Безопасность торговых точек, имеющих POS-терминалы

А. А. Комаров
ООО «Группа информационной безопасности» (Group-IB)

Введение

Хищение данных о пользователях кредитных карт и их реквизитов является устоявшимся направлением современного киберпреступного мира. Основными факторами, позволяющими осуществить подобный вид мошенничества, являются недостаточная защищенность и осведомленность самого владельца кредитной карты, а также проблемы с безопасностью непосредственно торговой точки (онлайн – VPOS, оффлайн – POS) (табл. 1).

В 2009 корпорация VISA[1] сделала первое уведомление о том, что была зафиксирована угроза компрометации POS-терминалов, размещенных на стороне мерчантов известных платежных систем, для последующего хищения данных о кредитных картах всех покупателей, обслуживающихся данной торговой точкой. Первостепенно подобного рода инциденты безопасности связаны с недостаточной организационной и технической защищенностью размещенных в сетях ресторанного бизнеса, магазинах и развлекательных заведениях мерчантов, несмотря на отраслевые стандарты и требования к их защите.

Несмотря на то что приложения, которые применяются на стороне Virtual Point-Of-Sale (VSOP) в Интернете, могут соответствовать всем требованиям Visa's Payment Application Best Practices (PABP), сам мерчант может оставаться под большой угрозой, находясь в уязвимом окружении.

Под уязвимостями окружения понимаются инфраструктурные бреши, связанные с ошибками конфигурации сетевого оборудования, организацией удаленного доступа к информации, механизмами установки обновлений прикладного и системного программного обеспечения, организационные аспекты допуска к обслуживанию и технической поддержке внедренных POS-терминалов.

Последний пункт требует особого внимания: как правило, торговые точки не способы осуществлять обслуживание POS-терминалов и установленных программных комплексов по учету и регистрации платежей, почему и нанимают стороннего подрядчика. В большинстве случаев недобросовестные подрядчики подключают сетевые узлы, имеющие непосредственное соединение с POS-терминалом, к Интернету, наделяя злоумышленника возможностью удаленного злонамеренного воздействия.

Классификация современных POS-терминалов по устройству их памяти

По устройству памяти POS-терминалов различают три их основных типа.

***1. POS-терминалы, использующие статическую RAM* (рис. 1).**

Многие POS-терминалы используют статическую RAM для хранения информации о кредитных картах. После насыщения RAM записи переписываются новыми данными. Как показала практика, резкое или штатное отключение питания от устройства не позволяет очистить память от остаточных данных.

Рис. 1. ***Verifone TRANZ 380***

Отдельные модели POS-терминалов имеют специальные комбинации кодов, позволяющие просмот-

[1] *VISA: Point-of-Sale Terminal Tampering Is a Crime... and You Can Stop It [Электронный ресурс]. – Режим доступа: http://usa.visa.com/download/merchants/alert-pos-terminal-tampering-020311.pdf.*

реть список последних транзакций из памяти, чем часто пользуются опытные злоумышленники.

В отдельных случаях удается извлечь всю остаточную информацию, хранящуюся в емкости RAM (скажем, если устройство имеет 16 МБ RAM, вся она доступна злоумышленнику) (табл. 2).

Администраторы могут сконфигурировать POS-терминал с помощью пароля супервайзера (мастер-пароль), чтобы не хранить данную информацию, с последующим запретом создания отчетов о проведенных операциях.

***2. POS-терминалы, использующие Compact Flash* (рис. 2).**

Многие из производителей POS-терминалов используют Compact Flash (CF) в качестве альтернативы статической RAM и энергозависимым носителям информации.

Рис. 2. ***Panasonic's 7900 POS***

Пример риска, связанного с подобными устройствами: они поставляют достаточно гибкий механизм для создания резервных копий и восстановления данных через отдельный ПК и непосредственное отделение CF-карты, на которой хранится вся информация о транзакциях.

***3. POS-терминалы, имеющие подключение к ПК* (рис. 3).**

Отдельный тип POS-терминалов использует жесткий диск подключенного к нему ПК (АРМ оператора или кассира). Данные POS-терминалы более всего подвержены вредоносному коду под платформу Microsoft Windows, чему свидетельствует волна масштабных хищений треков кредитных карт в США и странах ЕС. Большая часть подобных инцидентов происходит по причине внутреннего сговора допущенных к обслуживанию торговой точки лиц либо ввиду слабой защищенности сетевого периметра, из-за чего внешние злоумышленники получают возможность проникнуть в окружение торговой точки.

