БАНКОВСКИЙ ПРОЦЕССИНГОВЫЙ ЦЕНТР

ОТЧЕТ

о тенденциях и случаях мошенничества в сфере банковских платежных карточек за 2019 год

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. **При сравнении данных в абсолютных значениях используются значения в условных единицах.**

Общая информация:

Уровень мошенничества на территории Республики Беларусь, как и ранее, можно охарактеризовать как стабильно низкий, при этом следует отметить постоянное увеличение случаев мошенничества с применением фишинга и социальной инженерии, что свидетельствует о необходимости повышения уровня финансовой грамотности населения.

Количество случаев установки скимминговых устройств, массовой компрометации данных держателей карточек на территории Республики Беларусь значительно снизился. Также уменьшился ущерб, наносимый мошенниками. В 2019 году причиненный держателям ущерб от скимминга на территории Республики Беларусь составил около 3 600 белорусских рублей, причем виновником единственного случая компрометации в апреле 2019 предположительно является тот же мошенник, который устанавливает скимминговые устройства старого образца на банкоматы в Минской области с 2016 года.

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

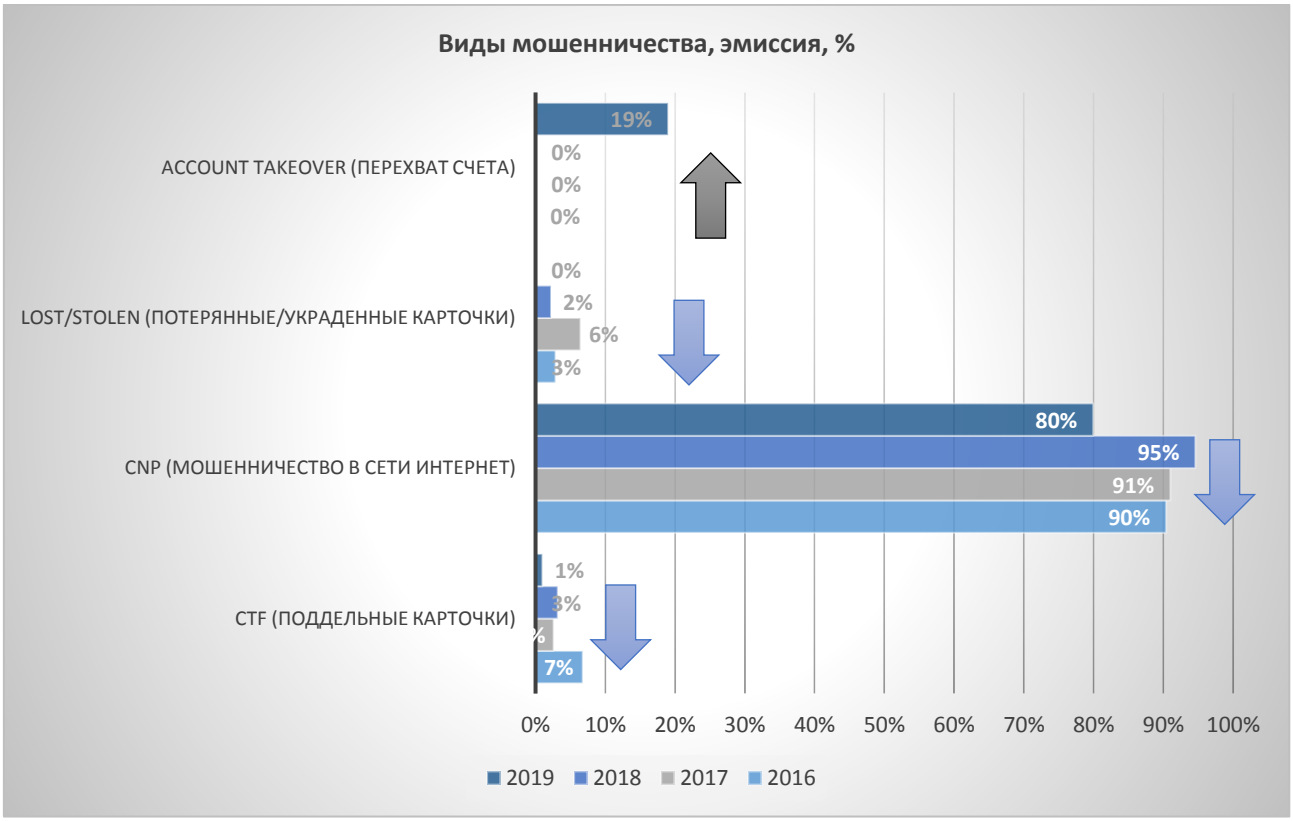
Как и в предыдущие годы, основной тенденцией остается увеличение доли мошеннических операций с использованием реквизитов карточек наряду со значительным снижением количественных показателей мошенничества с использованием поддельных и утерянных/украденных карточек, а также увеличение доли мошенничества по типу account takeover мошенничество, при котором осуществляется перехват данных держателей и, получая контроль над счетом, мошенники совершают безаутентификационные операции (мошеннические операции после компрометации с использованием социальной инженерии с 2 квартала 2019 года по рекомендациям международных платежных систем Visa и Mastercard заявляются банками-эмитентами как операции без аутентификации account takeover), что соответствует общемировой тенденции увеличения уровня мошенничества с использованием реквизитов карточек, которые были скомпрометированы посредством социальной инженерии, и непосредственно связано с недостаточным уровнем киберграмотности и неосторожностью держателей карточек, а также появлением большого количества новых схем фишинга для выманивания у держателей под различными предлогами реквизитов карточек и конфиденциальных данных, необходимых для проведения операций, включая логины и пароли от систем дистанционного банковского обслуживания.

