Мошенничество в сфере платежных инструментов и сервисов в 2024 году:

общая статистика и тенденции

Банковский Процессинговый Центр

Содержание:

Отчет подготовлен ОАО «Банковский процессинговый центр» на основании имеющейся информации по операциям с банковскими платежными карточками. Данные не охватывают всю территорию Республики Беларусь, однако, учитывая долю рынка ОАО «Банковский процессинговый центр», могут свидетельствовать об основных тенденциях в Республике Беларусь.

Общая информация:

В 2024 году основная доля мошенничества в Республике Беларусь приходилась на мошенничество с банковскими платежными карточками в среде без физического присутствия карточки при проведении операции. Случаев установки скимминговых устройств и массовой компрометации данных держателей карточек на территории Республики Беларусь в 2024 году зафиксировано не было.

Эмиссия (данные по операциям с банковскими платежными карточками, выпущенными банками, которые обслуживаются в ОАО «Банковский процессинговый центр»):

Характерными тенденциями 2024 года являются мошенничество с использованием реквизитов карточек, социальная инженерия, а также единичные случаи мошенничества по поддельным карточкам и утерянным/украденным карточкам. Основная доля мошенничества с использованием реквизитов карточек приходится на e-commerce – около 70%. Высокий уровень e-commerce мошенничества свидетельствует о том, что злоумышленниками все чаще используются автоматизация процессов, машинное обучение и искусственный интеллект. При этом значительная доля мошенничества приходится и на методы социальной инженерии, которые приносят злоумышленникам высокий доход при минимальных финансовых затратах. Мошенники стремятся получить личные данные держателей карточек, доступы к их счетам, системам дистанционного банковского обслуживания, МСИ и мобильным устройствам.

Генерация тестовых операций и атаки на БИН банков - процесс инициирования 1-2 тестовых транзакций для проверки карточки с целью ее дальнейшего использования в мошеннических целях, один из наиболее распространённых видов мошенничества в рамках e-commerce в 2024 году. При этом используются программные средства для генерации номеров карточек и база скомпрометированных карточек, а атаки осуществляются в торговых точках электронной коммерции, которые имеют слабые механизмы контроля и защиты от мошенничества.

Активно развивались и использовались схемы мошенничества, связанные с токенизацией скомпрометированных карточек. В рамках данной схемы мошенничества после получения необходимых реквизитов карточки с использованием методов социальной инженерии или фишинговых рассылок, мошенники привязывают карточку на свое мобильное устройство и совершают оплаты в сети Интернет, в организациях торговли и сервиса, снимают наличные денежные средства в банкоматах, которые находятся за рубежом.

В 2024 году для хищений средств держателей и получения персональных данных злоумышленники по-прежнему использовали различные методы социальной инженерии, такие как: звонки от имени работников банков, правоохранительных органов, работников службы поддержки сотовых операторов и других различных организаций; направляли сообщения в социальных сетях и мессенджерах от имени организаторов рекламных акций, почтовых операторов, торговых площадок, под видом знакомых и родственников.

Использовалась схема мошенничества, связанная с установкой приложений удаленного доступа на мобильные устройства держателей, в результате реализации которой злоумышленники получали полный контроль над счетами и денежными средствами держателей.

Участились случаи, когда держатели переходили по фишинговым ссылкам, считая, что это официальные ресурсы банков, почтовых служб и служб доставки, где вводили логин и пароль от интернет-банкинга или реквизиты своей карточки для оплаты услуг, в результате чего конфиденциальные данные становились доступны злоумышленникам и/или держатели лишались своих денежных средств.

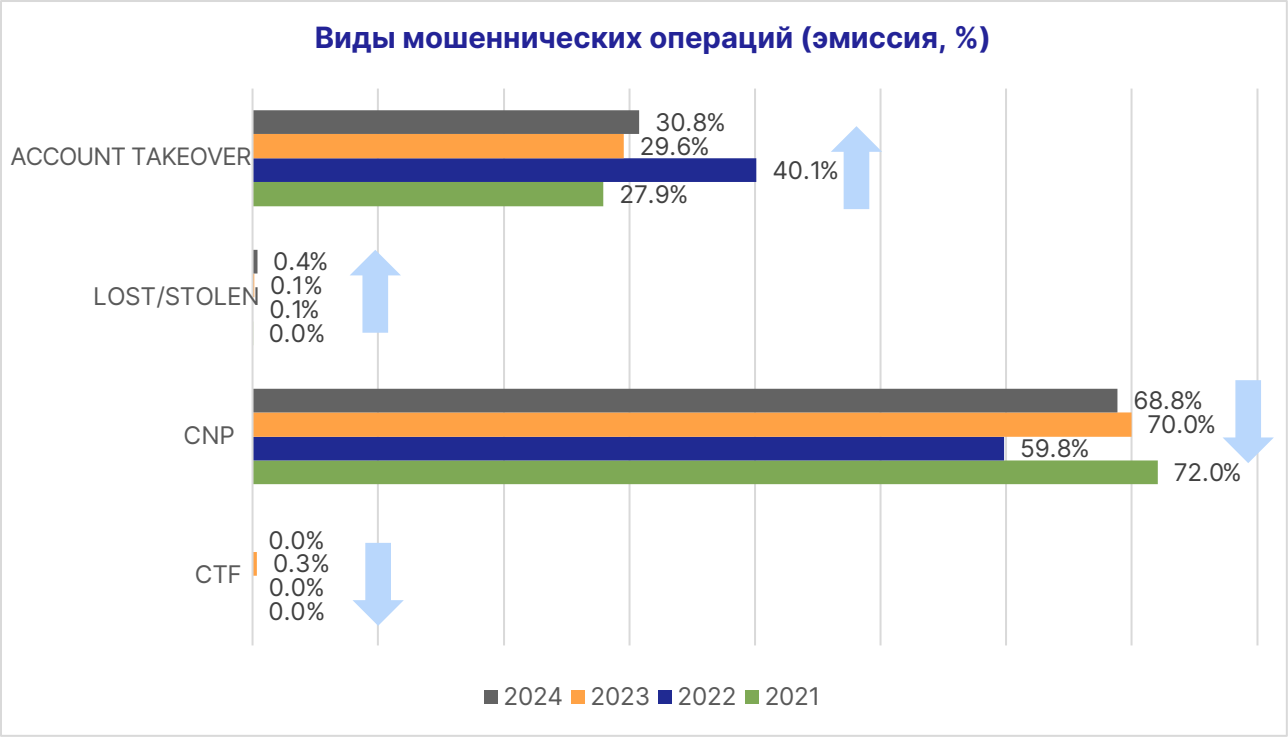
Схема мошенничества с инвестициями, так называемые «лжеброкеры». Мошенники предлагают осуществить инвестиции, открыть брокерский счет в Интернете, тем самым заработать значительную сумму денег за короткий промежуток времени. Инвестиции, сделанные подобным образом, гражданам не возвращаются.

По-прежнему использовалась схема мошенничества, связанная с сайтами знакомств, когда злоумышленники для якобы организации встречи присылали держателям фишинговые ссылки на покупку билетов в театр, кино или в другие места для развлечений. В случае, если клиент переходит по данной ссылке и соглашается с проведением оплаты, с его счета списывается денежная сумма.

Случаи мошенничества с кредитами, которые держатели самостоятельно оформляют, а затем переводят денежные средства в адрес мошенников посредством инфокиосков сократились до единичных случаев. Однако увеличилось количество случаев использования СДБО для подобных целей. В данном случае злоумышленникам удается внушить держателям, что они оказывают содействие правоохранительным органам. В случае потери бдительности и следованию алгоритму аферистов граждане вынуждены погашать оформленный на них кредит.

