внучке, которая якобы попала в ДТП и по телефону попросила деньги. Чтобы на молодую женщину не завели дело, пенсионерка не пожалела все свои сбережения, но позвонить родным додумалась только после ухода курьера.* *Когда полиция задержала юношу, он рассказал, что в поисках подработки оставил заявку в группе с вакансиями в соцсетях. Вскоре ему предложили работу в инвестиционной компании: забирать деньги у клиентов и пересылать их через банкомат на определенные счета и получать процент от перечисленных денег. Юноша согласился, отправил "работодателю" свои паспортные данные и стал курьером.*	Мошенники по телефону или в социальной сети предлагают ребенку или подростку оказать услуги курьера: лично забрать деньги у одного человека и перевести их на банковский счет другого, оставив себе часть за сделанную работу. В мессенджере несовершеннолетние получают от мошенников четкие инструкции, как себя вести с людьми, у которых они забирают деньги и как переводить средства. **Задание:** 1. Изучите ситуацию, описанную на слайде. 2. Какая мошенническая схема тут была реализована? 3. Когда стало понятно, что подросток стал соучастником преступления? 4. Как вы думаете, есть ли какое-то наказание за такие действия подростка? **Предполагаемые ответы:** Сначала мошенники обманным путем вымогают денежные средства у граждан, рассказывая истории о необходимости помочь

Также он предложил подзаработать своему знакомому сверстнику. Они вместе отправились на "дело" в соседний город. И пока один следил за обстановкой на улице, второй забрал более 700 тысяч рублей у 12-летней девочки, поверившей, что ее мама попала в аварию и нуждается в дорогостоящем лечении.» 	близкому родственнику, попавшему в беду. Обманутые граждане **передают деньги** несовершеннолетним **курьерам**. Курьер за вознаграждение перечисляет оставшуюся сумму на банковскую карту злоумышленников, **становясь пособником в совершении преступле**ния. Кроме этого, он привлек к таким схемам своего друга. Участие в подобных схемах может грозить уголовной ответственностью, а наказанием будут не только штрафы и обязанность вернуть деньги, но **реальное лишение свободы**. Аферисты, нанявшие несовершеннолетних курьерами, поручают им самую грязную работу - забрать деньги.
Слайд 24 **Соучастие в мошенничестве - дропперы** **Дропперы** - люди, которые помогают обналичивать и выводить деньги после совершения преступниками финансового преступления **Ситуация*:*** *Подросток Петя хочет найти подработку в свободное время.* *На одном из сайтов по поиску работы Петя увидел объявление:* *‘Требуется сотрудник для удаленной работы с денежными переводами. Серьезный заработок за несколько часов в день. Трудоустройство без проверок и заполнения документов. Опыт*	Следующая мошенническая финансовая схема - это схема незаконного обналичивания денежных средств и номинальных директоров. В этих схемах используются, в том числе, **дропперы** - люди, которые помогают обналичивать и выводить деньги после совершения преступниками финансового преступления. Чаще всего дропперы даже не подозревают, что являются частью большого преступного паззла. **Задание:** 1. Рассмотрите пример вербовки дроппера на слайде. 2. Какие подозрительные признаки в этом объявлении, которые могут говорить о том, что схема – мошенническая? 3. Кто в данном случае будет дроппером?

работы не требуется. Гарантия высокого дохода. Требования: наличие карты любого банка РФ». **Важно!** Люди, откликнувшиеся на подобные объявления, часто становятся участниками мошеннических схем.  	4. Как вы думаете, какие трудовые обязанности должен выполнять подросток на такой работе? 5. Какую цель преследуют мошенники, нанимая дропперов? **Предполагаемые ответы:** Что в данном случае является подозрительным? В объявлении нет требований к кандидату, а только наличие у него банковской карты. Документы для трудоустройства не требуются. Обещание быстрого и большого заработка. Дроппером будет откликнувшийся подросток. Чаще всего эти люди предоставляют данные своей банковской карты злоумышленникам за вознаграждение. Иногда ничего не подозревающего подростка просят **завести несколько банковских карт**. Дропперы не являются инициаторами преступления, однако они выполняют указания, получая за это деньги. На карты подростка мошенники переводят похищенные средства, а затем по цепочке подростки переводят средства другому человеку. Кроме этого, подростков просят обналичить поступившие на карту деньги в разных банкоматах, забрав себе небольшой процент. Таким образом преступники усложняют правоохранителям поиск средств и конечных получателей.
Слайд 25 **Схемы вербовки дропперов** 1. Объявления в Интернете, социальных сетях и мессенджерах о быстром заработке, о подработке, связанная с денежными переводами, обналичиваем, работой в IT-сфере. 2. Звонки под видом правоохранительных органов о работе или о помощи в поимке преступников. 3. Случайный перевод денег на карту с просьбой вернуть.	Схемы вербовки дропперов мошенниками разные, например: 1) мошенники размещают на улицах и в интернете, в том числе, в социальных сетях, объявления, в которых предлагается работа, связанная с переводом и обналичиванием денег; 2) мошенники размещают в телеграмм-каналах и социальных сетях объявления об интересной работе в IT-сфере с быстрым ростом заработка; 3) мошенники, размещая объявления о работе, делают фишинговые сайты (поддельные) крупных компаний, чтобы усыпить бдительность и предлагают такие подработки;



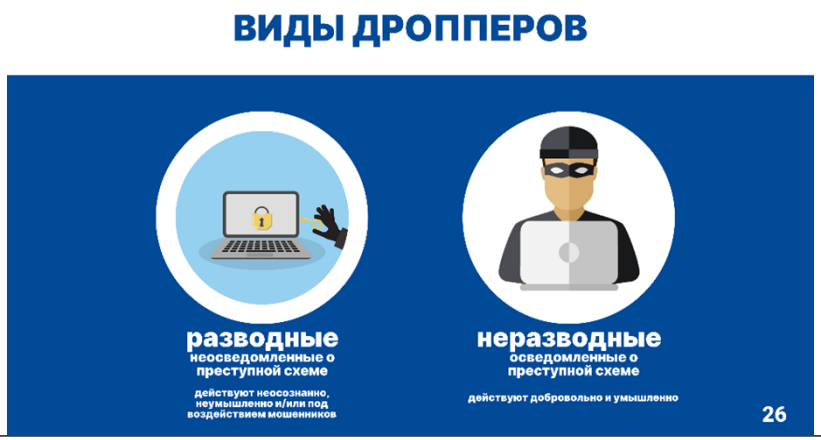
4) под видом сотрудников правоохранительных органов мошенники звонят подростку с предложением официально устроиться на работу по поиску преступников и обещают ежемесячный доход. Если человек соглашается, то мошенники переводят на его банковскую карту похищенные деньги и затем под видом сотрудников банка требуют снять эти деньги в банкомате;

5) Под видом ошибившегося человека мошенники "случайно" переводят на банковский счёт деньги, а затем просят их вернуть наличными или перевести на карту.

Слайд 26

Виды дропперов:

- *неразводные*, осведомленные о преступной схеме
  - действуют добровольно и умышленно
- *разводные*, неосведомленные о преступной схеме
  - действуют неосознанно, неумышленно и/или под воздействием мошенников



Чаще всего дропперами становятся наименее финансово грамотные, доверчивые люди, и те, кто верит, что может быстро и легко заработать.

Различают два вида дропперов: «неразводные» и «разводные».

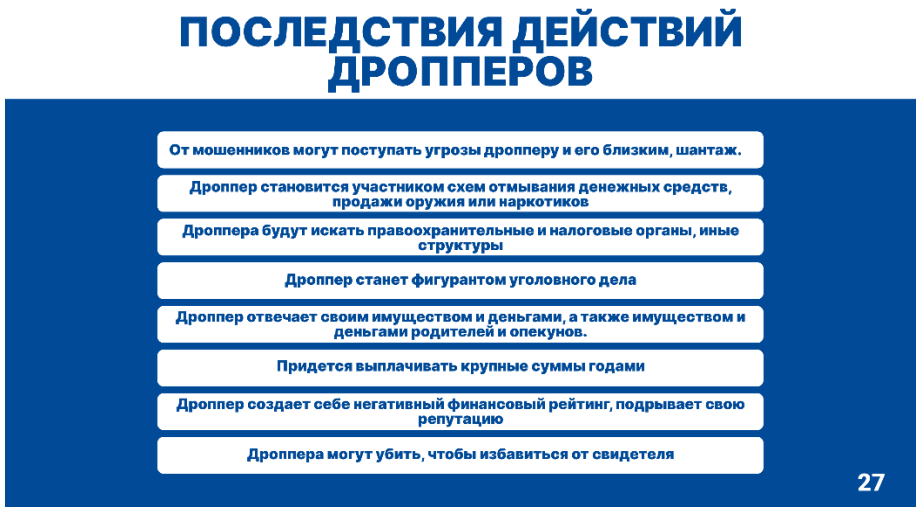
К первому типу подставных относятся люди, которые осведомлены о криминальной составляющей своей деятельности и действуют добровольно и умышленно.

Ко второму — те, кто не понимает, что находится в ловушке у мошенников, и не отдает себе отчета, что участвует в схеме, нарушающей закон.

Слайд 27

Последствия действий дропперов:

1. От мошенников могут поступать угрозы дропперу и его близким, шантаж;
2. Дроппер становится участником схем отмывания денежных средств, продажи оружия или наркотиков;
3. Дроппера будут искать правоохранительные и налоговые органы, иные структуры;
4. Дроппер станет фигурантом уголовного дела;
5. Дроппер отвечаешь своим имуществом и деньгами, а также имуществом и деньгами родителей и опекунов;
6. Придется выплачивать крупные суммы годами;
7. Дроппер создает себе негативный финансовый рейтинг, подрывает свою репутацию;
8. Дроппера могут убить, чтобы избавиться от свидетеля.



Злоумышленники стремятся максимально усложнить правоохранительным органам процесс выявления и отслеживания денежных средств, проходящих через цепочки обналичивания.

Сами мошенники прибегают к услугам подставных лиц - дропперов, чтобы избежать ответственности за перевод или обналичивание денежных средств. Большинство организаторов афер живут за границей и даже вычислить их весьма сложно, **зато посыльных-дропперов ловят практически всех.**

Дропперы, соглашаясь на такую деятельность, несут очень большие последствия, которые могут затронуть не только свои и родительские деньги и имущество, но и жизнь и свободу себя и своей семьи.

Слайд 28

Действия дропперов уголовно наказуемы.

Задание:

1. Подумайте, на какие виды преступлений похожи действия дропперов?
2. Подумайте, в каком размере может быть наказан дроппер? Могут ли дроппера посадить в тюрьму?

Предполагаемые ответы:

Действия дроппера могут квалифицироваться как мошенничество, легализация (отмывание) денежных средств, полученных преступным путем, как неправомерный оборот средств платежей.

В случае, если деяния будут так квалифицированы, то он понесет наказание не только в виде большого штрафа (от 100 тысяч рублей), но и в виде лишения свободы на долгий срок (в среднем, 6-7 лет, но может достигать и 10 лет, в зависимости от тяжести совершенного преступления).

Жертве мошенничества необходимо возместить ущерб.

А с 14 лет это должен делать сам подросток: он оплачивает штраф либо с заработка, со стипендии, с алиментов или другого вида дохода. Если возможностей заработка нет, то в счет ущерба может пойти движимое или недвижимое имущество (например, компьютер, телефон, приставка). А вот в том случае, если штраф довольно большой и собственных средств подростку не хватает, ему обязаны помочь родители или опекуны.

Также данные о правонарушении направят в Комиссию по делам несовершеннолетних и защите их прав.

Слайд 29

Использование искусственного интеллекта для финансовых преступлений

1. фальшивые документы
2. создание поддельных картинок и иллюстраций
3. фейковые новости и рассылки
4. фишинг, мошеннические веб-сайты
5. социальные боты и манипуляция в социальных сетях
6. беседа (телефонная и в переписке)
7. "клон" человека (deepfake)
8. поддельные голосовые сообщения
9. фальшивая регистрация в ChatGPT

Искусственный интеллект (ИИ) дает невероятные новые возможности бизнесу, промышленности, науке, образованию. Но одновременно с этим использовать нейросети начали киберпреступники (черные шляпы, скамеры).

Задание:

1. Рассмотрите основные стратегии мошенников с использованием искусственного интеллекта, представленные на слайде.
2. Объясните, что каким образом ИИ используется в каждой из этих стратегий?

Предполагаемые ответы:

Злоумышленники применяют алгоритмы машинного обучения и используют нейронные сети, чтобы получить доступ к личной информации людей для обмана. Преступники могут использовать алгоритмы ИИ для создания поддельных личностей и проведения мошеннических операций, которые трудно обнаружить.

1. С помощью искусственного интеллекта злоумышленники могут делать **фальшивые документы**: нейросеть подделает банковские выписки, нарисует фальшивый паспорт или водительское удостоверение.

2. Нейросети мастерски умеют **создавать картины и иллюстрации**. А это значит, что подобные изображения легко используются для фейковых сборов. Так что перед тем, как отправить кому-то финансовую помощь, стоит проверить в других соцсетях и интернете "реальность" адресата.

3. Мошенники могут использовать нейросети для создания **фейковых новостей и рассылок**. В них включаются различные ссылки на ресурсы, при переходе по которым можно потерять данные своей банковской карты или другую персональную информацию.