По итогам 2019 года количество мошеннических операций по карточкам банков, которые обслуживаются в ОАО «Банковский процессинговый центр», по типу мошенничества распределилось следующим образом: **80%** мошеннических операций приходятся на мошенничество **с использованием реквизитов карточек**, **19%** незаконных операций с банковскими платежными карточками приходятся на **account takeover (социальная инженерия)**, **1%** приходится на мошенничество по **поддельным карточкам**, при этом в 2019 году были зафиксированы **2 случая** проведения мошеннических операции с использованием **утерянных/украденных карточек.** По сравнению с 2018 годом в 2019 году на 15% уменьшилась доля мошеннических операций без присутствия карточки за счет выделения отдельного мошенничества по типу account takeover, доля операций с использованием поддельных карточек снизилась до уровня 1%, при этом практически до 0% уменьшилась доля мошеннических операций по утерянным/украденным карточкам.

В 2019 году по сравнению с предыдущим годом следует отметить увеличение общего количества мошеннических операций по всем видам в 2,7 раза, при этом общая сумма всех мошеннических операций увеличилась в 1,8 раза, а средняя сумма 1 мошеннической операции в 2019 году уменьшилась практически в два раза и составила 28 долларов США (43 доллара США в 2018 году). Изменение показателей в 2019 году обусловлено увеличением мошенничества account takeover (включено в других видах мошенничества) после компрометации данных с использованием социальной инженерии, а также устойчивой тенденцией увеличения количественных показателей мошенничества с применением социальной инженерии в мире в целом наряду со снижением средней суммы мошеннической операции для сокрытия мошенничества под видом характерного поведения держателя.

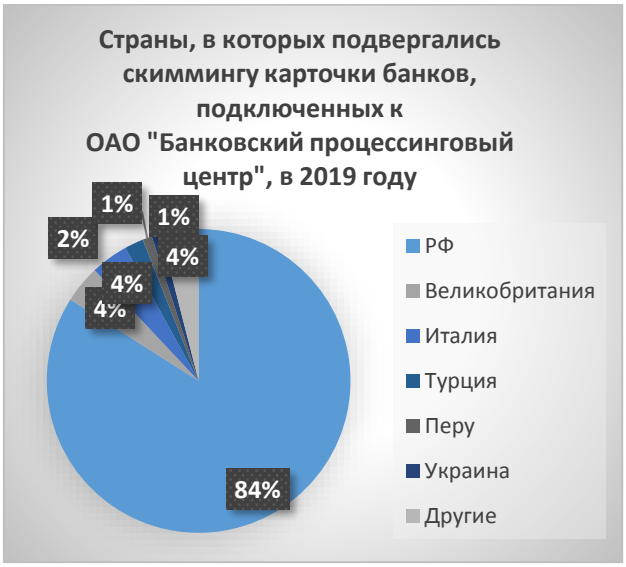
По сравнению с 2018 годом на 18% снизилось количество успешных мошеннических операций с использованием поддельных карточек, что обусловлено постоянным совершенствованием Центром правил мониторинга Fraud Management, так как **98%** таких операций были выявлены работниками отдела контроля операций.

