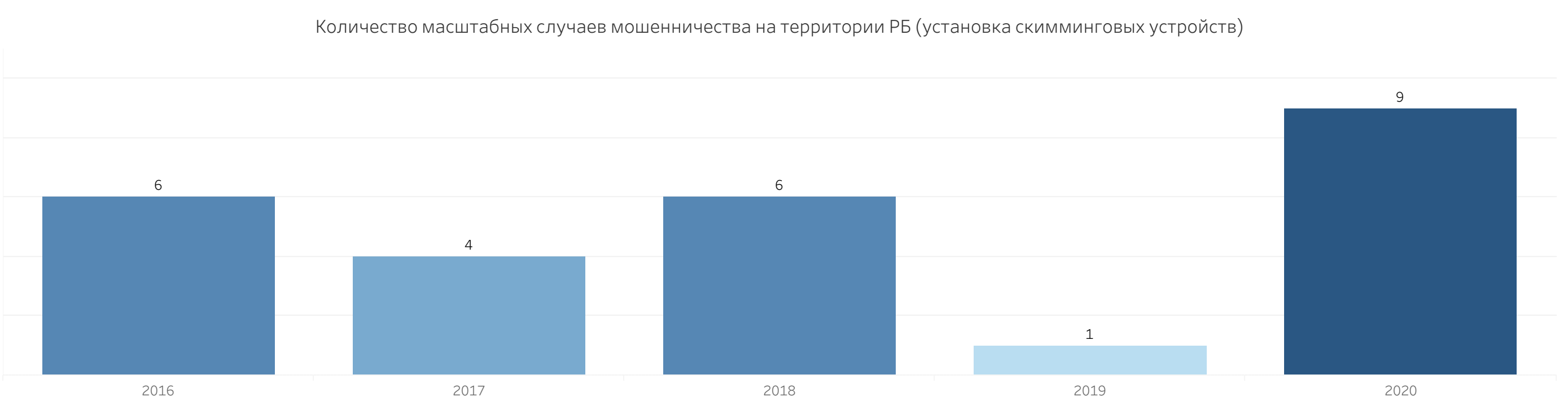
Отчет о тенденциях и случаях мошенничества в сфере платежных инструментов и сервисов за 2020 год

Общая информация

Ключевыми особенностями 2020 года являются всплеск мошенничества с банковскими платежными карточками в среде без присутствия карточки, увеличение случаев мошенничества с использованием методов социальной инженерии и рост числа случаев установки скимминогового оборудования.

Количество масштабных случаев мошенничества на территории РБ (установка скимминговых устройств)

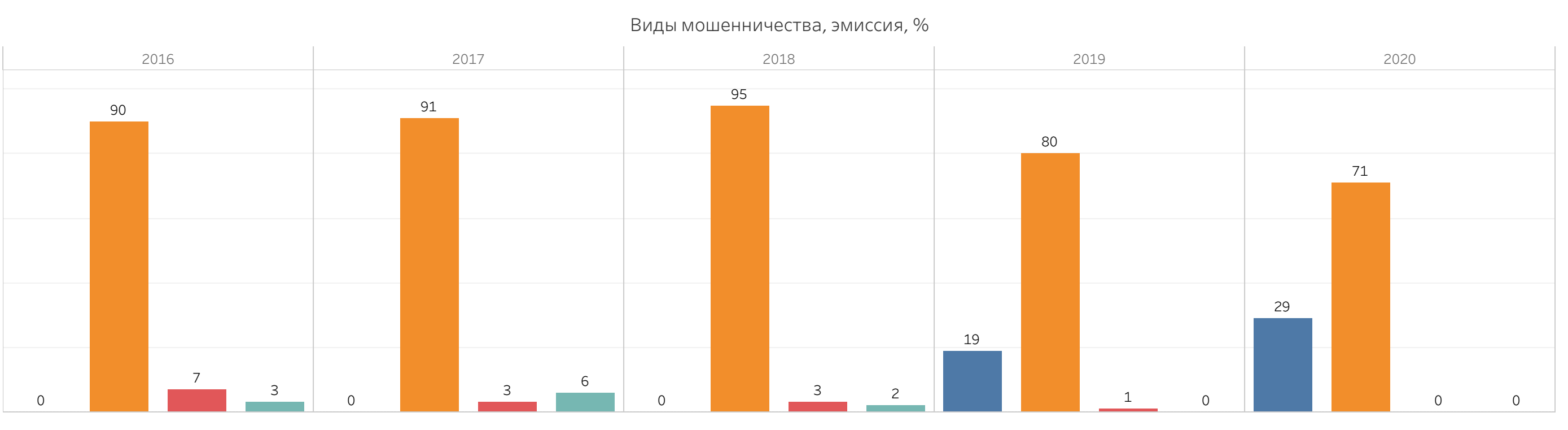


В июне 2020 года был зафиксирован первый случай установки скиммингового устройства на банкомате в г. Могилеве. По информации от правоохранительных органов, мошенники были задержаны на месте преступления, утечки карточных данных не было. В 3 квартале 2020 года было выявлено 8 случаев установки скимминговых устройств на банкоматах в г. Минске. Мошенник обналичивал денежные средства по поддельным карточкам после компрометации магнитной полосы также в банкоматах г. Минска, при этом были зафиксированы случаи использования поддельных карточек в Канаде и Перу. Злоумышленник был задержан правоохранительными органами 06.09.2020. В результате массовой компрометации карточных данных общий подтвержденный ущерб составил порядка 18 120 белорусских рублей.

