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

Методические рекомендации по подготовке и проведению тематического урока на тему:

«Темная сторона искусственного интеллекта»

Москва, 2026

Оглавление

Аннотация

Методические рекомендации подготовлены в помощь педагогам образовательных организаций для проведения тематического урока, посвященного противодействию вовлечения молодых людей школьного возраста (8-11 классы, 14-18 лет) в финансовые преступления в качестве жертв и соучастников.

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

Актуальность темы

Финансовая грамотность в эпоху искусственного интеллекта приобретает новое, критически важное значение. Она перестаёт быть просто умением вести бюджет и становится навыком цифровой самообороны, выражающейся в цифровой гигиене, критическом мышлении и способности противостоять алгоритмическим угрозам, исходящим из сети Интернет. Значимость финансовой грамотности на текущий момент сложно переоценить.

Наверное, ни для кого не будет секретом и тем более удивлением, что искусственный интеллект незаметно проник во все сферы нашей жизни и играет огромную роль в современном обществе. Благодаря стремительному росту вычислительных способностей ЭВМ и алгоритмов машинного обучения нейросети помимо написания текстов и решения математических задач научились распознавать объекты. Это особенно отразилось на увеличении числа беспилотного транспорта (автомобили, грузовики, трамваи и др.) и на улучшении сферы логистики (например, в части составления оптимального маршрута доставки).

Рассмотрим некоторые аспекты влияния ИИ на нашу жизнь.

- ***Медицина и здравохранение.*** Алгоритмы компьютерного зрения анализируют рентгеновские снимки, МРТ и КТ, обнаруживают опухоли, переломы и другие патологии быстрее и точнее человека. ИИ активно применяется для разработки лекарств, для общения в чат-ботах, которые позволяют пациентам осуществлять запись на прием к нужным врачам. ИИ участвует в развитии, так называемой, персонализированной медицины, задачей которой является прогнозирование потенциальных заболеваний пациента и применение индивидуальных схем лечений на основе анализа больших данных.
- ***Банковская сфера.*** ИИ активно применяется в принятии решений о выдаче кредитных продуктов в рамках, так называемого, скоринга, где

оценивается не только кредитная история клиента, но и большой объем прочей информации, что позволяет принимать грамотные решения. Учитывая стремительное повышение финансовой грамотности населения, все больше граждан инвестируют свои сбережения в фондовый рынок (акции, облигации, паевые инвестиционные фонды) с целью получения потенциально большей доходности, чем такие сберегательные продукты, как вклады и накопительные счета. Банки же, в свою очередь, применяют ИИ для мгновенной, автоматической покупки тех или иных ценных бумаг на бирже за клиента, реагируя на малейшие изменения на рынке.

- ***Сфера образования.*** На сегодняшний день существует множество образовательных платформ/агрегаторов и других организаций, активно использующих технологии ИИ. Именно они подстраивают учебный материал под темп и уровень знаний каждого ученика, в том числе выявляя недостаток знаний по той или иной теме, подбирая соответствующие дополнительные задания, что непременно положительно сказывается на процессе обучения.
- ***Наука***. Это та сфера, где модели ИИ активно используются, поскольку являются незаменимым инструментом в научных исследованиях. ИИ позволяет находить закономерности за короткий промежуток времени там, где у человека уходили бы дни/недели/годы. В качестве примера можно привести разработку программного обеспечения российских ученых с использованием ИИ для оперативного автоматического обнаружения изменений состояния лесов – пожаров, вырубки и др. Именно эта инновация способна оперативно устранять либо сводить к минимуму негативные последствия.

Кроме вышесказанного, ИИ применяется для защиты нашей кибербезопасности. Например, один из крупнейших сотовых операторов РФ создал «Кибербабушку» – это ИИ-модель, которая общается с мошенниками

под видом пожилой клиентки.[1] В результате кибермошенник тратит время и ресурсы, общаясь с ИИ вместо реального человека, который мог бы пострадать от его активности.

Также ИИ активно применяется и в сфере бизнеса. Так, один из крупнейших маркетплейсов РФ внедрил ИИ во многие процессы, чтобы упростить жизнь сотрудников. Например, 95% карточек товаров теперь модерируются без участия человека.

В сфере HR произошли большие изменения. Например, популярный в РФ онлайн-сервис по подбору персонала и поиска работы в ноябре 2025 года запустил ИИ-помощника для рекрутеров, который взял на себя рутину и освободил время специалистам для живой работы с людьми.

Список того, как ИИ положительно влияет на жизнь всех людей на нашей планете, можно продолжать очень долго. Вместе с тем есть обратная сторона, одна из них – это финансовые преступления с использованием ИИ.

Федеральная служба по финансовому мониторингу (Росфинмониторинг) при активном участии подразделений финансовой разведки стран СНГ, взаимодействующих в рамках Евразийской группы по противодействию легализации преступных доходов и финансированию терроризма, проводит активную работу, в том числе, по противодействию противоправным действиям с похищенными денежными средствами.

Для начала посмотрим на общую картину в этой сфере за последнее время: по сведениям Центрального банка России, объем операций без добровольного согласия клиентов за 9 месяцев 2025 года составил 21 млрд руб., за 2024 год этот объем составлял 27,5 млрд руб.[2]. Сравнение этих

[1]Билайн создал «Кибербабушку». Как она поможет бороться с телефонными мошенниками?//Lenta.ru.13.11.2025.URL:https://lenta.ru/articles/2025/11/13/bilayn-sozdal-kiberbabushku/?ysclid=mk5pb3lwx2509443586

[2]Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций//ЦБ РФ.12.02.2025.URL:https://cbr.ru/analytics/ib/operations_survey/2024/

показателей говорит о том, что несмотря на усилия ЦБ РФ, коммерческих банков, МВД РФ, Роскомнадзора и других учреждений вопрос финансовой безопасности стоит очень остро и не теряет своей актуальности. По сведениям МВД РФ, только в ноябре 2025 года ведомство смогло предотвратить хищение на сумму свыше 222 млн руб.[3].

Важно обратить особое внимание на рост числа пострадавших от кибермошенников среди несовершеннолетних[4]. По данным МВД РФ, целью мошенников являются деньги родителей подростков. Используя личные данные несовершеннолетних, злоумышленники звонят или отправляют сообщения подросткам от имени образовательной организации, органов госвласти или операторов сотовой связи, чтобы заполучить коды авторизации. Также зафиксированы случаи мошенничества при продаже или покупке игровых аккаунтов и ответов на ГИА.

Для отмывания средств, полученных в результате противоправных действий, кибермошенники по-прежнему активно используют классические банковские механизмы. Финансовые потоки проходят через множество подставных счетов, где незаконные деньги смешиваются с легальными операциями, после чего часто направляются на криптоплатформы для окончательной легализации или финансирования дальнейшей преступной деятельности, например, террористической. Стоит отметить, что масштаб данной проблемы часто недооценивается, а сама угроза носит транснациональный характер, затрагивая не только Россию и страны Содружества Независимых Государств, но и весь мир.

---

[3]МВД раскрыло результаты борьбы с телефонными мошенниками//Lenta.RU. 02.12.2025 URL:https://lenta.ru/news/2025/12/02/mvd-raskrylo-rezultaty-borby-s-telefonnymi-moshennikami/?ysclid=miq22ihex2658176800

[4]МВД фиксирует рост числа пострадавших от кибермошенников несовершеннолетних//Коммерсант.28.06.2025.URL: https://www.kommersant.ru/doc/7851537?ysclid=mitybkryl3160727529

Киберпреступники вынуждены активнее вовлекать в процесс отмывания денег не только молодых людей, но и зачастую подростков в возрасте от 14 лет. По сведениям Банка России, в РФ было выявлено более 1 млн дропперов[3], поэтому этот вопрос нельзя оставлять без внимания. По данным МВД РФ, чаще всего дропперами становятся безработные жители небольших городов с низкими зарплатами; студенты и школьники, находящиеся в поисках легких денег.