Таблица 1. ***Основные векторы хищения данных о кредитных картах клиентов банков РФ и стран СНГ***

Наименование	Угроза	Статистика, %
Физическое окружение	«Скимминг» на банкоматах и размещение закладных устройств для перехвата данных[2]	75
	Хищение банкоматов[3]	15
	Несанкционированное использование мастер-ключей банкоматов	7
	Применение ложных POS-терминалов и модификация PED (Pin-Entry-Device)	3
Интернет-окружение	Применение программ web-inject[4] в интернет-браузерах зараженных клиентов	70
	Атаки класса «Content-spoofing» для перехвата реквизитов кредитных карт (распространение ложных страниц оплаты известных платежных систем, PSP, интернет-магазинов, страниц систем e-Wallet и др.)	30

Таблица 2. ***Список комбинаций для извлечения отчетности о проведенных операциях через POS-терминал, данные отчета включают в себя сведения о кредитной карте, что используется злоумышленниками, имеющими допуск к обслуживанию в торговой точке***

POS-терминал	Комбинация для извлечения данных
Verifone TRANZ 380	FUNC/ENTER + 2
Verifone TRANZ 330	ENTER + 31 + ENTER + 0 + ENTER

Рис. 3. ***IBM SurePOS***

Угрозы, направленные на осуществление НСД к информации в контуре сетевой инфраструктуры торговой точки (рис. 4), схожи с традиционными и классическими атаками в корпоративных ЛВС (атаки на перенаправление сетевого трафика – ARP spoofing, DNS poisoning, ICMP redirect) и имеют больший уровень эффективности по причине менее защищенных окружений, что характеризуется следующими факторами:

- отсутствием последних обновлений антивирусного ПО;
- отсутствием специализированных СЗИ по защите от НСД к информации;
- отсутствием профильного штата, отвечающего за вопросы ИБ;
- привлечение к вопросам ИБ аутсорсинговых организаций.

[2] *ATM Secure Revolving System – устройство, предложенное румынской компанией MB Telecom для борьбы со скимингом. Идея заключается в нестандартной вставке кредитной карты по широте, а не длинне, после чего устройство ее разворачивает и отправляет на считывание.*

[3] *ЦБ РФ 34-Т «О рекомендациях по повышению уровня безопасности при использовании банкоматов и платежных терминалов».*

[4] *Программы для автоматического тестирования web-сервисов и web-приложений.*

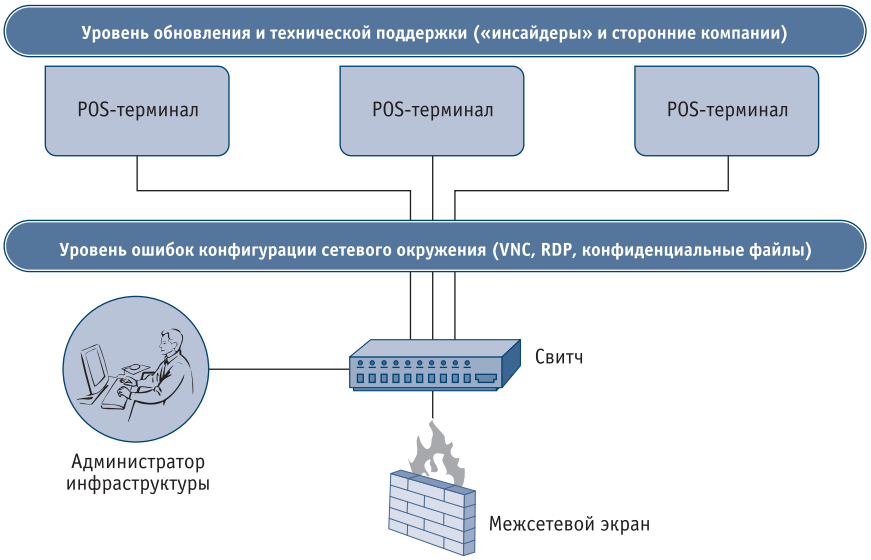

Рис. 4. ***Стандартная топология сетевой инфраструктуры торговой точки***

Рис. 5. ***Выявление POS-терминалов через уязвимые средства удаленного доступа (VNC-серверы, терминальные станции и протокол RDP, серверы Radmin и др.)***

Совокупность перечисленных факторов позволяет злоумышленнику удаленно осуществить выявление уязвимых персональных компьютеров с подключенными POS-терминалами (рис. 5).