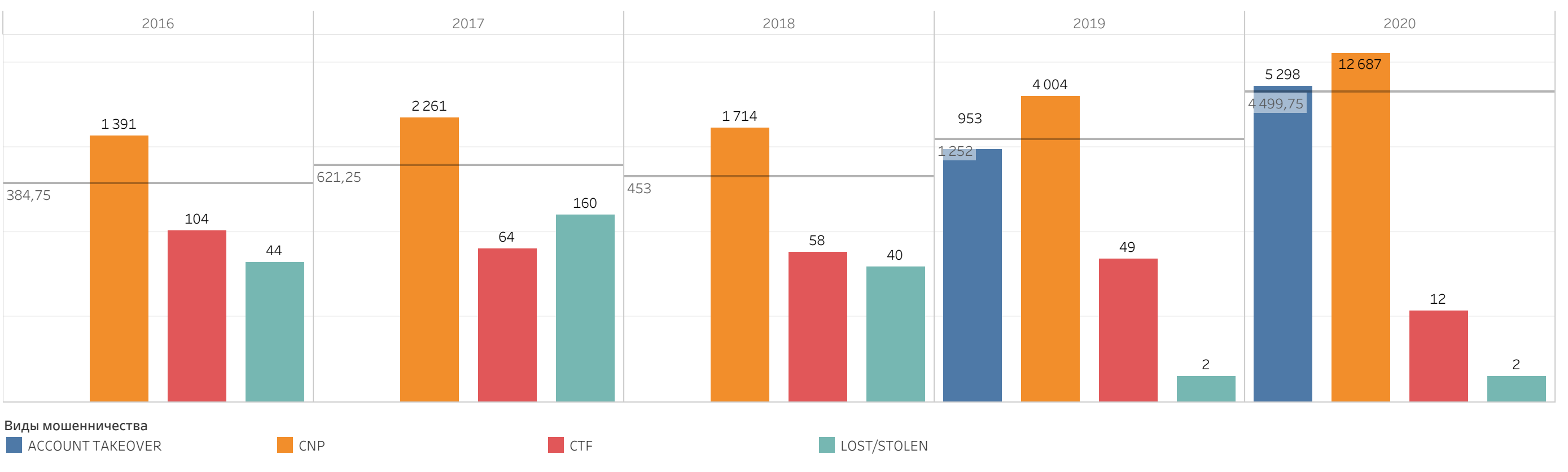
Эмиссия (данные по операциям с банковскими платежными карточками, выпущенными банками, которые обслуживаются в ОАО «Банковский процессинговый центр»)

В 2020 году практически все мошеннические операции приходились на мошенничество с использованием реквизитов карточек наряду с наличием незначительного количества мошенничества с использованием поддельных карточек и по утерянным/украденным карточкам. Количество случаев мошенничества по **поддельным карточкам уменьшилось в 4 раза** по сравнению с аналогичным показателем 2019 года.
По итогам 2020 года количество мошеннических операций по карточкам банков, которые обслуживаются в ОАО «Банковский процессинговый центр», по типу мошенничества распределилось следующим образом: **71%** мошеннических операций приходится на мошенничество **с использованием реквизитов карточек**, **29%** незаконных операций с банковскими платежными карточками приходится на **account takeover (перехват счета).**