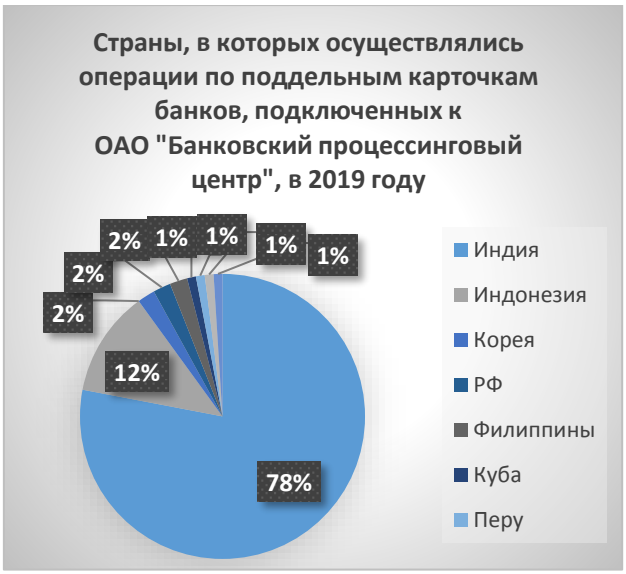
Детальная информация за последние годы представлена на диаграммах ниже.

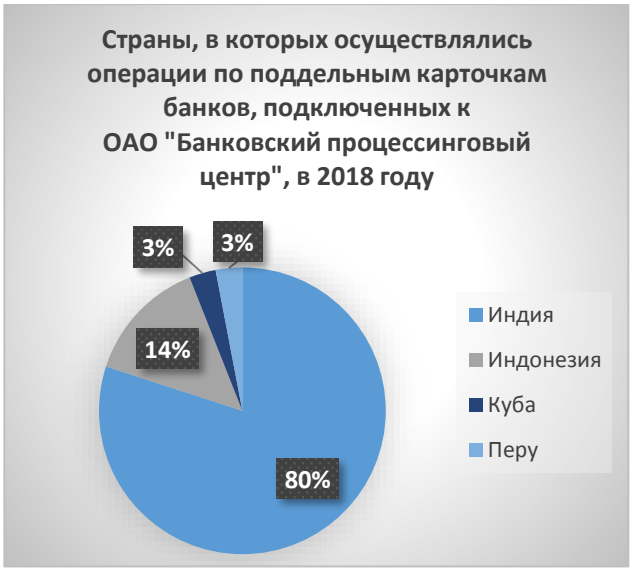

Виды мошенничества, эмиссия, %
ACCOUNT TAKEOVER (ПЕРЕХВАТ СЧЕТА)
LOST/STOLEN (ПОТЕРЯННЫЕ/УКРАДЕННЫЕ КАРТОЧКИ)
CNP (МОШЕННИЧЕСТВО В СЕТИ ИНТЕРНЕТ)
CTF (ПОДДЕЛЬНЫЕ КАРТОЧКИ)
19%
0%
0%
0%
0%
2%
6%
3%
80%
95%
91%
90%
1%
3%
7%
0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
2019 2018 2017 2016


Количество мошеннических операций в разрезе видов
(эмиссия, условные единицы)
4004
2261
1714
1391
953
49
104
64
58
2
0
0
0
CTF
CNP
LOST/STOLEN
OTHER
2016 2017 2018 2019