Известные инциденты информационной безопасности, связанные с безопасностью мерчантов платежных систем и POS- терминалов

Примеры зарегистрированных инцидентов:

Blanchard's Liquors (Бостон, США) – 27 марта 2013 года.

Владелец торговой точки оповестил своих клиентов о том, что их кредитные карты были скомпрометированы по причине обнаружения специализированного вредоносного кода на POS-терминалах касс магазина.

Сеть магазинов продуктов питания «Schnucks» (США) – 26 марта 2013 года.

Schnuck Markets Inc. проинформировала правоохранительные органы о том, что POS-терминалы кассовых автоматизированных рабочих мест магазина заражены вредоносным кодом. Компания имеет порядка 101 магазина на территории штата Миссури.

Точки продаж «Subway» (США) – 2012 год.

Более 100 точек продаж «Subway» были взломаны, более 146 000 кредитных карт было скомпрометировано, потери составили 10 миллионов долларов США. После этого, при участии представителей крупных сетей ресторанного бизнеса, был разработан так называемый «8-Point Data Security Plan»[5], представляющий собой перечень из восьми фундаментальных пунктов в части обеспечения информационной безопасности на торговых точках с наличием POS-терминалов. Среди них – проведение тестов на проникновение и защита удаленного доступа в случае его использования.

Сеть магазинов «Michaels» (США) – 2010 год.

Персоналом сети были обнаружены более 90 модифицированных PIN-падов (PED), и исследование 964 магазинов показало наличие «хакерских» следов. Модифицированные PIN-пады были изъяты и отправлены на экспертизу.

Устройство современного вредоносного кода под АРМ с подключенными к ним POS-терминалами

Полезная нагрузка современного вредоносного кода под POS-терминалы направлена на сканирование памяти основных функциональных процессов программного обеспечения, реализующего функции взаимодействия с самим устройством, после чего осуществляется выборка данных, характеризующих реквизиты кредитной карты, по сигнатурам (рис. 6).

В отдельных случаях злоумышленники используют специальные уточняющие алгоритмы, позволяю-

[5] *8-Point Data Security Plan [Электронный ресурс]. – Режим доступа: http://www.nacsonline.com/Products/BusinessServices/Documents/NACS_PCATS_WeCareProgram.pdf.*

щие им с высокой точностью выделять номер кредитной карты, дату ее окончания, трек. Одним из них является алгоритм Луна – алгоритм вычисления контрольной цифры номера пластиковых карт в соответствии со стандартом ISO/IEC 7812[6].

Говоря о выделении реквизитов кредитных карт, следует отметить разновидности треков (дорожек), хранящих информацию, записанную на магнитную полосу пластиковой карты.

Track 1. Первая дорожка на магнитной полосе платежной карточки. Представляет собой постоянное запоминающее устройство с плотностью записи 8,3 бит/мм. Содержание записи определяется стандартом ISO 7813. Доступна только для чтения. На первой полосе записан PAN карты (номер карты) и имя ее держателя (если карта именная).

Track 2. Вторая дорожка на магнитной полосе платежной карточки. Представляет собой постоянное запоминающее устройство с плотностью записи 8,3 бит/мм. Содержание записи определяется стандартом ISO 4909. Доступна только для чтения. На второй полосе карты находится главная информация. Она состоит из PAN (номера карты), Expiration Date (даты, по которую включительно карта действительна), Service Code (сервисного кода для работы программы терминала или банкомата с картой), Pin Verification Key Indicator, PVV (Pin Verification Value) и CVV1/CVC1.

Track 3. Третья дорожка на магнитной полосе платежной карточки. Представляет собой запоминающее устройство с оперативной записью и считыванием с плотностью записи 8,3 бит/мм. Содержание записи определяется стандартом ISO 4909. Доступна только для чтения.

Для обслуживания карты в POS-терминале или банкомате обязательно нужен track 2. Данные track 1 и track 3 часто являются необязательными, именно поэтому современный вредоносный код под POS-терминалы, имеющих подключение к персональному компьютеру с жестким диском и собственной RAM, направлен именно на хищение данных со второй дорожки (рис. 7). При наличии похищенного track 2 злоумышленник осуществляет запись track 1 на основе знания номера карты и имени ее владельца.