Виды мошенничества, эмиссия, %

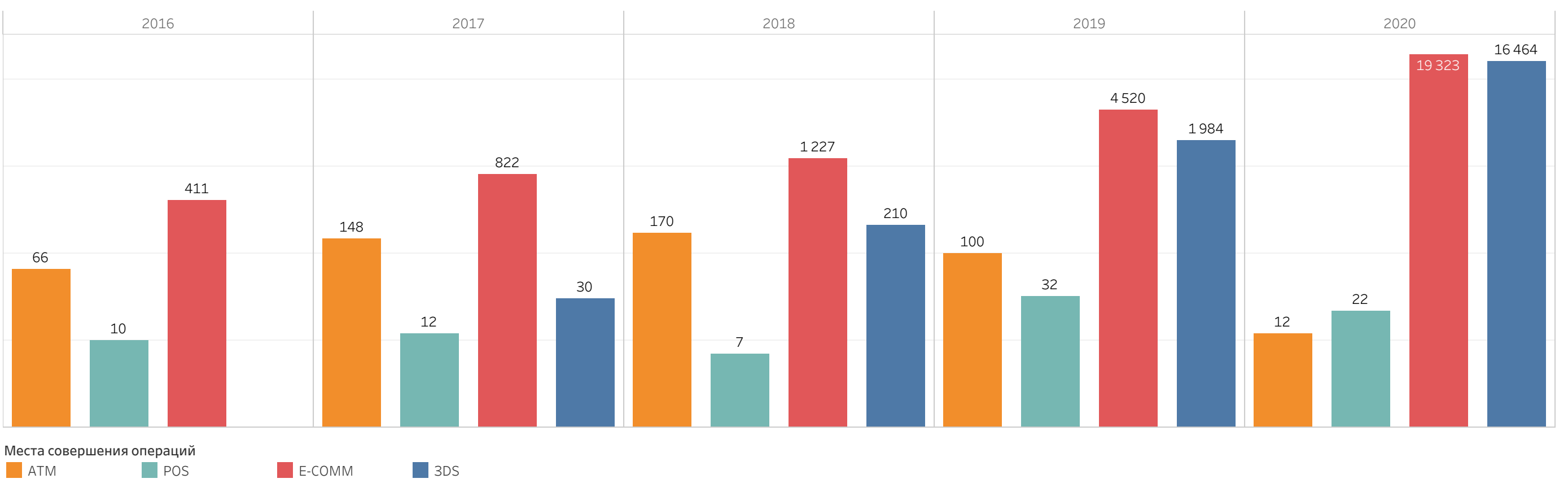


Количество мошеннических операций в разрезе видов (эмиссия, условные единицы)

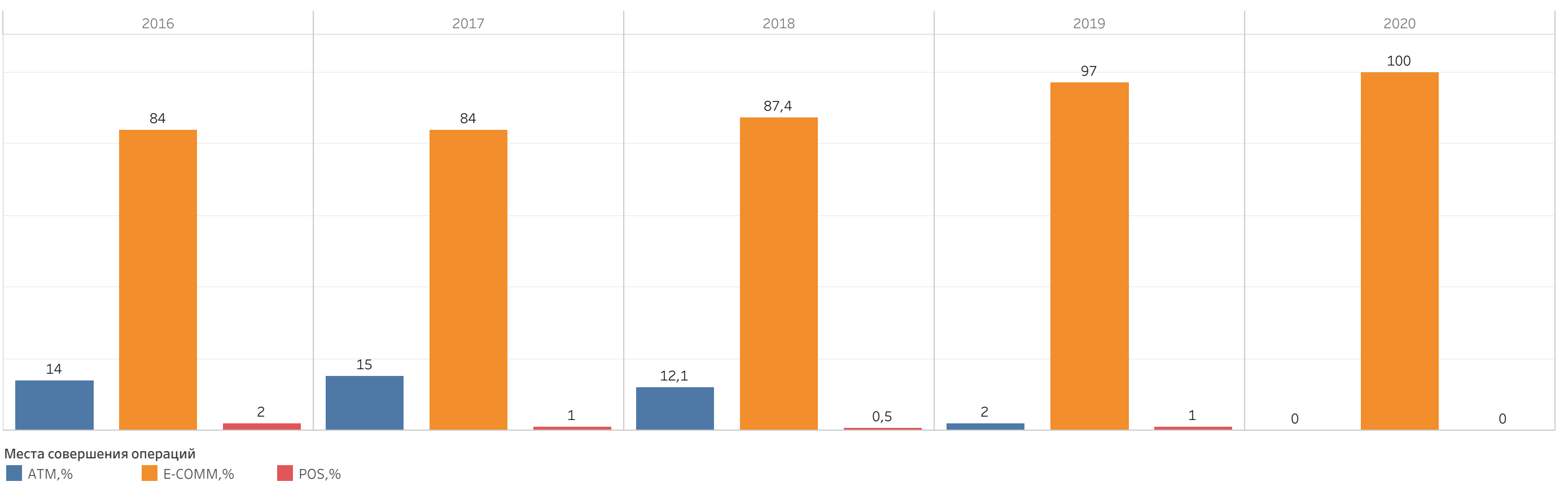


В 2020 году в связи с увеличением случаев мошенничества с использованием методов социальной инженерии выросло и количество мошеннических случаев по операциям с использованием технологии 3-D Secure. Так 85% мошеннических операций без присутствия карточки имеют признак использования технологии 3-D Secure. Мошенники научились различными методами выманивать все необходимые для осуществления платежей/переводов реквизиты, в том числе и пароли 3-D Secure.

Количество мошеннических операций в разрезе мест их совершения (эмиссия, условные единицы)