Операции с поддельными карточками:







В 2019 году выявлено значительное количество случаев неуспешных попыток проведения мошеннических операции с использованием магнитной полосы, а также попытки совершения операций с признаками технологии EMV и ввода пин-кода по сгенерированным карточкам в ОТС Бразилии; неуспешная попытка обналичить денежные средства по украденной карточке в г. Москва; случай обналичивания денежных средств по утерянной карточке в г. Минске; случаи неуспешных попыток проведения мошеннических операций по бесконтактной магнитной полосе в кафе быстрого питания в США: данные были скомпрометированы ранее также на территории США (вероятно в качестве пластика использовалась реальная карточка с чипом), а также на территории Индии (вероятно в качестве пластика использовалась реальная карточка с чипом); случай неуспешной попытки проведения мошеннических операций в торговой сети Target США после компрометации в транспортной сети г. Лондон (Великобритания); успешная мошенническая операция по магнитной полосе в терминале ОТС США на борту самолета (вероятно, держатель просто забыл о проведении операции); попытка использования поддельной карточки в ОТС занимающейся продажей разнообразных товаров в Корее после компрометации в банкомате в г. Санкт-Петербург.

По итогам 2019 года, как и в предыдущем году, лидером по использованию поддельных карточек в банкоматах остаются страны Азии: 78% – Индия (93% карточек было скомпрометировано в г. Санкт-Петербург, Российская Федерация), 12% – Индонезия, по 2% на Российскую Федерацию, Корею и Филиппины, оставшиеся 4% приходятся на Кампучию, Кубу, Перу и Тайланд. Выбор мошенников для осуществления мошеннических операций с использованием поддельных карточек соответствует распространению обязательных требований МПС по участию стран в программах переноса ответственности Chip Liability Shift Program.

Следует отметить, что 84% от общего количества скомпрометированных карточек, по которым прошли мошеннические операции с использованием поддельных карточек в 2019 году, подверглись скиммингу на территории Российской Федерации в г. Санкт-Петербург и г. Москва (68% в 2018 году), по 4% в Великобритании и Италии, 2% в Турции, и по 1% на Украину (14% в 2019 году), Австрию, Болгарию, Хорватию, Мексику и Перу.

Мошеннические операции с использованием реквизитов карточек:

Основными тенденциями мошенничества с использованием реквизитов карточек в 2019 являются:

- проведение мошеннических операции на интернет-ресурсах торговцев, зарегистрированных на территории Республики Беларусь и Российской Федерации (в том числе сервисы переводов, ЕРИП и телекоммуникационные услуги), обусловленное компрометацией данных держателей посредством фишинга с применением социальной инженерии и взлома учетных записей пользователей в социальных сетях, включая появление новых для Республики Беларусь, но широко известных методов фишинга: рассылка коммерческих предложений от имени банка и различных компаний, звонков мошенников от имени банка, создание поддельных сайтов имитирующих СДБО банков, выманивание необходимых реквизитов от имени покупателя на общедоступных ресурсах по продаже товаров и др.;

- появление нового вида мошенничества, основанного на проведении попыток мошеннических онлайн возвратов от ОТС, зарегистрированных на территории США. Вид мошенничества появился в 1 квартале 2019 года и основан на формировании авторизационного кредитового сообщения по операции возврат с последующим выводом денежных средств с карточек посредством снятия

кредитных денежных средств или переводом на другие карточки/счета «дропами» без последующего выставления ОТС операций возврат в клиринг;

- увеличение количества мошенничества с учетными записями Google Play и привязанными к ним карточками: мошенники, получая доступ к учетной записи, перепродают ее либо покупают различную игровую валюту с целью дальнейшего сбыта; также одной из разновидностей являются мошеннические приложения, которые обманом снимают со счетов деньги (их нельзя отнести к вредоносному ПО, поэтому исследователи предложили понятие fleeceware («обирать»)) после окончания пробного периода (часто 2-3 дня) либо за покупки в приложении без предварительного предупреждения о стоимости, в случае авторизации в них через Google account;