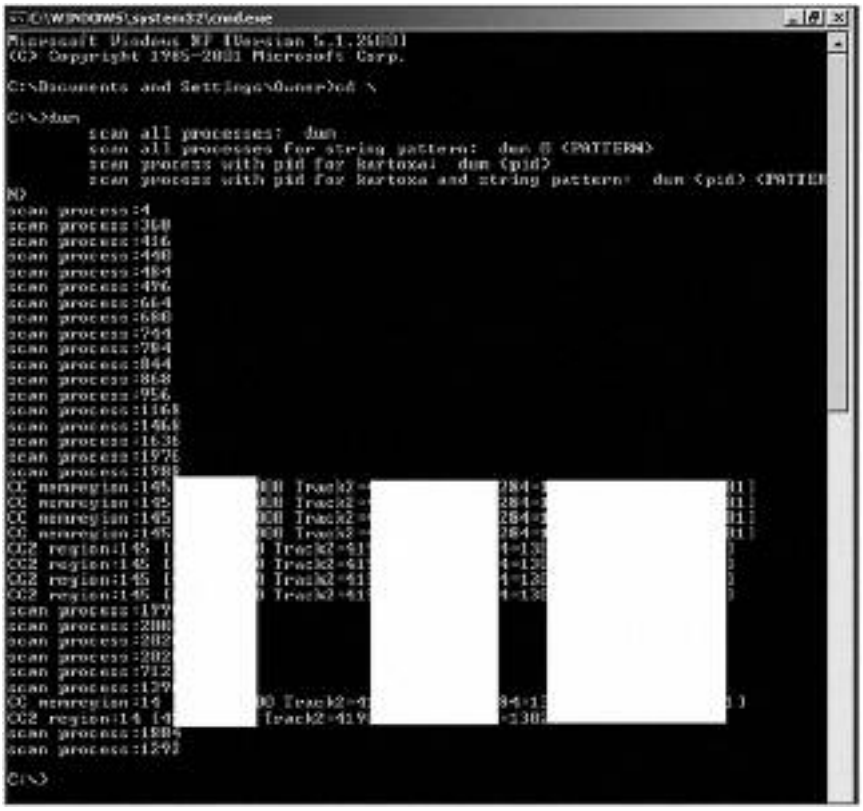

Рис. 6. ***Пример сканирования RAM ПК (АРМ кассира) и выделения Track 2 из остаточной информации***

Рис. 7. ***Командный центр трояна vSkimmer, направленного на хищение Track 2***

В апреле 2012 года специалистами Group-IB была обнаружена модификация подобного вредоносного кода – BlackPOS (рис. 8).

Тем не менее в отдельных случаях вредоносный код ориентируется на длины соответствующих элементов последовательности извлекаемых данных и отдельные критерии для ее различения в дальнейшем (табл. 3).

Модификация электронной компонентной базы PED (Pin-Entry-Device)

Одним из профессиональных методов хищения данных о кредитных картах, включая их PIN-коды,

[6] *ISO/IEC 7812-1:2006 Карточки идентификационные. Идентификация эмитентов. Часть 1. Система нумерации [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/ru/catalogue_detail?csnumber=39698.*

Рис. 8. ***Командный центр BlackPOS с перехваченными данными, которые удалось извлечь после детального реверс-инжиниринга***