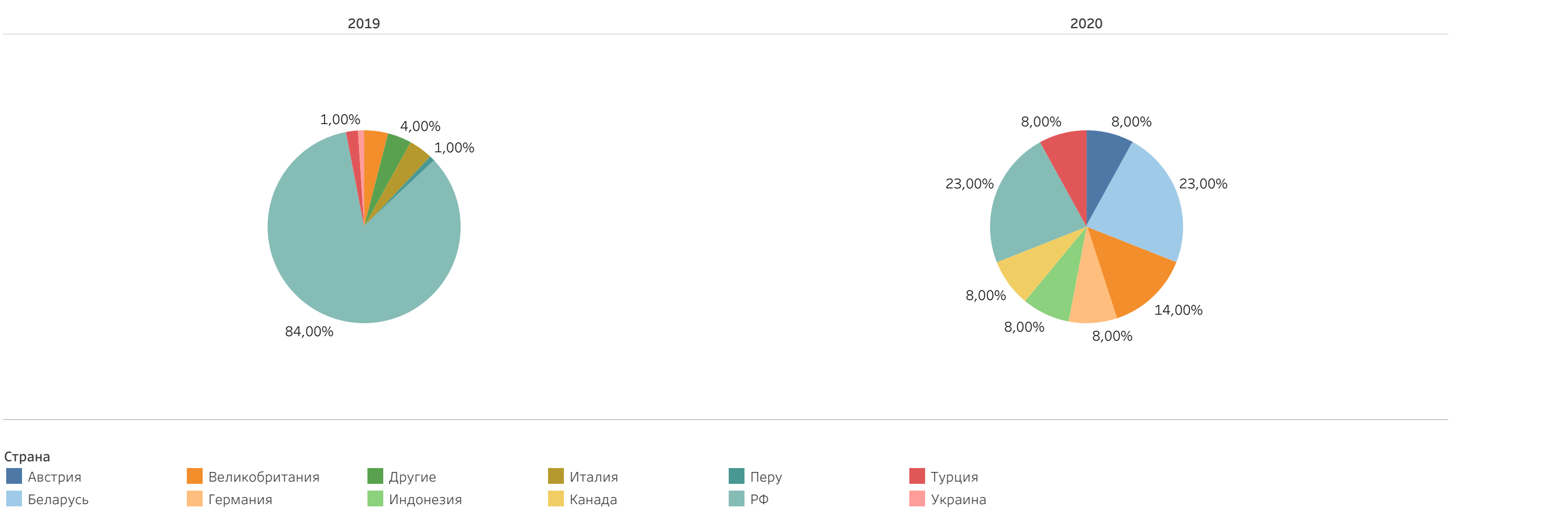


Количество мошеннических операций в разрезе мест их совершения (эмиссия, %)

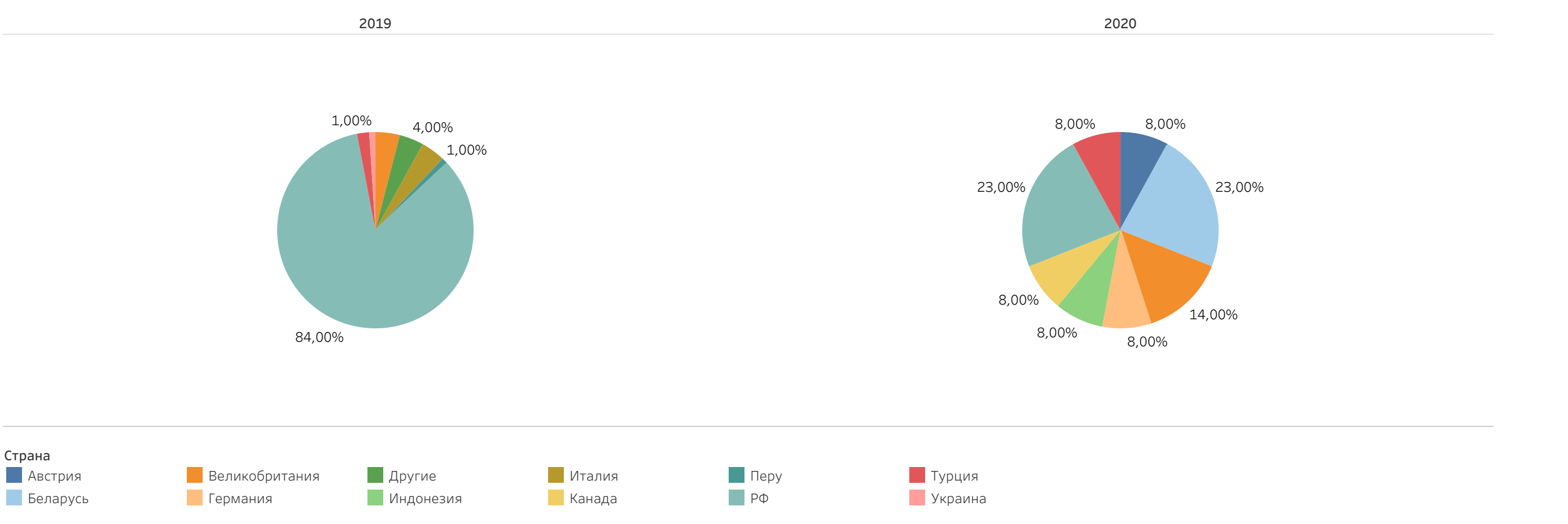


Операции с поддельными карточками (CFT)

Страны, в которых осуществлялись операции по поддельным карточкам банков, подключенных к ОАО "Банковский процессинговый центр"