- большое количество попыток мошеннических атаках на БИНы банков (сгенерированные номера карточек);

- появление в сети Интернет объявлений со ссылкой на скам-сайты, призывающие принять участие в опросах и получить за это вознаграждение, целью таких опросов является получение данных банковской платежной карточки и доступа к денежным средствам на ней. Все операции инициируют сами держатели, им приходят оповещения о выигрыше или компенсации крупной суммы в долларах США за прохождение опроса. Учитывая, что выигрыш предлагается в иностранной валюте, то за конвертацию необходимо уплатить комиссию. Никакого выигрыша участники опроса не получают, но оставляют реквизиты карточек;

- 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;

- стабильно высокий уровень количества компрометации данных держателей карточек посредством вредоносного программного обеспечения, а также на различных сайтах с сомнительной репутацией.

Стремительное развитие высокотехнологичных устройств в определенной степени способствует появлению и такому же активному распространению новых видов мошенничества, совершаемых с использованием мобильных средств связи. Предлагаем ознакомиться с рекомендациями по безопасному использованию мобильных устройств на сайте ОАО «Банковский процессинговый центр», в частности, изучить новый раздел «Рекомендации по безопасному использованию мобильных устройств».

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

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

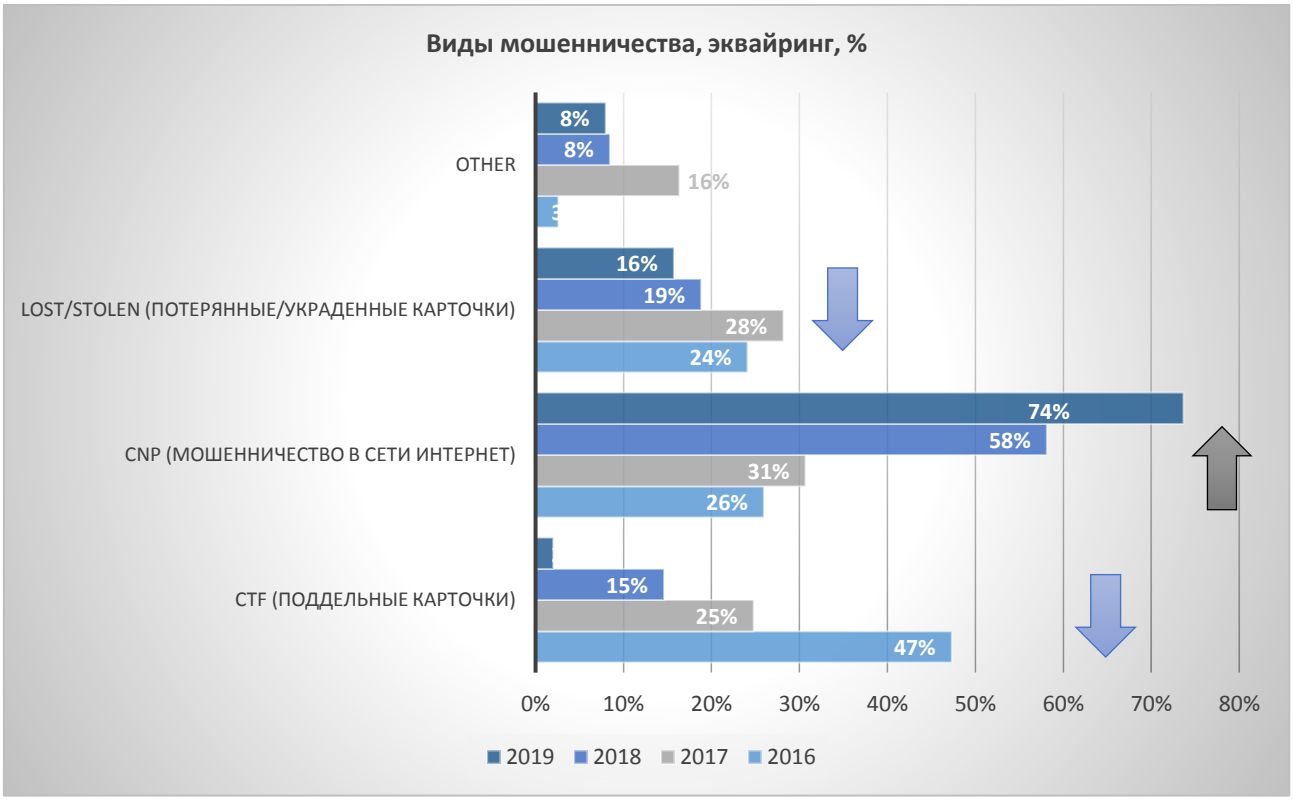
В 2019 году были зафиксированы 1291 случай операций мошеннического характера в эквайринговой сети банков, которые обслуживаются в ОАО «Банковский процессинговый центр», что в 4 раза превышает показатель предыдущего года. Из них: **74%** мошеннических операций с банковскими платежными карточками банков-нерезидентов приходятся на долю **операций без присутствия карточки, 16%** составляет мошенничество **по утерянным/украденным карточкам, 2%** приходятся на операции с использованием **поддельных карточек** и **8%** на **другие виды мошенничества,** из них: 67% приходятся на **account takeover** - мошенничество, при котором осуществляется перехват данных держателей и, получая контроль над счетом, мошенники совершают безаутентификационные операции, 23% составляют **multiple imprint fraud** - вид мошенничества, при котором сотрудники торгового предприятия делают на импринтере более одного отпечатка карточки (multiple imprints), используя их в дальнейшем для генерации новых платежных документов, или изменяют значения размера транзакции уже после того, как клиент подписал слип (**multiple imprint fraud** с высокой долей вероятности был ошибочно заявлен иностранным банком-эмитентом), 8% составляют **never received as issued** - вид мошенничества при котором карточка выпущена банком, но не получена держателем и 2% приходятся на **fraudulent application** - мошенничество по карточке, выпущенной на украденный или поддельный документ, принадлежащий другому человеку.