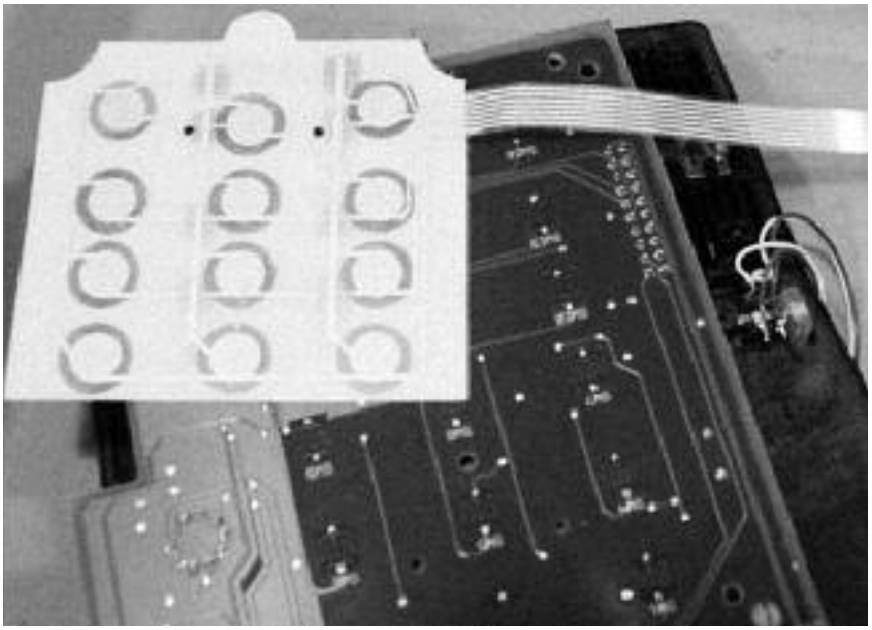

Рис. 9. ***Пример ложной клавиатурной мембраны для PED/POS-терминала, перехватывающей вводимые PIN-коды после считывания Track 2***

Таблица 3. ***Длины элементов последовательности извлекаемых данных и ее критерии***

Наименование	Критерий
Номер карты (PAN)	Между 14 и 16 символами
Платежная система	Первый символ BIN: • VISA – «4»; • MasterCard – «5»; • American Express – «3»; • Discover – «6»
Срок годности	Даты в пролете (2008–2015)

является модификация электронной компонентной базы PED-устройств, в том числе в случаях наличия слабых организационных и регламентных мер по защите информации на торговой точке.

Злоумышленники, пользуясь ослабленным контролем за персоналом, осуществляют несанкционированный физический доступ к PED-устройству, после чего внедряют в него вносимую программно-аппаратную закладку, позволяющую осуществлять отправку перехватываемых данных по беспроводному или альтернативному каналу связи для последующего извлечения.

Наиболее распространенные модели для модификации – VeriFone (PINpad 101, 201, 2000, Everest), Hypercom (S7S, S8) и Ingenico (i3070MP01, i3070EP01, eN-Crypt 2100).

Как правило, модификация PED затрагивает следующие аспекты:

- использование дополнительного считывателя Track 2;
- размещение ложной клавиатурной мембраны (рис. 9);
- размещение радиопередающего модуля;
- интеграция дополнительных ЗУ различной емкости.

Отдельное внимание следует обратить на POS-терминалы, использующие беспроводные каналы связи для взаимодействия, в частности, основанные на протоколах стека IEEE 802.11 (Wi-Fi) и Bluetooth[7]. Подобные беспроводные инфраструктуры, размещенные в общественных местах (ресторанах, ночных клубах, гостиничных комплексах, курортных зонах и др.), представляют для злоумышленников первостепенный интерес.

Ключевыми векторами атак в беспроводных окружениях торговых точек являются:

- атаки на уровень шифрования сетевого эфира для извлечения из него значимых для злоумышленника данных (WEP/WPA);
- эмуляция ложных беспроводных точек доступа и устройств для последующей реализации MitM (Rogue AP/Evil Twin).

Для защиты беспроводных окружений PCI Council разработал специальные методические рекомендации (PCI DSS Wireless Guidelines), направленные на повышение их защищенности и систематический аудит информационной безопасно-

[7] *https://www.wallmob.com/mobilepayment/.*

сти. Одной из рекомендаций является интеграция WIPS (беспроводной системы предотвращения вторжений) – достаточно дорогостоящее решение в условиях традиционных торговых точек.

С учетом обозначенной угрозы, рекомендуется применять только PED, сертифицированные по требованиям PCI PIN Transaction Security Testing and Approval Program Guide[8], обеспечивая средства дополнительного контроля за использованием самих устройств и допущенным к ним персоналом.