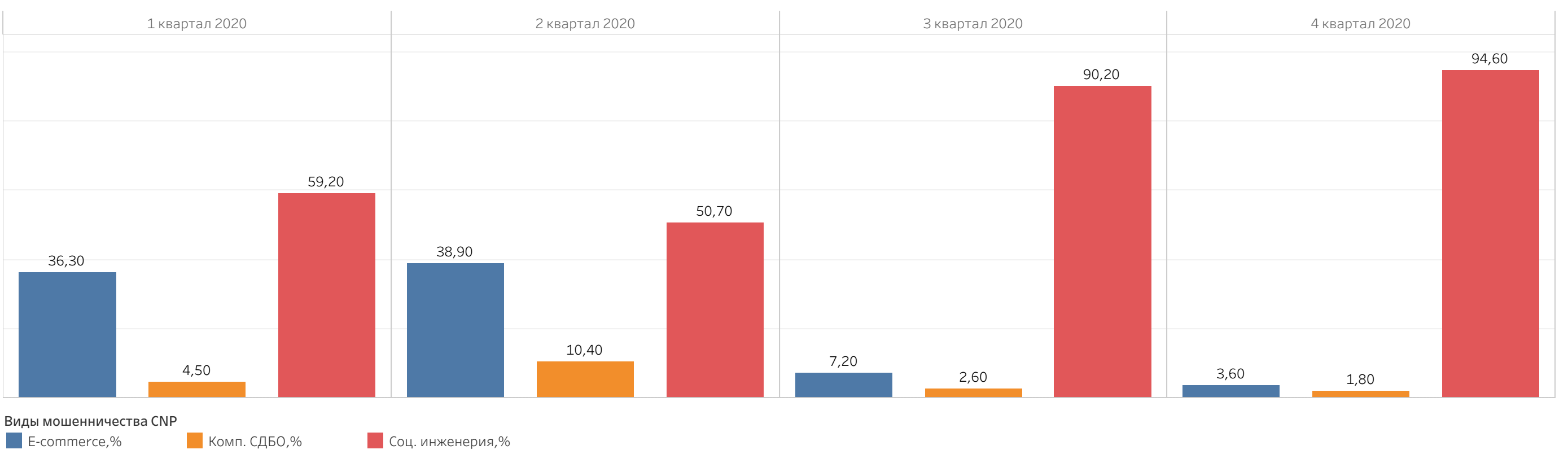
Страны, в которых подвергались скиммингу карточки банков, подключенных к ОАО "Банковский процессинговый центр"



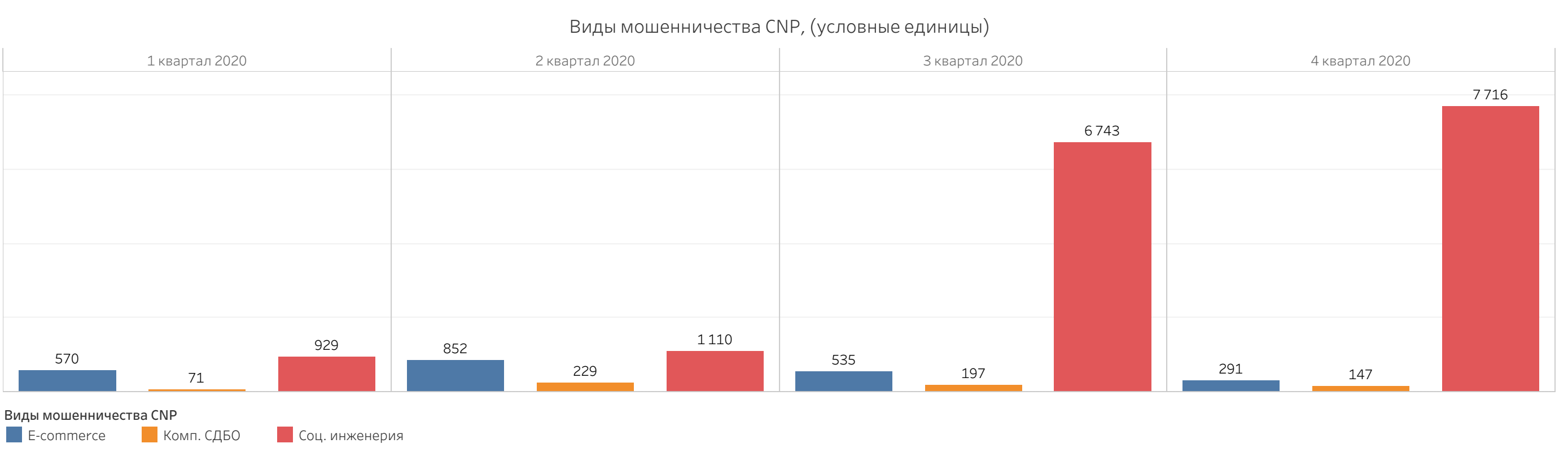
Мошеннические операции с использованием реквизитов карточек (CNP)

Основными тенденциями мошенничества с использованием реквизитов карточек в 2020 году являются:
- всплеск мошенничества с использованием методов социальной инженерии (фишинг, вишинг, взлом учетных записей пользователей в социальных сетях);
- мошеннические звонки держателям в результате утечки в марте 2020 года персональных данных на маркетплейсе «Joom»;
- наличие фактов компрометации СДБО клиентов в рамках социальной инженерии. Злоумышленники получают логины/пароли и ключи доступа к СДБО;
- мошенничество по токенам. Злоумышленники с использованием методов социальной инженерии выманивают у держателей не только номер карточки и 3-D Secure пароль, но и данные, необходимые для присвоения токена к карточке, привязывают токен держателя на свое мобильное устройство;
- рассылка в социальных сетях уведомлений о выигрышах, держатели сами вводят реквизиты карточек для получения приза/выигрыша;
- увеличение доли мошеннических операций на онлайн-сервисах, которые занимаются продажей цифровых товаров: компьютерных программ и игр (взлом аккаунтов учетной записи Google, после чего злоумышленники осуществляют большое количество операций оплаты Google сервисов на мелкие суммы в пределах остатка баланса на счете держателя);
- большое количество мошеннических тестовых операций и атак на БИНы банков (сгенерированные номера карточек) на сайтах, зарегистрированных на территории США, Индии и Бразилии;
- возобновление в начале 2020 года попыток мошеннических онлайн возвратов от ОТС, зарегистрированных на территории США;
- присутствие фактов «friendly fraud» мошенничества.

