

# безопасность

## Отпетые кибермошенники

— технологии —

Сколько современные системы безопасности способны предотвращать нанесение ущерба как банкам, так и их клиентам.

В частности, для защиты клиентов в банке «Открытие» используется система фрод-мониторинга (фрод — мошенничество), система уведомления клиентов о проведенных операциях, системы защиты дистанционных каналов обслуживания, информирование клиентов о правилах безопасного пользования банковскими сервисами. В прошлом году банк «Открытие» запустил зонтичный комплекс превентивного мониторинга для выявления мошеннических схем, который позволяет централизованно контролировать более 15 систем банка.

На днях пресс-служба ВТБ сообщила, что банк завершил тестирование голосового антифрода — системы, которая позволяет распознавать звонки клиентам и в банк со стороны мошенников. Массовый запуск новой технологии запланирован на 2021 год. «В конце 2020 года был запущен обновленный ВТБ-онлайн, который стал значительно безопаснее. Теперь мы готовы запустить в работу систему голосового антифрода, которая минимизирует активность злоумышленников при звонках в контакт-центр. Мы последовательно усиливаем защиту всех каналов коммуникаций между клиентом и банком», — комментирует внедрение новой технологии заместитель президента — председателя правления ВТБ Анатолий Печатников.

В работе контакт-центра ВТБ уже применяется биометрическая идентификация клиентов с помощью голосовых слепков. Технология представляет собой идентификацию по голосу, которую можно сделать добровольно, и позволяет узнавать клиента с точностью, близкой к 100%. Комплекс мер по противодействию мошенничеству и применению фрод-мониторинга в 2020 году позволили предотвратить финансовые потери свыше 9,2 млрд руб. для 100 тыс. клиентов — физических лиц, сообщает пресс-служба ВТБ.

Киберпреступники могут пытаться обойти банковские антифрод-си-



Популярность среди киберпреступников набирают схемы отъема денег с использованием QR-кодов

стемы, которые могут охватывать весь спектр каналов проведения операций, а также искать уязвимости в антивирусном программном обеспечении банковских приложений, не сомневаются специалисты Центробанка. Но для мошенников это более трудный путь, поскольку банки заинтересованы в своей информационной безопасности и совершенствуют свои системы защиты от кибератак и несанкционированного доступа. Появляются новые, современные меры и технологии защиты.

Партнер адвокатского бюро «Ахметов, Хозяйкин и партнеры» Иван Хозяйкин подтверждает, что обращений за юридической помощью от пострадавших стало больше, и связывает это с формированием нового вир-

туального рынка и многократным ростом спроса на дистанционные услуги. При этом сейчас, по его словам, и без того невысокие шансы вернуть похищенное еще уменьшились. «На заре зарождения этого „бизнеса“ мошенники действовали несколько топорно, с ними научились бороться крупные сервисы типа „Авито“, а также банки, которые вели просветительскую работу среди клиентов. Но противодействие научило и мошенников — они стали более изощренными. На мой взгляд, хищение теперь сложнее доказать, да и мало кто вообще пишет заявления по данному факту», — говорит адвокат.

Объясняется это тем, что большинство похищенных сумм не превышает 50 тыс. руб. «Если мошенничество персонифицировано, установлено, кто общался, тогда шансы выйти на мошенника есть, хотя и минимальные. А когда в хищении задействованы „колл-центры“ из мест лишения

свободы, когда списываются деньги посредством получения доступа к персональным данным карты, вероятность найти мошенников практически нулевая. Даже если можно установить адресата, кому эти деньги пришли, реквизиты карты часто бывают не связаны непосредственно с мошенниками (это так называемые «номиналы»). Состав преступления в их действиях практически невозможно установить. В моей практике ни разу не было, чтобы нашли конечного адресата», — подытожил Иван Хозяйкин.

### Основы кибергигиены

Банки не возвращают потери, если человек сам скомпрометировал данные своей платежной карты и добровольно перевел деньги мошенникам или сообщил свою конфиденциальную информацию. В 2019 году клиенты смогли вернуть лишь седьмую часть потерь — 870 млн руб., предупреждает Центробанк и дает совет, что делать

в случае мошенничества. Прежде всего пострадавшему необходимо как можно скорее связаться со своей кредитной организацией для блокировки карты и обратиться в банк для подачи заявления о несогласии с операцией и возврате денежных средств.

По закону банк обязан вернуть деньги при выполнении двух условий: сообщение от клиента о краже денег поступило в банк не позднее следующего дня, после того как банк уведомил его о подозрительной операции; клиент сам не сообщил мошенникам данные карты (при краже карты — не хранил ПИН-код вместе с картой и не писал его на самой карте, а также не позволял никому фотографировать карту или делать ее ксерокопии). Если банк докажет обратное, то не вернет украденные деньги.

Необходимо также написать заявление в полицию. Если клиент не нарушал договор с банком и вовремя сообщил о незаконной операции,

но банк отказывает в возврате денег, необходимо обращаться в судебные органы. По закону банк обязан уведомлять клиента обо всех операциях. Если мошенники украли деньги, а банк не сообщил об операции, то по закону он обязан возместить потери (даже если кража была обнаружена клиентом не сразу).