Для привлечения молодежи в сомнительные схемы мошенники используют следующие психологические уловки:

- срочность – «предложение только до вечера», «места заканчиваются»;
- простота – «ничего сложного, справится даже школьник»;
- безопасность – «это совершенно легально», «все так делают»;
- постепенность – начинают с мелких сумм, постепенно увеличивают обороты;
- социальное доказательство – «у нас уже работают 500 человек», «посмотри отзывы».

Опасность для школьников и студентов заключается в том числе в непонимании ответственности за участие в подобных схемах.

В июне 2025 года президент РФ В.В. Путин подписал закон, дополняющий статью 187 УК РФ конкретной ответственностью за участие в дропперских схемах. Так, документ устанавливает уголовное наказание до 3 лет лишения свободы для лиц, предоставляющих свои банковские реквизиты за вознаграждение, и до 6 лет – для организаторов такой деятельности[5]. В 2025 году в России возбудили первое в стране уголовное дело против, так

[5]Путин подписал закон об уголовной ответственности для дропперов//РИА.24.06.2025.URL:https://ria.ru/20250624/putin-2025132619.html?ysclid=miu0fzlqlw280946511

называемого, дроповода, то есть организатора схемы по незаконному обналичиванию средств. По сведениям МВД РФ, наводку на него дал один из задержанных дропперов взамен на освобождение от уголовной ответственности[6].

Таким образом, рассматриваемая в настоящем уроке тематика является особенно актуальной в современной жизни для каждого человека.

[6] Как первое уголовное дело против дроповода скажется на работе мошеннической схемы //Коммерсант.07.08.2025.URL:https://www.kommersant.ru/doc/7943692?ysclid=miu0s6vpbe158946376

Раздел 1. ИИ – опасный инструмент в руках преступников

Технологии искусственного интеллекта стремительно развиваются, и одним из самых впечатляющих и в то же время тревожных проявлений является дипфейк.

Дипфейк (от англ. *deepfake* – «глубокий подлог») – это видео, аудио или фото, созданные искусственным интеллектом, на которых человек делает или говорит то, чего никогда не было в реальности. Можно себе представить, что компьютер научился настолько хорошо копировать голос и лицо актёра, что может «вставить» его в новый фильм без его участия. Подобная технология зародилась много лет назад. Так, еще в 2015 году при создании известного фильма «Форсаж 7» был воссоздан образ главного героя с помощью доступных компьютерных технологий. Это было сделано в связи с гибелью одного из главных актеров и необходимостью завершить важную сюжетную линию.

Стоит отметить, что это был первый масштабный случай в мире. Но сегодня дипфейки вышли на новый уровень. Современные технологии позволяют сделать полноценный голосовой дипфейк, используя всего несколько секунд записанного голоса реального человека. С этой целью злоумышленники в РФ стали массово звонить гражданам под видом социологических опросов, чтобы записать их голоса для последующего создания дипфейков[7].

Широкую известность получил случай, произошедший в 2019 году в Великобритании: мошенники с помощью ИИ скопировали голос генерального директора немецкой энергетической компании. Они позвонили его подчинённому, приказав срочно перевести €220 000 на счёт венгерского

[7] Эксперт предупредил о новых мошеннических схемах с дипфейками //Известия.11.06.2025. URL:https://iz.ru/1902358/2025-06-11/ekspert-predupredil-o-novykh-moshennicheskikh-skhemakh-s-dipfeikami

поставщика. Деньги перечислили мгновенно. Это один из первых задокументированных случаев[8].

Рассмотрим пример аналога дипфейков под названием ***«Злой близнец» (Evil Twin Attack).*** Это достаточно классическая и при этом очень опасная атака. Опасность заключается в том, что ничего не подозревающий пользователь сети Интернет передает свои данные незаметно для себя злоумышленникам, а работает это по следующей схеме:

- *клонирование («дипфейк для сети»):* злоумышленник создаёт Wi-Fi сеть с идентичным названием SSID. С помощью современных устройств он делает сигнал своей точки доступа гораздо сильнее, чем у оригинала;
- *заманивание жертвы:* пользователь в кафе, аэропорту или торговом центре видит список сетей. Сеть-«близнец» часто оказывается вверху списка (из-за сильного сигнала) и выглядит как знакомая. Человек подключается к ней, думая, что это легальный бесплатный Wi-Fi;
- *перехват трафика (Man-in-the-Middle):* вся интернет-активность жертвы (пароли, переписка, история посещений, данные банковских карт) теперь проходит через устройство атакующего. Он становится «человеком посередине», который всё видит и записывает;
- *фишинг и принуждение:* часто «злой близнец» показывает фейковую страницу входа, требующую подтверждение номера телефона или авторизацию через соцсети. Это делается для кражи ещё большего количества данных.

Следовательно, в процессе серфинга в сети Интернет пользователь может передать злоумышленникам логины и пароли от электронной почты, социальных сетей, банков; платежные данные своих банковских карт; историю посещений сайтов и многое другое.

---

[8] Голос как у начальника — не отличишь: как искусственный интеллект позвонил и украл сотни тысяч долларов//Бизнес.ФМ.04.09.2019. URL:https://www.bfm.ru/news/423702?ysclid=mivres04zq489735366

Наглядным примером может стать реальная ситуация, произошедшая с ученицей одной из школ, которая направлялась в другой город на олимпиаду. В аэропорту ученица подключилась к сети Wi-Fi с названием соответствующего аэропорта, тем более это была первая сеть в списке доступных на мобильном устройстве. Школьница несмотря на предупреждение мобильного телефона о незащищенности сети прошла регистрацию. Введя свой номер телефона и код доступа, который поступил на телефон в одном из популярных мессенджеров, девочка потеряла к нему доступ, так как этот код являлся одноразовым паролем для входа в мессенджер. Невнимательность стала роковой – для подобных форм регистрации никакие коды из мессенджеров вводить не требуется.

ИИ – фишинг. Фишинг приобретает все новые формы, более тонкие и изощренные методы для усыпления бдительности потенциальных жертв. Раньше фишинговые письма были шаблонными, с ошибками и общими обращениями, например, «Уважаемый клиент!». Теперь ИИ, в том числе, на базе ChatGPT анализирует данные жертвы из различных социальных сетей, корпоративных сайтов, сайтов школ или утечек, которые происходят регулярно, и генерирует идеальное письмо. Под утечками подразумеваются хакерские атаки на серверы различных компаний, где хранятся данные их клиентов, например, сведения владельцев дисконтных карт.

В качестве примера можно привести один случай, произошедший в государственном учреждении. Сотруднику организации якобы с аккаунта его высокопоставленного руководителя в чате одного из мессенджеров поступило сообщение о том, что в рамках проверки представителями ФСБ России (Федеральная служба безопасности РФ) было выявлено распространение персональных данных внутри организации. Помимо этого, жертве была направлена скан-копия письма, написанная якобы от лица ФСБ России в адрес руководителя государственного учреждения, причем составлено письмо было грамотно, с учетом всех норм входящей корреспонденции с указанием всех

корректных сведений (ФИО жертвы, должность и ФИО руководителя, название организации). Все это усыпило бдительность пострадавшего. Дальше ситуация развивалась по следующему сценарию: в письме среди прочего было указано, что с жертвой должен был связаться «представитель ФСБ» с указанием его ФИО, далее после его звонка жертве поступил звонок уже от «представителя Росфинмониторинга», в результате чего жертву убедили снять свои личные денежные средства и передать, так называемому, «курьеру наличности».

ИИ-вишинг (англ. vishing = voice + phishing). Это разновидность дипфейков, в котором ИИ работает как голосовой «копировальщик». На сегодняшний день ИИ в своем арсенале достаточно лишь иметь несколько секунд оригинальной записи разговора человека для того, чтобы создать полноценное аудиосообщение или совершить звонок с возможностью ведения диалога.