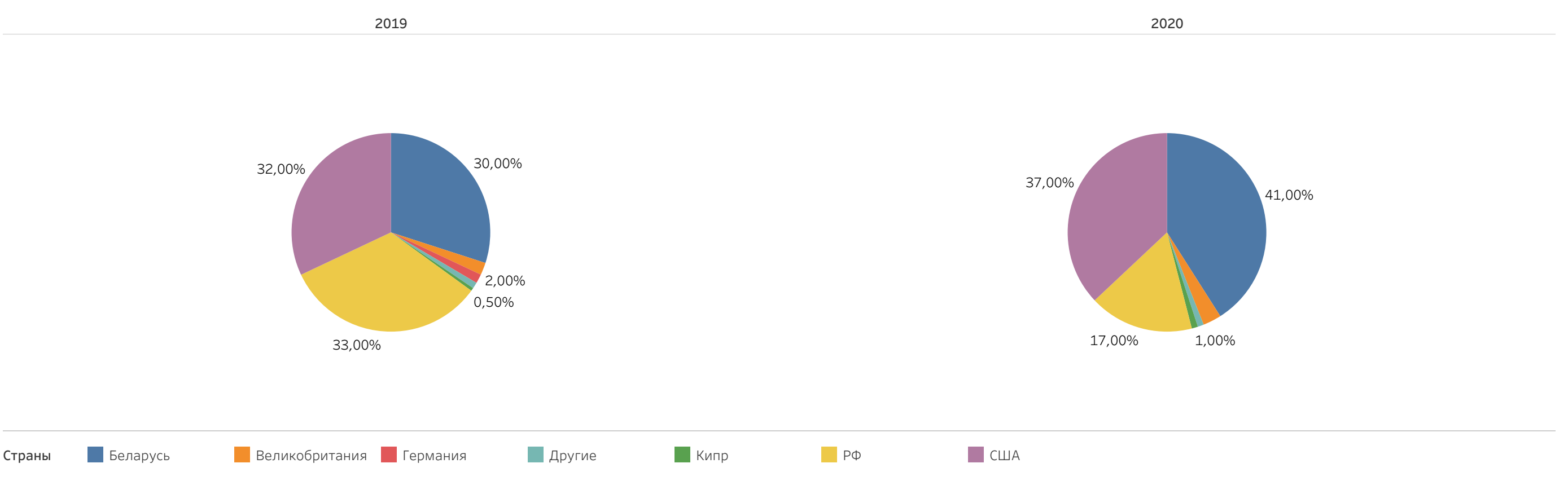
Виды мошенничества CNP, %



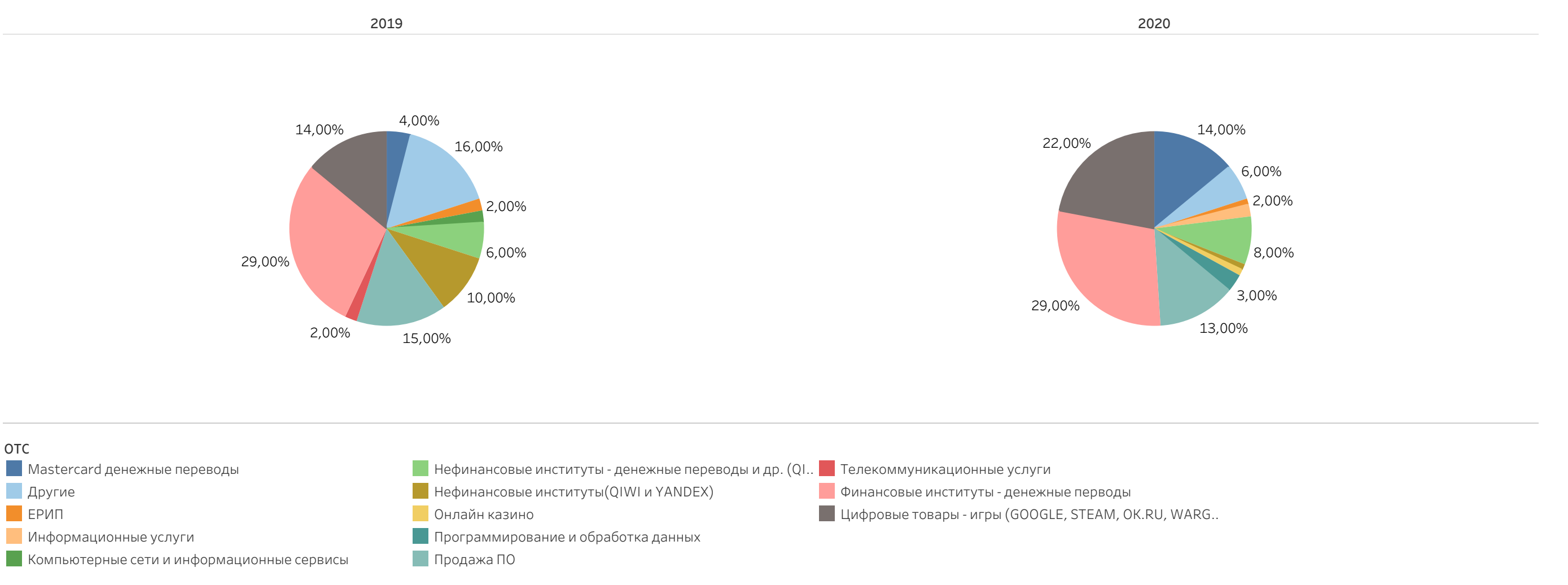
Виды мошенничества CNP, (условные единицы)