4. **Фишинг, мошеннические веб-сайты:** ИИ используется для создания поддельных электронных писем (генерацию любых писем)

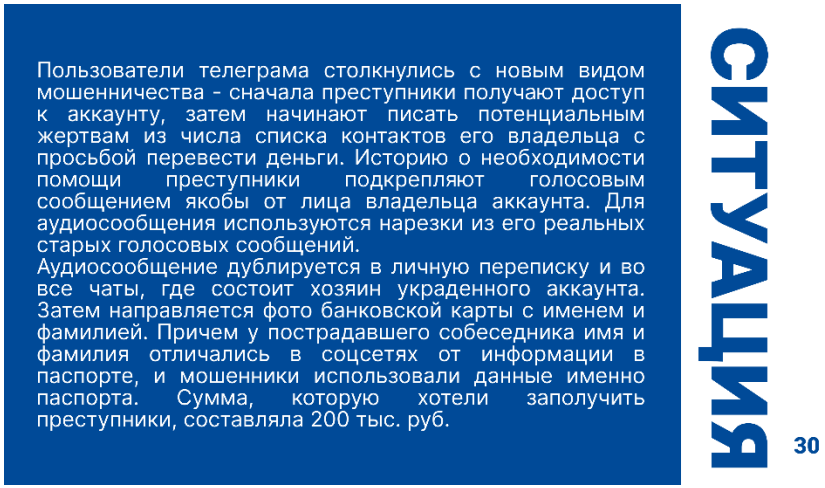
	и веб-сайтов (парсинг и считывания любых WEB файлов, и даже закрытых от индексации, и сразу генерацией любых уникальных материалов взамен), чтобы обмануть пользователей и получить доступ к их личным данным и финансовым ресурсам. 5. **Социальные боты и манипуляция в социальных сетях**: ИИ используется для создания чат ботов (телеграм) оплаты и возможностью сохранять платежные данные. Все эти схемы объединяет необходимость ввода своего номера телефона и SMS-кода. Полученные данные затем используются злоумышленниками для несанкционированного доступа к учетной записи и последующей рассылки спама или вымогания денег. 6. Нейросети учатся **поддерживать разговор**. Искусственный интеллект может взять на себя роль мнимых сотрудников контакт-центров банков и других организаций, которыми представляются мошенники для обмана свои жертв, и вести разговор. 7. ИИ может создавать **"клон" голоса и образа человека (deepfake)**. Кроме этого, Deepfakes — это манипулированные видео, в которых алгоритмы ИИ накладывают лицо одного человека на тело другого, создавая впечатление, что человек на видео говорит или делает то, чего на самом деле никогда не делал и не говорил. С учетом развития биометрии и возможности оформить кредит по звонку (современные технологии идентифицируют человека по тембру голоса), Deepfake будет иметь стопроцентную схожесть с оригиналом, а значит, жертва рискует остаться в должниках, ничего об этом не зная. 8. Злоумышленники могут использовать схему мошенничества, связанную с фальшивой регистрацией в ChatGPT, через фишинговые сайты или приложения, маскируемые под сервисы продажи за небольшие деньги аккаунта в нейросети ChatGPT. При регистрации на данном ресурсе необходимо будет заполнить форму с данными для оплаты, либо будет предоставлена ссылка на вредоносную программу

Слайд 30

Ситуация

Пользователи телеграма столкнулись с новым видом мошенничества - сначала преступники получают доступ к аккаунту, затем начинают писать потенциальным жертвам из числа списка контактов его владельца с просьбой перевести деньги. Историю о необходимости помощи преступники подкрепляют голосовым сообщением якобы от лица владельца аккаунта. Для аудиосообщения используются нарезки из его реальных старых голосовых сообщений.

Аудиосообщение дублируется в личную переписку и во все чаты, где состоит хозяин украденного аккаунта. Затем направляется фото банковской карты с именем и фамилией. Причем у пострадавшего собеседника имя и фамилия отличались в соцсетях от информации в паспорте, и мошенники использовали данные именно паспорта. Сумма, которую хотели заполучить преступники, составляла 200 тыс. руб.



Преступники часто используют искусственный интеллект для подделки голосовых сообщений в мессенджерах с целью краж денег и аккаунтов.

На первом этапе происходит взлом аккаунта Telegram или WhatsApp, например, через фейковые голосования. Затем мошенники скачивают сохраненные голосовые сообщения и с помощью сервисов искусственного интеллекта синтезируют новые «голосовушки» с необходимым контекстом. Наконец, происходит рассылка сообщений в «личку» или групповые чаты с просьбой одолжить крупную сумму денег, для убедительности используют сгенерированные искусственным интеллектом «голосовушки» и отфотошопленную банковскую карту с поддельным именем получателя.

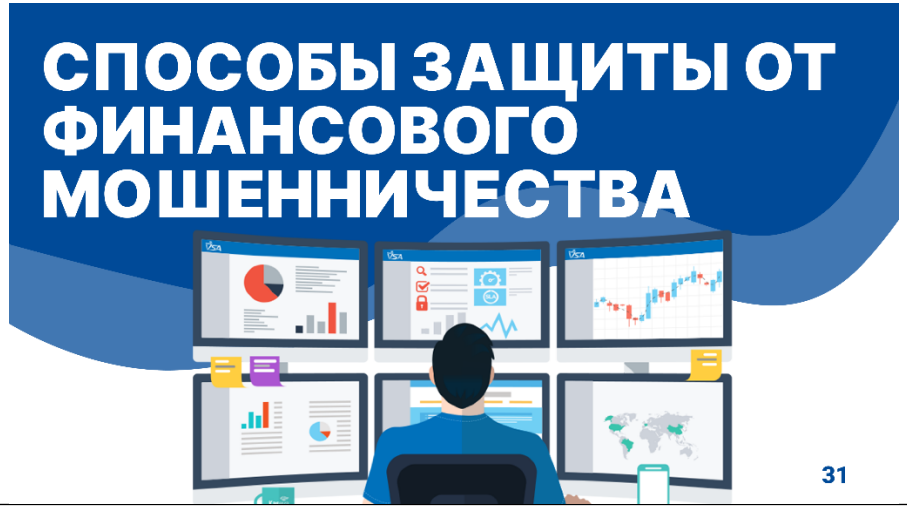
Задание:

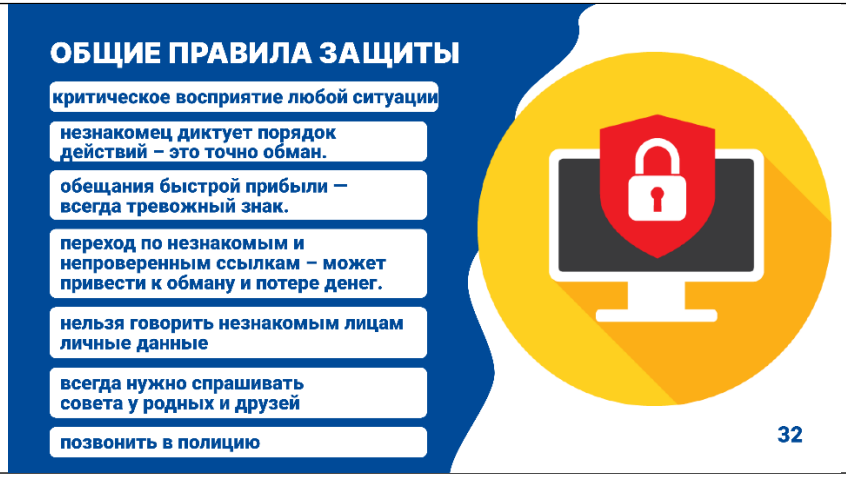
1. Подумайте, чем такая мошенническая схема более опасна чем традиционная?
2. Подумайте, какое самое простое действие поможет избежать стать жертвой мошенника?

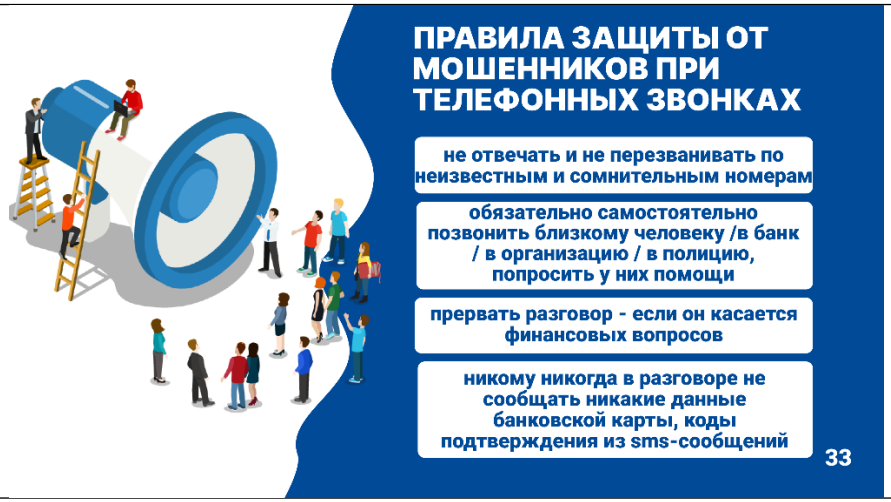
Предполагаемые ответы:

Данная схема опасна тем, что мошенники используют **несколько факторов идентификации жертвы** — аккаунт, голос и банковскую карту. С помощью ИИ генерируется нужная нарезка аудиофайлов и создаётся фейковое голосовое сообщение. С помощью ИИ генерируется нужный документ на основе украденных личных данных.

Самый простой способ не попасться на такую уловку - перепроверить, действительно ли владелец аккаунта обращается с подобной просьбой, например, перезвонив ему по телефону.

Слайд 31 **Способы защиты от финансового мошенничества**  	Мы рассмотрели различные виды мошеннических схем, которые применяются для совершения финансовых преступлений. Жертвами таких преступлений могут стать люди любого возраста и взрослые, и молодые. Поэтому необходимо запомнить ряд приемов, которые позволят защититься от финансового мошенничества и не стать жертвой преступников.
Слайд 32 **Общие правила защиты** 1. Критическое восприятие любой ситуации 2. Незнакомец диктует порядок действий – это точно обман. 3. Обещания быстрой прибыли — всегда тревожный знак. 4. Переход по незнакомым и непроверенным ссылкам – может привести к обману и потере денег. 5. Нельзя говорить незнакомым лицам личные данные. 6. ВСЕГДА нужно спрашивать совета у родных и друзей 7. Позвонить в полицию	К любой ситуации необходимо относится **с критическим восприятием**. Рекомендуется воспринимать с сомнением все звонки и сообщения, когда собеседник вас куда-то отправляет, склоняет вас к каким-то действиям, требует переводить деньги или что-то оформлять. Необходимо запомнить несколько ***общих простых правил***: - если незнакомые лица начинают диктовать порядок действий, значит они пытаются вас «развести»; - обещания быстрой прибыли — всегда тревожный знак; - не переходить по незнакомым ссылкам; - не давать незнакомым лицам данные банковских карт. Не стоить реагировать на тревожные звонки, письма, SMS или сообщения в соцсетях о том, что родственнику или знакомому нужны деньги. В этом случае обязательно стоит попытаться связаться с этим родственником или знакомым и сообщить, что от их имени рассылаются такие сообщения, возможно их аккаунт взломали.

	Если возникает хоть одно сомнение, происходит какое-то непонятное или пугающее действие, о котором мы говорили ранее, необходимо остановится, **спросить совета у родных и друзей!** Если до них невозможно дозвониться, нужно позвонить в полицию по номеру 112.
Слайд 33 **Правила защиты от мошенников при телефонных звонках** • Не отвечать и не перезванивать по неизвестным и сомнительным номерам; • ОБЯЗАТЕЛЬНО самостоятельно позвонить близкому человеку /в банк / в организацию / в полицию, попросить у них помощи; • Прервать разговор, если он касается финансовых вопросов; • Никому никогда в разговоре не сообщать НИКАКИЕ данные банковской карты, коды подтверждения из SMS-сообщений.	1. Внимательно проверять входящий номер. 2. Вообще не отвечать и не перезванивать по неизвестным и сомнительным номерам. Даже если телефон кажется верным, стоит всегда проверять номера в официальных справочниках и на официальных сайтах. 3. ОБЯЗАТЕЛЬНО самостоятельно позвонить близкому человеку /в банк / в организацию / в полицию, попросить у них помощи. 4. Прервать разговор, если он касается финансовых вопросов. 5. Запомнить, что Центральный банк, Росфинмониторинг никогда не звонят физическим лицам. 6. Не совершать никаких операций или действий по инструкциям звонящего. 7. Никому никогда не сообщать коды подтверждения из SMS-сообщений. 8. Не сообщать CVV/CVC и иные данные банковских карт по телефону и в переписках. 9. Не торопиться принимать решение. 10. Сразу заканчивать разговор при любых сомнениях. 11. Поставить приложение для фильтрации входящих вызовов. Заблокировать звонки с подозрительных номеров.