Здесь можно привести пример, произошедший в 2025 году в Италии: мошенники, используя данную технологию и представляясь министром обороны Италии Гвидо Крозетто и другими чиновниками, совершали звонки итальянским предпринимателям с целью убедить их в необходимости перевода денег. Стоит отметить, что жертвами в данном случае стали известные мировому сообществу такие люди, как президент Prada Патрицио Бертелли, модельер Джорджио Армани, исполнительный вице-председатель Pirelli & C. SpA Марко Тронкетти Провера, миллиардер Массимо Моратти, бывший владелец миланского футбольного клуба «Интер» и др.[9]

Социальный инжиниринг через соцсети и приложения знакомств (романтический скам). Всем людям важна эмоциональная близость с родственниками, друзьями, любимыми. Вырабатываемые при этом

[9] В Италии мошенники украли деньги с помощью ИИ с голосом министра//РБК.10.02.2025.URL: https://www.rbc.ru/rbcfreenews/67a9c0499a7947e77f1f612f?ysclid=mj1mdsssip490024673

организмом гормоны вызывают у нас чувство привязанности, желание продолжить общение, и это, как следствие, приводит к снижению уровня критического мышления ввиду вовлеченности в процессе коммуникации. Для этой цели киберпреступники охотно пользуются нейросетями, способными общаться в чатах с тысячами людей одновременно. Стоит отметить, что само общение перед тем, как вовлечь жертву в схему, при которой она останется без денег, для правдоподобности может занимать дни, недели, месяцы. Более того, с целью повышения доверия жертвы к собеседнику (по имени «нейросеть») злоумышленники предварительно обогащают нейросеть данными о потенциальной жертве, например, на основе данных со страницы в социальной сети. Главная опасность такого подхода заключается в том, что ИИ не устает, не допускает ошибок, подстраивается под собеседника по эмоциональному контакту, хорошо считывает психологический портрет пользователя. При этом жертве отправляются не какие-то шаблонные фразы, а применяется настоящий индивидуальный подход, который позволяет достичь высокого уровня иллюзорной связи и близости. Все это усыпляет бдительность человека, после чего его просят, например, вложить средства в финансовую пирамиду, купить криптовалюту и так далее[10].

Рассмотрим пример. Мужчине пришло сообщение в личный чат в социальной сети от незнакомой ему девушки. Она задала вопрос относительно эффективности методов работы одного из коуч-тренеров, на которого мужчина был подписан. Получив ответ, девушка активно поддержала разговор в чате, задавала вопросы о хобби, о путешествиях, об открытии собственного бизнеса. Через некоторое время мужчине было направлено голосовое сообщение, очевидно, для создания более доверительной коммуникации. Постепенно тема

[10] «Любовная переписка с ботом»: на россиян обрушились тонны «романтического скама» //Газета.РУ.10.11.2025.URL:https://www.gazeta.ru/social/news/2025/11/10/27144032.shtml?ysclid=mj5rmkvcr507205716&updated

разговора перешла в сферу ставок на футбольные матчи. Девушка сообщила, что обладает инсайдерской информацией, позволяющей легко заработать. Далее она прислала еще несколько голосовых сообщений о том, что она решилась сделать ставки, а также скриншоты, подтверждающие ее выигрыш, в разы превышающий ставки. Мужчина понял, что это опасное общение и прекратил его. Несмотря на это собеседница продолжила направлять сообщения, в частности, прислала фотографию с обновками в виде смартфона последней модели, купленный на указанный ранее выигрыш. После этого мужчина добавил собеседницу в черный список и общение прекратилось.

Правила безопасности

Не пользуйтесь незащищенными беспроводными сетями!

«Злые двойники» – это почти всегда незащищенные подключения. Злоумышленники рассчитывают на то, что пользователь не знает о сопутствующих рисках и подключится к поддельной точке доступа.

Не игнорируйте предупреждение системы о безопасности сети. За ним может скрываться реальная угроза. Вместо того, чтобы бездумно закрывать уведомление, уделите секунду, чтобы понять, от чего оно вас защищает. Это простое действие может предотвратить утечку данных или потерю денег.

Запретите себе вводить логины, пароли и данные банковских карт в публичных сетях Wi-Fi. Это золотое правило цифровой безопасности. Преступники легко перехватывают такой трафик. Единственная гарантия – полный отказ от авторизации в подобных условиях.

Обязательно подключайте многофакторную аутентификацию (MFA) везде, где это возможно. Этот метод защищает ваш аккаунт в два и более шага: например, после пароля нужно ввести одноразовый код из SMS или приложения. Это простой, но крайне эффективный барьер для злоумышленников. Не пренебрегайте этой настройкой.

Необходимо обращать внимание на адресную строку. При использовании публичного Wi-Fi заходите только на сайты с протоколом HTTPS (в начале адреса стоит значок замка). Буква **S** означает «secure» (безопасно) – такое соединение защищено сквозным шифрованием, которое скроет ваши действия от перехвата. Это не гарантия, но существенно снижает риски компрометации своих данных.

Не поддавайтесь панике!

Самое главное правило, которое можно применить ко всем видам мошенничества, особенно в рамках подделки голоса с просьбой о деньгах или совершения любых срочных действий, даже если голос звучит как «родной» – это не поддаваться панике. Первое – необходимо положить трубку при первых подозрениях, второе – необходимо самостоятельно перезвонить по номеру телефона своему родственнику или другу, указанному в телефонной книге, для уточнения информации и достоверности. Третье – учитывая способности ИИ качественно подделывать голос, рекомендуется в рамках своей семьи придумать кодовое слово, которое будет известно только узкому кругу лиц, что позволит сразу понять, кто находится на «том конце провода». Это самый простой и гарантированный способ. Четвертое – задайте личный вопрос, ответ на который знаете только вы и ваши близкие, например, «Мы ездили к дедушке Диме в деревню этим летом?» или «Как зовут нашу собаку?». Прямого ответа ИИ на данные вопросы не даст, так как он не владеет нашими воспоминаниями.

Соблюдайте цифровую гигиену!

Вместе с тем мы сами не должны давать возможность ИИ клонировать наш голос, для чего необходимо соблюдать следующие правила:

- закрыть доступ к своим социальным сетям (настроить приватность только для друзей);

- не выкладывать в открытый доступ слепки своего голоса (статусы в мессенджерах, социальных сетях, стримах).

Контролируйте свое эмоциональное состояние!

Базовое правило безопасности – при поступлении информации, несущей в себе позитивные или негативные эмоции, требующие от нас каких-либо немедленных действий, мы должны понимать, что это скорее всего обман. В этом случае необходимо остановиться, пригласить коллегу, друга, близких для обсуждения ситуации, скорее всего вам сразу подскажут, что это воздействие мошенников. Нужно всегда помнить, что сотрудники ЦБ РФ, Росфинмониторинга, ФСБ России, ФНС России никогда не будут звонить и тем более решать вопросы «государственной важности» в режиме телефонного звонка. Учитывая активное использование ИИ в сборе информации о нас, в грамотности составления писем и в том, что подобного рода звонки совершают специально обученные люди, способные запугать и ввести человека в ступор и нестабильное эмоциональное состояние, то на первом месте нашим главным оружием может стать только наша бдительность и критическое мышление.

Отсекайте подозрительные контакты!

Онлайн-знакомства – в настоящее время очень развитый инструмент для расширения круга общения, в связи с чем ограничить себя в целом от такого инструмента было бы неправильным. Но, если в переписке вдруг возникает разговор про деньги, ставки, криптовалюты и подобного рода слова, разговор нужно прекратить немедленно раз и навсегда, ведь с вероятностью 99% это мошенники. Романтический скам – это долгая игра на доверии, где финальной ставкой являются ваши деньги, а разменной монетой – ваши чувства. Мошенники – талантливые психологи, а современные технологии, такие как ИИ дают им небывалые возможности для массовости и убедительности.

Ваш главный щит – критическое мышление ко всему, что видите и слышите, а также правило: «Никаких денег, ни под каким предлогом человеку, которого никогда не видел вживую».

Если вы или ваш знакомый стали жертвой, важно прекратить общение; не винить себя; заблокировать мошенника; в случае необходимости сообщить в правоохранительные органы и администрацию платформы.