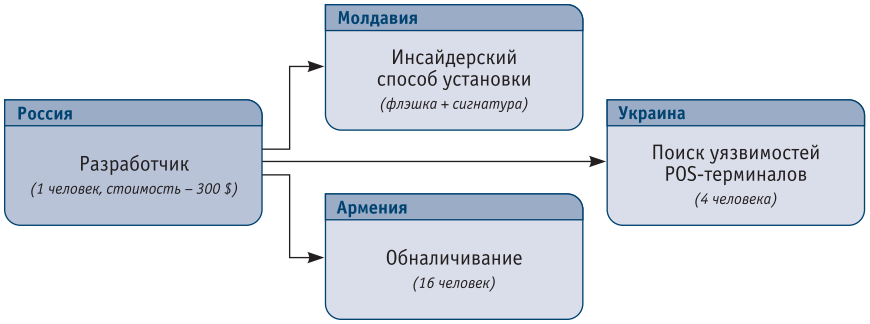

Рис. 10. ***Выявленная преступная группа по мошенничеству с кредитными картами, извлеченными с инфицированных POS-терминалов, отмечается слаженной транснациональной работой в нескольких государствах мира (вывод денег осуществлялся через проведение ложных платежей через заведомо подготовленный мерчант-аккаунт)***

Практика расследований высокотехнологичных преступлений в торговых точках с POS-терминалами

Подобного рода инциденты являются сравнительно затруднительными в расследовании по причине того, что современные злоумышленники накапливают достаточное количество похищенных кредитных карт, после чего постепенно, в разное время года, осуществляют мошеннические действия с ними (рис. 10).

При уведомлении представителей платежных систем о скомпрометированных картах существует возможность уточнить перечень последних использованных преступниками торговых точек и их мерчантов. Для обмена информации о скомпрометированных кредитных картах отдельные платежные системы предоставляют для использования специальные сервисы, например VISA CAMS[9].

Методика исследования мерчантов, где были проведены мошеннические операции либо те, которые были зафиксированы в качестве легитимных, позволяет найти точку распространения угрозы, в частности вредоносного кода. Безусловно, это потребует определенного аналитического подхода и инструментария для установления взаимосвязей между целым перечнем скомпрометированных кредитных карт и использованных ранее мерчантов. Провести

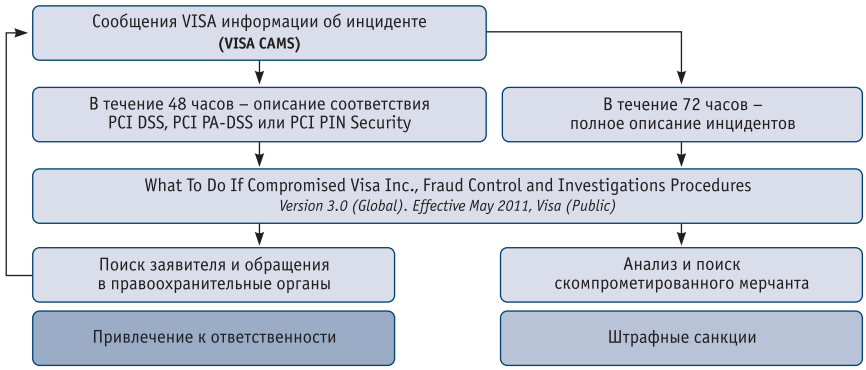

Рис. 11. ***Возможный план реагирования***

подобное исследование можно с помощью инструментария класса I2, позволяющего устанавливать взаимосвязи на основе изучения структурированных данных (рис. 11).

Предложения по повышению безопасности торговых точек и POS-терминалов

По результатам проведенных исследований современного состояния защищенности торговых точек и POS-терминалов в Росии и странах СНГ представляется целесообразным реализация следующих мероприятий, направленных на исправление текущей ситуации:

- разработка рекомендаций со стороны ведущих платежных систем по отношению к торговым точкам, использующих POS-терминалы, систематическое информирование сообщества клиентов;
- разработка перечня требований по обеспечению информационной безопасности торговых точек от лица национальных регуляторов (некоторые требования могут быть заимствованы из отраслевого стандарта PCI DSS и рекомендательных документов PCI Council);
- разработка единой системы мониторинга скомпрометированных кредитных карт и обмена информацией об уязвимых мерчантах, адаптированной к эксплуатации в масштабах государства со стороны ключевых ведомств – ЦБ РФ, Росфинмониторинга, ФСБ РФ, МВД РФ (пример – Group-IB FraudMonitor).

В свою очередь, необходимо обратить внимание владельцев торговых точек, а также обслуживающих их банков на необходимость контроля состояния информационной безопасности. ■

[8] *https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php.*

[9] *Visa's Compromised Account Management System (CAMS) [Электронный ресурс]. – Режим доступа: http://usa.visa.com/merchants/operations/adcr.html.*