Общая сумма мошеннических операций в 2019 году по сравнению с 2018 годом увеличилась на 52%, при этом средняя сумма 1 мошеннической операции снизилась в 2,7 раза по сравнению с 2018 годом и составила 76 долларов США (208 долларов США в 2018 году). Рост количества и общей суммы мошеннических операций обусловлен всплеском заявленного иностранными банками-эмитентами мошенничества с использованием реквизитов карточек в интернет-магазинах цифровых услуг и приложении по оплате топлива на заправках, количество мошеннических операций в этих трех торговцах составляет 65% от общего мошенничества в 2019 году в эквайринговой сети банков, подключенных к ОАО «Банковский процессинговый центр».

Увеличение количественных показателей мошенничества в сети Интернет связано с ростом количества интернет-магазинов, находящихся на обслуживании у банков, подключенных к ОАО «Банковский процессинговый центр», при этом сфера интернет-торговли неизменно вызывает повышенный интерес у злоумышленников, т.к. не требует дополнительных сопутствующих расходов и позволяет быстро получить «легкий доход». В целях дополнительного контроля банкам-эквайерам необходимо осуществлять тщательное слежение за выплатами возмещений обслуживаемым интернет-торговцам и обращать внимание на резкие увеличения сумм возмещений и количества операций. Также актуальной мерой безопасности является введение страховых депозитов в размере половины от предполагаемого оборота денежных средств по карточкам в терминалах торговца за месяц или увеличение сроков осуществления возмещения денежных средств для высоко-рисковых и новых клиентов. Дополнительно в качестве меры безопасности для новых торговцев можно рассмотреть запрет проведения операций без проверки дополнительной аутентификации 3D Secure по карточкам иностранных банков. Заключение договора на эквайринговое обслуживание и выдача терминального оборудования даже одному недобросовестному клиенту может повлечь скачек уровня мошеннических операций и, как следствие, финансовые потери со стороны банка.

В целом, уровень мошенничества в эквайринговой сети можно охарактеризовать как стабильно низкий, при этом доля мошеннических операций к общему объему операций составляет всего 0,000063%.