Раздел 2. Вербовка дропперов с применением ИИ

Технологии не стоят на месте. При этом у кибермошенников, как и прежде, насущным вопросом является вывод или обналичивание похищенных средств. Для этих целей мошенники по-прежнему привлекают, как правило, молодых людей, которых принято называть дропами.

Дроп – это посредник между злоумышленниками и их жертвами. Дроп выполняет достаточно простую функцию: принимает на свой счет похищенные деньги и переводит их следующим участникам схемы либо снимает наличные средства и передает их своим кураторам с учетом небольшой комиссии. Еще один вариант стать дропом – оформить банковскую карту и передать ее вместе с доступом к онлайн-банку злоумышленникам.

Стоит отметить, что дропами можно стать случайно, а можно и намеренно. При этом молодые люди не осознают, что так или иначе они являются соучастникам уголовного преступления. Если в 2024 году в РФ не было отдельной статьи за дропперство, то в 2025 году ситуация коренным образом изменилась, так как президент РФ В.В. Путин подписал федеральный закон №176 ФЗ, который вводит уголовную ответственность за дропперов – подставных лиц, которые мошенники используют для обналичивая или перевода украденных денежных средств. Данный ФЗ вносит изменения в статью 187 УК РФ «Неправомерный оборот средств платежей», в котором наказание зависит от степени участия в схеме. Отдельное внимание стоит обратить на следующий пункт: «Приобретение либо передача карты лицами, не являющимися клиентами банка» – за данное нарушение гражданин может быть лишен свободы сроком до шести лет с выплатой штрафа. Это важно знать, ведь, как известно, «незнание закона не освобождает от ответственности». При этом, если нарушение совершил несовершеннолетний, то за его действия будут отвечать родители или законные представители.

К сожалению, статистика удручающая: по сведением ЦБ РФ, число клиентов-дропов в российских банках превысило 1 млн человек[11]. Более того, регулятор сообщает, что порядка 20% граждан, вовлеченных в дропперские схемы, являются подростками, очевидно не осознавая серьезность последствий своих действий.[12]

Дропперы являются важными звеньями преступной цепочки легализации денежных средств, полученных неправомерным способом, в связи с этим их можно также привлечь к уголовной ответственности в рамках статьи 174 УК РФ «Легализация (отмывание) денежных средств или иного имущества, приобретённых другими лицами преступным путём».

Дропперов условно распределяют на группы в соответствии с выполняемыми функциями:

- ***заливщики*** – принимают наличные от преступников, зачисляют их на личный банковский счет и отправляют дальше другим участникам схемы;
- ***транзитники*** – получают переводы на свою банковскую карту и перенаправляют их на сторонние счета либо электронные кошельки;
- ***обнальщики*** – снимают наличные деньги в банкоматах и передают их организаторам преступлений.

Особое внимание стоит уделить вербовке дропперов с учетом развития таких ИИ-алгоритмов как нейросети и NLP (Алгоритмы обработки естественного языка – Natural Language Processing). Именно они позволяют злоумышленникам быстрее находить подходящих на эту роль людей, поскольку поиск становится более умным, таргетированным. Вышеупомянутые ИИ-алгоритмы сканируют открытые источники (соцсети, форумы, маркетплейсы) для поиска уязвимых групп: людей с финансовыми трудностями, студентов, безработных, ищущих быстрый заработок, или тех,

[11] Число клиентов-дропов в российских банках превысило миллион//РБК.26.09.2025. URL :https://www.rbc.ru/finances/26/09/2025/68d69e149a79472e16862f06?ysclid=mj640dqn50530339087

[12] ЦБ сообщил о доле подростков среди участников дропперских схем//ЦБ РФ.08.12.2025. URL:https://www.rbc.ru/rbcfreenews/693680f39a79477f253137c2

кто выражает недовольство работой и прочих. Также ИИ-алгоритмы способны оценить психологический профиль потенциального сотрудника: анализируются лайки, посты, стиль общения, чтобы определить уровень внушаемости, склонность к риску, отчаяние или алчность. Это позволяет строить максимально персонализированные подходы к поиску нужных людей.

Как правило, первый контакт с потенциальным дроппером устанавливают не люди, а продвинутые ИИ чат-боты, способные вести длительные, естественные беседы на разных языках. Иногда используются дипфейк-аватары (видеозапись или общение в реальном времени) для создания ложного доверия, например, представителя HR-агентства или успешного спекулянта акциями. Если же диалог ведет сам человек, то ИИ подсказывает ему, что нужно ответить на тот или иной вопрос соискателя, например, о законности потенциальной работы.

Разберем некоторые примеры вербовки дропперов.

«Простая подработка». Старшеклассник решил заработать свои первые деньги, на просторах сети Интернет он увидел заманчивое объявление о работе: образование не требуется; опыт работы не требуется; работа из дома несколько часов в день. И, наконец, главное условие – наличие банковской карты или доступ к онлайн-банку. Нетрудно догадаться, о чем идет речь в подобной подработке. Используя отработанные легенды, мошенники убеждают ничего не подозревающих людей, чаще всего молодёжь, совершать переводы или предоставлять доступ к своим счетам. Таким образом, жертвы, не осознавая истинной сути происходящего, становятся соучастниками преступных операций.

«Ошибочный перевод». По-прежнему актуальная схема на текущий день. Данная уловка рассчитана на невнимательность и добросовестность людей. Вас вводят в заблуждение: после «случайного» перевода средств на счет поступает звонок с просьбой о помощи и возврате денег на «правильный» счёт. Важно помнить: возвращать платеж по указанным злоумышленником

реквизитам – значит стать соучастником преступления. Единственно верное решение – незамедлительно связаться с банком и действовать по его инструкциям.

«Администратор лотереи». Суть схемы очень проста: вербовщик под видом работодателя нанимает человека для технической работы: распределения денежных призов между «победителями» лотереи. Фактически нанятый человек (дроппер) становится конечным звеном, который легализует украденные у других жертв деньги, переводя их преступникам под видом «выигрышей». В реальности поступившие на карту дроппера деньги – это средства, собранные с десятков обманутых людей (например, через фейковые онлайн-магазины, инвестиционные схемы, взломы), а карты «победителей» – это счета других дропперов, подставных лиц или напрямую мошенников. Таким образом, дроппер дробит и «очищает» преступный поток, делая его отслеживание для банков и правоохранительных органов сложнее.

«Социальные сети». Как уже сообщалось ранее, ИИ активно применяется для таргетированного (целевого) поиска подходящих людей с релевантным психологическим укладом. В качестве примера можно привести поиск человека, который в постах или обсуждениях жалуется на нехватку денег, ищет работу, состоит в группах типа «Подработка», «Быстрые деньги» и др. или активно участвует в розыгрышах. Когда человек найден, ему поступает сообщение от аккаунта с фотографией привлекательной девушки или мужчины (фотографии, разумеется, украдены), при этом аккаунт выглядит живым: есть добавленные друзья, загруженные фотографии, репосты. Сообщения могут содержать предложения о работе или, например, о помощи:

– «Привет! Видела твой комментарий, что ищешь подработку. Мы как раз ищем ответственных людей для удалённого сопровождения платежей в социальных проектах. Официально не оформляем, но платим сразу. Если интересно, расскажу подробнее. Пиши сюда…»

– «Здравствуйте! Обращаюсь к Вам как к активному и, судя по профилю, адекватному человеку. Мы собираем средства для детского хосписа. Нужен

волонтёр на 2–3 часа в день, чтобы оперативно принимать небольшие пожертвования от людей через СБП и аккумулировать их на одном счёте. Есть небольшое вознаграждение. Это спасёт жизни. Можете помочь?»

Далее, если человек отвечает на это сообщение, вербовщики вовлекают его дополнительно, делая акцент на легальности работы, детализируя легенду. Сообщение вербовщика на примере легенды «Администратор платежей» для стримера или блогера может выглядеть следующим образом: «Я продюсер популярного стримера. Ему постоянно донатят (жертвуют деньги) зрители, но, если получать всё на его карту, банк заблокирует счёт из-за огромного количества входящих переводов от разных лиц. Поэтому мы распределяем поток по картам ассистентов. Ты будешь получать донаты, удерживать 10%, а остальное переводить на наш основной счёт. Мы предоставим тебе график и скриншоты из стрима для сверки».