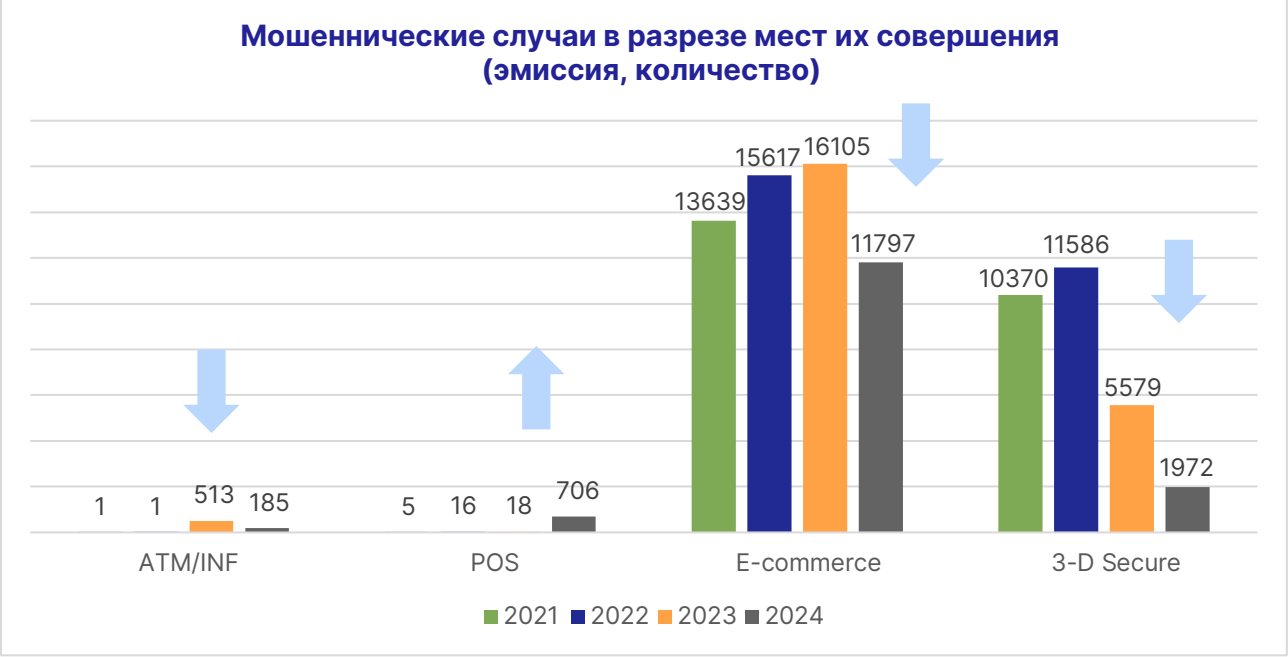
По итогам 2024 года количество успешных мошеннических операций по карточкам банков, которые обслуживаются в ОАО «Банковский процессинговый центр», по типу мошенничества распределилось следующим образом: **68,8%** мошеннических операций приходится на мошенничество **с использованием реквизитов карточек, 30,8%** незаконных операций с банковскими платежными карточками приходится на **account takeover (перехват счета), 0,4%** приходится на операции по **утерянным/украденным карточкам.** Успешных мошеннических операций по **поддельным карточкам** зарегистрировано не было.

По итогам 2024 года на 12% увеличилось общее количество успешных мошеннических операций, заявленных в платежные системы, общая сумма успешных мошеннических операций увеличилась на 161%, а средняя сумма 1 мошеннической операции составила 82 доллара США (35 долларов США в 2023 году), что на 132% больше алогичного показателя прошлого года. Увеличение количества и суммы успешных мошеннических операций, заявленных в международные платежные системы, обусловлено тем, что в связи с изменениями правил МПС Visa и введением программы Visa's Fraud Reporting and Control Program, эмитенты обязаны заявлять в МПС о всех мошеннических операциях, не исключая on-us операции.

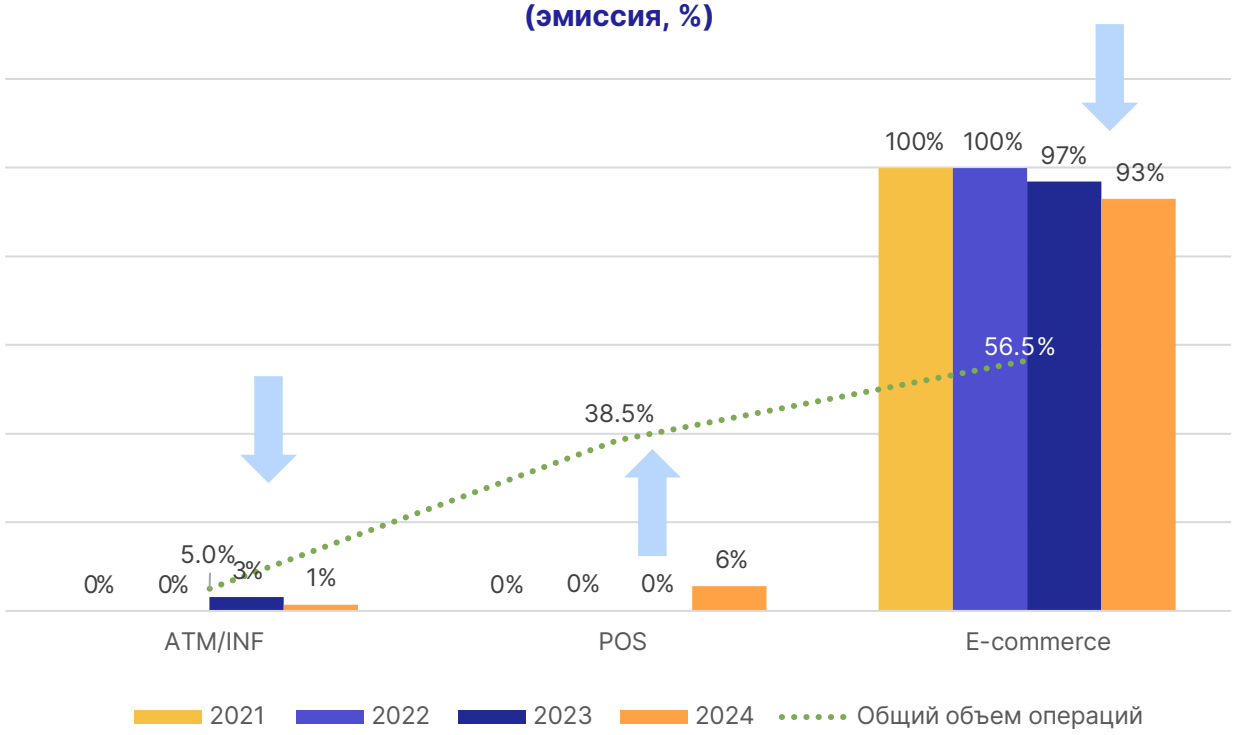


В 2024 по количеству мошеннических случаев в разрезе мест их совершения 93% мошеннических случаев приходится на среду без присутствия карточки. В POS-терминалах прошло 6% случаев ввиду активного использования токенизации карточек держателей, при которой злоумышленники осуществляли оплаты в физических терминалах. Доля в 1% мошеннических случаев в ATM/INF обусловлена схемой мошенничества в рамках социальной инженерии, когда держатели переводили денежные средства в пользу злоумышленников посредством использования сервисов инфокиосков, а также мошенничеством с использованием поддельных карточек.

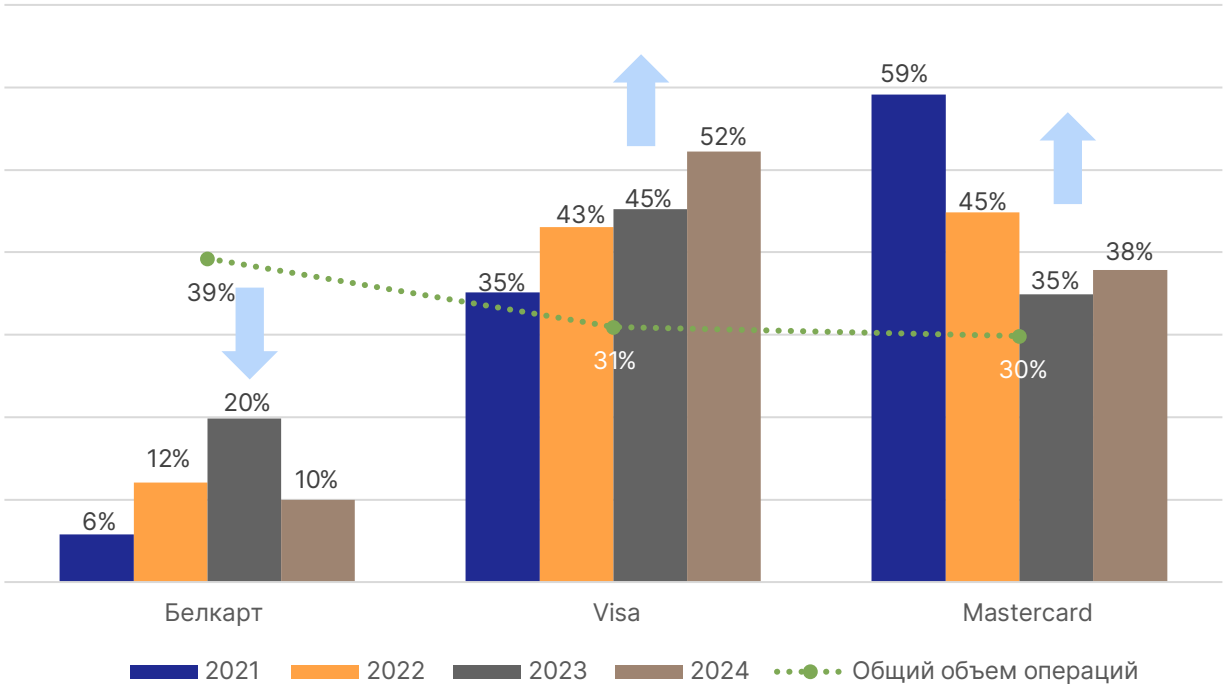
В 2024 году количество мошеннических случаев по операциям с использованием технологии 3-D Secure составило 16% (в 2 раза меньше по сравнению с 2023 годом). Снижение показателя связано с тем, что схемы мошенничества становятся все более разнообразными и подстраиваются под новые технологии и платежные решения, не требующие постоянной проверки дополнительной аутентификации, например, мошенники все чаще используют COF-операций (ранее сохраненные карточные реквизиты).