	12. Проверить, не было ли сомнительных операций за время разговора (по карте, в смс). 13. Проиграть с родителями в игру, имитирующую звонки от представителя банка или полиции. Отвечать нужно чётко и быстро: "Спасибо, до свидания, я сам перезвоню". И так повторить раз 10, чтобы у человека сформировалась модель поведения. А дальше перезвонить в банк и узнать, чего же от вас хотели и хотели ли. 14. Можно придумать с родителями и близкими кодовое слово, которое покажет, что что-то не так.
Слайд 34 **Правила действий с банковскими картами и при расчетных операциях** • Никому никогда не сообщать и не фотографировать НИКАКИЕ данные банковской карты, коды подтверждения из SMS-сообщений; • Заблокировать карту, если она потерялась или пришло уведомление о совершенной без вас операции; • Не верить подозрительным смс с неизвестных номеров о карте; • Оплачивать покупки только через официальные сайты магазинов и площадок. Через переводы оплачивать покупки нельзя; • Не давать незнакомцам в руки мобильный телефон с установленными банковскими приложениями; • ОБЯЗАТЕЛЬНО самостоятельно позвонить близкому человеку /в банк / в организацию / в полицию, попросить у них помощи.	1. Не передавать банковскую карту посторонним. Требовать проведения операций с ней только в личном присутствии и стараться никогда не терять ее из виду. 2. Не делать покупки и не вводить код CCV/CVC на сомнительных сайтах. На сайте надежного интернет-магазина никогда не будут запрашивать личную информацию: пин-код карты, пароли от мобильного банка и привязанных к пластику электронных почтовых ящиков. Эти данные нигде нельзя оставлять! 3. Данные карты (номер, пин-код, CVC-код) нельзя сообщать никому, даже сотрудникам банка. 4. Нельзя писать пин-код на карте и хранить его отдельно. Набирая пин-код, всегда необходимо прикрывать клавиатуру рукой. В том числе, при расчете в кафе и магазинах. 5. Если банковская карта потерялась, необходимо немедленно сообщить родителям, далее в банк и заблокировать ее. То же самое — если пришло SMS-сообщение о покупке или снятии денег в банкомате, а вы этого не делали. Для этого полезно иметь телефон службы поддержки банка под рукой. 6. При поступлении подозрительных смс о том, что карта заблокирована или с нее были переведены средства по транзакции,

<table>
<tr>
<td> 
</td>
<td>которая не совершалась, необходимо сообщить родителям. Перезванивать на номер, с которого поступило сообщение, нельзя.
7. Всегда осматривать банкомат перед использованием. Необходимо убедиться, что над клавиатурой и на картоприемнике нет посторонних прикрепленных предметов, а клавиатура не шатается.
8. Не использовать открытые точки Wi-Fi (интернет в общественных местах: транспорте, кафе, кинотеатрах), когда заходите в интернет-банк или пользуетесь мобильным банковским приложением.
9. Оплата в интернет-магазине не должна происходить как перевод средств на чей-то личный счет. Если такое происходит, отправлять деньги нельзя. В таком случае необходимо обратиться к родителям, чтобы они помогли выбрать надежный магазин.
10. Нельзя передавать посторонним лицам мобильные устройства, на которых установлены приложения онлайн банков.</td>
</tr>
<tr>
<td>Слайд 35

Правила действий в интернете и в переписке для защиты от фишинга и кибермошенничества

• Не верить информации о выигрышах и о легком заработке;
• Не устанавливать неизвестные приложения, особенно по просьбе незнакомцев;
• Не переходить по неизвестным и по странным ссылкам;
• Сверять официальные источники с полученной информацией, письмами и т.д.;
• Никому в переписке не сообщать никакие личные данные;
• Не вводить личные данные на подозрительных сайтах и в приложениях;
• Всегда проверять у настоящего близкого и друга (лучше позвонить) полученную информацию.</td>
<td>1. Не следует верить информации о выигрышах, платить деньги за участие в челленджах и обольщаться легким заработком.
2. Не переходить по ссылкам в письмах или сообщениях о выигрыше денег, гаджета или другого приза, не кликайте на подозрительные объекты. Скорее всего, по ссылке вы получите только вирус.
Наведите курсор мыши на подозрительную ссылку/объект, и вы увидите, куда она ведёт на самом деле. Сравните её с официальным сайтом компании.
3. Опасно скачивать по просьбе незнакомцев какие-либо приложения, открывать незнакомые и странные ссылки. Даже если ссылка кажется надежной, стоит всегда сверять адреса с доменными именами официальных сайтов организаций.
4. Обращать внимание на почтовый домен, с которого приходят письма. Мошенники обычно используют общедоступные домены gmail.com, mail.ru и т.п., или домены, похожие на</td>
</tr>
</table>

официальные имена компаний (напр. sberbankc[.]ru, lc-sberbank[.]com и т.д.)

5. Изучить тему письма или сообщения, контент письма и название файлов. Обращать внимание на грамотность письма. Если в сообщение побуждает вас к немедленному действию – это подозрительный признак.

6. Обращать внимание на обращение и подпись. Если они являются безличными, или есть признак автоподстановки в обращении, то высока вероятность фишинга.

7. Быть осторожными с вложениями в письма или сообщения. Открывайте только те вложения, которые ждали. Проверьте расширение вложения.

8. ***Никому никогда*** в переписке не сообщать коды подтверждения из SMS-сообщений.

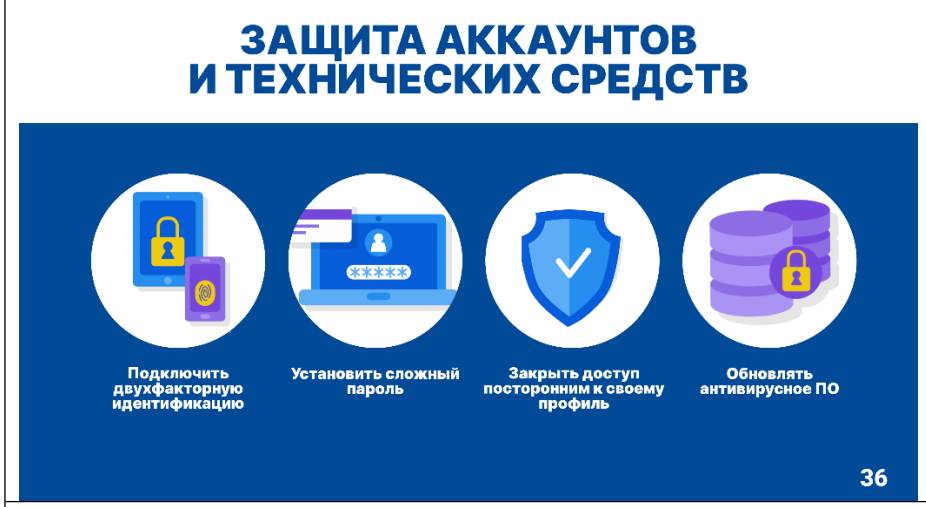
9. Если письмо или сообщение требует ввода данных (логина, пароля) на подозрительных сайтах или в анкетных формах, то необходимо удалить это письмо.

10. Нельзя фотографировать и отправлять свои личные данные и данные родителей, копии паспортов и других документов, банковских карточек и деньги незнакомым людям.

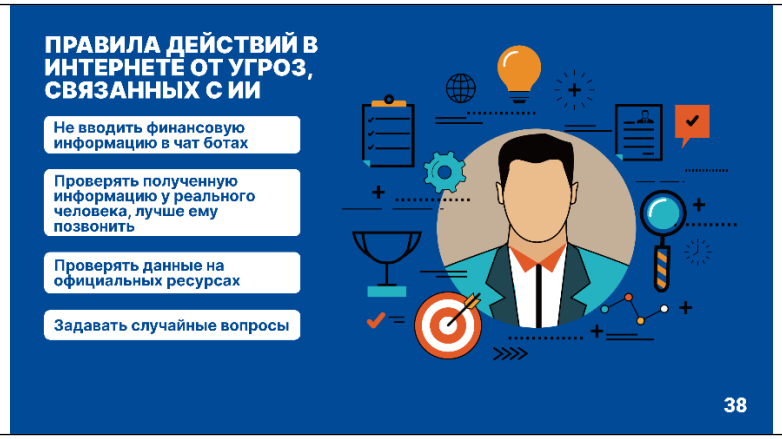
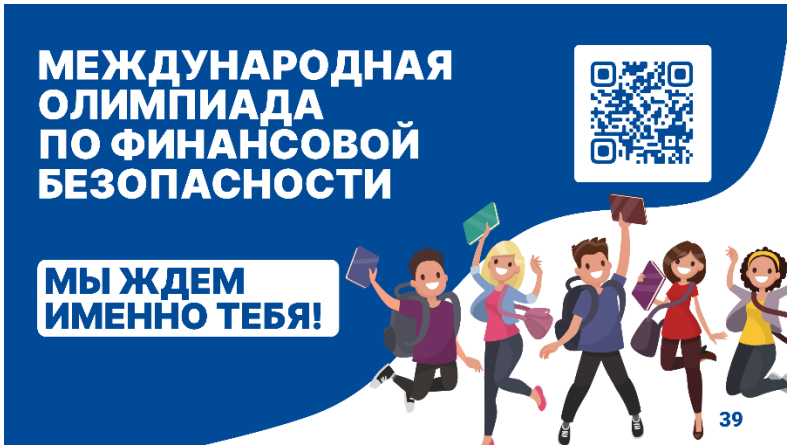
11. Нельзя ни с кем делиться информацией об адресе дома, школы, о месте работы родителей, какие приложения стоят у членов семьи на телефоне, любыми паролями и ПИН-кодами.

12. Лучше общаться только с друзьями и близкими, которые пишут со знакомых номеров и страниц. А если написал незнакомец и просится в друзья, а потом начал спрашивать информацию, перечисленную выше, то он точно не может быть твоим другом.

13. Необходимо лично проверять всю информацию, поступающую от друзей или родственников в соцсетях, мессенджерах. То есть, если друг или подруга вдруг попросила денег, чтобы оплатить посылку, лучше перезвонить и услышать просьбу в разговоре.

Слайд 36 **Защита аккаунтов и технических средств** • Двухфакторная идентификация • Сложный пароль • Закрыть доступ посторонним к своему профиль • Обновлять антивирусное ПО  	1. Нужно защитить свои аккаунты — необходимо везде, где это возможно, подключить двухфакторную идентификацию. 2. Пароли в соцсетях в честь любимых домашних питомцев и даты рождения, конечно, легко запомнить, но лучше выбрать что-то посложнее. Потому что мошенники их легко подберут. А если они где-то записаны, то нельзя фотографировать этот листок и отправлять снимок куда-то. 3. Следует обеспечить безопасность профиля в социальных сетях - следует закрыть доступ посторонним к личной информации на страницах соцсетей, сделав их приватными. 4. Важно использовать антивирусное программное обеспечение и регулярно обновлять его, чтобы защитить свой компьютер от вредоносных программ.
Слайд 37 **Правила действий при интернет-покупках** 1. Проверять интернет-магазин; 2. Не общаться с продавцом в мессенджерах вне торговой площадки; 3. Оплачивать покупки только через официальные магазины, платформы и т.д.; 4. Советоваться с родными и близкими.	1. Совершать покупки можно только по согласованию с родителями, в проверенных интернет-магазинах, нельзя переводить полную предоплату за товар, если не уверены в надежности продавца. 2. Опасно приобретать виртуальные деньги, улучшения для игр, а также платный игровой контент и другие бонусы. Это следует делать только на официальной платформе или игре, оплачивая через эту платформу.

	3. Признак мошенника - предложение перейти общаться в мессенджере, а не через официальные сайты магазинов или площадок (например, «Авито» или «Юлу»). 4. Необходимо проверять рейтинг и отзывы на продавца. Желательно совершать покупку вместе с родителями или оплачивать товары только через безопасную сделку на самом сайте бесплатных «Авито» или «Юлу».
Слайд 38 **Правила действий в интернете от угроз, связанных с ИИ** • Не вводить финансовую информацию в чат ботах • Проверять полученную информацию у реального человека, лучше ему позвонить • Проверять данные на официальных ресурсах • Задавать случайные вопросы	1. Если в ходе общения в мессенджере бот или робот предлагает ввести личную финансовую информацию (коды из смс от банка, полные данные карты, ФИО, паспортные данные и т. д.), необходимо прервать общение, обратиться в отделение банка либо самостоятельно связаться с организацией по официальным контактам, которые указаны на официальном сайте компании. 2. Если вы решили самостоятельно воспользоваться услугами нейросети, убедитесь, что действительно оказались на официальном ресурсе. Не переходите по сомнительным ссылкам, предлагающим ввести данные для оплаты, и не устанавливайте на свои устройства неизвестные приложения. 3. Если вы в разговоре почувствовали что-то неладное, лучше всего будет задать собеседнику случайный вопрос — это поможет понять, что вы общаетесь с живым человеком, а не с ботом. 4. Использовать нейросети для распознавания подделки

	
Слайд 39-40 	Ознакомление обучающихся с возможностью принять участие в Международной олимпиаде по финансовой безопасности.


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.
Участники: обучающиеся 8-10 классов / 1-3 курсы бакалавриата / 1-4 курсы специалитета / 1 курс магистратуры
40

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

Методические рекомендации по подготовке и проведению Всероссийского тематического урока на тему:

«НЕдетские игры: как не стать участником финансовых преступлений»

Москва, 2024

Оглавление

Аннотация

Методические рекомендации подготовлены в помощь педагогам образовательных организаций и ориентированы на оказание методической по организации и проведению тематического урока, посвященного противодействию вовлечения молодых людей школьного возраста 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 проведением данного мероприятия. Предлагаемые материалы носят рекомендательный характер, поэтому преподаватель может провести занятие, опираясь на данные разработки, исходя из собственного опыта, учитывая возрастные особенности, уровень подготовки обучающихся, а также традиции региона.

Пояснительная записка

Финансовое грамотность молодежи способствует принятию грамотных решений, минимизирует риски и тем самым способно повысить финансовую безопасность населения. Низкий уровень финансовой грамотности может привести не только к банкротству, но и к неграмотному планированию выхода на пенсию, уязвимости к финансовым мошенничествам, чрезмерным долгам и социальным проблемам, включая депрессию и прочие личные проблемы.

Согласно статистическим данным МВД России в настоящее время молодые люди (младше 18 лет) всё чаще становятся жертвами мошенников: пользуясь неопытностью и доверчивостью детей и подростков, злоумышленники крадут деньги с их карт и со счетов их родителей. Для обмана используются игры, призы и даже предложения о подработке. Вместе с развитием онлайн-услуг и цифровых сервисов мошенничество с похищением личных средств физических лиц стало одним из основных рисков во многих странах. При этом они затрагивают и детей – в России самой юной жертве финансовых мошенников всего 11 лет. Подобные угрозы отмечены не только в России и могут быть актуальны для стран СНГ.

По мнению психологов, виктимность – склонность стать жертвой преступлений – закладывается в детском возрасте. Задача урока – снизить эту самую виктимность, опираясь на знания о видах и формах финансового мошенничества и опыт противостояния манипуляциям преступником.

Поэтому важно объяснить молодым людям о подобных угрозах в реальной жизни, Интернете, социальных сетях и мессенджерах и научить самостоятельно определять мошенников по отличительным признакам.

Согласно опросу школьников, проведенному в рамках Зимней школы по финансовой безопасности 2024, организованной Центром межолимпиадной подготовки школьников и студентов в ноябре-декабре 2023 года, одной из наиболее интересующих тем (73% опрошенных из потенциальных участников Международной олимпиады по финансовой безопасности) является тема вовлечения молодых людей в финансовые преступления в качестве жертвы или соучастника. Более того, почти каждый второй школьник (47% опрошенных) уже сталкивался с подобной ситуацией (сам или слышал о негативном опыте от друзей). Также молодых людей интересовали вопросы возникновения последствий и степени ответственности за совершенные действия.