Страны, в которых осуществлялись мошеннические операции с использованием реквизитов карточек банков, подключенных к ОАО "Банковский процессинговый центр"



ОТС (категории ОТС), в которых осуществлялись мошеннические операции с использованием реквизитов карточек банков, подключенных к ОАО "Банковский процессинговый Центр"

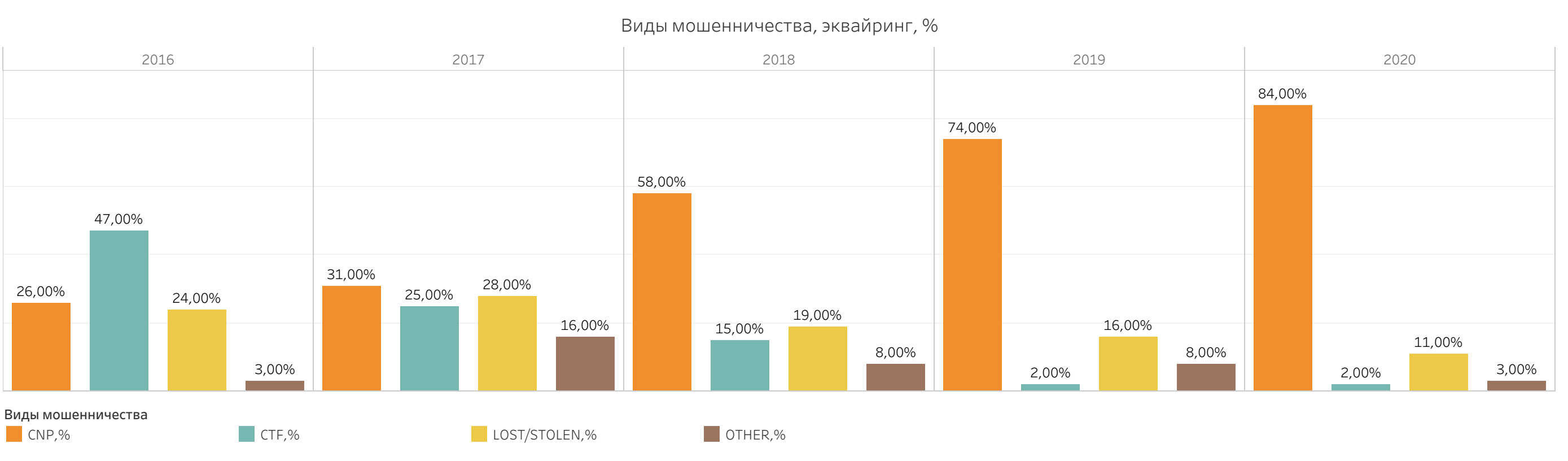


В связи с увеличением количества случаев мошенничества, обусловленных применением социальной инженерии, в частности телефонного мошенничества, для предотвращения несанкционированного доступа злоумышленников к денежным средствам, напоминаем о необходимости соблюдения простых мер безопасности, которые не позволят мошенникам ввести Вас в заблуждение и получить конфиденциальную информацию. Предлагаем ознакомиться с актуальными рекомендациями по противодействию мошенничеству с использованием социальной инженерии и обучающими роликами на сайте ОАО «Банковский процессинговый центр».

