

06.03.2025

Григорий Осипов: «Россию атакуют мошеники. Что делать?»

Использование искусственного интеллекта и уязвимостей западного ПО, атаки на инфраструктуру и кража персональных данных — главные киберугрозы 2025 года.

Как сообщил ЦБ России, в прошлом году мошенники похитили у граждан рекордную за всю историю наблюдений сумму — 27,5 млрд рублей, что на 74,4% больше, чем в 2023 году. По данным «Лаборатории Касперского», преступники смогли дозвониться до 60% граждан.

Ситуация печальная, потому что годом ранее этот показатель был на уровне 43%. В Госдуме принимают новые законы, стремясь защитить потребителей от мошенников, а банки, не дожидаясь официальных распоряжений, сами «охлаждают» подозрительные переводы, однако ситуация не меняется к лучшему. Какие методы используют киберпреступники, чтобы добраться до кошельков россиян, и почему без решения геополитических вопросов победить мошенников не получится, в интервью BM Moscow Foresight рассказал директор по расследованиям платформы безопасности цифровых активов «ШАРД» Григорий Осипов.

Согласно информации МВД, только за первые семь месяцев 2024 года было совершено 577 тыс. преступлений в информационно-телекоммуникационной сфере, из которых более половины —хищения и мошенничества, которые осуществляются в основном с использованием криптовалют.

В прошлом году ряд популяных криптомонет вырос в цене. В связи с этим практически пропорционально увеличилось и число преступлений, особенно инвестиционных мошенничеств. Люди больше «клюют» на аферистов в состоянии упущенной возможности заработать, чем с радостью пользуются преступники. Практика эффективного расследования таких преступлений только формируется, и необходимый инструментарий и навыки для этого пока есть не у всех представителей МВД.

Надо также признать, что человек, оказавшийся жертвой мошенников с криптовалютой, часто даже не знает, к кому обратиться, так как на рынке много аферистов, лжеюристов и разных псевдопомощников.

Как отличить инвестиционное мошенничество от других видов преступлений?

Инвестиционным следует считать такой вид мошенничества, когда преступники под разными предлогами — помощи в выводе средств, получении образования — затягивают потенциальную жертву в псевдоинвестиционный проект, обещая заработки, связанные с «работой на связках курсов валют», «торговлей ценными бумагами и криптовалютами», «вложением в новую перспективную монету». Участие в таких проектах для потерпевшего всегда заканчивается тем, что он теряет свои деньги.



Вы сталкивались с жертвами таких преступлений?

Конечно. Так, в прошлом году к нам обратился мужчина, который сначала просто искал в интернете образовательные курсы по криптовалютам, однако в результате был убеждён мошенниками вложить средства в прибыльный псевдокриптовалютный проект. Аферисты смогли затуманить его внимание. Ему показывали криптокошелек, в котором множество монет, в том числе и «фейковые», росли в цене.

Потерпевший радовался сначала, что его «сумма инвестиций» выросла вдвое. Мошенники же вывели его деньги и решили «развести» жертву ещё раз. Они сообщили ему о блокировке счетов за вывод средств из-за «незаконной деятельности». Когда же пострадавший заявил им, что денег у него больше нет, они предложили ему отправить определённую сумму на банковскую карту. На эти средства он должен был купить криптовалюту в обменном сервисе и отправить мошенникам для разблокировки.

В этом примере потерпевший послушался мошенников и, получив деньги на банковскую карту от других обманутых граждан, стал сам соучастником мошеннической схемы.

Какие ещё модели использовалось в 2024 году для обмана граждан?

Одним из видов инвестиционного мошенничества совершенно справедливо считаются финансовые пирамиды. Они практически переживают ренессанс. Так, по информации Банка России, в 2024 году официально в эту категорию было отнесено 4772 организаций. Для понимания, в 2023-м их было 2226 штук, а в 2022-м — 1961.

Самое общее представление о финансовой пирамиде — это организация, которая выплачивает деньги вкладчикам за счёт средств других участников, которые инвестировали в пирамиду позже. Говоря языком финансистов, использует «схему Понци» (название идёт от американского аферист Чарльза Понци, который впервые реализовал эту схему в 1920-х годах — *прим.ред.*).

Есть какие-то яркие примеры современных пирамид?

В прошлом году была пресечена деятельность Sincere Systems Group LTD. Ущерб от её работы специалисты оценили в $100 млн.