В связи с этим рассматриваемая в настоящем уроке тематика является очень актуальной.

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

Задачи данного урока:

- заложить у обучающихся установки грамотного финансового поведения;
- сформировать у обучающихся представление о признаках ситуаций финансового мошенничества, признаки фишинговых и других мошеннических сайтов.

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 операциях с ними;

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

Дать понимание того, что за все финансовые решения отвечает собственник средств (своими деньгами), даже если решения приняты под влиянием рекламы и под давлением мошенников.

Основные тезисы урока, которые будут рассмотрены:

1. Легкие деньги – тяжелые последствия: способы вовлечения молодежи в преступную деятельность.
   1.1. Дети – жертвы финансовых мошенников
   1.2. Дети – соучастники финансовых мошенников
2. Нейросеть как современный инструмент финансовых преступлений. Мошеннические схемы с помощью искусственного интеллекта.
3. Защищен – значит вооружён: как защититься от финансового мошенничества.

Раздел 1. Легкие деньги – тяжелые последствия: способы вовлечения молодежи в преступную деятельность.

1.1. Дети – жертвы финансовых мошенников

В жизни дети и молодежь становятся жертвами аферистов наравне со взрослыми. Количество дистанционных мошенничеств в отношении несовершеннолетних неуклонно растёт. Например, в 2023 году в Москве количество таких преступлений увеличилось на 29%, а среди обманутых жертв 10% – это подростки до 14 лет.[1]

Как правило, злоумышленники пытаются добраться до банковской карты родителей или самих детей. "Им удается безошибочно играть на качествах, присущих детям и подросткам, — доверчивости, неумении критически мыслить, легком отношении к деньгам, дефиците общения и жажде поощрения и признания"[2].

Форм и видов финансового мошенничества в отношении несовершеннолетних становится все больше и больше. С развитием информационных и коммуникационных технологий схемы мошенников становятся все более сложными. Но наша задача – научиться распознавать такие угрозы и противостоять им.

Приведем пример из реальной жизни применения схемы **телефонного мошенничества**: преступники убедили 12-летнюю девочку, что её бабушка попала под машину, и она передала незнакомцу наличные деньги на лечение.

21 ноября дома у Вики зазвонил домашний телефон — на том конце провода кто-то сильно плакал. Школьнице показалось, что голос принадлежит её бабушке. После Вике сразу же позвонили на мобильник, неизвестный сказал, что бабулю сбила машина — она получила серьёзные травмы, на лечение которых нужно 600 тысяч рублей. Вика пообещала помочь: по инструкции от звонившего она подготовила полотенце, бумагу, постельное бельё, взяла у отца 50 тысяч и упаковала их так, чтобы было не видно, что внутри.

Вскоре к ней домой пришёл неизвестный мужчина — он был в спортивных штанах и с тёмной бородой. Вика отдала ему деньги, надеясь, что бабуля скоро поправится. Позже о подвиге дочери узнал отец — мужчина сразу обо всём догадался и написал заявление в полицию.

Данный пример является очень частым примером обмана мошенниками детей и подростков. Далее мы более подробно рассмотрим, как эта схема реализуется в жизни.

Рассмотрим следующий пример **использования фейковой учётной записи в социальной сети**.

«В начале октября 14-летней девочке в социальной сети пришло сообщение якобы от знакомого. Он утверждал, что счета и деньги родителей школьницы в опасности. Все из-за того, что в интернете есть их персональные данные, которыми могут воспользоваться мошенники.

«Приятель» сразу же предложил решение проблемы. Он рассказал девочке, как спасти семейные сбережения. Школьница последовала совету. Взяла банковские карты родителей, которые лежали на пуфике в прихожей, сфотографировала их со всех сторон и отправила снимки знакомому.

В итоге со счетов взрослых пропали 280 тысяч рублей. Потерпевшие обратились в полицию. Установлено, что страницу знакомого девочки взломали, и от его лица с ней общались аферисты».

В данном случае мы видим, что мошенники использовали схему создания фейковой учётной записи, не имеющей отношение к пользователю и вели переписки от имени другого лица.

---

[1] В Москве аферисты стали чаще похищать деньги у детей // РИА НОВОСТИ. 18.12.2023. URL: https://1prime.ru/finance/20231218/842595387.html

[2] Россиян предупредили, что новая цель мошенников — дети // Прайм. Агентство Экономической информации. 24.11.2023. URL: https://1prime.ru/exclusive/20231124/842355112.html

К сожалению, приведенные примеры – это далеко не единственные формы мошенничества, с которыми сталкиваются взрослые, дети и подростки. Самым уязвимым звеном этой цепочки все же остается **человек, его реакции и эмоции**. «Взломай» человека - взломаешь все остальное. Именно этим и пользуются мошенники.

У мошенника есть две цели – обмануть и украсть. Это азартный человек, игрок. Угрызений совести от своих действий он не чувствует и надеяться, что он одумается или остановится, наивно.

Более того, поведение мошенника и жертвы в какой-то мере схожи.[3]

Для мошенника его действия – это всегда азарт, желание получить адреналин, со временем преступление становится его любимым делом. Портрет мошенника выглядит так: это умный, артистичный, разговорчивый, увлеченный человек, лицедей, который располагает к себе, он постоянно разрабатывает новые варианты обмана.

Психология жертвы – это тоже особенности личности, которые позволяют ей попасться на уловку мошенника, плюс особая социальная программа поведения. Например, кто-то хочет спасать мир и тут получает СМС о том, что родственник в опасности; кто-то боится сотрудников полиции, и ему звонят, представляясь полицейским.

В данном случае, мошенники пользуются методами Социальной инженерии.

Социальная инженерия – это:

...психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации

Социальная инженерия – зло.

Социальная инженерия лежит в основе всех методов и видов кибермошенничества и телефонного мошенничества:

1 Обман или злоупотребление доверием;
2 Психологическое давление;
3 Манипулирование.

Под влиянием социальной инженерии жертва добровольно расстается с деньгами или раскрывает личные и финансовые данные, которые нужны злоумышленникам для кражи средств

<u>Как работает этот метод:</u>

1. Злоумышленники используют чувства и эмоции

- Невнимательность
- Жадность
- СТРАХ
- Доверие
- Сочувствие

2. Злоумышленники используют новостную повестку.

Злоумышленники всегда эксплуатируют наиболее «горячие» темы:

- Мобилизация
- Специальная военная операция
- COVID-19
- Выборы
- Игровые и спортивные чемпионаты

Эмоции, которые вызывает информация от мошенников бывают двух видов:

1) отрицательные

- страх паника

---

[3] Федяшева Е. Как не стать жертвой кибермошенников: новые схемы обмана, портрет аферист и правила безопасности от воронежских экспертов. 24.11.2023. URL: https://www.vrn.kp.ru/daily/27586.5/4856275/

- чувство стыда

«С вашего счета списали все деньги»

«Ваш родственник попал в аварию и сбил человека»

«Вас беспокоит следователь Следственного комитета, ваша мама - участник уголовного дела о... коррупции или...»

2) положительные

- радость надежда
- желание получить деньги

«Вы выиграли крупную сумму денег»

«Вам положены бонусы в игре».

ФОРМУЛА УСПЕХА МОШЕННИКОВ

1 этап – мошенники воздействуют на базовые эмоции (страх, радость, печаль, удивление, любопытство, злость). Эти чувства выходят на первый план в любой стрессовой ситуации как защитный механизм человека, когда мы неожиданно слышим какую-то новость.

2 этап – после активизации основных эмоций мошенники применяют определенные **психологические техники**[4], особенно успешно применяемые в устных и телефонных разговорах:

- Комплекс коротких вопросов, отработанный мошенниками сотни раз. Быстро отвечая на них, не перебивая мошенника, человек входит в состояние, близкое к трансу или гипнозу.
- Определенный тон голоса: официальный, либо вкрадчивый и доверительный, либо радостный и восторженный. Это усиливает эмоциональную реакцию жертвы.
- Поторапливание и ускорение событий, при котором жертва временно теряет способность к логике и анализу и выполняет инструкции мошенников.
- Угрозы, запугивание, ложные данные.
- Если человек попал в круговорот обмана, ему могут внушить, что вокруг все враги, никому не нужно верить и делиться, что же с вами происходит. Поэтому так сложно разубедить жертву, и она ничего не говорит своим близким и окружающим.

Мы уже рассмотрели несколько реальных примеров действий мошенников. Давайте рассмотрим более подробно формы мошенничества, в которые могут попадать несовершеннолетние.

1. **Телефонное и мобильное мошенничество**[5]

Происходит звонок / смс потенциальной жертве

«У меня зазвонил телефон. Кто говорит?..»

И далее на другой стороне трубки можно услышать разные варианты:

- *Служба безопасности*
- *Сотрудник банка*
- *Сотрудник Центрального банка*

---

[4] Халезова Н. «Я была одурманена»: реальные истории жертв мошенников. Как их распознать и можно ли помочь? // LifeProfit, 15.08.2023. - URL: https://life.akbars.ru/personal-finance/istorii/ya-byla-odurmanena-realnye-istorii-zhertv-moshennikov-kak-ikh-raspoznat-i-mozhno-li-pomoch/

[5] Кибербезопаность_как_не_стать_жертвой_в_финансовом_мире. SBER Cyber Security.

- *Майор ФСБ*
- *Капитан полиции*
- *Старший следователь Следственного комитета*
- *Дочка, это я….*
- *Это Вася, папин друг….*

Если мошенник представляется сотрудником службы безопасности банка, то обычно говорит следующее:
«Ваша карта (счет) заблокирована»
«С вашей карты пытаются перевести деньги»
«К вашим счетам (счетам вашего отца) получили доступ злоумышленники и деньги нужно перевести на защищенный банковский счет...»
«По вашей карте выявлены подозрительные операции...»
«На ваше имя пытаются взять кредит...»

Когда звонит «лейтенант полиции», сотрудник МВД/СК/ФСБ могут быть произнесены такие фразы:
«Ваш родственник сбил человека…»
«По вашим поддельным документам кто-то пытается взять кредит на крупную сумму... Нам необходимо уточнить ее реквизиты….»
«Вы стали свидетелем по уголовному делу на вашего одноклассника…»

В таких схемах, злоумышленники предлагают решить проблему следующим способом и предлагают это своей жертве:

- Вывести все деньги с банковских карт жертвы или ее родителей и перевести их на «безопасный» счет или на специальный счет в банке или в Центральном банке.
- Исчерпать лимит кредитов по карте и перевести их на «безопасный» счет.

Лжесотрудники банков или правоохранительных органов, органов государственной власти присылают своим жертвам фальшивые документы, сделанные через онлайн редакторы документов. Общение происходит в мессенджерах и в социальных сетях. На аватаре зачастую стоит значок банка или органа государственной власти (например, МВД). Часто в схеме участвует не один человек, и после звонка одного сотрудника происходит звонок другого сотрудника из другого ведомства, отдела и с другого номера.

Если мошенник представляется родственником / другом / сыном знакомых, то обычно говорит:
«Наша бабушка попала в аварию, ей срочно нужны лекарства...»
«Я сбил на машине ребенка, но уже договорился о взятке, срочно нужны деньги».
«Ваш отец только что в результате ДТП сбил человека. Я готов помочь избежать наказания»

В таких схемах часто мошенник сообщает, что родственник попал в больницу или аварию. Все это говорится быстро и с максимально достоверной актерской игрой, чтобы ввести потенциальную жертву в стресс и не дать мыслить рационально.

Затем «чужой голос» просит собрать все деньги в доме, какие-либо предметы и сложить их в пакет. Злоумышленники отправляют курьера по адресу жертвы, чтобы забрать деньги. «Посылку» забирает специальный курьер. После чего и деньги и мошенники исчезают. Часто в схеме участвует не один человек.

Таким же образом мошенники выманивают данные родительских карт без участия курьеров и наличных денег. Пример*:*

«21 ноября у 15-летнего школьника Пети зазвонил мобильный телефон. На том конце провода мошенник представился стримером. Он сообщил, что случайно выбрал Петю для участия в онлайн-стриме, он готов оплатить ему билет в другой город для участия в стриме, но для этого, ему потребуются фотографии паспорта Пети и фотография его банковской карты или карты его родителей».

Признаками того, что позвонил или написал мошенник могут быть следующие:

- Звонок поздно вечером, ночью или рано утром в выходные.
- От вас требуют немедленных действий.
- Торопят и запугивают, давят на эмоции.
- Требуют сообщить конфиденциальную информацию: данные карты, ПИН-код или одноразовый пароль из СМС.
- При отказе называть данные угрожают, что деньги с вашей карты прямо сейчас уйдут к мошенникам.

2. Кибермошенничество

Постепенная информатизация мира привела к появлению нового вида злодеев – кибермошенников.

За время пандемии ковида многие сферы жизни перешли в онлайн, и киберпреступники (**скамеры**, **черные шляпы**[6], мошенники) также активизировали свою деятельность в интернете.

Исследователи определяют киберпреступность как любое противозаконное деяние, нарушающее права и свободы человека с помощью компьютерных систем и сетей.

Кибермошенничество - один из видов киберпреступлений.

Целью *кибермошенничества* является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.). Оно реализуется в разных формах, о которых мы поговорим далее.

Существует множество форм кибермошенничества, жертвами которых становятся несовершеннолетние. Рассмотрим несколько из них.

2.1. Фишинг

...вид мошенничества, при котором злоумышленники рассылают письма и пытаются обманом заставить получателей совершить какое-то действие:

- перейти по вредоносной ссылке
- загрузить зараженное вложение
- сообщить персональные данные и иную конфиденциальную информацию

С английского «phishing» - созвучно с «fishing» (рыбалка).

Фишинг зачастую лежит в основе большинства финансовых киберпреступлений.
Пример реализации схемы фишинга:

Фишинговое письмо – письмо, которое содержит вредоносное вложение, ссылку на мошеннический сайт или вредоносное программное обеспечение.

Вирусные вредоносные программы нарушают работу системы на телефоне или компьютере, собирают данные, копируют или уничтожают файлы.