Мошеннические случаи в разрезе мест их совершения (эмиссия, %)



Мошеннические случаи в разрезе платежных систем (эмиссия, %)



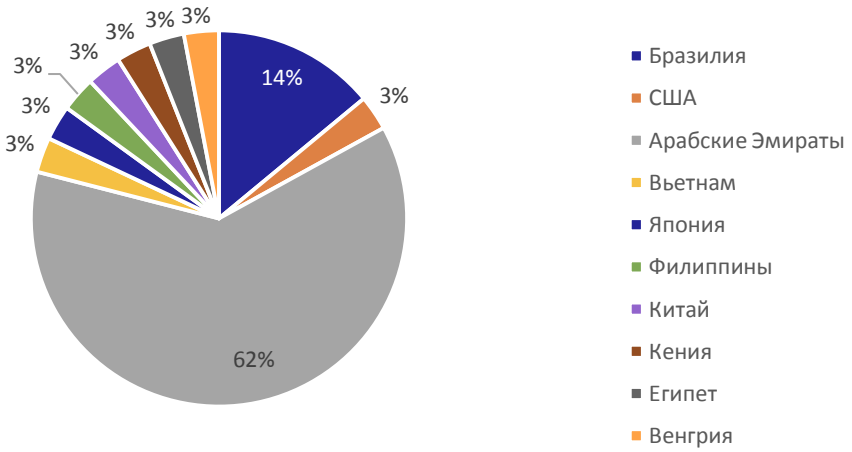
Банковский Процессинговый Центр

Операции по поддельным карточкам:

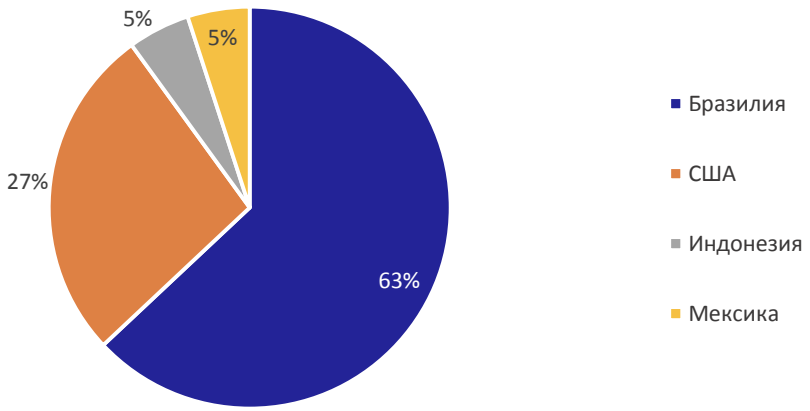
В 2024 году количество мошеннических случаев с использованием поддельных карточек увеличилось в 1,5 раза относительно 2023 года за счет проведения операций по сгенерированным карточкам, также расширилась география стран их применения. В 2024 году было выявлено 5 случаев проведения мошеннических операций с использованием поддельных карточек в ОТС на территории Японии, Венгрии, США и Китая. Случаи проведения мошенниками сгенерированных операций с использованием бесконтактной технологии на территории Бразилии, Арабских Эмиратов и Кении. С использованием поддельных карточек в ОТС в 2023 году были выявлены случаи неуспешных попыток оплаты в США, по сгенерированным операциям в ОТС Бразилии и Мексики.

Также в 2024 году было зафиксировано использование злоумышленниками поддельных карточек в АТМ на территории Бразилии, Вьетнама, Филиппин и Египта, в 2023 году мошенники проводили операции по поддельным карточкам в АТМ в США, Бразилии и Индонезии.

Страны, в которых осуществлялись операции по поддельным карточкам банков в 2024 году



Страны, в которых осуществлялись операции по поддельным карточкам банков в 2023 году



Банковский Процессинговый Центр

Мошеннические операции с использованием реквизитов карточек:

Основными тенденциями мошенничества с использованием реквизитов карточек в 2024 году являются:

- рост уровня мошенничества с использованием реквизитов карточки в среде e-commerce на 26% по отношению к 2023 году, который обусловлен компрометацией данных держателей карточек с последующими мошенническими операциями на онлайн-сервисах, которые занимаются продажей цифровых товаров, компьютерных программ и игр. По-прежнему наблюдались случаи взлома аккаунтов учетной записи Google, Facebook, после чего злоумышленники осуществляют большое количество операций оплаты сервисов на различные суммы в пределах остатка баланса на счете держателей. Данные сервисы преимущественно зарегистрированы на территории США и Великобритании, чем объясняется высокий процент операций с использованием реквизитов карточек в ОТС, зарегистрированных на территории США;

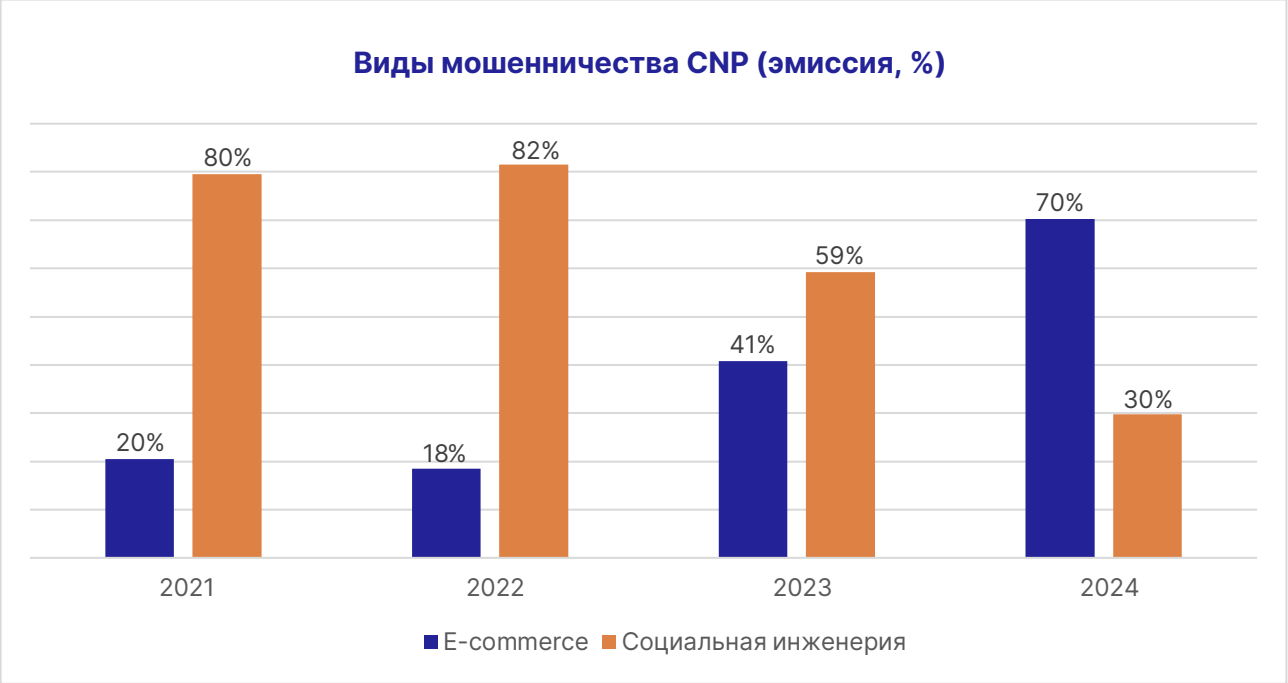
- рост количества мошеннических тестовых операций и атак на БИН банков (сгенерированные номера карточек) с целью выявления реальных карточек для дальнейшего использования их реквизитов в мошеннических целях. Для данных операций в 2024 году использовались ОТС, зарегистрированные на территории США, Канады, Мексики, Японии, Бразилии и Арабских Эмиратов;