Подобные примеры можно продолжать бесконечно. Они разнообразны и часто заманчивы. Однако ни одна легальная организация не будет переводить деньги неизвестного происхождения на карту случайного человека из соцсетей для дальнейших манипуляций. Такие предложения – 100% мошенничество.

Правила безопасности

Помните, что за участие в схемах легализации денежных средств, добытых преступным путем, в Российской Федерации могут быть применены сразу несколько статей уголовного кодекса:

- 174 УК РФ «Легализация (отмывание) денежных средств или иного имущества, приобретённых другими лицами преступным путём»;
- 159 УК РФ «Мошенничество»;
- 187 УК РФ «Неправомерный оборот средств платежей».

Все это говорит о том, что дропперство – это все же не «лёгкий заработок», а уголовно наказуемая деятельность, караемая реальными сроками лишения свободы. При этом вышеупомянутая законодательная база позволяет

привлекать к ответственности как организаторов, так и рядовых исполнителей, которые своими действиями (или бездействием) способствовали совершению преступлений.

Важно помнить, что ничего бесплатного и легкодоступного без обратной стороны медали не существует, поэтому любые предложения о работе с якобы легким и быстрым заработком должны оставаться без внимания. При этом на примерах, приведенных выше, мы видим, что разговор в социальной сети может начаться с непринужденной беседы, плавно перетекающей в необходимость предоставления персональных данных, в том числе, сведений о банковской карте, или вовсе передаче данных, необходимых для доступа в банковское приложение третьим лицам.

Если все же случилось так, что вы обнаружили признаки вербовки, то:

1. немедленно прекратите все контакты;
2. ничего не переводите. Если вам уже перевели деньги, ни в коем случае не снимайте и не переводите их дальше;
3. заблокируйте карту. Если вы уже передавали реквизиты или получали подозрительные переводы, позвоните в банк и заблокируйте карту, объяснив, что на неё поступили сомнительные средства;
4. сохраните переписку. Сделайте скриншоты переписки, номеров телефонов, реквизитов. Они могут понадобиться полиции;
5. обратитесь в правоохранительные органы.

Раздел 3. Актуальные мошеннические схемы использования криптовалют

История криптовалюты начинается с 3 января 2009 года, именно тогда был сгенерирован первый блок сети Bitcoin, который в январе 2026 года отметил свое 17-летие. Когда-то криптовалюта была экспериментом, который спустя годы стал частью мирового финансового сектора.

Криптовалюта представляет собой форму цифровых денег. Эмиссия, то есть их выпуск и оборот, не зависят от государственных институтов или банков. Криптовалюта функционирует на так называемой базе блокчейна. Так как криптовалюта децентрализована, то есть нет единого центра управления, то и информация обо всех операциях с данными типами валют распределена на множестве компьютеров по всему миру. Простыми словами, блокчейн можно себе представить в виде таблицы с записями обо всех когда-либо совершенных транзакциях между всеми участниками, которая хранится на каждом компьютере, подключенном к сети. Следовательно, для того, чтобы смошенничать и, например, отменить вчерашний перевод другу, придется подключиться к каждому компьютеру и внести изменения в той самой таблице, а точнее полностью ее переписать, что практически невозможно, так как в сети огромное количество независимых компьютеров.

Создание (выпуск) криптовалюты сегодня организовать технически достаточно просто, поэтому на начало 2026 года насчитывается несколько тысяч криптоактивов. Однако основными криптоактивами все же являются Bitcoin, Ethereum, Tether, Binance Coin и другие, поскольку именно они занимают 85–90% всего рынка. Оставшиеся 10–15% – это проекты с очень маленькой капитализацией, низкой ликвидностью или вообще неактивные. Многие создаются для спекуляций, шуток (мемкоины) или конкретных узких задач.

Доходность Bitcoin за счет роста его стоимости феноменальна с момента его основания, поскольку в начале своего пути он стоил меньше 1 цента США,

а его исторический пик приходился на октябрь 2025 года – на уровне 126,2 тыс. долларов США за биткоин.

В любых инвестициях, в том числе и с криптоактивами, важно понимать, что доходность в прошлом не гарантирует доходности в будущем. Например, если рассмотреть его месячную доходность в 2025 году, то мы увидим, что в течение 6 месяцев его стоимость была отрицательной, при этом важно отметить его волатильность: от –2,3% в марте до –17,67% в ноябре. В результате к концу 2025 года стоимость биткойна снизилась почти на 8% относительно начала января, до $87 160,08 на конец торгового дня 29 декабря того же года[13]. Если посмотреть на его историческую волатильность, то она составляла на коротком сроке порядка 10–30%, после резких взлетов часто случались коррекции и наоборот.

Вместе с тем в 2026 году биткоин – один из самых популярных активов в мире, всерьез рассматриваемый финансовыми организациями и даже государствами: от Сальвадора и Бутана до США, где сформировали госрезерв биткоина[14].

Стоит обратить внимание, что помимо криптоактивов существуют еще цифровые валюты. В разных источниках информации под цифровыми валютами подразумевают в том числе и криптоактивы. Мы же рассмотрим данный термин на примере цифровой формы российской национальной валюты. По сведениям ЦБ РФ, цифровой рубль – это цифровая форма рубля. В настоящее время в России существуют наличная (банкноты и монеты в кошельках) и безналичная (деньги на счетах в банках) формы национальной валюты, а в дополнение к ним появится еще и цифровая. Цифровые рубли будут храниться на счетах цифрового рубля (цифровых кошельках) граждан и

---

[13]Обзор рынка криптовалют. Почему криптовалютный рынок завершает год в минусе//Коммерсант.Инвестиции.30.12.2025.URL://http://www.kommersant.ru/doc/8335648?ysclid=mjzuox1u5p49491307

[14] Биткоину исполнилось 17 лет//РБК.03.01.2026.URL:// https://www.rbc.ru/crypto/news/694ea0e39a79477ff9a91f40?ysclid=mjzu0a7o95499260960

организаций. Счета цифрового рубля, в свою очередь, будут открываться на платформе Банка России, где и будут совершаться операции с цифровыми рублями. При этом доступ к счетам цифрового рубля будет возможен через привычные дистанционные каналы: мобильные приложения банков и интернет-банки[15]. Исходя из данной информации сразу заметно первое важное отличие цифрового рубля от криптовалюты, которая, как уже сообщалось ранее, является децентрализованной, то есть ее оборот и эмиссия не контролируются ни государствами, ни банками, чего нельзя сказать о цифровых валютах, которые является централизованными, то есть подконтрольными государствам и финансовым институтам. Помимо этого, криптовалюта во многих странах не является средством платежа на законодательном уровне, а рассматривается лишь как актив, имущество, товар.

Конечно, важно отметить такой важный аспект как безопасность с точки зрения анонимности, ведь криптовалюту можно назвать псевдонимной – она привязывается к публичному адресу кошелька, что, конечно же, привлекает злоумышленников. В то время как цифровой рубль регулируется обязательной процедурой KYC (Know you customer) или «Знай своего клиента», целью которой является предотвращение мошенничества, отмывания денег и финансирования незаконных действий.

По некоторым данным, в 2024 году переводы на криптокошельки, связанные с преступной деятельностью, составили 0,14% от всех блокчейн-транзакций, годом ранее эта доля составляла 0,61%[16]. Вместе с тем, по сведениям этого же источника, сообщается, что множество преступных группировок, в том числе транснациональные организованные преступные группировки, все чаще используют криптовалюту для совершения

[15] Цифровой рубль//ЦБ РФ.24.12.2025.URL:// https://cbr.ru/fintech/dr/

[16] Более $40 млрд в криптовалютах было получено незаконно в 2024 году//РБК.16.01.2025. URL://https://www.rbc.ru/crypto/news/6788d1249a7947c7393ae148?ysclid=mk0vvqopej809733382&from=copy

традиционных преступлений, таких как незаконный оборот наркотиков, азартные игры, кража интеллектуальной собственности, отмывание денег.