Эти письма могут выглядеть как сообщения из вполне респектабельных источников: интернет-магазинов, банков, сервисов и пр.

Какие уловки используют мошенники в таких письмах:

- Службы доставки
- Маркетплейсы
- Криптовалюта
- Горячие новости

---

[6] Хакеры Черные шляпы, Белые шляпы и Серые шляпы – определение и описание. URL: https://www.kaspersky.ru/resource-center/definitions/hacker-hat-types

- Лотереи
- Дополнительный заработок и инвестиции
- Туроператоры и отдых
- Билеты на мероприятия
- Подписки и онлайн-сервисы

Итоговая цель мошенников чаще всего состоит в получении доступа к финансам обманутых пользователей.

Тем не менее преступникам интересны логины-пароли, которые могут использоваться для входа на разные сервисы, а также информация, содержащаяся в ноутбуках и компьютерах. Завладеть ею им помогают ***ссылки-ловушки***. Их направляют подросткам с предложением посмотреть интересные фотографии "с вечеринки или концерта", и при переходе по ссылке или при открытии файла, на компьютер или телефон устанавливается вредоносное программное обеспечение.

Другим детям мошенники предлагают зарегистрироваться на специальных сайтах, чтобы участвовать в голосованиях, после чего телефон ребенка заражается вредоносными программами, и у мошенников появляется доступ к личной информации.

Поддельные сайты или приложения

Мошенники могут создавать фишинговые сайты, предлагающие товары и услуги, например, компьютерную технику, по более низким ценам. Существует много мошеннических сайтов, которые занимаются перепродажей внутриигровой валюты, графических оформлений (скинов) или предметов для компьютерных и телефонных игр.

После выбора товара или услуги и формы оплаты пользователя просят ввести реквизиты своей банковской карты (номер карты, CVV-код). После согласия осуществить оплату происходит передача реквизитов кредитной карты злоумышленникам, о чем пользователь даже и не догадывается.

Метод кибермошенничества в различных областях бизнеса с целью присвоения денежных средств называется **фрод**[7].

Кроме этого, мошенники создают поддельные сайты банков, чтобы узнавать данные клиентов от их личного кабинета. Обычно в таких интернет-ресурсах в доменное имя отличается от настоящего.

Фишинговые игровые ресурсы также создаются для ***кражи аккаунтов*** у геймеров и последующего вымогательства денег в обмен на возвращение доступа.[8]

В 2022 г. рунете появились 183 домена с именами, связанными с онлайн-игрой Warface.По всем ссылкам на ресурсы открывается сайт с одинаковым оформлением. На странице изображены четыре класса бойцов из Warface с премиальной амуницией, а также текст с призывом получить дорогие предметы в подарок. При нажатии кнопки «Войти и забрать» открывается окно авторизации, где нужно ввести логин и пароль от аккаунта в игре. Украв аккаунт от игры, злоумышленник оценивает персонажа и амуницию и обращается к жертве с предложением выкупа. Сумма, которую просят мошенники у игроков Warface, варьируется в районе от 100 до 4 тыс. руб.

Мошенническая схема следующая: человек думает, что участвует в акции от разработчиков, вводит на фейковом сайте свои логин и пароль и теряет доступ к аккаунту, так как логин и пароль попадают в руки злоумышленников.

Еще одна волна мошенничества – это появление ресурсов, которые предлагают пострадавшим от интернет-преступников пользователям получить компенсацию за участие

---

[7] «Назовите пароль от своей карты»: как защитить себя и ребёнка от кибермошенников? / Е. Полякова // Где мои дети. URL: https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov

[8] От фишинга до вирусов: как мошенники обкрадывают российских геймеров // Газета.ru. 06/07/2022. URL: https://www.gazeta.ru/tech/2022/07/06/15079700.shtml

в популярных фейковых опросах, «недобросовестных» лотереях или компенсацию налогов, но вместо этого списывают деньги и похищают данные банковских карт[9].

Эта схема называется «**Двойной обман»**. Её авторы применят так называемый «синдром обманутого вкладчика», когда обманутые жертвы отдают свои деньги, чтобы им помогли вернуть потерянные средства.

2.2. Киберугрозы в играх, социальных сетях и мессенджерах

В последнее время мошенничество с использованием мессенджеров и социальных сетей все больше набирает обороты.

Оно реализуется в различных формах, наиболее распространённые примеры которых мы рассмотрим далее.

- Мошенничество в социальных сетях и мессенджерах, в том числе,
- Голосования
- Взлом аккаунтов
- Цифровое клонирование
- Быстрый заработок
- Онлайн-пирамиды
- Инфоцыгане

Мошенничество в **социальных сетях и мессенджерах** зачастую схоже с телефонным мошенничеством, но сначала может происходить переписка, а далее схема обмана может реализовываться различными способами – по телефону, через фишинг и т.д. Самая популярная цель такого мошенничества – это махинация с банковскими картами, то есть получение данных карточки.

Один из способов обмана: приходит сообщение от имени популярного блогера о подарке или о потенциальном бонусе, для получения которого необходимо прислать реквизиты карты, на которую и поступит «заветный выигрыш». В таком состоянии дети и подростки отправляются данные своих карт или карт родителей, а также пароли или личные данные. Далее мошенник крадет все средства со счета карточки.

В полицию обратилась женщина, которая рассказала, что к ее сыну в социальной сети Telegram, представившись блогером, обратился неизвестный. Он сообщил, что мальчик выиграл в конкурсе, и для получения награды ему необходимо взять телефон мамы и сделать скриншот экрана. Он был нужен мошенникам для того, чтобы посмотреть, какие приложения установлены на телефоне, и выяснить, приложением какого банка пользуется мама мальчика. Таким образом мошенники поняли, какое приложение для удаленного доступа можно установить. Дальше ребенок действовал по указаниям аферистов, однако не помнит, что именно делал. На следующий день после общения с «блогером» переписка автоматически удалилась, а со счета мамы мальчика исчезли 235 тысяч рублей.

Зачастую кибермошенничество связано с различными играми.

Мошенники придумали аферу на основе популярной мобильной игры. Они создали телеграм-канал для любителей онлайн-шутера и предлагали делать ставки с обещанием заработать на турнирах по этой игре. 14-летний подросток сделал очень крупные ставки и перевел 100 тыс. рублей со счета своей мамы на Qiwi-кошелек и номера телефонов. В итоге никаких ни денег он не получил.

Какая схема мошенничества здесь применена: общение переходит в мессенджер, что является первым подозрительным признаком. Игрока просят делать ставки с реальными деньгами, что также является подозрительным признаком. Используется официальная

[9] Как защититься от кибермошенников — шесть основных схем обмана // РБК. URL: https://trends.rbc.ru/trends/industry/6027ef6c9a7947206e6aec96?from=copy у

оплата не через игровой аккаунт, а через сторонние кошельки и приложения, оплата в пользу частных лиц, что является подтверждающим признаком мошеннической операции.

В последнее время отдельной популярностью пользуются онлайн (мультиплеерные) игры, в которых за деньги можно повышать уровень игрока, покупать дополнительные возможности и переходить на более высокий игровой уровень. Игрокам приходится вводить данные банковских карт для оплаты этих улучшений или покупки внутриигровой валюты, и эти данные хранятся в персональном игровом аккаунте.

Мошенники ловят игрока в игре, предлагая внутриигровую валюту, графические оформления (скины) или предметы. ***Общение переходит в мессенджер.*** А дальше игрока просят дать логин и пароль от аккаунта, предлагая «выгодную сделку», от которой трудно отказаться.

То есть за персональные данные обещается солидный бонус в виде крупной суммы, золото по промокоду либо редкие скины. Дети и подростки не сразу могут понять, что оказались в сетях мошенников, однако результат остается один – мошенники крадут все деньги и персональные данные.

Точно такая же схема мошенничества используется с покупкой улучшений для игр, внутриигровой валюты и пр., различных товаров и услуг через сайты бесплатных объявлений или сайты частных объявлений, например, Авито, Юла.

«Подросток потерял деньги из-за обмана мошенников в канун новогодних праздников, когда пытался купить подарок на сайте бесплатных объявлений «Авито». Продавец наушников предложил общаться в ватсапе. Написал, что нужно оплатить товар, доставку. Подросток все перечислил, а продавец перестал выходить на связь».

В данном случае, сайты, на которых вывешены объявления – известные и авторитетные (Авито, Юла, Плати), однако сами объявления размещаются мошенниками. С ними ведется переписка, оплачивается товар или услуга, но взамен, в лучшем случае, покупатель ничего не получает, а в худшем случае – дает доступ мошенникам к банковским картам и к персональным данным.

Обман при знакомствах в Интернете – это еще одна сторона кибермошенничества. Главной целью мошенников, орудующих по такой схеме, является скорейшее получение персональных данных потенциальной жертвы и доступа к ее счетам.

Мошенническая ловушка со знакомствами рассчитана на молодых людей и девушек. Парень знакомится с девушкой онлайн, она предлагает провести время и назначает первое свидание в конкретном месте - в театре, на концерте. Она присылает ссылку на покупку билетов, сайт фейковый (поддельный). Жертва теряет все деньги с карты.

Приведем еще пример.

«Молодой человек познакомился в соцсетях с девушкой и общался с ней две недели. Периодически она просила купить просила оплатить ей всякие недорогие «плюшки», чтобы они встретились – положить деньги на телефон, купить комикс, оплатить маникюр и тд. И вот она пишет: «Я забронировала нам билеты в кино, сейчас тебе придет смс-ка с кодом для оплаты, можешь, пожалуйста, ее продиктовать, чтобы эти билеты оплатить».

Парень продиктовал ей коды из смс. После этого с карточки списались все деньги, а девушка перестала отвечать на сообщения и звонки и удалила свой аккаунт»

Подозрение на мошенничество в таких случаях должно возникнуть, когда появляются странные предложения. В первую очередь финансового характера.

Мошенничество в социальных сетях и мессенджерах, в том числе связно с тем, что мошенники взламывают чужие аккаунты, создают цифровых двойников каких-то знакомых

лиц или других людей. Это так называемая схема ***захвата учётной записи мессенджера или социальной сети***.[10]

Нередко дети и подростки становятся объектами обмана от имени своих «друзей / знакомых», просящих в долг на пару дней или оказавшихся в «трудной жизненной ситуации».

Мошенники с фейковых (поддельных) аккаунтов, иногда подделывая страницы взрослых людей, знакомых ребенку, входят к нему в доверие, налаживают контакт. Пока идет общение, злоумышленники пытаются узнать у детей и подростков всевозможные подробности жизни семьи: где работают родители, когда бывают дома, с кем общаются, что покупают, куда ездят, как зовут членов семьи, какие машины у мамы и папы. Действуют не в лоб, вопросы задают аккуратно, издалека. Всю эту информацию мошенники могут незаметно выудить у ребенка, общаясь с ним в соцсетях.

Потом они умело используют эту информацию. Зная имена и детали чужой семейной жизни, звонят родителям детей и подростков, их родственникам, оперируя информацией, которая вызывает доверие у потенциальных жертв и притупляет их бдительность. Далее мошенник всеми возможными способами пытается завладеть денежными средствами жертвы.

В данном случае, получив от ребенка информацию, мошенник позвонит какой-нибудь бабушке и сообщит не просто, что «ваша дочь попала в аварию», а он называет эту дочь по имени, знает марку автомобиля, имена ее друзей и родственников, место работы.

Кроме этого, может прийти сообщение от друга, знакомого с различными просьбами: проголосовать, поставить лайк, дать денег в долг, купить билет и прочее.

«Проголосуй за меня пожалуйста, если не сложно конечно) https://goo.su/CTcZ34nN»

Ссылка, отправляемая злоумышленниками, сделана при помощи сервиса для сокращения ссылок. Этот инструмент часто применяется, когда отправитель не хочет, чтобы реальный адрес сайта бросался в глаза.

На сайте злоумышленника, указав номер телефона, вы тут же получите код подтверждения, с помощью которого у вас угонят учётную запись. В данном случае мы квалифицировать данную схему как фишинг.

Схема мошенничеств с быстрыми заработками

В Интернете или мессенджерах постоянно предлагают дополнительный заработок или вложение денег в якобы выгодные проекты. Набирает популярность и схема с легким заработком, например, за просмотры видеороликов популярных блогеров, оценку картинок и отелей, голосование в рейтингах.

Перед началом "работы" мошенник отправляет ссылку и просит ввести банковские данные карты (своей или родителя), а также код из СМС-уведомления, объяснив, что по этим реквизитам в дальнейшем будет оплачивать услугу или необходимо предварительно заплатить налог. После ввода СМС все средства со счета списываются.

Более взрослым подросткам преступники рекламируют быстрые заработки с помощью букмекерских ставок[11].

Злоумышленники устанавливают с подростком контакт и предлагают ему быстро заработать, делая букмекерские ставки на своих ресурсах. Системы визуально показывают якобы успешность такой деятельности ребенка. Для вывода якобы заработка подростков

---

[10] Памятка УБК МВД России: актуальные способы совершения мошеннических действий. URL: https://78.мвд.рф/citizens/ваша/security/item/45404472

[11] Мошенники стали красть у россиян деньги с помощью их детей // Правмир. 23.10.2023. URL: https://www.pravmir.ru/moshenniki-stali-krast-u-rossiyan-dengi-s-pomoshhyu-ih-detej/

просят оплатить комиссию. В итоге деньги вместе с данными карты оказываются в руках киберпреступников.

Кроме этого, по данным Банка России увеличилось число финансовых пирамид, маскирующихся под экономические или бизнес онлайн-игры. [12]

Более 22% таких проектов привлекало к себе пользователей возможностью быстрого и легкого заработка внутри игры - в формате «заплати и выиграй».

Особенностью таких проектов является *отсутствие соревновательного элемента. Ты платишь – ты выигрываешь.*

Большинство таких пирамид — это небольшие анонимные проекты с коротким сроком длительности и незначительной суммой участия.

Их организаторы таргетируют предложения с учетом возраста и предпочтений потенциальных участников, а для продвижения используют соцсети и мессенджеры.