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

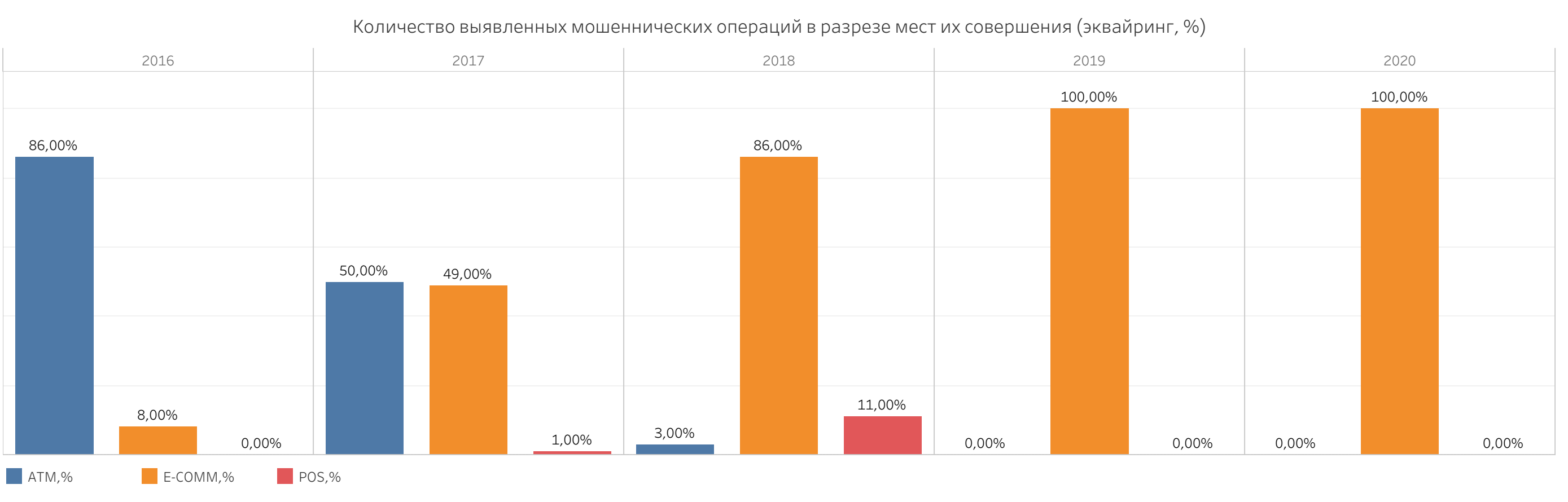
В 2020 году операций мошеннического характера в эквайринговой сети банков распределились следующим образом: **84%** составляют мошеннические операции **без присутствия карточки** (78% это операции с использованием 3-D Secure); **11%** приходится на долю мошеннических операций **по утерянным/украденным карточкам; 2%** приходится на мошеннические операции с использованием **поддельных карточек** и **3%** приходится на **другие виды мошенничества:** 50% составляет account takeover, 30% - мошенничество, при котором карточка выпущена банком, но не получена держателем; 18% - мошенничество, связанное с выпуском карточки по поддельным данным; 2% - incorrect processing.
В целом уровень мошенничества в эквайринговой сети можно охарактеризовать как стабильно низкий, доля мошеннических операций к общему объему операций составляет всего около 0,000063%.

Виды мошенничества, эквайринг, %



Количество мошеннических операций в разрезе видов (эквайринг, условные единицы)

Количество выявленных мошеннических операций в разрезе мест их совершения (эквайринг, %)



Прогноз на 2021 год:

Согласно последним мировым тенденциям мошенничество с использованием платежных инструментов и сервисов все больше смещается в сферу электронной коммерции, при этом наблюдается и рост мошенничества с использованием методов социальной инженерии. Ситуация с мошенническими операциями в Республике Беларусь имеет аналогичные тенденции.
Принимая во внимание общее увеличение случаев мошенничества с большой долей вероятности в 2021 году для злоумышленников будут актуальны следующие способы мошенничества:

- **Социальная инженерия**. Мошенничество с использованием приемов социальной инженерии по-прежнему останется на первом месте по степени распространения угрозы и будет существовать пока держатели сами не начнут проявлять осознанность и с разумной осторожностью относиться к любым сообщениям и входящим звонкам.
- **Перехват доступа к СДБО и МСИ**. Мошенничество предоставляет злоумышленникам широкий спектр возможностей, ввиду получения контроля над всеми карточками и счетами держателей, появляется возможность открывать кредитные линии. Также одной из самых больших проблем для СДБО будет использование атакующими одноразовых ссылок на веб-фишинг.
- **Атаки шифровальщиков**. Трояны-вымогатели, блокирующие доступ к данным и требующие выплаты определённой суммы злоумышленникам для возвращения доступа к ценной информации, будут оставаться серьезной угрозой. При этом киберпреступники теперь не только блокируют информацию, но и угрожают её разглашением, если пострадавшая сторона откажется от уплаты выкупа.
- **Атаки на удалённых сотрудников**. Непростая ситуация с пандемией коронавируса вынудила организации массово переводить персонал на дистанционную работу. Согласно прогнозам Acronis, в 2021 году количество атак, направленных на удалённых сотрудников, возрастёт, поскольку защита систем вне корпоративной сети легче поддаётся взлому.
- Мошенники станут чаще использовать **искусственный интеллект**. Для достижения своих целей злоумышленники всегда стараются применять новейшие цифровые разработки. Уже сейчас технологии искусственного интеллекта используются в криминальной среде для создания так называемых дипфейков. Также злоумышленники активно применяют искусственный интеллект для повышения эффективности вредоносного ПО, обхода механизмов защиты CAPTCHA, подбора паролей, анализа больших массивов данных с целью извлечения номеров телефонов и карточек. Специалисты Trend Micro Incorporated считают, что в перспективе искусственный интеллект будет активно использоваться в мошенничестве, связанном с социальной инженерией, а также в схемах с автообзвоном.

Стоит понимать, что любые новые технологии влекут за собой и новые идеи у мошенников, направленные на хищение денежных средств, поэтому финансовым институтам стоит стараться быть всегда на шаг впереди, чтобы успешно отражать атаки.