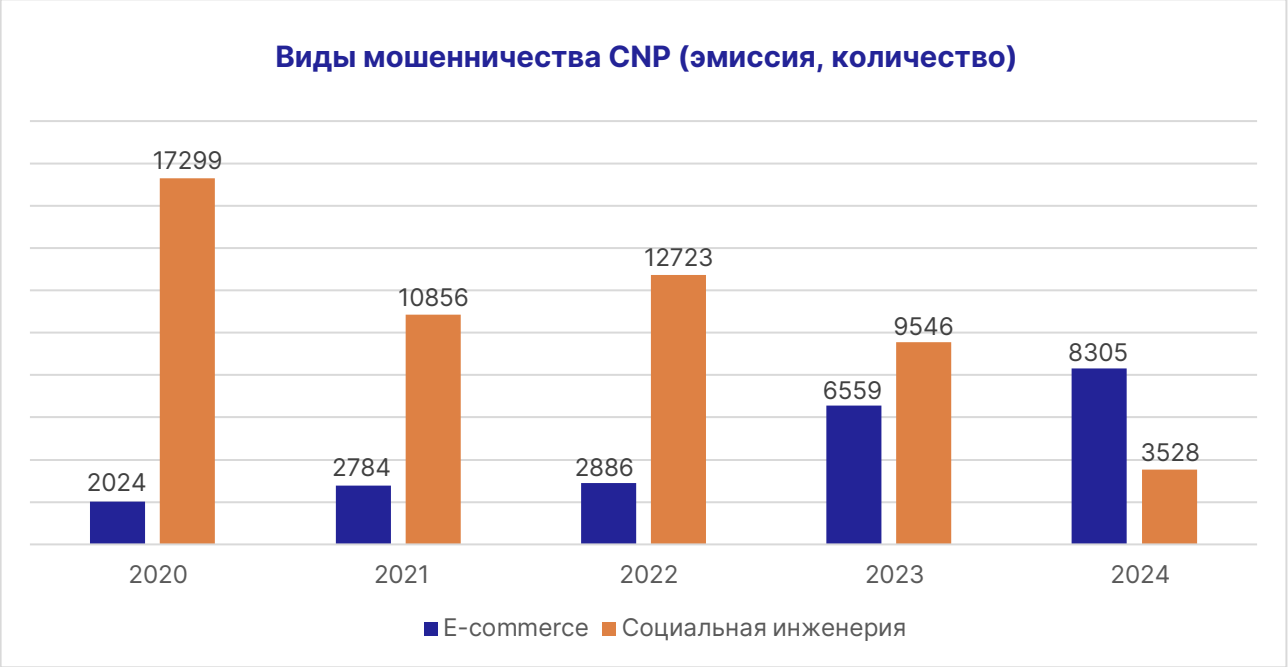
- уменьшение доли мошенничества с применением методов социальной инженерии. В 2024 году относительно 2023 года наблюдалось снижение на 49% уровня мошенничества с использованием методов социальной инженерии. Следует отметить, что с 01.03.2024 года в соответствии с Указом Президента Республики Беларусь от 29 августа 2023 г. № 269 «О мерах по противодействию несанкционированным платежным операциям» заработал новый механизм взаимодействия и обмена информацией между банками, правоохранительными органами посредством АСОИ. Несмотря на снижение количества мошенничества с применением социальной инженерии, схемы мошенников постоянно видоизменяются и подстраиваются под текущую ситуацию. Злоумышленники вынуждают граждан не только отдать все доступные денежные средства, но и взять кредиты, займы, даже продать недвижимость. Для вывода же похищенных денежных средств в 2024 году злоумышленники на чаще использовали платежные сервисы, зарегистрированные на территории Республики Беларусь: ЕРИП, сайты P2P переводов, криптовалютные биржи;

- мошенничество по токенам, рост мошенничества в 5 раз относительно 2023 года. При данной схеме мошенничества злоумышленники привязывают токен карточки держателя на свое мобильное устройство и совершают несанкционированные платежи с использованием заведенного электронного кошелька в сети Интернет, наземных ОТС и АТМ. В 2024 году 38% всех мошеннических операций по токенам пришлось на операции e-commerce в интернет-сервисах, зарегистрированных на территории США, Мальты, Гонконга и Великобритании; 59% - на токенизированные операции в наземных ОТС, зарегистрированных в таких странах как Арабские Эмираты, Перу, Чили, Вьетнам, Пакистан, Италия и др.; 3% - обналичивание денежных средств с токенизированных карточек в АТМ, зарегистрированных в таких странах как Словакия, Российская Федерация, Австрия, Беларусь.

- компрометация СДБО клиентов посредством социальной инженерии. Данный показатель снизился на 70% по сравнению с 2023 годом. Перехват таких данных как логины/пароли способствует получению полного доступа к финансам держателя посредством компрометации ДБО. Получение доступа к системам ДБО преимущественно осуществлялось путем установки злоумышленниками на мобильное устройство держателя программ удаленного доступа (AnyDesk, TeamViewer, RustDesk);

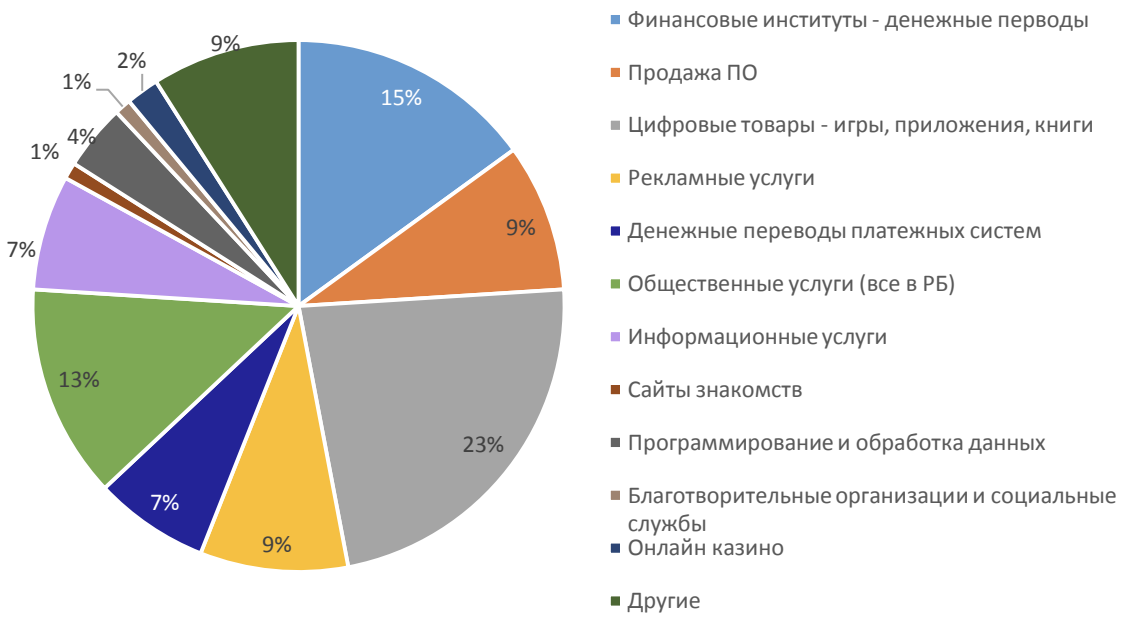
- присутствие фактов «friendly fraud» мошенничества, т.е. «дружественного мошенничества», тип мошенничества, при котором владелец карточки либо его родственники/знакомые оплачивают товар или услугу, получают его/ее, пользуются, а затем намеренно инициируют возврат платежа, утверждая, что данные их карточки были скомпрометированы.