«При поступлении звонка из псевдобанка нужно просто прекратить разговор. Ни в коем случае не вступать с мошенником в дискуссию, так как мошенник в своем разговоре использует приемы и методы психологического воздействия. Вследствие этого он добьется своей цели и похитит ваши деньги. Сотрудник банка никогда не будет спрашивать у вас номер карты, СМС-коды, просить установить программы и уж тем более угрожать, что заблокирует карту, если вы не согласны делать то, что он говорит», — дают рекомендации в пресс-службе УВД по Пермскому краю.

«Необходимо, насколько возможно, минимизировать предоставление своих паспортных данных (в особенности — копий паспортов) лицам и организациям. При подаче заявки на получение кредита через сайт любого банка (что стало очень популярным в последнее время) необходимо убедиться в том, что именно этот ресурс является официальным порталом кредитной организации», — предупреждают в банке «Открытие».

«В последнее время мошенники часто представляют работниками социальных служб и сообщают о „начисленной субсидии“ или „единовременной выплате к празднику“. При возникновении сомнений необходимо прервать разговор и ни в коем случае не предоставлять любые данные (номера документов, банковских карт, CVV-коды, пароли из SMS-сообщений) — сотрудники банков и государственных органов никогда не задают подобных вопросов», — подчеркивает Валентина Жильцова.

Во избежание проблем с кредитными и займами, незаконно оформленными мошенниками на добросовестных граждан, эксперты советуют регулярно проверять наличие задолженностей с помощью доступных электронных и иных официальных сервисов, например портала «Госуслуги». **Татьяна Власенко**

## Уроки безопасности

Умные технологии и цифровые сервисы сегодня не только упрощают быт. Они являются эффективными инструментами для создания безопасной среды в школах, детских садах и на других социальных объектах. Но помимо технической оснащенности требуются грамотное управление современными системами безопасности. В Перми выработали свой уникальный подход в этой сфере. В 2018 году несколько образовательных учреждений Дзержинского района были объединены по территориальному принципу в единый кластер безопасности. В итоге количество правонарушений сократилось на 10%. Сегодня таких кластеров уже три, в них вошли несколько десятков объектов.

### ДЕЛО ТЕХНИКИ

Идея с кластерами стала новым этапом в работе муниципалитета по усилению безопасности в системе образования. Вопросы безопасности город начал активно заниматься еще в начале 2010-х, когда школы постепенно стали передавать непрофильные функции по обеспечению порядка частным охранным организациям, которые занимаются этим профессионально. К 2018 году уже 99% школ, за исключением круглосуточных интернатов, пользовались услугами лицензированных охранных предприятий.

Кроме того, в течение нескольких лет проводилась работа по техническому оснащению детских садов и школ. Прежде всего, были установлены ограждения по периметру всех образовательных учреждений. «Мы начали в 2013 году с детских садов — с закрытия всех периметров. В 2018 году дошла очередь до школ. Мы устанавливали заборы и домофонные системы, чтобы ограничить доступ посторонних лиц. Теперь попасть на территорию школы можно только через пост охраны, получив пропуск», — рассказывает начальник управления имуществом комплекса департамента образования администрации Перми Рената Шарипова. Кроме того, школы и детские сады стали оснащать дополнительными камерами на-

блюдения. Это было связано с новыми требованиями по установке камер: необходимо было обеспечить стопроцентный охват всей территории учреждений. Это места общего пользования: зоны рекреации, коридоры, столовые, вестибюль и прилегающая территория.

Помимо этого, на все эвакуационные выходы были установлены магнитные замки. При срабатывании автоматической пожарной сигнализации (АПС) они открываются автоматически. «Не нужен никакой специальный ключ и человек, который будет бегать и открывать двери. Например, если в ночное время произошло задымление или ложное срабатывание АПС, двери откроются автоматически, пожарные смогут попасть в здание без наличия административного персонала. Тем более что мы отказались от ночных сторожей, объекты стоят на сигнализации», — добавляет Рената Шарипова. Параллельно с усилением технической составляющей в сфере безопасности социальных объектов муниципалитет задумался о более эффективных подходах к управлению этой сферой. К поиску новых эффективных решений подтолкнули и происшествия в российских школах. В пермском департаменте образования разработали пилотный проект по созданию кластера безопасности. Его суть в том,

что разные социальные объекты, расположенные на одной территории, обслуживаются одной лицензированной охранной организацией.

В городском департаменте образования говорят, что для сокращения времени реагирования в различных ситуациях руководствуются географическим принципом, он является основополагающим. Одна охранная организация обслуживает один микрорайон.

Охранники меняются по объектам внутри района. Они знают обстановку, а также примерный контингент учащихся и сотрудников школ.