Механика подобных игр заключается в следующем. На первом этапе пользователям предлагают зарегистрироваться, затем — приобрести персонажа или некие игровые атрибуты, которые в дальнейшем должны приносить «доход». Это могут быть веселые гномы, добывающие руду, птицы, несущие золотые яйца, или рыбаки, которые ловят рыбу. После «добычи» ресурс конвертируется в игровое золото, которое в теории затем можно обменивать на реальные деньги. Подвох в том, что вывести деньги на карту, несмотря на обещания организаторов, просто так не выйдет. Так как основная цель всех финансовых пирамид в привлечении как можно большего числа новых игроков, перед выводом вас попросят «привести» в игру определенное количество рефералов. Для этого создатели советуют распространять информацию о проекте в социальных сетях, мессенджерах и личных блогах. Вложенные средства оседают в карманах организаторов, а игроки, в лучшем случае, возвращают себе малую часть вложений, а в худшем — остаются ни с чем.[13]

Основные признаки финансовой пирамиды:

- Отсутствие геймплея - отсутствие соревновательного элемента, рутинные и повторяющиеся действия. Чем проще механика, тем больше вероятность мошеннической схемы.
- Выплата средств за привлечение новых участников. Если требуется привлекать новых игроков, это признак мошеннической схемы.
- Сложная схема начисления дохода: если получение дохода очень сложная, требуется множество действий, есть какая-то формула начисления дохода, скорее всего, цель этого – запутать игрока.
- Гарантия высокого дохода без всякого риска и агрессивная реклама в соцсетях. Если реклама игры очень агрессивная, обещания заработка без риска, то, скорее всего, это мошенническая схема.

Реклама объявлений быстрого заработка, как правило, обещает высокий доход при минимальной трате времени и минимуме рисков. В первом случае мошенники убеждают людей оплатить текущие расходы (например, составление анкет, налоги) или попросить оплатить услуги, во втором – просят людей, показывая вымышленные графики прибыли, перевести как можно больше денег для выгодного инвестировании. Всегда помните о том, что любые инвестиции могут обернуться убытками.

---

[12] Центробанк зафиксировал рост финансовых пирамид под видом онлайн-игр // РБК, 24.07.2023. URL: https://www.rbc.ru/rbcfreenews/64be1dbf9a794745f0991516?from=copy

[13] Финансовые пирамиды в России маскируются под онлайн-игры: как распознать мошенников // Mail.ru. URL: https://hi-tech.mail.ru/review/101527-finansovye-piramidy-pod-vidom-onlajn-igr/

Все проекты с признаками нелегальной деятельности Банк России вносит в специальный черный список[14]. Перед вложением денег обязательно надо проверить ресурс в реестре, и не вкладывать в него, если он есть в данном списке.

Схема мошенничеств с криптовалютами и ICO

Одним из самых популярных видов мошенничества в последние годы стали махинации с криптовалютами, в частности, со сбором средств на запуск различных проектов в сфере блокчейн, а также краудфандинд (коллективный сбор средств) на различные новые проекты (будь то создание новой игры, перевод книги и прочее). Люди вкладывают средства, а результатов нет, вложенные деньги исчезают. Такие мошеннические проекты называются **скам-проектами (скамом).**

Пример реализации такой схемы.

Злоумышленники презентуют на специальных сайтах якобы хороший проект, на реализацию которого требовались средства. Для этого используется так называемое поддельное ICO (Initial Coin Offering - первичное размещение ***токенов*** (монет)). Это формат сбора средств на развитие проектов в сфере криптовалют. Прикрываясь этим инструментом, мошенники продают фальшивую криптовалюту за биткоин или эфириум, которые имеют реальную стоимость (чтобы их купить, надо заплатить реальные (фиатные) деньги).

После нескольких раундов сбора средств «новаторы» (мошенники) пропадали без вести вместе с собранными средствами. При этом отследить их было практически невозможно, т.к. всеми собранными средствами можно распоряжаться анонимно.

Вторая схема мошенников с криптовалютами – это **Rug n Pull (раг пулл, дернуть коврик)** [15]. Смысл схемы заключается в выпуске токенов, большую часть которых оставляют себе мошенники, и лишь небольшая часть монет распределяется среди «инвесторов».

Важная характеристика возможного «вытягивания коврика» – монета, стремительно дорожающая в течение нескольких часов. После пампа (искусственного взлета) курса токена мошенники распродают все свои монеты и выводят средства, а обычные пользователи остаются с ненужными им токенами, которые обесцениваются почти на 100%. Такой токен невозможно продать (он становится неликвидным).

В 2023 году мошенники украли по такой схеме свыше $32 млн у приблизительно 42 000 пользователей[16].

Третья схема мошенников с криптовалютами - **Pump and dump (Накачка и сброс)**[17] – вид скама, при котором создается ложный ажиотаж, хайп вокруг монеты. Мошенники создают или покупают по низкой и выгодной для них цене токены (обычно сомнительные). Далее с помощью различных чатов, новостных постов, создается мнимый ажиотаж. Используются шумиха и дезинформация для создания ложного интереса к монетам, не имеющим известной и непосредственной ценности.

Люди, не умеющие проводить грамотный анализ криптовалют, начинают закупаться монетами. Приходит волна таких покупок и стоимость токена начинает сильно расти. Когда цена достигает своего пика, а дезинформация вызывает покупательский ажиотаж, мошенники и влиятельные инвесторы «сбрасывают» все свои криптовалюты, обналичивая

---

[14] Список компаний с выявленными признаками нелегальной деятельности на финансовом рынке // Банк России. URL: https://cbr.ru/inside/warning-list/

[15] Что такое скам в криптовалюте // Banki.ru. URL: https://www.banki.ru/news/daytheme/?id=10979400

[16] Эксперты выявили автоматизированную скам-схему на $32 млн. URL: https://forklog.com/news/eksperty-vyyavili-avtomatizirovannuyu-skam-shemu-na-32-mln

[17] Как вас могут скамнуть в щитках? Все виды скама в DEFI в одной статье. URL: https://vc.ru/u/2548531-nikita-slimkobag/927300-kak-vas-mogut-skamnut-v-shchitkah-vse-vidy-skama-v-defi-v-odnoy-state

их с огромной прибылью. В результате распродажи, цена монеты опустится значительно ниже первоначальной, и их невозможно будет продать[18].

Поэтому перед началом вложения реальных средств в различные проекты для начала надо изучить рынок криптовалют и создателей проекта более детально. Не следует покупать токены, которые не понимаете.

Специалисты компании ReasonLabs обратили внимание на то, что в браузер Chrome начали массово устанавливать ***несколько вредоносных расширений, маскировавшихся под VPN***. На фоне санкций против России спрос на VPN, позволяющий обходить блокировки, значительно вырос, подобные расширения установлены во многих браузерах. Однако в данном случае речь идёт о вредоносных программах.

Источником заражения стали установщики пиратских игр (Grand Theft Auto, Assassin's Creed и The Sims 4), загруженных с торрент-трекеров. Поддельный VPN человек получал вместе с игрой.

Установленное на компьютер расширение получало обширные полномочия. Например, могло запускать другие вредоносные скрипты, похищать конфиденциальные данные, изменять веб-запросы, отключать расширения, установленные в браузере.

[18] Как уберечься от мошенничества при “накачке” и “сбросе” криптовалют URL: https://bit.team/blog/ru/kak-uberechsya-ot-moshennichestva-pri-nakachke-i-sbrose-kriptovalyut/

1.2. Дети – соучастники финансовых мошенников

Вместе с тем, не всегда дети и подростки становятся лишь жертвами финансовых мошенников, так как злоумышленники вовлекают их в свою преступную деятельность.

Подростки и молодежь часто ищут подработку в интернете. Этим пользуются мошенники, заманивая несовершеннолетних в свои преступные сети. Опасными схемами заработка можно назвать те, когда подросткам предлагают за процент или вознаграждение быть посредниками или курьерами при передаче денег, заработанных нелегальным путем.

Схемы вовлечения несовершеннолетних бывают разные.

Например, звонят подростку и просят **оказать услуги курьера**: лично забрать деньги у одного человека и перевести их на банковский счет другого, оставив себе часть за сделанную работу.

Как правило, инициируется такая преступная деятельность из-за рубежа с использованием телефонных звонков, мессенджеров, компьютерных программ. В мессенджере подростки получают от мошенников четкие инструкции, как себя вести с людьми, у которых они забирают деньги и как переводить средства.

Перед этим мошенники обманным путем вымогают денежные средства у граждан, рассказывая истории о необходимости помочь близкому родственнику, попавшему в беду. Граждане передают деньги несовершеннолетним курьерам. Те за вознаграждение перечисляют оставшуюся сумму на банковскую карту злоумышленников, становясь **пособниками в совершении преступления**.

«Курьер собрал у трех пожилых женщин больше миллиона рублей. Им оказался 16-летний молодой человек. Он признался, что хотел быстро заработать деньги на карманные расходы. По данному факту было возбуждено уголовное дело по статье 159 УК РФ («Мошенничество в крупном размере»).

Участие в подобных схемах может грозить уголовной ответственностью, а наказанием будут не только штрафы и обязанность вернуть деньги, но реальное лишение свободы.

Еще один вид мошенников из числа несовершеннолетних представляют те, кто звонит и, ***представляясь*** попавшими в беду (к примеру, в аварию) ***сыном, дочерью или внуком***, выманивают деньги на "решение" проблемы. Затем к разговору подключается якобы сотрудник полиции и, не давая опомниться, говорит, что деньги нужно срочно передать через курьера. Застигнутые врасплох пожилые люди нередко попадаются на этот крючок. Курьером также может являться несовершеннолетний (в том числе тот, которые звонил под видом другого человека), которых находят в интернете. При этом аферисты, нанявшие несовершеннолетних, самую грязную работу - забрать деньги - поручают специальным курьерам.

«17-летний подросток - оказался в поле зрения оперативников после того, как в полицию обратилась 81-летняя пенсионерка, у которой он забрал 100 тысяч рублей. Бабушка думала, что помогает внучке, которая якобы попала в ДТП и по телефону попросила деньги. Чтобы на молодую женщину не завели дело, пенсионерка не пожалела все свои сбережения, но позвонить родным додумалась только после ухода курьера.

Когда полиция задержала юношу, он рассказал, что в поисках подработки оставил заявку в группе с вакансиями в соцсетях. Вскоре ему предложили работу в инвестиционной компании: забирать деньги у клиентов и пересылать их через банкомат на определенные счета. Юноша согласился, отправил "работодателю" свои паспортные данные и стал курьером.

Следователи выяснили, что несовершеннолетний участвовал еще в нескольких аналогичных преступлениях на в регионе своего проживания. Также он предложил подзаработать своему знакомому сверстнику. Они вместе отправились на "дело" в соседний город. И пока один следил за обстановкой на улице, второй забрал более 700

тысяч рублей у 12-летней девочки, поверившей, что ее мама попала в аварию и нуждается в дорогостоящем лечении. Такая крупная сумма находилась в этот момент дома, и ребенок об этом знал.»

Следующая мошенническая финансовая схема - это **схема «обнальщиков» и «номинальных директоров»**.

«Подросток Петя хочет найти подработку в свободное время.

На одном из сайтов по поиску работы Петя увидел объявление:

«Требуется сотрудник для удаленной работы с денежными переводами. Серьезный заработок за несколько часов в день. Трудоустройство без проверок и заполнения документов. Опыт работы не требуется. Гарантия высокого дохода. Требования: наличие карты любого банка РФ»».

В этих схемах используются, в том числе, физические лица, которые помогают обналичивать и выводить деньги после совершения преступниками финансового преступления, так называемые «**дропперы»** (от английского drop — бросать, капать) – люди[19]. В законодательстве, данный термин не используется, однако все чаще государственные организации, правоохранительные органы данный термин используют, ввиду отсутствия емких англоязычных аналогов[20]. Мы также будем использовать далее по тексту данный термин, а также – «лицо, обналичивающее средства, полученные преступным путем».

Чаще всего дропперы даже не подозревают, что являются частью большого преступного паззла. Дропперы не являются инициаторами преступления, они *выполняют указания*, получая за это деньги. Чаще всего эти люди предоставляют данные своей банковской карты злоумышленникам за вознаграждение. Иногда ничего не подозревающего подростка просят завести несколько банковских карт.

На карты подростка мошенники переводят похищенные средства, а затем по цепочке подростки переводят средства другому человеку. Таким образом преступники усложняют правоохранителям поиск средств и конечных получателей. Кроме этого подростков просят обналичить поступившие на карту деньги в разных банкоматах, забрав себе небольшой процент.

Чаще всего дропперами становятся наименее финансово грамотные, доверчивые люди, те, кто верит, что может быстро и легко заработать.

Различают два вида дропперов: «неразводные» и «разводные»[21].

К первому типу подставных относятся люди, которые осведомлены о криминальной составляющей своей деятельности и действуют добровольно и умышленно.

Ко второму – те, кто не понимает, что находится в ловушке у мошенников, и не отдает себе отчета, что участвует в схеме, нарушающей закон.

Схемы вербовки дропперов мошенниками разные, например:

---

[19] Мошенник не по своей воле. Как не стать соучастником киберпреступления // Рамблер. URL: https://finance.rambler.ru/money/52094791-moshennik-ne-po-svoey-vole-kak-ne-stat-souchastnikom-kiberprestupleniya/

[20] Прокурор разъясняет. Прокуратура Хабаровского края. 11.07.2023. URL: https://epp.genproc.gov.ru/web/proc_27/activity/legal-education/explain?item=89000905

Об ответственности владельцев денежных счетов (дропперов») в связи с использованием их в мошеннической схеме. Янтиковский муниципальный округ Чувашской Республики. URL: https://yantik.cap.ru/action/activity/pravoohraniteljnaya-deyateljnostj/prokuratura-yantikovskogo-rajona/prokuratura-razjyasnyaet/2023-god/ob-otvetstvennosti-vladeljcev-denezhnih-schetov-dr

Дропперы: преступление и наказание. URL: https://nefteyuganskij-r86.gosweb.gosuslugi.ru/netcat_files/userfiles/Finansovaya_gramotnost_/Info_materialy/Droppery_prestuplenie_i_nakazanie_.pdf

Банки отбили более 20 млн попыток похитить деньги клиентов. 31.01.2024 ЦБ РФ. URL: https://cbr.ru/press/event/?id=18382 .

