Вайт пейпер

ПОЧЕМУ ВИДЕОНАБЛЮДЕНИЕ ЗА БАНКОМАТАМИ НУЖНО НЕ ТОЛЬКО СЛУЖБЕ БЕЗОПАСНОСТИ БАНКА

СОДЕРЖАНИЕ

Введение 1
Быть ближе к своим клиентам 2
Спорных ситуаций больше нет 3
Распознавание лица 4
Выводы 5

ВВЕДЕНИЕ

Комплексные системы обеспечения безопасности устройств самообслуживания и другого банковского оборудования являются крайне чувствительной частью инфраструктуры финансовых учреждений и других организаций. Зачастую их работа регламентируется множеством документов, в том числе законодательством страны, требованиями национального финансового регулятора и различными международными стандартами безопасности.

Однако к использованию видеонаблюдения, как одного из наиболее эффективных методов защиты от физических атак на устройства самообслуживания, а также мошеннических действий, можно подходить не только с позиции сотрудника службы безопасности. Важным драйвером для внедрения систем видеонаблюдения является повышение лояльности клиентов банка при оперативном разрешении спорных ситуации.

1 БЫТЬ БЛИЖЕ К СВОИМ КЛИЕНТАМ

14 дней – стандартный период разрешения спорных ситуаций при использовании банкоматов для большинства банков в мире

Квалифицированный персонал банка, используя передовые и наиболее зарекомендовавшие себя на рынке решения для видеонаблюдения за банкоматами получает возможность помочь клиенту, забывшему банковскую карту или денежные средства. Оператор системы может восстановить детальную картину произошедшего, используя записи с нескольких камер, в том числе фиксирующих работу картридера, диспенсера наличных и даже внутреннего сейфа.

При этом набор фотографий и видео привязывается к конкретному действию пользователя устройства или транзакции, что существенно сокращает время реакции сотрудников банка и повышает скорость разбора нештатной ситуации. Таким образом, банк приходит на помощь именно в тот момент, когда клиент нуждается в этом больше всего.

65 000+

банковских карт в год остаются забытыми в банкомате

450 000+

случаев оставления наличных в банкомате в год

2 СПОРНЫХ СИТУАЦИЙ БОЛЬШЕ НЕТ

Банкам и независимым сервисным операторам достаточно часто приходится сталкиваться с ситуацией, когда пользователь устройства не доволен качеством выдаваемых банкнот, а в некоторых случаях даже заявляет о не полностью выданной сумме. Зачастую подобные претензии со стороны клиента не являются обоснованными. Это далеко не всегда говорит о попытке манипуляции или мошенничества со стороны клиента, так как пользователь устройства мог по собственной невнимательности ошибиться при вводе суммы для выдачи или забрать не все банкноты, сразу же инициируя контакт со службой поддержки банка и адресуя им свои претензии.

“Исследования показывают, что за 2017 год спорные ситуации при использовании банкоматов обхошлись банковской индустрии в 20 миллионов долларов. Ассоциация ATMIA старается объединить усилия банков, поставщиков решений и других участников бизнеса и выработать эффективную стратегию по снижению этого показателя”

- Дэвид Тенте, исполнительный директор ATMIA U.S.[1]

Это, впрочем, является сомнительным утешением для финансовых организаций, так как ресурсов для разрешения подобной «виртуальной» проблемы требуется не меньше, чем для предотвращения реальных мошеннических действий. К счастью, системы видеомониторинга устройств самообслуживания позволяют банкам оперативно получать материалы, которые могут быть предоставлены самому клиенту, полиции или другим структурам.

Таким образом, само понятие «спорной ситуации» при внедрении соответствующих решений и процедур можно считать устаревшим. Для службы поддержки клиентов банка остаются только лишь нерассмотренные ситуации.

3 из 4

спорных ситуаций при снятии наличных не являются мошейническими[1]

3 УЗНАЙ СВОЕГО КЛИЕНТА

“При использовании технологии распознавания лица, время затраченное на авторизацию в банкомате уменьшается в два раза.”

- Thad Rueter, SecurelDNews, 2017. [2]

С развитием биометрических технологий использование систем видеонаблюдения для распознаваний лиц клиентов начинает набирать обороты. Считывание образа пользователя банкомата является одним из наиболее быстрых и удобных способов авторизации клиента, позволяя упростить работу с устройством. С другой стороны, обезличенные биометрические данные (например, пол или возраст) могут быть использованы для показа целевых рекламных предложений.

Новый пользовательский опыт не только интригует клиентов и мотивирует чаще пользоваться устройствами самообслуживания, но и существенно ускоряет выполнение стандартных банковских операций, уменьшая очереди перед банкоматами, платежными киосками и другими терминалами.

Система ATMeye.iQ является одним из самых популярных специализированных решений для обеспечения безопасности устройств самообслуживания и применяется в 80 странах мира. За последние годы сфера применения решения значительно расширилась: от стандартной функциональности системы видеонаблюдения решение ATMeye.iQ шагнуло в сторону оптимизации рабочих процессов банков или независимых поставщиков услуг видеомониторинга и обработки клиентских запросов.

Интеграция с платформой LUNA позволила банкам использовать ATMeye.iQ для сбора биометрических данных и авторизации технического персонала, инкассаторов или банковских клиентов.

Мошенник:

- Активация защитного сценария («черный список»)

Клиент:

- Более быстрое проведение операций
- Сценарии показа рекламы исходя их личных и обезличенных данных клиента

ВЫВОДЫ

Системы видеонаблюдения за банкоматами, созданные с единственной целью – обеспечивать сохранность денежных средств и самих устройств самообслуживания, можно использовать и для других задач. Главное понимать, что камеры в банках это один из наиболее полезных инструментов сбора данных, будь то данные о клиентах, преступлениях или эффективности отделов. Как использовать получаемую информацию и какие сценарии взаимодействия с клиентом затем реализовывать – исключительно вопрос фантазии самого заказчика.

Компания BS/2 предлагает внедрение современных решений в области видеонаблюдения за устройствами самообслуживания и распознавания лиц для банков и других организаций. Вместе с поставкой оборудования, внедрением программных решений мы разрабатываем оптимальные сценарии, которые позволяют компаниям отделить своих самых ценных клиентов из общей массы и помочь в решении спорных ситуаций.

Переосмысление роли видеонаблюдения позволяет говорить о том, что канал самообслуживания может быть куда более эффективным способом взаимодействия с клиентами банка, чем вы привыкли думать.

Даниэль Фуксон
Руководитель департамента развития бизнеса
Компания Penkiu kontinentu bankines technologijos (BS/2)
+370 (620) 21152 | daniel.fukson@bs2.lt | swsales@bs2.lt

ССЫЛКИ

[1] http://www.atmatom.com/atmia-addresses-atm-withdrawal-dispute-issues-in-the-u-s/
[2] https://www.secureidnews.com/news-item/biometric-atms-use-facial-recognition-instead-of-cards-and-pins/