Следует отметить, что, по нашим данным, а также информации ЦБ РФ, в 2024 году более 70% финансовых пирамид привлекали средства в криптовалюте. Это связано с особенностями самой крипты — псевдоанонимностью, сложностью отслеживания транзакций и недостаточной зрелостью регулирования этого рынка. Кроме того, практически все проекты вовлекают граждан в свои сети через интернет с помощью популярных мессенджеров и соцсетей.

Сколько денег им удаётся выманить у россиян?

Большие финансовые пирамиды, такие как «Финико», «S-Group» или «Amir Capital», выудили из кошельков своих жертв сотни миллионов долларов, в то время как в 2024 году новые подобные проекты часто не могли собрать столь крупные суммы: их «средний чек» намного меньше. Однако число мелких проектов увеличилось, и общий ущерб также вырос.

Кроме того, в таких финансовых пирамидах преступники используют более сложные и технологичные методы, включая создание собственных криптовалют и токенов, агрессивную рекламу и привлечение реферальных систем, то есть каких-то партнёрских каналов, внешне вроде занимающихся честным бизнесом, что помогает им быстро набирать аудиторию.

Долго ли может существовать такая пирамида?

В последнее время новые проекты функционируют всего 2-4 месяца. Они быстро набирают свою аудиторию и нужный объём средств, а затем прекращают деятельность. Однако не всегда делают это одномоментно, в связи с чем нет множества обращений от пострадавших в полицию. Здесь я хочу подчеркнуть, что все участники подобных проектов подвергаются поэтапной психологической обработке. Их постоянно приучают находиться в состоянии ожидания прибыли. Иногда человек живёт несколько месяцев в уверенности, что его средства сами вернутся, либо что-то изменится, и не обращается в полицию.

Организаторы криптовалютных пирамид зачастую используют непрозрачные международные каналы и анонимные

криптовалютные сети, что значительно усложняет задачу их поимки для сотрудников МВД.

Обычно, когда ведут речь о мошенниках, в первую очередь рассказывают о звонках из «службы безопасности Сбербанка», «Следственного комитета», «МФЦ», «ФСБ» и т.д. Социальная инженерия актуальна?

Тип мошенничества с так называемым «безопасным счётом» по-прежнему остаётся самым массовым и по количеству получивших такие звонки, и по объёму потерь. Речь идёт о преступлениях, когда в ходе телефонного разговора аферисты убеждают доверчивых россиян переводить свои деньги на «безопасный» или «спецсчёт», чтобы якобы спасти средства от кражи. Мошенники используют классическую схему социальной инженерии, но с новыми элементами. Преступники сначала связываются с потенциальной жертвой, обычно через телефонный звонок или сообщения, и заявляют, что с её счёта была предпринята попытка несанкционированного списания средств и проводится спецоперация по поимке мошенников.

Чтобы «спасти» накопления, аферисты предлагают перевести средства на так называемый «безопасный счёт», который якобы принадлежит «Центробанку», «Росфинмониторингу» или любому другому ведомству.

Преступники уверяют, что это «временная мера», пока полиция ищет жуликов, а деньги будут возвращены после того, как злоумышленники будут пойманы. При этом в качестве такого «безопасного счёта» выступают банковские карты третьих лиц, на которые «жертва» переводит свои средства, а мошенники чаще всего сразу отправляют средства с таких карт для покупки криптовалюты и выводят украденные деньги за рубеж.

Для большего эффекта они требуют от жертвы не разглашать информацию о происходящем, вообще запрещают с кем-либо обсуждать эту тему, пугая, что за это якобы предусмотрена уголовная ответственность. Такое мошенничество бывает многоролевым: сначала с потенциальной жертвой связываются от лица сотрудника полиции, затем от лица представителя Росфинмониторинга или Банка России.


Earn
Square
More
TRUMP/USDT
OFFICIAL TRUMP Price
54.70
$54.70
24h Change
-18.16 -24.92%
24h High
77.24
24h Low
37.35
24h Volume(TRUMP)
177,000,853.52
10,202,71
Chart
Info
Trading Data
Square
Time
1s
15m
1H
4H
1D
1W
2025/01/20 11:25:20 Open: 54.70 High: 54.70 Low:
55.32
MA(25): 54.76
Order Book
0.01
Price (USDT)
Amount (TRUMP)
Total
54.83 529.691 29.04K
54.82 279.367 15.31K
54.81 613.156 33.61K
54.80 356.740 19.55K
54.79 797.898 43.72K
54.78 417.498 22.87K
54.77 532.753 29.18K
54.76 531.587 29.11K
54.75
54.74

А были ли какие-то нестандартные решения, которые использовали мошенники при взаимодействии с жертвами в прошлом году?