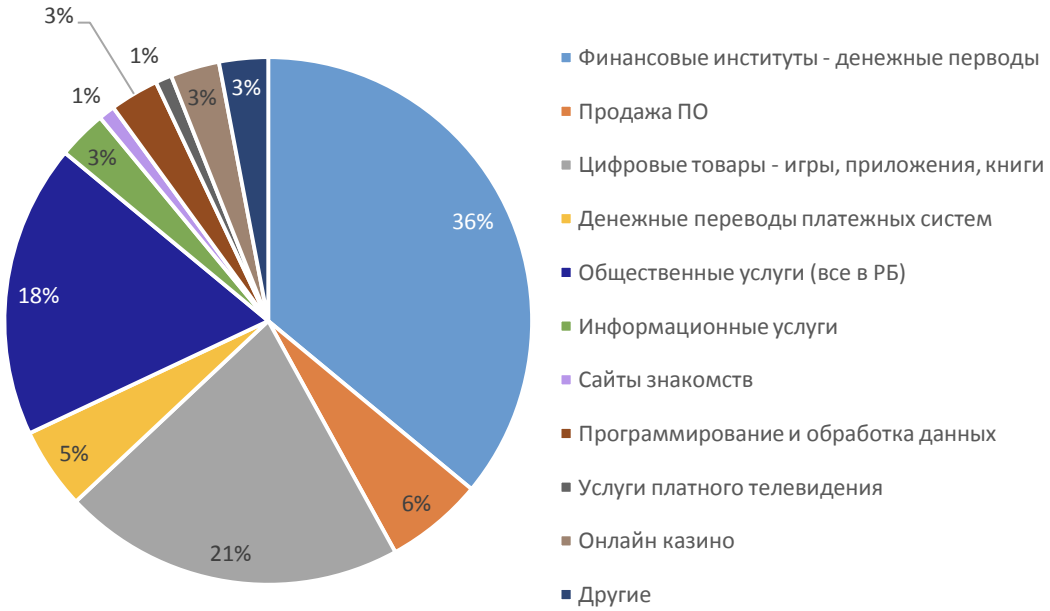


Банковский Процессинговый Центр

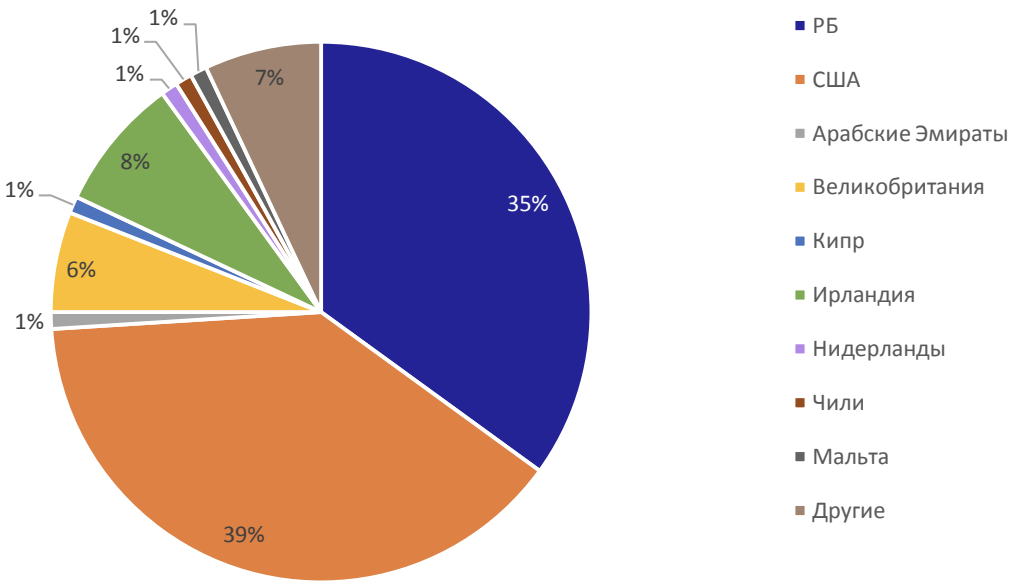
В каких ОТС (категориях ОТС) осуществлялись мошеннические операции с использованием реквизитов карточек в 2024 году



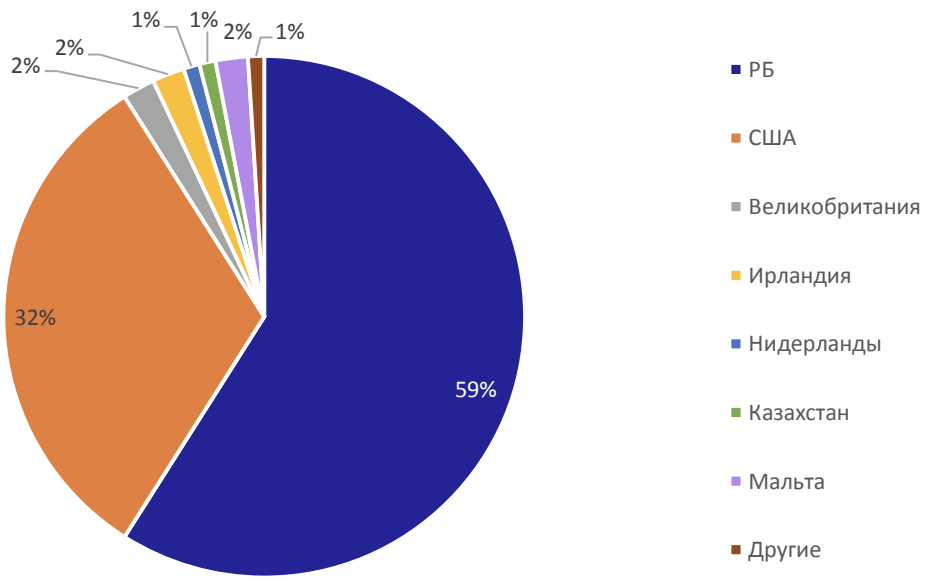
В каких ОТС (категориях ОТС) осуществлялись мошеннические операции с использованием реквизитов карточек в 2023 году



Страны, в которых осуществлялись мошеннические операции с использованием реквизитов карточек в 2024 году



Страны, в которых осуществлялись мошеннические операции с использованием реквизитов карточек в 2023 году



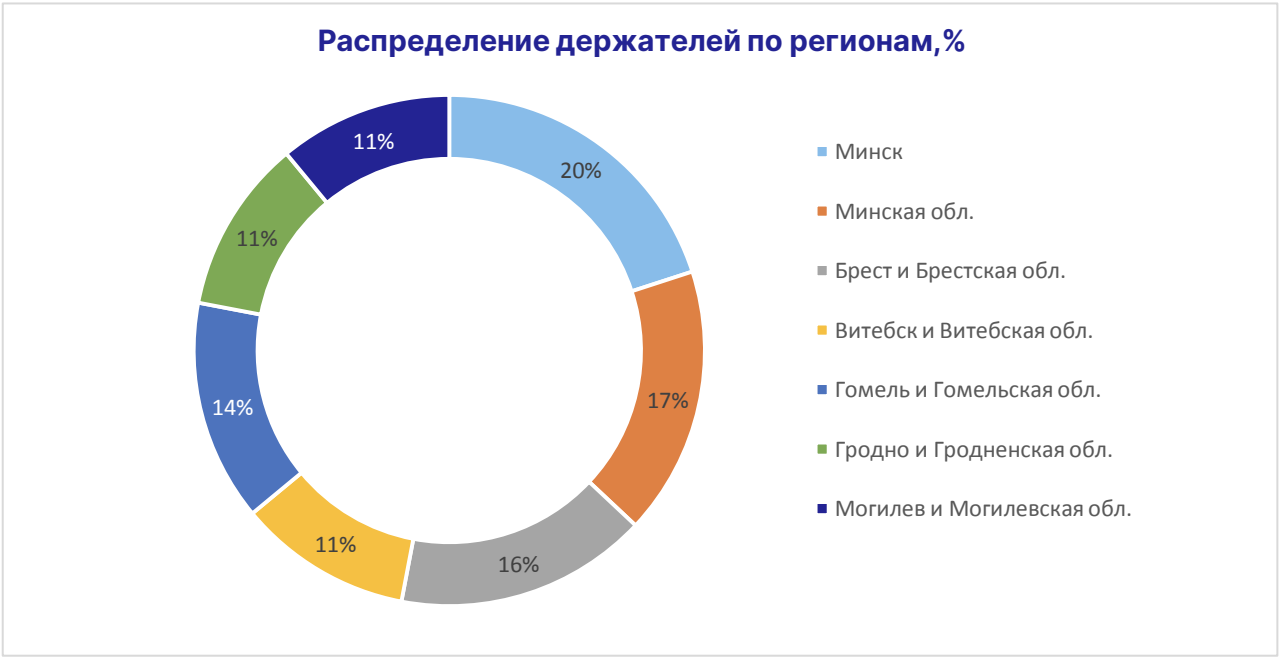
Банковский Процессинговый Центр

Статистика держателей, подвергшихся мошенничеству:

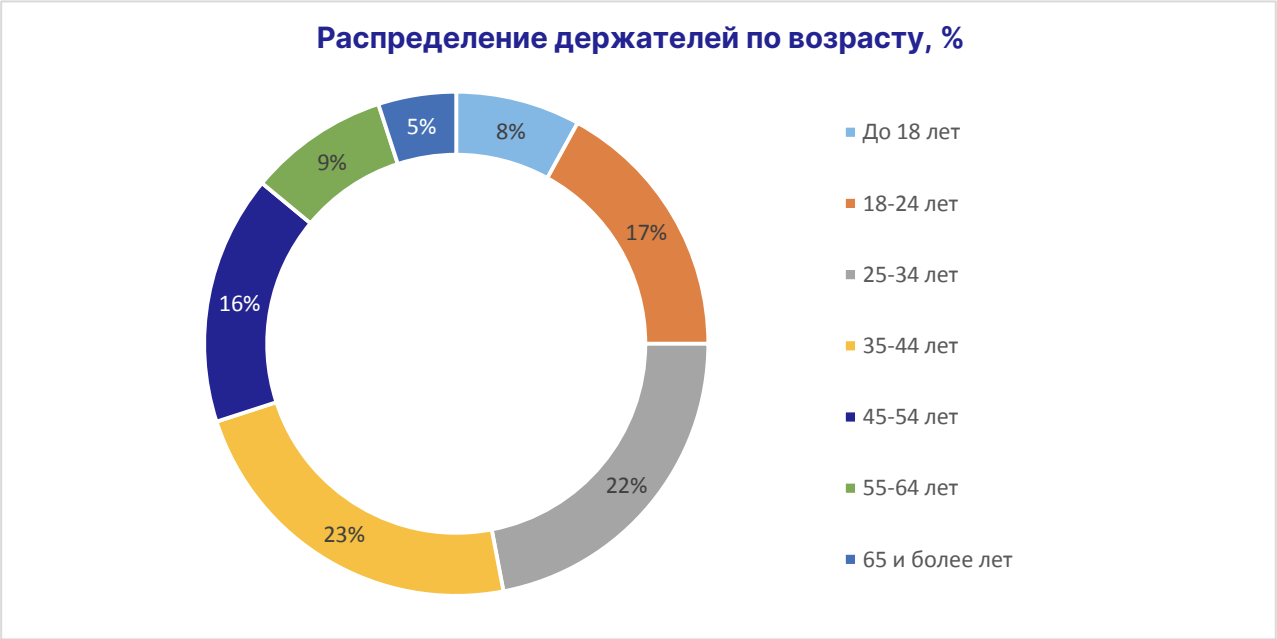
Согласно аналитическим данным ОАО «Банковский процессинговый центр» в 2024 году более доверчивыми оказались женщины – в 56% случаев. В 20% случаев жертвами злоумышленников стали держатели, проживающие в городе Минске, а 80% случаев мошенничества приходится на проживающих в других регионах Беларуси.