Детальная информация за последние годы представлена на диаграммах ниже.


Виды мошенничества, эквайринг, %
OTHER
LOST/STOLEN (ПОТЕРЯННЫЕ/УКРАДЕННЫЕ КАРТОЧКИ)
CNP (МОШЕННИЧЕСТВО В СЕТИ ИНТЕРНЕТ)
CTF (ПОДДЕЛЬНЫЕ КАРТОЧКИ)
8%
8%
16%
16%
19%
28%
24%
74%
58%
31%
26%
15%
25%
47%
0%
10%
20%
30%
40%
50%
60%
70%
80%
2019
2018
2017
2016


Количество мошеннических операций в разрезе видов
(эквайринг, условные единицы)
951
203
103
255
88
34
45
140
109
179
130
100
58
14
58
26
CTF
CNP
LOST/STOLEN
OTHER
2016
2017
2018
2019

Прогноз:

Ситуация с мошенническими операциями в Республике Беларусь, как в части эмиссии, так и в эквайринговой сети, по сравнению с другими странами, находится на достаточно низком уровне. При этом распределение по типам мошенничества и способам хищения данных соответствует общемировым тенденциям.

Основываясь на последних тенденциях, электронная коммерция постепенно вытесняет традиционных ритейлеров. При этом у каждого пользователя сети Интернет более 100 учетных записей. Перехват данных учетных записей в мире удваивается каждый год на протяжении последних четырех лет. Принимая во внимание увеличение количества случаев компрометации личных данных пользователей в социальных сетях в 2019 году, с большой долей вероятности в 2020 году мошенничество с использованием приемов социальной инженерии выйдет на первое место по степени распространения угрозы. Социальная инженерия может иметь множество форм. Широко известны схемы, при которых жертв вынуждают раскрывать логины, пароли, данные банковских платежных карточек, осуществлять переводы через банкоматы и мобильные приложения. При этом злоумышленники используют различные каналы, чтобы связаться с жертвой: телефонные звонки, мессенджеры, социальные сети. Развиваются и новые формы: например, набирает популярность схема, когда мошенники просят пользователя установить на мобильный телефон средство удаленного управления и таким образом получают доступ к любым приложениям и данным на устройстве. Атаки на личные устройства пользователей не потеряют актуальности, поскольку для большинства людей удобство при работе с гаджетом важнее, чем безопасность личных данных. Вероятнее всего, злоумышленники будут совмещать атаки на гаджеты с классическими методами социальной инженерии (например, с мошенническими звонками по телефону с целью получить банковские данные). Мошенники очень изобретательны, поэтому гарантированно противостоять им может только сам пользователь, для этого достаточно действовать более осознанно и с разумной осторожностью относиться к любым сообщениям и входящим звонкам, а также повышать уровень финансовой грамотности.

Атаки с использованием уязвимостей сайтов продолжатся и в 2020 году ввиду их высокой эффективности. Обычный пользователь не может обезопасить интернет-ресурс, на котором он оплачивает покупку, ответственность за противодействие атакам несут владельцы сайтов. При этом держателям карточек стоит более внимательно относиться ко всем ресурсам, где они вводят данные: если это неизвестный или не проверенный сайт, то стоит взвесить все за и против, прежде чем рисковать своими данными. Считается, что более крупные и известные на рынке компании надежнее защищают пользователей от атак, но одной только широкой известности бренда недостаточно, есть примеры атак, когда именно крупные бренды становились жертвами и ставили под угрозу своих пользователей. В свою очередь участники финансового рынка могут столкнуться с необходимостью открыть инфраструктуру и данные для сторонних субъектов, желающих предоставлять дополнительные услуги их клиентам, в этих условиях существует вероятность, что злоумышленники попытаются эксплуатировать эти механизмы взаимосвязи при помощи новых мошеннических схем.

В 2019 году появились совершенно новые семейства вредоносных программ для банкоматов. В связи с сокращением количества банкоматов в мире вредоносные программы для банкоматов становятся более таргетированными. В 2020 году возможно увеличение количества атак на банки и процессоры.