Разумеется. Так, одной из интересных схем стали романтические мошенничества. Это разновидность инвестиционного мошенничества, когда жертву — обычно это состоятельная женщина — жулик-участник преступной схемы обманывает, вовлекая в эмоциональную связь. Он создаёт видимость «настоящей любви», постепенно завоевывая доверие пострадавшей. Как только эта «связь» налажена, преступник начинает использовать доверие, предлагая перевести криптовалюту под различными ложными предлогами. Например, могут быть выдуманы истории о неотложных семейных проблемах или предложены «выгодные» инвестиции, которые на самом деле не существуют.

К вам обращались такие пострадавшие?

В прошлом году к нам за помощью пришла замужняя неработающая женщина с ребенком. Она познакомилась в соцсетях с мужчиной, который после нескольких недель общения предложил инвестировать в криптопроект. Однако мошенник для создания стимула траты денег в большем объёме целенаправленно романтизировал отношения, перевёл их в формат общения между влюбленными, строящими совместные планы, которым суждено сбыться только при инвестировании в предлагаемый проект. Для реализации задуманного использовалось давление, психологические манипуляции финансовой зависимостью от мужа, благополучием ребёнка. Одновременно преступник уверял, что якобы сам вносил в этот проект большую часть средств. Женщина, которая общалась с мошенником, по рекомендации своего нового возлюбленного на протяжении трёх месяцев вносила средства мужа на сервис–кошелек и под контролем аферист якобы зарабатывала средства. Для повышения доверия преступник один раз даже позволил вывести небольшую сумму, однако после этого капкан захлопнулся, и жертва потеряла огромные деньги, а впоследствии и семью.

И много таких печальных историй в России?

Точной статистики нет, но я могу поделиться своими наблюдениями: хоть романтические мошенничества и стали набирать популярность среди аферистов в прошлом году, но на общем фоне их доля остается очень незначительной.

А о каких-то массовых проектах можете рассказать?

Яркий пример здесь — мошенничество с играми-«тапалками». Так называются простые мобильные «игрушки», которые основываются на механике постоянного нажатия на экран — тапа — для выполнения действий, зарабатывания очков или внутриигровых валют. Такие игры часто имеют элемент цикличности, где основной задачей игрока является непрерывное взаимодействие с экраном, например, путём тапания по кнопкам или объектам на экране. Игры этого жанра весьма популярны среди детей и молодёжной аудитории из-за своей простоты.

Беда в том, что с увеличением популярности мобильных игр аферисты стали использовать этот жанр для реализации различных преступных схем, особенно нацеленных на неопытных пользователей. Мошенники обещают, что криптовалюту, заработанную в игре, игрокам можно будет обменивать на реальные деньги. Но на практике эта криптовалюта не имеет реальной стоимости и не может быть использована на реальных торговых платформах. А ещё преступники создают поддельные сайты и приложения, имитирующие популярные криптовалютные игры, такие как Hamster Kombat — знаменитого «хомяка», которого нужно «тапать». Эти сайты обещают игрокам прибыль за простое нажатие на экран, а на самом деле используют такие ресурсы для кражи данных криптовалютных кошельков.

Власти постоянно принимают законы, направленные на защиту от мошенников. Многие банки уже по собственной воле ввели периоды «охлаждения», чтобы защитить клиентов. В прессе регулярно освещают проблему мошенничества, однако объём подобных преступлений продолжает расти. Почему?

Главная проблема здесь в том, что мошенничество стало целым отдельным направлением информационной войны против России. После начала СВО в феврале 2022 года, резко увеличилось число взломов информационных систем российских компании: в открытый доступ попали персональные данные и банковские реквизиты десятков миллионов соотечественников, которые до сих пор активно «отрабатывают» мошеннические группировки.

Как изменились действия преступников за прошлый год?

В банковском секторе мошеннические схемы стали сложнее, более продвинутыми, активно используются манипуляции и информационное давление, а механизмы таких преступлений более технологичные. Всё это указывает на стратегический подход преступников: фактически это системный бизнес, который идёт в основном с Украины и существует при поддержке правоохранительных органов, в том числе и СБУ.

Участвуют ли в этом представители других стран?

С течением времени ситуация ухудшилась. Если в начале спецоперации практически все преступления такой категории совершались со стороны Украины, то сейчас те же колл-центры, действуют в том числе и на территории России и стран СНГ. То же самое касается и вектора атак банковской инфраструктуры.

Почему так мало пойманных киберпреступников?