Отдельное внимание стоит уделить финансовым пирамидам в целом и с использованием криптовалюты в частности. Так, по сведениям ЦБ РФ, в январе – июне 2025 года Банк России выявил 4183 субъекта (компаний, проектов, индивидуальных предпринимателей и др.) с признаками нелегальной деятельности, в том числе, с признаками финансовых пирамид. Это почти на 20% больше, чем за аналогичный период прошлого года, но на 24% меньше по сравнению со вторым полугодием 2024 года. Продолжает увеличиваться доля мошеннических проектов, использующих криптовалюты и как способ привлечения средств пользователей, и как актив, инвестиции в который гарантируют быстрый доход[17]. Также ЦБ РФ сообщает, что на фоне снижения доверия к инвестированию в иностранные ценные бумаги мошенники стали активнее вовлекать заинтересованную аудиторию, в основном из соцсетей, к игре на разнице курсов криптовалют. Очевидно, что и здесь злоумышленники для большего охвата потенциальных жертв активно используют ИИ, помогающий найти подходящих на эту роль людей на просторах сети Интернет (сетевые игры, социальные сети, каналы в мессенджерах, тематические форумы и прочее).

Финансовая реальность молодых людей радикально отличается от опыта их родителей. На смену очередям в банках и обменниках пришли несколько иконок на смартфоне. Для многих теперь криптокошелёк, та или иная социальная сеть/мессенджер, маркетплейсы – все это стало естественной средой, где инвестиции становятся рутиной, а операции с цифровыми активами – не сложнее установки игры.

[17] Противодействие нелегальной деятельности на финансовом рынке//ЦБ РФ. 05.08.2025. URL:// https://cbr.ru/analytics/inside/2025_1/

Рассмотрим некоторые схемы с использованием криптоактивов и ИИ.

«Мошеннический p2p треугольник». На онлайн-площадке по продаже бывших в употреблении товаров, в социальной сети или мессенджере мошенник размещает объявление о продаже чего-либо, например, смартфона, по цене, как правило, ниже рыночной. Жертва соглашается оплатить товар, здесь и происходит самый важный момент: вместо своих реквизитов мошенник предоставляет реквизиты peer 2 peer (p2p) трейдера криптоактивов. В это же время мошенник открывает ордер на покупку криптовалюты у трейдера на бирже, а покупатель, переводя деньги трейдеру, уверен, что переводит деньги продавцу за телефон. В результате покупатель остается без денег и телефона, мошенник на свой счет получает перевод криптовалюты от трейдера, а тот, в свою очередь, ничего не подозревая, получает угрозу попасть под уголовное преследование, если покупатель подаст соответствующее заявление в полицию, поскольку именно на его карту поступили денежные средства от потерпевшего. Разумеется, для большего охвата злоумышленники активно применяют ИИ, поскольку сегодняшние технологии позволяют ИИ выстраивать алгоритмизированный диалог с потенциальной жертвой, с учетом ответов последней. Кроме того, ИИ способен вести диалоги сразу с неограниченным кругом лиц.

Для минимизации рисков стоит использовать только известные p2p платформы и следить за рейтингами контрагентов. Также желательно выбирать сделки с популярными способами оплаты, где легко подтвердить транзакцию. Продавцам товаров же лучше пользоваться соответствующими проверенными и известными платформами.

Скам SQUID криптовалюта. Токен Squid был создан в конце октября. Разработчики обещали, что его можно будет использовать в онлайн-игре по одному очень популярному сериалу. Всего за два дня криптовалюта аномально выросла на целых 44 000%. Об этом писали крупные мировые СМИ. К 1 ноября Squid уже стоила 2860 долларов за штуку, а днем она резко

обесценилась до нуля. Сайт и соцсети разработчиков оказались заблокированы. Всего мошенники вывели свыше 3 млн долларов, в валюту вложились больше 40 000 человек[18]. Криптоинвесторов должно было насторожить многое: невозможность продать данный токен, отсутствие листинга (размещения) токена на крупных и известных криптобиржах, наконец, грамматические и орфографические ошибки на сайте проекта.

Важно помнить, что подобных проектов может быть много, поэтому перед тем, как решить принимать ли в них участие, необходимо получить как можно больше любой информации, в том числе об их создателях.

Финансовая пирамида Bitconnect. Bitconnect – вероятно, один из самых печально известных и масштабных криптовалютных скам-проектов в истории, действовавший с 2016 по 2018 годы. Он был классической финансовой пирамидой с элементами Понци, искусно замаскированной под инновационную криптоплатформу. Инвесторам обещали астрономическую прибыль при минимальным рисках, так как во главе угла якобы стоял торговый робот на базе искусственного интеллекта. Однако сердцем пирамиды являлась реферальная программа: приглашая новых участников, инвестор получал 7–15% от их вкладов, помимо обещанного 1% в день. Деньги новых инвесторов шли на выплаты «прибыли» старым, на реферальные бонусы и в карманы организаторов. Никакого торгового робота не существовало. Пострадавшими в результате данной финансовой пирамиды являлись граждане более чем из 40 стран, которые понесли убытки на сумму свыше $17 млн[19].

Финансовая пирамида Финико. Финансовая пирамида Финико появилась в РФ в г. Казань еще в 2019 году и обещала избавить жителей от

[18] Криптовалюта «Игры в кальмара» оказалась фейком. Вкладчики потеряли более $3 млн // БФМ.02.11.2021.URL:// https://www.bfm.ru/news/485082

[19] Жертвы криптопирамиды BitConnect получат возмещение на сумму $ 17 млн // РБК.13.01.2023.URL://https://www.rbc.ru/crypto/news/63c0feab9a79474a0596ca84

кредитов. Как уверяли создатели, их ключевая компетенция – это уметь зарабатывать на различных фондовых рынках, и для того, чтобы снизить абсолютно все риски, они разработали соответствующие математические модели, то есть должен был использоваться ИИ. Отличительной особенностью данной финансовой пирамиды было наличие различных программ, например, были программы, с помощью которых можно было купить квартиру или машину за 35% от их стоимости, а можно было просто открыть депозит под 20–30% в месяц. Вероятно, именно это повлияло на высокую популярность схемы среди граждан. Стоит отметить, что счет в данной программе нельзя было пополнить фиатными деньгами, поскольку все операции совершались в биткоинах и криптовалюте Tether. Это было важным моментом в судебном процессе, поскольку денежные средства в привычном для нас виде от населения получать организация не имела права, так как на это требуется соответствующая лицензия ЦБ РФ, а криптовалюта – это не деньги.

Правила безопасности

В РФ, чтобы предупредить граждан и снизить риски вовлечения в незаконную деятельность, на сайте Банка России ежедневно обновляется список компаний с выявленными признаками нелегальной деятельности на финансовом рынке: признаками «финансовой пирамиды», нелегального кредитора, нелегального профессионального участника рынка ценных бумаг (в том числе нелегального форекс-дилера) и иных нелегальных участников финансового рынка. Участник рынка для предоставления большинства финансовых услуг на территории Российской Федерации должен иметь лицензию Банка России или быть включенным в его реестр. Проверить это можно в справочнике финансовых организаций. Если это условие не соблюдается, то, скорее всего, организация ведет деятельность нелегально, а

потребители могут быть обмануты[20]. Сайт для проверки – https://cbr.ru/inside/warning-list/.

Помимо этого, следует обращать внимание на следующие признаки финансовых пирамид:

- нереалистичные обещания: большая доходность, в разы опережающая любые легальные аналоги, особенно подкреплённая гарантиями – это универсальная и главная приманка любой пирамиды;
- привлечение новых участников или реферальная программа: выплаты новым вкладчикам за счет денег старых – классический признак;
- отсутствие лицензии: нет лицензии ЦБ РФ на финансовую деятельность (страховую, инвестиционную);
- агрессивная реклама: давление, срочность («только сегодня!»);
- непрозрачность: нет информации о руководстве, регистрации, отсутствие официальных документов;
- прием наличных: отказ от официального оформления, прием денег наличными или в криптовалюте без документов.