В 87% случаев мошенничество направлено на экономически активных граждан в возрасте от 18 до 64 лет, 5% – на держателей старше 65 лет, 8% атак пришлось на держателей младше 18 лет.

Детальная информация представлена на диаграммах.



Банковский Процессинговый Центр



Рекламации эмиссия (данные по операциям с банковскими платежными карточками, выпущенными банками, которые обслуживаются в ОАО «Банковский процессинговый центр»):

В 2024 году общее количество рекламаций эмиссии увеличилось в 1,7 раза относительно 2023 года, что обусловлено несанкционированными операциями, проводившимися в сети Интернет преимущественно на таких сайтах, как APPLE.COM, FACEBK, GOOGLE, Onlyfans.Com, PokerStars и Stars. В рамках процесса оспаривания сохраняется тенденция роста количества оспоренных мошеннических операций без присутствия карточки, при этом с развитием технологий в сфере безопасности платежей мошенники стали использовать не только реквизиты карточек, но и реквизиты токенов для несанкционированного списания денежных средств со счетов держателей карточек.

В 2024 году рекламации по причинам оспаривания распределились следующим образом:

89,1% от общего количества рекламаций были инициированы по причине мошенничества (85,8% в 2023 году);

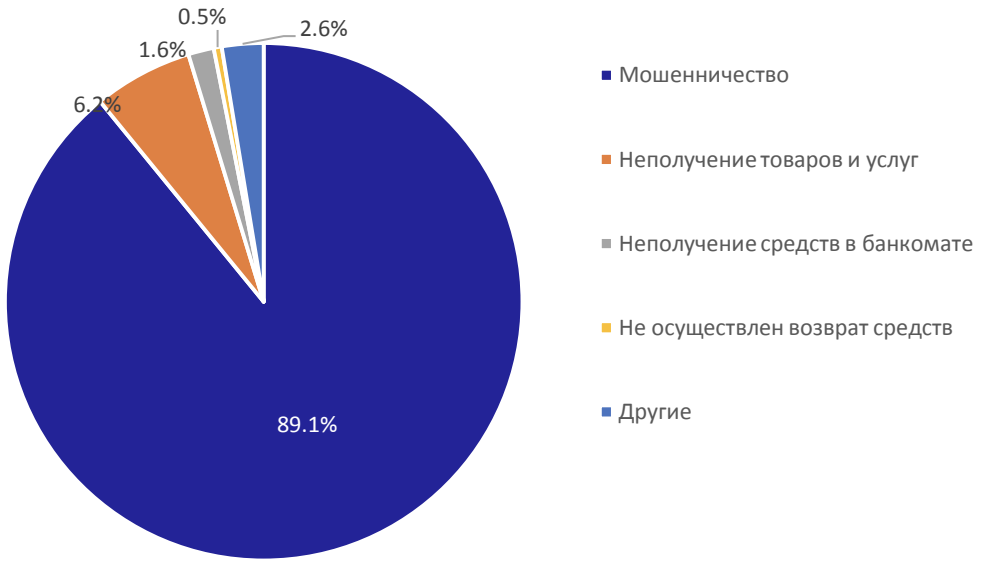
6,2% составляют операции, оспоренные по причине неполучения держателем карточки товаров/услуг (5,5% в 2023 году);

1,6% приходится на долю рекламаций по операциям неполучения денежных средств в банкоматах (4,2% в 2023 году);

0,5% - операции, оспоренные по причине неполучения возврата денежных средств (1,2% в 2023 году);

2,6% от общего количества оспоренных операций составили остальные виды рекламаций (3,3% в 2023 году).

Распределение рекламаций по причинам оспаривания в 2024 году (эмиссия, %)



Эквайринг (данные по операциям в эквайринговой сети банков, подключенных к ОАО «Банковский процессинговый центр»):

В 2024 году в 1,8 раз увеличилось количество операций мошеннического характера в эквайринговой сети банков, которые обслуживаются в ОАО «Банковский процессинговый центр». Из них 23% составляют мошеннические операции **без присутствия карточки, 65% - другие виды мошенничества:** 97% составляет мошенничество с перехватом данных держателей и мошенничество, связанное с манипуляцией владельцем счёта; 3% - мошенничество, связанное с выпуском карточки по поддельным данным; **11%** приходится на долю мошеннических операций **по утерянным/украденным карточкам** и **1%** приходится на мошеннические операции с использованием **поддельных карточек.**

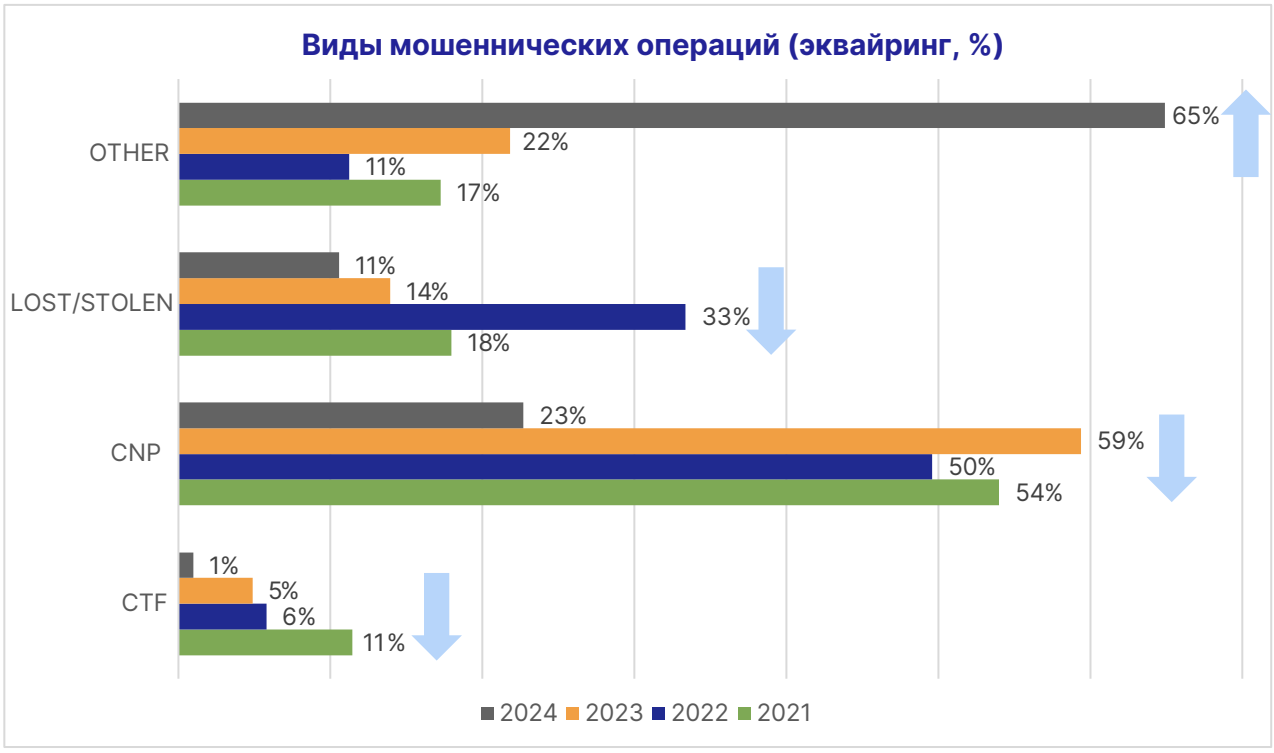
Мошеннические операции **без присутствия карточки** в 32% случаев прошли с использованием реквизитов карточки в среде e-commerce, 36% — это операции с использованием технологии 3-D Secure, 24% - COF-транзакции и 8% - это операции в ОТС с физическим или бесконтактным использованием карточки.