[21] Дроппер поневоле: как не стать соучастником мошеннической схемы с банковскими картами // HSE.Daily. URL: https://economics.hse.ru/ecjourn/news/847434104.html

1) Мошенники размещают на улицах и в интернете, в том числе в социальных сетях, объявления, в которых предлагается работа, связанная с переводом и обналичиванием денег;

2) Мошенники размещают в телеграмм-каналах и социальных сетях объявления об интересной работе в IT-сфере с быстрым ростом заработка;

3) Мошенники, размещая объявления о работе, делают фишинговые сайты (поддельные) крупных компаний, чтобы усыпить бдительность и предлагают такие подработки;

4) Под видом сотрудников правоохранительных органов мошенники звонят подростку с предложением официально устроиться на работу по поиску преступников и обещают ежемесячный доход. Если человек соглашается, то мошенники переводят на его банковскую карту похищенные деньги и затем под видом сотрудников банка требуют снять эти деньги в банкомате;

5) Под видом ошибившегося человека мошенники "случайно" переводят на банковский счёт деньги, а затем просят их вернуть наличными или перевести на карту.

Злоумышленники стремятся максимально усложнить правоохранительным органам процесс выявления и отслеживания денежных средств, проходящих через цепочки обналичивания. Сами мошенники прибегают к услугам подставных лиц – дропперов, чтобы избежать ответственности за перевод или обналичивание денежных средств. Большинство организаторов афер живут за границей и даже вычислить их весьма сложно, зато посыльных-дропперов ловят практически всех. Им так же грозит реальное лишение свободы, и придется возмещать нанесенный ущерб.

Мошенники могут заметать следы оплат при очень серьезных преступлениях, могут уклоняться от уплаты налогов, а подросток становится пособником мошенника.

Дропперы, соглашаясь на такую деятельность, несут очень большие последствия, которые могут затронуть не только свои и родительские деньги и имущество, но и жизнь и свободу себя и своей семьи.

Какие **последствия** могут последовать за дроппингом:[22]

1. От мошенников могут поступать угрозы дропперу и его близким, шантаж.
2. Дроппер становится участником схем отмывания денежных средств, продажи оружия или наркотиков.
3. Дроппера будут искать правоохранительные и налоговые органы, иные структуры.
4. Дроппер станет фигурантом уголовного дела.
5. Дроппер отвечаешь своим имуществом и деньгами, а также имуществом и деньгами родителей и опекунов.
6. Придется выплачивать крупные суммы годами.
7. Дроппер создает себе негативный финансовый рейтинг, подрывает свою репутацию.
8. Дроппера могут убить, чтобы избавиться от свидетеля.

Уголовный кодекс не содержит такого состава преступления, как дроппинг, однако это действие может квалифицироваться **как кража, мошенничество, легализация (отмывание) денежных средств, полученных преступным путем**.

В случае, если деяния подростка будут так квалифицированы, то он понесет наказание не только в виде большого штрафа (от 100 тысяч рублей), но и в виде лишения свободы на долгий срок (в среднем, 6-7 лет, но может достигать и 10 лет).

Как сообщают в Ассоциации юристов России, 19-летнюю жительницу Курской области, которая работала на мошенников, обязали выплатить пострадавшим 800 тыс.

[22] Подробнее: https://cloud.mail.ru/public/bfkn/2QSFPyEyJ

₽, а заработала она всего 15 тыс. ₽. Если курьер несовершеннолетний, эта обуза ляжет на родителей.

Жертве мошенничества необходимо возместить ущерб. А с 14 лет это должен делать сам подросток: он оплачивает штраф либо с заработка, со стипендии, с алиментов или другого вида дохода. Если возможностей заработка нет, то в счет ущерба может пойти движимое или недвижимое имущество (например, компьютер, телефон, приставка). А вот в том случае, если штраф довольно большой и собственных средств подростку не хватает, деньги выплачивают родители или опекуны.

Также данные о правонарушении направят в Комиссию по делам несовершеннолетних и защите их прав.

Какую ответственность могут нести несовершеннолетние мошенники.[23]

Если мы посмотрим на определение этого деяния, то мошенничество – это преступление, которое заключается в присвоении чужих денег путём обмана или введения в заблуждение. Да, чаще всего человек передает свои денежные средства преступнику добровольно.

И пользуясь тем, что уголовная и административная ответственность по большинству преступлений наступает на следующий день после 16-летия[24], взрослые мошенники часто привлекают несовершеннолетних к совершению обманных действий посулами получения быстрых и "лёгких" денег.

Именно поэтому подростки должны знать, что отвечать за деяния им тоже придётся. Даже если они младше 16 лет.

В том случае, если ущерб для жертвы мошенников составил менее 1000 руб., это квалифицируется как административное правонарушение, предусмотренное ч. 1 **ст. 7.27 КоАП РФ «Мелкое хищение»**. Пойманным за совершение данного действия грозит штраф в размере до пятикратной стоимости похищенного имущества (но не менее 1000 руб.), административный арест до 15 суток или обязательные работы на срок до 50 часов.

А вот если размер ущерба выше – 1000-2500 рублей, то работает часть 2-ая той же статьи с увеличением штрафа – не менее 3000 руб., возможные сроки ареста – 10-15 суток, обязательных работ – до 120 часов.

Понятно, что если совершен более серьезный проступок, то и наказание будет значительно серьезнее. Если ущерб составил более 2500 рублей, применяется **ст. 159 Уголовного кодекса РФ (мошенничество).**

Здесь и размеры взимаемых штрафов составляют сотни тысяч рублей и доходят до миллионов, а сроки ареста могут составляют до нескольких лет, принудительных работ – годы. Возможно вынесение решения о лишении свободы, то есть отправка в колонию для несовершеннолетних на срок от 2 лет.

Так, если подросток участвовал в мошенничестве в составе организованной группы, и пострадавший указывает размер краденных средств более 1 млн рублей либо потерю своего жилья, то участникам преступного сообщества, и несовершеннолетнему тоже, может грозить максимальное наказание – до 10 лет лишения свободы, а штраф составит до 1 млн. руб.

Услуги «дропперов» по обналичиванию криминальных доходов могут квалифицироваться также как легализация (отмывание) денежных средств, за совершение которой наступает уголовная ответственность, предусмотренная статьей **174 Уголовного кодекса РФ** (совершение финансовых операций и других сделок с денежными средствами или иным имуществом, заведомо приобретенными другими лицами преступным путем, в

---

[23] А если ребенок совершил мошенничество? Что ему за это будет? // Я.Кью. URL: https://yandex.ru/q/article/a_esli_rebenok_sovershil_moshennichestvo_41010554/

[24] КоАП РФ Статья 2.3. Возраст, по достижении которого наступает административная ответственность.

УК РФ Статья 20. Возраст, с которого наступает уголовная ответственность.

целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами или иным имуществом). Наказывается штрафами в размере сотен тысяч рублей, в зависимости от составов преступления. Максимальное наказание в виде лишения свободы за совершение указанного преступления - лишение свободы на срок до 2 лет.

На имя дропперов часто оформляются банковские карты (дроп-карты), их количество может достигать больше 2-3, а то и 10. **Статьей 187 Уголовного кодекса РФ** предусмотрена уголовная ответственность за неправомерный оборот средств платежей, под которым понимается изготовление, приобретение, хранение, транспортировка в целях использования или сбыта, а равно сбыт поддельных платежных карт, распоряжений о переводе денежных средств, документов или средств оплаты, а также электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств. Максимальное наказание в зависимости от тяжести деяния – лишение свободы на срок до 7 лет и штраф до 1 млн. руб.

Незрелость и легкомысленное отношение к финансовым инструментам может стоить очень дорого!

Раздел 2. Нейросеть как современный инструмент финансовых преступлений. Мошеннические схемы с помощью искусственного интеллекта.

Искусственный интеллект (ИИ) дает невероятные новые возможности бизнесу, промышленности, науке, образованию. Но одновременно с этим использовать нейросети начали киберпреступники (черные шляпы, скамеры).

Эксперты отмечают, что растет волна случаев мошенничества, связанных с кражей личных аккаунтов в Telegram.

Все чаще злоумышленники применяют алгоритмы машинного обучения и используют нейронные сети, чтобы получить доступ к личной информации людей для обмана. Преступники могут использовать алгоритмы ИИ для создания поддельных личностей и проведения мошеннических операций, которые трудно обнаружить.

Основные стратегии мошенников с использованием искусственного интеллекта:

1. С помощью искусственного интеллекта злоумышленники могут делать **фальшивые документы**: нейросеть подделает банковские выписки, нарисует фальшивый паспорт или водительское удостоверение.
2. Нейросети мастерски умеют **создавать картины и иллюстрации**. А это значит, что подобные изображения легко используются для фейковых сборов. Так что перед тем, как отправить кому-то финансовую помощь, стоит проверить в других соцсетях и интернете "реальность" адресата.
3. Мошенники могут использовать нейросети для создания **фейковых новостей и рассылок**. В них включаются различные ссылки на ресурсы, при переходе по которым можно потерять данные своей банковской карты или другую персональную информацию.
4. **Фишинг, мошеннические веб-сайты:** ИИ используется для создания поддельных электронных писем (генерацию любых писем) и веб-сайтов (парсинг и считывания любых WEB файлов, и даже закрытых от индексации, и сразу генерацией любых уникальных материалов взамен), чтобы обмануть пользователей и получить доступ к их личным данным и финансовым ресурсам.
5. **Социальные боты и манипуляция в социальных сетях**: ИИ используется для создания чат ботов (телеграм) оплаты и возможностью, сохранять платежные данные. Все эти схемы объединяет необходимость ввода своего номера телефона и SMS-кода. Полученные данные затем используются злоумышленниками для несанкционированного доступа к учетной записи и последующей рассылки спама или вымогания денег.
6. Нейросети учатся **поддерживать разговор**. Искусственный интеллект может взять на себя роль мнимых сотрудников контакт-центров банков и других организаций, которыми представляются мошенники для обмана свои жертв, и вести разговор.
7. ИИ может создавать **"клон" голоса человека (deepfake)**.

Кроме этого, Deepfakes – это манипулированные видео, в которых алгоритмы ИИ накладывают лицо одного человека на тело другого, создавая впечатление, что человек на видео говорит или делает то, чего на самом деле никогда не делал и не говорил.

С учетом развития биометрии и возможности оформить кредит по звонку (современные технологии идентифицируют человека по тембру голоса), Deepfake будет иметь стопроцентную схожесть с оригиналом, а значит, жертва рискует остаться в должниках, ничего об этом не зная.

Кроме этого, преступники начали использовать искусственный интеллект для подделки голосовых сообщений в телеграм с целью краж денег и аккаунтов. Приведем пример из жизни.[25]

«Пользователи телеграма столкнулись с новым видом мошенничества - сначала преступники получают доступ к аккаунту, затем начинают писать потенциальным жертвам из числа списка контактов его владельца с просьбой перевести деньги. Историю о необходимости помощи преступники подкрепляют голосовым сообщением якобы от лица владельца аккаунта. Для аудиосообщения используются нарезки из его реальных старых голосовых сообщений.

Аудиосообщение дублируется в личную переписку и во все чаты, где состоит хозяин украденного аккаунта. Затем направляется фото банковской карты с именем и фамилией. Причем у пострадавшего собеседника имя и фамилия отличались в соцсетях от информации в паспорте, и мошенники использовали данные именно паспорта. Сумма, которую хотели заполучить преступники, составляла 200 тыс. руб.

На первом этапе происходит взлом аккаунта Telegram или WhatsApp, например, через фейковые голосования. Затем мошенники скачивают сохраненные голосовые сообщения и с помощью сервисов искусственного интеллекта синтезируют новые «голосовушки» с необходимым контекстом. Наконец, происходит рассылка сообщений в «личку» или групповые чаты с просьбой одолжить крупную сумму денег, для убедительности используют сгенерированные искусственным интеллектом «голосовушки» и отфотошопленную банковскую карту с поддельным именем получателя.

Данная схема опасна тем, что мошенники используют несколько факторов идентификации жертвы – ***аккаунт, голос и банковскую карту***.

Чтобы не потерять деньги, необходимо перепроверить, действительно ли владелец аккаунта обращается с подобной просьбой, например, перезвонив ему по телефону.

Принципиальной разницы в том, что общаетесь ли вы с реальным злоумышленником или роботом, нет. Правила безопасности не зависят от применяемых мошенниками схем – с привлечением ИИ или без него.

8. Также злоумышленники могут использовать схему мошенничества, связанную с **фальшивой регистрацией в ChatGPT**[26].

Мошенники предлагают «облегчить» доступ к популярной иностранной нейросети с использованием специального сервиса или приложения. В свою очередь, ссылка на сервис может вести на фишинговые ресурсы, маскируемые под сервисы продажи за небольшие деньги аккаунта в нейросети ChatGPT. Чаще всего мошенники создают поддельные сайты, ***очень похожие*** на официальный сайт ChatGPT,

При регистрации на данном ресурсе необходимо будет заполнить форму с данными для оплаты, либо будет предоставлена ссылка на вредоносную программу, например, удаленного управления устройством, при установке которой злоумышленники получают полный контроль над гаджетом пользователя. В конечном итоге все это приведет к потере денежных средств.

---

[25] Вымогатели начали использовать ИИ для подделки голосовых в Telegram Чем новая схема опасна для пользователей // РБК. 10.01.2024. URL: https://www.rbc.ru/technology_and_media/10/01/2024/659d37899a79473f8a99e35f

[26] Темная сторона искусственного интеллекта. Криминальные таланты нейросетей. URL: https://neuralinsight.ru/kriminalnye-talanty-nejrosetej/

Раздел 3. Защищен – значит вооружён: как защититься от финансового мошенничества.