Оказалось, что, при всей их сложности, современные технологии позволяют злоумышленникам оставаться трудно идентифицируемыми. Так, мошенники используют одноразовые учётные записи в социальных сетях, чужие фотографии, искусственный интеллект позволяет генерировать даже изображения для видеозвонков. Оплату мошенники принимают либо через криптовалюту напрямую, либо на карты третьих лиц, которые её продают. Пока полностью исключить возможность совершения оплаты на карту от третьего лица остаётся невозможным.

Борьба с такими явлениями осложняется ещё и политическими аспектами, влияющими на сложность пресечения деятельности таких мошенников. Без взаимодействия с правоохранительными органами Украины трудно точно отслеживать и блокировать преступные схемы, если они выводятся на их территорию в криптовалюте и на банковские карты.

Конечно, сложность проблемы заключается не только в быстром развитии новых форм мошенничества, но и в том, что преступники адаптируются к изменениям в законодательстве и совершенствуют свои методы.

Что могло бы помочь сократить объёмы мошенничества в России?

В настоящее время борьба с киберпреступлениями — это политический вопрос, поскольку это часть активной информационной войны. Как только в первом вопросе будет какая-то ясность, мошенничества пойдут на спад.

Вторая проблема, которая очевидна, — это, как ни странно, вопрос доверия. Большинство людей, которые подверглись мошенничеству, совершаемых от лиц государственных органов, всё ещё верят в порядочность, неподкупность «службы безопасности банка», «сотрудника Росфинмониторинга» и «офицера спецслужб» и т.д. При этом часть населения, особенно старшего поколения, не доверяет и не понимает преимущества цифровых технологий. С учётом этого нужно скорректировать информационно-пропагандистскую политику в этой области.

Третья проблема — слабая собственная инфраструктура и использование большого числа иностранных мессенджеров, программ, мобильных телефонов, уязвимости которых хорошо известны и активно эксплуатируются мошенниками. Правильным решением тут будет переход на отечественное программное обеспечение (ПО) и такие же решения обеспечения их безопасности.

По вашим прогнозам, в результате действия всех принятых антимошеннических законов, к концу 2025 года объём мошенничества снизится или нет?

Информационное поле пока достаточно открытое, а возможности использования банковских карт третьих лиц и криптовалюты, повсеместно установленное зарубежное ПО в среднесрочной перспективе пока дают возможности по увеличению числа таких мошенничеств концу 2025 года.

В случае, если политическая ситуация стабилизируется, заработает международное сотрудничество и новые законодательные барьеры для мошенников будут эффективно внедрены, то при повышении уровня осведомленности о мошенничествах среди граждан в более долгосрочной перспективе ситуация будет улучшаться.

Каковы главные вызовы в сфере киберпреступлений в 2025 году?

Отмечу три явных угрозы. Во-первых, это атаки на инфраструктуру. Сюда относятся попытки поразить энергетику, транспорт, воду и системы здравоохранения. Подобные нападения уже были, но в 2025 году этот тренд может усилиться. Атаки на критическую инфраструктуру способны не только вызвать сбои в работе важных объектов, но и нанести серьёзный экономический ущерб, а также создать угрозу для национальной безопасности.

Вторая опасность — это рост угрозы со стороны искусственного интеллекта (ИИ) и автоматизированных атак. ИИ и машинное обучение становятся мощными инструментами как для киберпреступников, так и для национальных разведывательных служб. В 2025 году возможно массовое ведение автоматизированных атак с их использованием, таких как фишинг с помощью дипфейков, генерация ложных данных или обход многократной аутентификации.

Третья угроза — глобальные кибервойны между странами. Кибервойна становится неотъемлемой частью глобальной геополитики.

В 2025 году можно ожидать усиление государственных кибератак, направленных на вмешательство во внутренние дела других стран, воздействие на выборы, разрушение национальных экономик или дестабилизацию общества. Кибершпионаж, кибертерроризм и атаки на финансовые системы могут стать частью более масштабных стратегий противостояния.

Как людям в таких условиях защитить свои сбережения?

Вспомним лозунг «Знание — сила!». Если вы хотите защитить свои сбережения, вкладывайте их в те сферы, в которых есть понятные механизмы проверки, соблюдайте принципы диверсификации средств, развивайте цифровую грамотность. Помните, мошенники постоянно совершенствуют свои схемы. Вы тоже критично относитесь к заманчивым предложениям любой рекламы? Так и здесь нужно поступать! Зачастую тонкое место в системе защиты — это человек, который, под влиянием мошенников, сам переводит им свои средства, обойдя установленные им же и «умным» программным обеспечением способы защиты.

Анна СОЛНЦЕВА