### ЭКСПЕРИМЕНТАЛЬНЫМ ПУТЕМ

Пилотный проект «Кластер безопасности» был запущен с сентября 2018 года в объектах социальной сферы (образование, спорт, культура) микрорайона Пролетарский, Железнодорожный и Ануловский. В него вошли семь образовательных учреждений Дзержинского района Перми: школы №55, 111, «Мастерград» и «Мультипарк», а также детские сады №203, 407, «Конструктор успеха». На оснащение участников кластера было направлено около 7 млн рублей.

С сентября 2019 года в городе начал функционировать еще один кластер безопасности. В него были объединены учреждения в Индустриальном районе Перми: 13 объектов образования, четыре объекта спорта и один объект культуры (всего 18 объектов, 31 здание). С октября 2019-го в городе был запущен кластер №3 в Мотовилихинском районе города Перми в части физической охраны (без дооснащения оборудованием). В него вошли 14 объектов образования и один объект спорта (всего 15 объектов и 24 здания).

В каждом кластере был выбран единый подрядчик —

учреждения проводили совместные торги и заключали контракт с охранной организацией. Срок контракта составляет три года, договоры действуют до настоящего времени.

В департаменте образования администрации Перми отмечают, что еще на этапе разработки конкурсной документации были установлены более жесткие требования к потенциальным исполнителям. Помимо стандартных условий о наличии лицензии на охранную деятельность и удостоверений у охранников, появились требования по количеству штатных сотрудников, по обязательному наличию в штате группы быстрого реагирования (ГБР), которая курсирует по району. При этом время ее прибытия должно составлять не более восьми минут.

Образовательные учреждения периодически проверяют выполнение этого норматива. Они проводят «контрольные закупки»: вызывают ГБР, фиксируют, за какое время группа прибывает на место. По данным ведомства, на практике это происходит за пять-шесть минут. Кроме того, ГБР дежурит, когда охраннику необходимо отлучиться, например на обед. Это обеспечивает взаимозаменяемость на объекте.

Все охранники обеспечены кнопкой тревожной сигнализации. В учреждениях есть стационарные устройства, так и мобильные кнопки. Педагоги также могут установить специальное платное мобильное приложение на телефон. Обслуживание тревожной сигнализации с 2018 года осуществляет Росгвардия. Это обеспечивает взаимозаменяемость на объекте.

Кластерный подход подразумевает, что обслуживанием всех охранных систем (АПС, система оповещения, видеонаблюдение) также за-



нимается один подрядчик. У него аккумулируется вся информация о технической оснащенности и работоспособности систем. В рамках реализации проекта кластеров безопасности создан единый центр хранения видеоданных в облачном хранилище. При этом полномочный сотрудник администрации города может просматривать эти видеоданные в режиме реального времени. «Данные хранятся 30 дней. В случае каких-то инцидентов камеры помогают установить хронологию событий, прояснить, что в реальности произошло. Например, если кто-то из учеников травмировался, можно посмотреть, сам он упал или кто-то случайно толкнул, или была драка, или что-то еще. В таких случаях мы всегда смотрим данные камер, это помогает выявить ответственных», — рассказывает Рената Шарипова.

Этим техническим возможностями систем безопасности в кластерах не ограничиваются. Так, в школе «Мастерград» внедрена инновационная технология распознавания лиц. Электронная карта школьника запрограм-

мирована на биометрические данные держателя карты и синхронизирована с видеонамерами на входе в школу. Таким образом, постороннее лицо не сможет пройти в учебное заведение по карте школьника. Такие же системы установлены в школах «Петролеум», №108, 127, гимназии №1 и лицее №8.

Кластерный подход доказал свою эффективность еще на этапе пилотного проекта. Например, в микрорайонах Железнодорожном и Пролетарском, где он был запущен в 2018 году в качестве эксперимента, количество правонарушений сократилось на 10%. Кроме того, качество услуг, предоставляемых охранными предприятиями, стало выше. Изначально при создании кластеров не было задачи удешевить стоимость услуг лицензированных ЧОП. «Но мы стали предъявлять более жесткие требования, в итоге качество охраны стало выше, а цена осталась примерно на том же уровне (100–110 рублей в час). Охранники в школах и детских садах сегодня более подготовлены, в том числе физически. Они знают нормативную базу, порядок

действий при разных ситуациях — при угрозе теракта, при звонке об угрозе теракта, при посещении постороннего», — поясняет Рената Шарипова. Наряду с этим снизились расходы на охрану учреждений в ночное время. Этого удалось добиться за счет отказа от услуг ночных сторожей и перехода на более надежный вариант — автоматическую сигнализацию.

В департаменте образования администрации Перми отмечают, что с введением кластерного принципа во время различных проверок школ и детских садов стало существенно меньше замечаний, связанных с вопросами безопасности. Такие проверки проводит не только департамент образования, но и Федеральная служба безопасности, Росгвардия. «Результаты мы рассматриваем на антитеррористической комиссии, и претензий к отрасли образования в части безопасности нет. Поэтому, думаю, мы продолжим развивать историю с кластерами, будем рекомендовать и другим учреждениям переходить на эту систему», — заключает Рената Шарипова.