Мы рассмотрели различные виды мошеннических схем, которые применяются для совершения финансовых преступлений. Жертвами таких преступлений могут стать люди ***любого возраста и взрослые, и молодые***. Поэтому необходимо запомнить ряд приемов, которые позволят защитится от финансового мошенничества и не стать жертвой преступников. Рассмотрим их от общего к частному.

В первую очередь, мошенники используют методы социального инжиниринга и психологического давления.

В этом случае эксперты[27] предлагают самую действенную рекомендацию – перестать разговаривать, отключиться, посмотреть вокруг, на обстановку в комнате, вернуться в реальность и спокойно все обдумать в тишине.

К любой ситуации необходимо относится **с критическим восприятием**. Рекомендуется воспринимать с сомнением все звонки, когда собеседник вас куда-то отправляет, склоняет вас к каким-то действиям, требует переводить деньги или что-то оформлять.

Необходимо запомнить несколько ***общих простых правил***:

- если незнакомые лица начинают диктовать порядок действий, значит они пытаются вас «развести»;
- обещания быстрой прибыли – всегда тревожный знак;
- не переходить по незнакомым ссылкам;
- не давать незнакомым лицам данные банковских карт.

Не стоить реагировать на тревожные звонки, письма, SMS или сообщения в соцсетях о том, что родственнику или знакомому нужны деньги. В этом случае обязательно стоит попытаться связаться с этим родственником или знакомым и сообщить, что от их имени рассылаются такие сообщения, и возможно их аккаунт взломали.

Если возникает хоть одно сомнение, происходит какое-то непонятное или пугающее действие, о котором мы говорили ранее, необходимо остановится, **спросить совета у родных и друзей!** Если до них невозможно дозвониться, нужно позвонить в полицию по номеру 112.

Далее рассмотрим алгоритм действий в типичных мошеннических схемах, которые позволят минимизировать или предотвратить финансовые риски.

Правила действий при телефонных звонках:

1. Внимательно проверять входящий номер.
2. Вообще не отвечать и не перезванивать по неизвестным и сомнительным номерам. Даже если телефон кажется верным, стоит всегда проверять номера в официальных справочниках и на официальных сайтах.
3. ОБЯЗАТЕЛЬНО самостоятельно позвонить близкому человеку /в банк / в организацию / в полицию, попросить у них помощи.
4. Прервать разговор - если он касается финансовых вопросов.
5. Запомнить, что Центральный банк, Росфинмониторинг никогда не звонит физическим лицам.
6. Не совершать никаких операций или действий по инструкциям звонящего.
7. Никому никогда не сообщать коды подтверждения из SMS-сообщений.

---

[27] Как не стать жертвой кибермошенников: новые схемы обмана, портрет афериста и правила безопасности от воронежских экспертов. URL: https://www.vrn.kp.ru/daily/27586.5/4856275/

8. Не сообщать CVV/CVC и иные данные банковских карт по телефону и в переписках.

9. Не торопиться принимать решение.

10. Сразу заканчивать разговор при любых сомнениях.

11. Поставить приложение для фильтрации входящих вызовов. Заблокировать звонки с подозрительных номеров.

12. Проверить, не было ли сомнительных операций за время разговора (по карте, в смс).

13. Проиграть с родителями в игру, имитирующую звонки от представителя банка или полиции. Отвечать нужно чётко и быстро: "Спасибо, до свидания, я сам перезвоню". И так повторить раз 10, чтобы у человека сформировалась модель поведения. А дальше перезвонить в банк и узнать, чего же от вас хотели и хотели ли.

14. Можно, придумать с родителями и близкими кодовое слово, которое покажет, что что-то не так.

Правила действий с банковскими картами и при расчетных операциях:

1. Не передавать банковскую карту посторонним. Требовать проведения операций с ней только в личном присутствии и стараться никогда не терять ее из виду.

2. Не делать покупки и не вводить код CCV/CVC на сомнительных сайтах. На сайте надежного интернет-магазина никогда не будут запрашивать личную информацию: пин-код карты, пароли от мобильного банка и привязанных к пластику электронных почтовых ящиков. Эти данные нигде нельзя оставлять!

3. Данные карты (номер, пин-код, CVC-код) нельзя сообщать никому, даже сотрудникам банка.

4. Нельзя писать пин-код на карте и хранить его отдельно. Набирая пин-код, всегда необходимо прикрывать клавиатуру рукой. В том числе, при расчете в кафе и магазинах.

5. Если банковская карта потерялась, необходимо немедленно сообщить родителям, далее в банк и заблокировать ее. То же самое – если пришло SMS-сообщение о покупке или снятии денег в банкомате, а вы этого не делали. Для этого полезно иметь телефон службы поддержки банка под рукой.

6. При поступлении подозрительных смс о том, что карта заблокирована, или с нее были переведены средства по транзакции, которая не совершалась, необходимо сообщить родителям. Перезванивать на номер, с которого поступило сообщение, **нельзя**.

7. Всегда осматривать банкомат перед использованием. Необходимо убедиться, что над клавиатурой и на картоприемнике нет посторонних прикрепленных предметов, а клавиатура не шатается.

8. Не использовать открытые точки Wi-Fi (интернет в общественных местах: транспорте, кафе, кинотеатрах), когда заходите в интернет-банк или пользуетесь мобильным банковским приложением.

9. Оплата в интернет-магазине не должна происходить как перевод средств на чей-то **личный счет**. Если такое происходит, **отправлять деньги нельзя**. В таком случае необходимо обратиться к родителям, чтобы они помогли выбрать надежный магазин.

10. Нельзя передавать посторонним лицам мобильные устройства, на которых установлены приложения онлайн банков.

Правила действий в интернете и в переписке для защиты от фишинга и кибермошенничества:

1. Не следует верить информации о выигрышах, платить деньги за участие в челленджах и обольщаться легким заработком.

2. Не переходить по ссылкам в письмах или сообщениях о выигрыше денег, гаджета или другого приза, не кликайте на подозрительные объекты. Скорее всего, по

ссылке вы получите только вирус. Наведите курсор мыши на подозрительную ссылку/объект и вы увидите, куда она ведёт на самом деле. Сравните её с официальным сайтом компании.

3. Опасно скачивать по просьбе незнакомцев какие-либо приложения, открывать незнакомые и странные ссылки. Даже если ссылка кажется надежной, стоит всегда сверять адреса с доменными именами официальных сайтов организаций.

4. ***Никому никогда*** в переписке не сообщать коды подтверждения из SMS-сообщений.

5. Обращать внимание на почтовый домен, с которого приходят письма. Мошенники обычно используют общедоступные домены gmail.com, mail.ru и т.п., или домены, похожие на официальные имена компаний (напр. sberbankc[.]ru, lc-sberbank[.]com и т.д.)

6. Изучить тему письма или сообщения, контент письма и название файлов. Обращать внимание на грамотность письма. Если в сообщение побуждает вас к немедленному действию – это подозрительный признак.

7. Обращать внимание на обращение и подпись. Если они являются безличными, или есть признак автоподстановки в обращении, то высока вероятность фишинга.

8. Быть осторожными с вложениями в письма или сообщения. Открывайте только те вложения, которые ждали. Проверьте расширение вложения.

9. Если письмо или сообщение требует ввода данных (логина, пароля) на подозрительных сайтах или в анкетных формах, то необходимо удалить это письмо.

10. Если в ходе общения в мессенджере бот или робот предлагает ввести личную финансовую информацию (коды из смс от банка, полные данные карты, ФИО, паспортные данные и т. д.), необходимо прервать общение, обратиться в отделение банка либо самостоятельно связаться с организацией по официальным контактам, которые указаны на официальном сайте компании.

11. Пароли в соцсетях в честь любимых домашних питомцев и даты рождения, конечно, легко запомнить, но лучше выбрать что-то посложнее. Потому что мошенники их легко подберут. А если они где-то записаны, то нельзя фотографировать этот листок и отправлять снимок куда-то.

12. Нельзя фотографировать и отправлять свои личные данные и данные родителей, копии паспортов и других документов, банковских карточек и деньги незнакомым людям.

13. Нельзя ни с кем делиться информацией об адресе дома, школы, о месте работы родителей, какие приложения стоят у членов семьи на телефоне, любыми паролями и ПИН-кодами.

14. Лучше общаться только с друзьями и близкими, которые пишут со знакомых номеров и страниц. А если написал незнакомец и просится в друзья, а потом начал спрашивать информацию, перечисленную выше, то он точно не может быть твоим другом.

15. Необходимо лично проверять всю информацию, поступающую от друзей или родственников в соцсетях, мессенджерах. То есть, если друг или подруга вдруг попросила денег, чтобы оплатить посылку, лучше перезвонить и услышать просьбу в разговоре.

16. Совершать покупки можно только по согласованию с родителями, в проверенных интернет-магазинах, нельзя переводить полную предоплату за товар, если не уверены в надежности продавца.

17. Опасно приобретать виртуальные деньги, улучшения для игр, а также платный игровой контент и другие бонусы.

18. Предложение общаться в мессенджере, а **НЕ ЧЕРЕЗ** официальные сайты торговых площадок (*например*, «Авито» или «Юлу») – первый признак мошенника. Необходимо проверять рейтинг и отзывы на продавца. Желательно совершать покупку

вместе с родителями или оплачивать товары только через безопасную сделку на самом сайте бесплатных «Авито» или «Юлу».

19. Нужно защитить свои аккаунты – необходимо везде, где это возможно, подключить двухфакторную идентификацию.

20. Следует обеспечить безопасность профиля в социальных сетях - следует закрыть доступ посторонним к личной информации на страницах соцсетей, сделав их приватными.

21. Важно использовать антивирусное программное обеспечение и регулярно обновлять его, чтобы защитить свой компьютер от вредоносных программ.

22. Если вы решили самостоятельно воспользоваться услугами нейросети, убедитесь, что действительно оказались на официальном ресурсе. Не переходите по сомнительным ссылкам, предлагающим ввести данные для оплаты и не устанавливайте на свои устройства неизвестные приложения.

23. Если вы в разговоре почувствовали что-то неладное, лучше всего будет задать собеседнику случайный вопрос – это поможет понять, что вы общаетесь с живым человеком, а не с ботом.

Приложения

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.

Инвестиционный проект – ограниченный по времени осуществления и затрачиваемым ресурсам комплекс мероприятий, направленных на создание и последующую эксплуатацию новых либо модернизацию существующих объектов (например, товаров, услуг), путем осуществления инвестиций (вложений, например, финансовых).

Краудфандинд – коллективное финансирование проекта, производства товара или услуги, фирмы и прочее. Осуществляется в различных формах.

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).

Фиатные деньги – (от лат. «fiat» — декрет, указание, «да будет так») – это не обеспеченные золотом или другими драгоценными металлами деньги, номинальная стоимость которых устанавливается и гарантируется государством вне зависимости от стоимости материала, использованного для их изготовления. Иными словами, это законная валюта любого государства, например, рубль, юань, доллар.

Финансовая пирамида – разновидность мошеннических схем, при которой основатели покрывают обязательства перед вкладчиками с помощью денег от новых вкладчиков.

Черные шляпы – это преступники, злонамеренно взламывающие компьютерные сети. Они также создают вредоносные программы, которые уничтожают файлы, блокируют компьютеры, крадут пароли, номера кредитных карт и другую личную информацию.

Приложение № 2.
Ресурсы

Материалы:

Как защититься от кибермошенничества. Правила безопасности в киберпространстве. Банк России [Электронный ресурс]. - Режим доступа: https://dni-fg.ru/16

Чадо кутежа: преступники подбираются к счетам россиян через детей. [Электронный ресурс]. - Режим доступа: https://iz.ru/1592828/ivan-petrov/chado-kutezha-prestupniki-podbiraiutsia-k-schetam-rossiian-cherez-detei

Как защитить себя и близких от киберугроз? Минцифры РФ [Электронный ресурс]. - Режим доступа: https://киберзож.рф

Кибербезопасность - это просто на ГосУслугах [Электронный ресурс]. - Режим доступа: https://www.gosuslugi.ru/cybersecurity

Ассоциация Развития Финансовой Грамотности [Электронный ресурс]. - Режим доступа: https://fincubator.ru/company/

Международный учебно-методический центр финансового мониторинга. Медиатека [Электронный ресурс]. - Режим доступа: https://mumcfm.ru/mediateka

Международная Олимпиада по финансовой безопасности. Материалы для подготовки: https://rosfinolymp.ru/prepare

Видеопрезентации

Кибермошенники: новые сценарии [Электронный ресурс]. - Режим доступа: https://iz.ru/1592828/ivan-petrov/chado-kutezha-prestupniki-podbiraiutsia-k-schetam-rossiian-cherez-detei

Безопасность в онлайн-играх [Электронный ресурс]. - Режим доступа: https://rosfinolymp.ru/prepare

Фишинг [Электронный ресурс]. - Режим доступа: https://моифинансы.рф/materials/video-lekcii-o-tom-kak-ne-popast-na-ulovki-finansovyh-moshennikov/

Фишинг в социальных сетях [Электронный ресурс]. - Режим доступа: https://rosfinolymp.ru/prepare

Современные финансовые пирамиды [Электронный ресурс]. - Режим доступа: https://mosobr.shkolamoskva.ru/release/13408

Дропперы [Электронный ресурс]. - Режим доступа: https://mosobr.shkolamoskva.ru/release/13326

Безопасность персональных данных [Электронный ресурс]. - Режим доступа: https://rosfinolymp.ru/prepare

Безопасность мобильных устройств [Электронный ресурс]. - Режим доступа: https://mosobr.shkolamoskva.ru/release/13321

Противодействие псевдоинвестиционным проектам [Электронный ресурс]. - Режим доступа: https://mosobr.shkolamoskva.ru/release/13320

Кибербезопасность. Виды мошенничества [Электронный ресурс]. - Режим доступа: https://mosobr.shkolamoskva.ru/release/12931

Не сообщайте мошенникам ваши личные данные! [Электронный ресурс]. - Режим доступа: https://mosobr.shkolamoskva.ru/release/12385