Главное всегда помнить: бесплатный сыр только в мышеловке!

[20] Список компаний с выявленными признаками нелегальной деятельности на финансовом рынке//ЦБ РФ.30.12.2025.URL://https://cbr.ru/inside/warning-list/

Раздел 4. Повторение – мать учения: еще раз о финансовом мошенничестве

Как мы все уже знаем, злоумышленники всегда находятся в поиске информационных поводов и очень хорошо к этой процедуре адаптировались, поэтому будет важно еще раз вспомнить актуальные схемы мошенничества на текущий момент. Важно отметить, что меняются схемы, однако суть остается та же – в приоритете снижение бдительности жертвы и отключение критического мышления.

Рассмотрим наиболее популярные схемы.

Фишинговые онлайн-магазины и не только. Эта схема актуальна круглый год, поскольку у людей всегда есть потребность в покупке чего-либо: от путевок, авиа- и железнодорожных билетов в связи с очередным отпуском или длительными праздниками до банальных покупок в виде продуктов питания. Те пользователи, которые совершают такие покупки через ранее установленные приложения с официальных магазинов того или иного производителя смартфона, защищены, но зачастую, если гражданин решил найти путевки для очередного путешествия и желательно со скидкой через известные поисковики, то в этом случае появляется риск совершить покупку на поддельном (фишинговом) сайте. В этом случае появляется риск не только потерять часть своих денег, но и скомпрометировать свои персональные данные, поскольку на сайтах требуется заполнять такие данные, как ФИО, номер телефона, адрес электронной почты, возможно, паспортные данные, если, например, мы хотим приобрести билет на поезд или самолет, и, конечно же, данные своей банковской карты. Стоит отметить, что чаще всего мошенники подделывают сайты авиакомпаний, банковских и микрофинансовых организаций и страницы авторизации и оплаты Интернет-магазинов.

Правила безопасности

Необходимо:

- совершать покупки через установленные с официальных магазинов производителя телефона приложения;
- при переходе по ссылкам, которые выдал поисковик, удостовериться, что название сайта начинается с «https», а не с «http»;
- убедиться в отсутствии грамматических ошибок на сайте; если они есть, это фишинговых сайт;
- проверить корректность названия сайта в поисковой строке, фишинговые сайты обязательно содержат ошибки;
- не переходить на соответствующие сайты по ссылкам, в том числе из электронной почты;
- не переходить по заманчивым ссылкам из объявлений, размещенных на просторах Интернета;
- использовать антивирусы, дополнительная защита никогда не будет лишней;
- использовать отдельную карту для совершения покупок в сети Интернет, пополнять ее на необходимую сумму перед совершением покупки.

Доставка цветов для кражи «Госуслуг». Мошенники постоянно находят новые информационные поводы для хищения денег, однако они еще и дорабатывают существующие схемы. Данная схема также не осталась без внимания. Теперь мошенники разработали новую двухэтапную схему обмана[21]. Сначала жертве звонят от имени службы доставки букетов и просят назвать код из СМС якобы для сверки заказа с курьером. После этого звонок прерывается сообщением от имени Роскомнадзора о небезопасности.

[21] Мошенники придумали схему с «доставкой букетов» для кражи «Госуслуг»// РБК.08.08.2025. URL://https://www.rbc.ru/rbcfreenews/689578ab9a794714d1a91a79

Затем злоумышленники звонят снова, уже в роли «сотрудников службы», предлагая помочь вернуть доступ к «Госуслугам» и отменить заявку на микрозаем. В это время на телефон приходят четырехзначные коды от имени микрофинансовых организаций, которые мошенники пытаются выманить для входа в «Госуслуги», взлом которых может привести к потере исчерпывающей информации о гражданине РФ.

Правила безопасности

Самое важное правило, применимое ко всем вариантам попыток мошенничества, никто и никогда не будет спрашивать смс-код, к нему следует относиться как к паролю.

Задать себе очевидный вопрос: ждали ли вы доставку цветов? Если нет, то скорее всего это аферисты.

Блокировка банковских карт с применением ИИ. Мошенники научились удаленно блокировать банковские карты, ведь для этого достаточно совершить звонок в call-центр банка и назвать ФИО, дату рождения. А для того, чтобы обман был еще более убедителен, мошенники имитируют голос клиента с помощью нейросетей ИИ. Причиной блокировки может являться все, что угодно, например, потеря карты или ее кража.

После блокировки карты мошенники связываются с жертвой и, угрожая расправой или блокировкой карт родственников и знакомых, вымогают деньги. Они уже демонстрируют «результат» – ваши действительно заблокированные карты.[22]

Правила безопасности

[22] Мошенники массово блокируют банковские карты россиян и вымогают деньги. Как защититься — советы экспертов//Банки.РУ.11.12.2025. URL://https://www.banki.ru/news/daytheme/?id=11020062

Необходимо:

- всегда относиться к ситуации критически, перезвонить для уточнения информации о блокировке карты в call-центр банка (по номеру телефона, указанному на оборотной стороне карты);
- ни при каких условиях не переводить деньги ни на чей счет, а обратиться в отделение банка;
- рассказать родственникам, особенно пожилым, об этой схеме.

В заключение отметим, что последние данные глобального исследования показывают тревожную картину: мошенничество превратилось в массовое явление, а его последствия выходят далеко за рамки финансовых потерь. В 2025 году 57% взрослого населения мира столкнулись с мошенничеством. Среди тех, кто лишился средств, 54% стали жертвами при онлайн-покупках, а 48% пострадали от инвестиционного мошенничества. Особое внимание стоит обратить на психологический урон: 69% испытывают сильный стресс, 17% теряют уверенность в себе, а 14% отмечают ухудшение отношений в семье.

Большинство людей декларирует: «Этого со мной точно не случится». При этом почти каждый четвёртый из этой уверенной группы всё равно теряет деньги, что указывает на серьёзный разрыв между восприятием риска и реальными угрозами. Мошенники совершенствуют тактики, а базовой бдительности порой уже недостаточно. Высокая самооценка собственной осторожности может создавать ложное чувство безопасности, делая человека уязвимым. Все это говорит о том, что необходимо постоянно повышать уровень цифровой грамотности и критического мышления.

Раздел 5. Международная олимпиада по финансовой безопасности

Международная олимпиада по финансовой безопасности – ежегодная олимпиада I уровня, которая проводится по поручению Президента Российской Федерации В.В. Путина. Проведение Олимпиады направлено на повышение информационной, финансовой и правовой грамотности молодого поколения, поиск талантливой молодежи, стимулирование учебно-познавательной и научно-исследовательской деятельности в области финансовой безопасности.

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

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

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

- юриспруденция;
- математика, информационная безопасность и пр.;
- экономика, финансы и кредит, экономическая безопасность;
- международные отношения, зарубежное регионоведение.

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

Олимпиада проходит в несколько этапов:

- тематический урок «Финансовая безопасность»;
- пригласительный этап;
- отборочный этап;
- квалификационный этап;
- финальный этап.

Приложение № 1. Глоссарий

Волатильность (от англ. volatility – «изменчивость», от лат. volatilis — «стремительный», «быстрый») – индикатор рынка ценных бумаг или валюты, который показывает уровень его изменчивости за определенное время.

Дипфейк (deepfake) – это технология создания реалистичных поддельных аудио, видео или изображений с помощью искусственного интеллекта, основанная на «глубоком обучении (deep learning) или подделке(fake).

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 (ИП) 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.

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.

Искусственный интеллект (ИИ) (Artificial intelligence) – это направление науки, которое занимается разработкой компьютерных систем, способных выполнять задачи, свойственные человеческому интеллекту. Сюда входит анализ данных, распознавание образов, обработка текстов и запросов, сформулированных естественным языком, обучение на потоках данных и принятие решений. ИИ базируется на алгоритмах, моделях и технологиях, которые позволяют машинам воспринимать окружающий мир, интерпретировать данные, делать выводы, принимать решения и адаптироваться к изменяющимся условиям.

Криптовалюта – 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 – площадка, на которой торгуются криптовалюты.