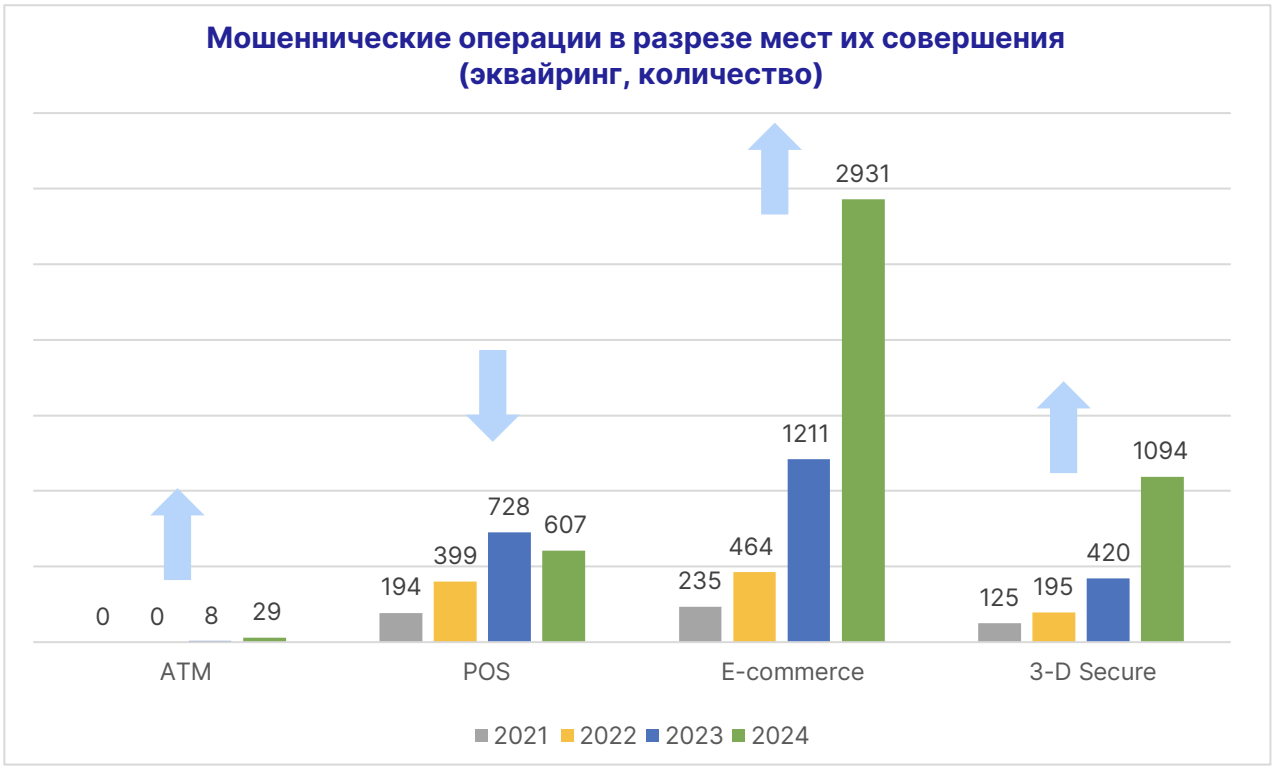
Мошеннические операции по **утерянным/украденным** карточкам в 79% случаев были осуществлены с признаком проведения бесконтактных операций, 7% — это операции с использованием 3-D Secure, 6% - COF-транзакции, в других 6% случаев мошеннические операции осуществлялись с использованием EMV технологии, 2% пришлось на операции с использованием реквизитов карточек. Бесконтактные операции позволяют мошенникам совершать большое количество операций в рамках
установленных лимитов без необходимости подтверждения совершения операции ПИН-кодом либо использования других методов подтверждения операции.

Мошенничество по **поддельным карточкам** в 57% случаев проходило по бесконтактному признаку, 20% из заявленных операций прошли с использованием реквизитов карточек, 15% — это операции с использованием 3-D Secure, 8% - COF-транзакции. В 2024 году в эквайринговой сети банков не было зафиксировано ни одного реального случая использования поддельных карточек.

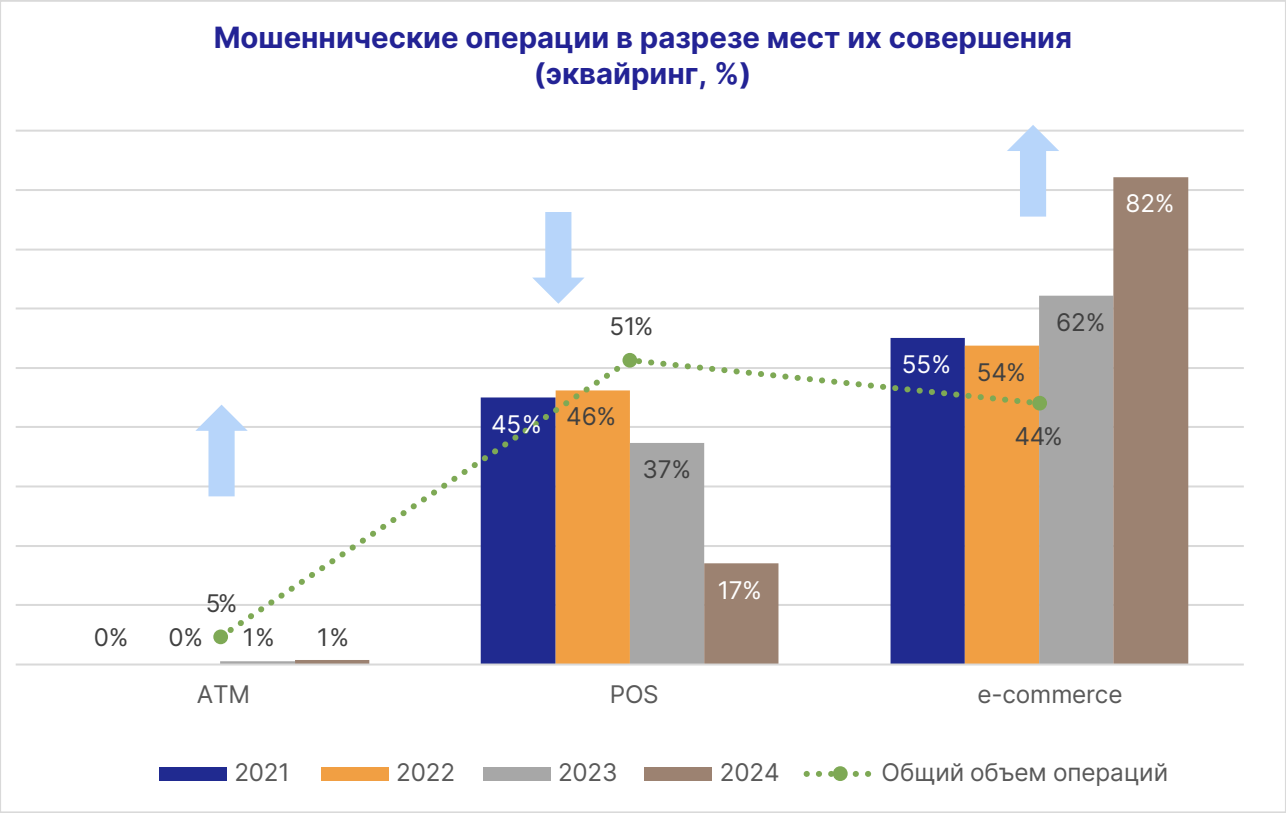
В 2024 году общая сумма успешных мошеннических операций по сравнению с 2023 годом увеличилось на 253%, средняя сумма 1 мошеннической операции составила 168 долларов США (87 долларов США в 2023 году). Увеличение количества и суммы успешных мошеннических операций обусловлено изменениями правил международной платежной системы Visa и введением программы Visa's Fraud Reporting and Control Program, которая обязывает эмитентов заявлять в МПС о всех мошеннических операциях, не исключая on-us операции.

В целом, развитие информационных технологий, совершенствование систем защиты банкоматов, постепенный выход из оборота карточек только с магнитной полосой, а также незначительные затраты злоумышленников при мошенничестве в среде без присутствия карточки значительно снижают привлекательность мошенничества с использованием поддельных карточек.





Банковский Процессинговый Центр



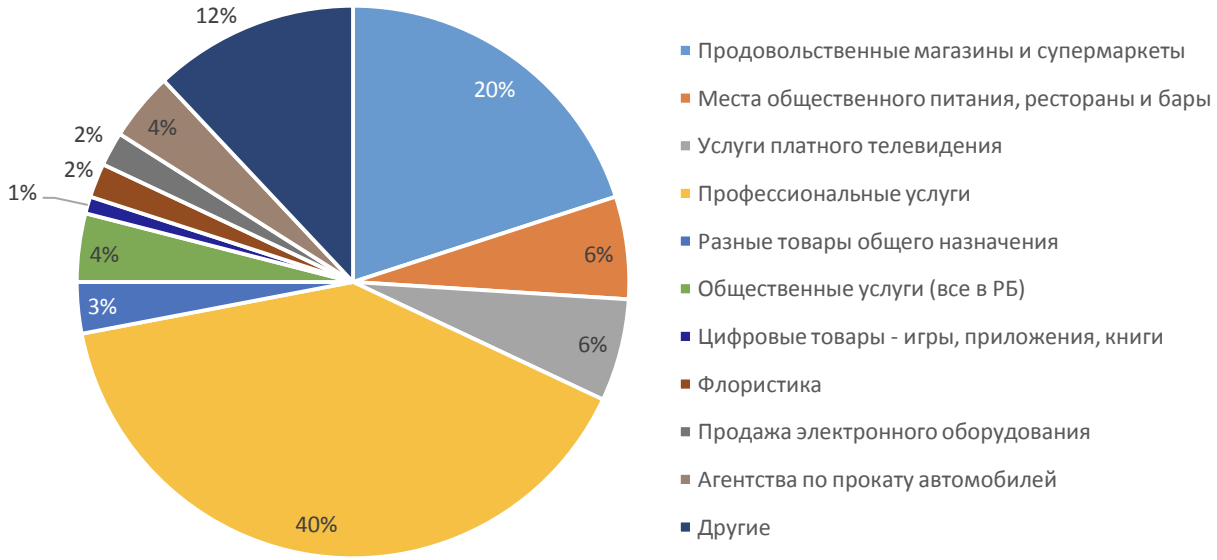
Рейтинг MCC, в которых осуществлялись мошеннические операции в эквайринге, распределился следующим образом: 30% мошеннических операций пришлось на денежные переводы; 16% на общественные услуги; 13% на сферу профессиональных услуг; 10% - агентства по прокату автомобилей; 8% - продовольственные магазины и супермаркеты; 5% - места общественного питания, рестораны и бары; 3% - услуги платного телевидения; 2% - оптовые клубы; по 1% приходится на автозаправочные станции и авиакомпании; 11% - другие ОТС.

Наиболее часто в 2024 году в эквайринговой сети в мошеннических целях использовались карточки банков США, ОАЭ и Беларуси.

В 2024 году по-прежнему имеет место мошенничество по карточкам ПС Мир, обусловленное притоком туристов из Российской Федерации, которые используют карточки данной платежной системы для проведения операций на территории Республики Беларусь. По карточкам платежной системы UnionPay Intarnational в эквайринговой сети не было зафиксировано ни одной мошеннической операции.

В каких ОТС (категориях ОТС) осуществлялись мошеннические операции в эквайерской сети по карточкам банков нерезидентов в 2024 году

В каких ОТС (категориях ОТС) осуществлялись мошеннические операции в эквайерской сети по карточкам банков-нерезидентов в 2023 году



Рекламации эквайринг (данные по операциям в эквайринговой сети банков, подключенных к ОАО «Банковский процессинговый центр»):

В 2024 году было обработано эквайерских рекламаций в 1,6 раз больше чем в 2023 году. В эквайринге наблюдается перераспределение количества поступающих рекламаций по правилам различных платежных систем в связи с геополитической ситуацией. Подавляющее большинство операций было оспорено по причине неполучения товаров/услуг.

В 2024 году рекламации по причинам оспаривания распределились следующим образом:

91,5% оспоренных операций относятся к операциям неполучения товаров и услуг (35,8% в 2023 году);

4,9% – не получен возврат денежных средств (2,1% в 2023 году);

1,9% от общего количества рекламаций были оспорены по причине мошенничества (12% в 2023 году);

0,5% - нарушение технологии проведения операций (47,1% в 2023 году). Высокий процент такого рода рекламаций в 2023 году был связан с большим количеством входящих диспутов на онлайн-ресурсе НСПК, а уже в 2024 году банки-эмитенты оспаривали такие операции по кодам оспаривания категории «Потребительские споры», так как для кода «Нарушение технологии проведения операций» ПС Мир предусмотрен срок на опротестование операций – до 180 дней, в то время как для потребительских споров этот срок достигает 360 дней;

0,2% от общего числа рекламаций составили операции, оспоренные по причине неполучения денежных средств в банкомате (1% в 2023 году). В 2024 году снизилась доля рекламаций по причине неполучения денежных средств в банкомате в общем объеме, но фактическое количество оспоренных операций неполучения средств в банкомате снизилось незначительно;

1,0% от общего количества оспоренных операций приходится на остальные виды рекламаций единичного характера (2,0% в 2023 году).

Распределение рекламаций по причине оспаривания в2024 году (эквайринг, %)

Прогноз:

Учитывая схемы мошенничества, которые были актуальными в 2024 году, можно предположить, что для 2025 года характерными будут:

• **Использование искусственного интеллекта (ИИ).** Ожидается, что в 2025 году искусственный интеллект укрепит свои позиции и станет повседневным рабочим инструментом для злоумышленников. В 2024 году начали распространяться дипфейки, голосовые клоны и фишинговые атаки с использованием искусственного интеллекта. Однако мошенники только использовали данные инструменты как пробные. В 2025 году ИИ-мошенничество станет главным трендом, угрожающим финансовой безопасности. Использование полностью автономных чат- ботов с искусственным интеллектом станет более обширным; мошенники будут использовать технологию дипфейков на основе ИИ для видеозвонков, голосовых клонов и чат-ботов, чтобы значительно расширить свою деятельность; схемы вымогательства с помощью дипфейков, скорее всего, распространятся на корпоративных клиентов по всему миру и будут нацелены и на высокопоставленных руководителей.

• **Социальная инженерия.** Мошенничество с использованием методов социальной инженерии, как и в предыдущие годы, останется серьезной угрозой. Многообразие форм данного вида мошенничества и возможность подстроиться под актуальную ситуацию в мире всегда дает быстрый и эффективный результат. Злоумышленники используют различные каналы связи с жертвами: телефонные звонки, мессенджеры, социальные сети и прочее, а в 2025 году социальная инженерия выйдет на новый уровень благодаря возможностям ИИ. Поддельные звонки и видеосообщения будут использоваться для создания иллюзии доверия. Жертвы будут подбираться на основе анализа их социальных связей, публичной активности и личных данных. Мессенджеры останутся основным инструментом атак благодаря их популярности и сложности отслеживания.

• **Блокчейн и цифровые активы.** Блокчейн продолжает укреплять свои позиции в финансовой сфере, растет популярность криптовалют. Кроме того, в 2024 году более 130 стран разрабатывали национальные цифровые валюты. В 2025 году также многие мировые эксперты прогнозируют рост количества атак на держателей криптовалютных активов и появления новых способов и схем обмана пользователей. Также будут распространены мошеннические схемы, связанные с цифровыми валютами, направленные на кражу денежных средств.

• **Фишинговые атаки.** Фишинговые рассылки и сайты все сложнее отличить от легитимных, что усложняет задачу для держателей по их выявлению. Случаи использования мошенниками фишинговых сайтов крупных белорусских банков и платежных ресурсов имели место в 2024 году. Злоумышленники стараются приурочить фишинговые кампании к громким событиям и инфоповодам, это означает, что подобные атаки будут иметь место и в 2025 году.

• **Перехват доступа к СДБО и МСИ.** Мошенничество, которое позволяет злоумышленникам получить полный доступ ко всем платежным инструментам и счетам держателя. Возможность открытия виртуальных, дебетовых и кредитных карточек с доставкой почтой, кредитных продуктов онлайн делает данный вид мошенничества очень привлекательным. Серьезной угрозой останутся программы удаленного доступа, которые мошенники по-прежнему устанавливают на мобильные устройства держателей и посредством их получают доступ к любым приложениям, а в частности, к СДБО.

• **Мошенничество с использованием токенов.** Тема токенизации и использование токенов в рамках социальной инженерии будет активно использоваться и в 2025 году. Все чаще в рамках социальной инженерии злоумышленники привязывают данные карточки держателя на свои мобильные устройства и совершают оплаты в сети Интернет и в наземных ОТС, а также снимают наличные в банкоматах.

• **Схемы с онлайн-заработком.** В данном случае мошенники по-прежнему будут использовать методы с фальшивыми инвестициями, когда гражданам предлагается вложить деньги в «перспективные активы», что якобы позволит увеличить их доход. В действительности же после перевода средств доступ клиенту к инвестиционной платформе блокируется и осуществить вывод инвестиций становится невозможным.

• **Вредоносное программное обеспечение (ВПО) и кибератаки.** В современных реалиях наблюдается эволюция рынка ВПО, которое применяется при кибератаках. В даркнете появляются аналоги легальных сервисов проверки файлов, которые дают возможность злоумышленникам обходить различные системы защиты. Кроме того, набирает популярность модификация вирусов «на заказ» под специфику конкретных атак и жертв, что свидетельствует о достаточно серьезных угрозах для финансового рынка.

• **Мошенничество с подписками и хищение аккаунтов.** Последние несколько лет мир активно переходит к подписочному формату распространения товаров и услуг, и мошенники активно пользуются этим. С ростом числа подписочных сервисов у некоторых пользователей может появиться соблазн «купить подписку подешевле» или вовсе «скачать программу бесплатно», что играет на руку мошенникам, потому что мошеннические ресурсы могут обнаружиться даже в легитимных магазинах приложений. Мошенники никогда не проходят мимо крупных релизов развлекательной индустрии — 2025 год не станет исключением.

• **Система мгновенных платежей (СМП) и QR-платежи.** Развитие любых новых сервисов не останется незамеченным злоумышленниками, так распространение СМП и QR-платежей будет привлекать внимание мошенников и не исключено их вовлечение в гибридные схемы мошенничества. Привязка номера телефона к счетам злоумышленников, подмена QR-кода и т.д. возможны в использовании мошенниками для хищения денежных средств.

Мошенничество можно назвать «динамичным» направлением, которое постоянно меняется, приспосабливается к новым условиям, особенно, когда схемы раскрываются и перестают приносить прибыль. Следовательно, не стоит ждать, что 2025 год принесет в глобальном понимании что-то совершенно новое. Скорее будут наблюдаться изменения привычных схем с целью усыпить бдительность и убедить граждан, что их не пытаются обмануть уже известными способами, тем более, что фишинг, утечки и социальная инженерия работают и стабильно продолжают приносить прибыль злоумышленникам.