Листинг в криптовалюте — это процедура включения токена в список активов, доступных для торговли на какой-либо площадке (чаще всего на бирже).

Реферальная программа – это маркетинговый инструмент, который мотивирует существующих клиентов (рефереров или рекомендателей) привлекать новых клиентов (рефералов).

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).

Транзакция (с лат. transactio) – это любая сделка или операция, для совершения которой используется банковский счет, при этом баланс на нем меняется в меньшую или большую сторону.

Токен — цифровой актив, разновидность криптовалюты, которая имеет определенную ценность и хранится в блокчейне.

Уголовный кодекс Российской Федерации (УК РФ) – основной источник уголовного права и единственный нормативный акт, устанавливающий преступность и наказуемость деяний на территории Российской федерации.

Федеральная служба безопасности Российской Федерации (ФСБ России) – федеральный орган исполнительной власти, в пределах своих полномочий осуществляющий государственное управление в области обеспечения безопасности Российской Федерации, борьбы с терроризмом, защиты и охраны государственной границы Российской Федерации.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, а также функции по организации деятельности радиочастотной службы.

Федеральная служба по финансовому мониторингу (Росфинмониторинг) – федеральный орган исполнительной власти, осуществляющий функции по противодействию легализации (отмыванию) доходов, полученных преступным путём, финансированию терроризма, экстремистской деятельности и финансированию распространения оружия массового уничтожения, по выработке государственной политики и нормативно-правовому регулированию в этой сфере, по координации соответствующей деятельности федеральных органов исполнительной власти, других государственных органов и организаций, а также функции национального центра по оценке угроз национальной безопасности, возникающих в результате совершения операций (сделок) с денежными средствами или иным имуществом, и по выработке мер противодействия этим угрозам.

Федеральный закон Российской Федерации – федеральный нормативный правовой акт Российской Федерации, принимаемый Государственной думой и подписываемый Президентом России в соответствии с Конституцией Российской Федерации по предметам ведения Российской Федерации и по предметам совместного ведения Российской Федерации и ее субъектов.

Фиатные деньги – это выпускаемые государством купюры (банкноты), ценность которых обеспечивается (гарантируется) государством и не зависит от материала, из которого они изготовлены.

Центральный банк РФ (ЦБ РФ, Банк России) – это мегарегулятор, высшее звено банковской системы России, финансовая структура, имеющая исключительное право на выпуск национальной валюты и отвечающая за защиту и обеспечение стабильности рубля

Цифровые финансовые активы (ЦФА) в России – финансовый инструмент, который удостоверяет цифровые права. К таким правам могут относиться, например, денежные требования, владение эмиссионными ценными бумагами, участие в капитале непубличного акционерного общества, требования передачи эмиссионных ценных бумаг. По сути, российские ЦФА представляют собой токенизированные версии реально существующих активов. Выпуск ЦФА осуществляется с применением технологии блокчейн.

Эмиссия – (от фр. Emission – «выпуск») выпуск денег в обращение, ведущий к увеличению денежной массы.

P2P (peer-to-peer) трейдинг — это форма торговли, при которой покупатели и продавцы напрямую обмениваются активами, минуя таких посредников, как банки и централизованные биржи. В криптовалютном пространстве это означает обмен цифровыми валютами между двумя участниками на своих условиях.

Приложение № 2. Ресурсы

1. Билайн создал «Кибербабушку». Как она поможет бороться с телефонными мошенниками? // Lenta.ru. 13.11.2025. URL: https://lenta.ru/articles/2025/11/13/bilayn-sozdal-kiberbabushku/?ysclid=mk5pb3lwx2509443586

2. Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций // ЦБ РФ. 12.02.2025. URL: https://cbr.ru/analytics/ib/operations_survey/2024/

3. МВД раскрыло результаты борьбы с телефонными мошенниками // Lenta.RU. 02.12.2025 URL: https://lenta.ru/news/2025/12/02/mvd-raskrylo-rezultaty-borby-s-telefonnymi-moshennikami/?ysclid=miq22ihex2658176800

4. МВД фиксирует рост числа пострадавших от кибермошенников несовершеннолетних // Коммерсант. 28.06.2025. URL: https://www.kommersant.ru/doc/7851537?ysclid=mitybkryl3160727529

5. Путин подписал закон об уголовной ответственности для дропперов // РИА. 24.06.2025. URL: https://ria.ru/20250624/putin-2025132619.html?ysclid=miu0fzlqlw280946511

6. Как первое уголовное дело против дроповода скажется на работе мошеннической схемы // Коммерсант. 07.08.2025. URL: https://www.kommersant.ru/doc/7943692?ysclid=miu0s6vpbe158946376

7. Эксперт предупредил о новых мошеннических схемах с дипфейками // Известия. 11.06.2025. URL: https://iz.ru/1902358/2025-06-11/ekspert-predupredil-o-novykh-moshennicheskikh-skhemakh-s-dipfeikami

8. Голос как у начальника — не отличишь: как искусственный интеллект позвонил и украл сотни тысяч долларов // Бизнес.ФМ. 04.09.2019. URL: https://www.bfm.ru/news/423702?ysclid=mivres04zq489735366

9. В Италии мошенники украли деньги с помощью ИИ с голосом министра // РБК. 10.02.2025. URL:

https://www.rbc.ru/rbcfreenews/67a9c0499a7947e77f1f612f?ysclid=mj1mdsssip490024673

10. «Любовная переписка с ботом»: на россиян обрушились тонны «романтического скама» // Газета.РУ. 10.11.2025. URL: https://www.gazeta.ru/social/news/2025/11/10/27144032.shtml?ysclid=mj5rmkvcr507205716&updated

11. Число клиентов-дропов в российских банках превысило миллион // РБК. 26.09.2025. URL: https://www.rbc.ru/finances/26/09/2025/68d69e149a79472e16862f06?ysclid=mj640dqn50530339087

12. ЦБ сообщил о доле подростков среди участников дропперских схем // ЦБ РФ. 08.12.2025. URL: https://www.rbc.ru/rbcfreenews/693680f39a79477f253137c2

13. Обзор рынка криптовалют. Почему криптовалютный рынок завершает год в минусе // Коммерсант. Инвестиции. 30.12.2025. URL: http://www.kommersant.ru/doc/8335648?ysclid=mjzuox1u5p49491307

14. Биткоину исполнилось 17 лет // РБК. 03.01.2026. URL: // https://www.rbc.ru/crypto/news/694ea0e39a79477ff9a91f40?ysclid=mjzu0a7o95499260960

15. Цифровой рубль // ЦБ РФ.24.12.2025.URL:// https://cbr.ru/fintech/dr/

16. Более $40 млрд в криптовалютах было получено незаконно в 2024 году // РБК. 16.01.2025. URL: https://www.rbc.ru/crypto/news/6788d1249a7947c7393ae148?ysclid=mk0vvqopej809733382&from=copy

17. Противодействие нелегальной деятельности на финансовом рынке // ЦБ РФ. 05.08.2025. URL:// https://cbr.ru/analytics/inside/2025_1/

18. Криптовалюта «Игры в кальмара» оказалась фейком. Вкладчики потеряли более $3 млн // БФМ. 02.11.2021. URL: https://www.bfm.ru/news/485082

19. Жертвы криптопирамиды BitConnect получат возмещение на сумму $ 17 млн // РБК. 13.01.2023. URL: https://www.rbc.ru/crypto/news/63c0feab9a79474a0596ca84

20. Список компаний с выявленными признаками нелегальной деятельности на финансовом рынке//ЦБ РФ. 30.12.2025. URL: https://cbr.ru/inside/warning-list/

21. Мошенники придумали схему с «доставкой букетов» для кражи «Госуслуг» // РБК. 08.08.2025. URL: https://www.rbc.ru/rbcfreenews/689578ab9a794714d1a91a79

22. Мошенники массово блокируют банковские карты россиян и вымогают деньги. Как защититься — советы экспертов//Банки.РУ.11.12.2025. URL://https://www.banki.ru/news/daytheme/?id=11020062