PBF-GROUP®

STOPSKIMMER®

ATM
В РОССИИ И В МИРЕ

По оценкам Ассоциации производителей банкоматов, в мире установлено более двух миллионов банкоматов, а общий объем расходов на изготовление и эксплуатацию этих машин достигает 30 миллиардов долларов, а через три года — приблизится к отметке в 50 миллиардов долларов.

Приблизительно каждые 5 минут устанавливается новый АТМ.

Банкомат — одно из самых важных технологических изобретений второй половины двадцатого века, которое является неотъемлемой частью жизни современного общества.

АТМ предоставляет миллионам владельцев кредитных карточек во всем мире удобный доступ 24 часа в сутки 7 дней в неделю 365 дней в году, предлагая клиенту громадное множество возможностей по работе со своим личным банковским счетом:

- Снятие наличных средств
- Ведение кассового баланса по банковскому счету,
- Получение информации и выписок по счету и всем операциям, депозитное обслуживание — прием вкладов населения,
- Проведение внешних платежей с печатью платежных документов (оплата мобильных операторов, коммунальные услуги, оплата ЖКХ, налогов, штрафов и пр.), в любое удобное для клиента время и в любом месте земного шара.

Банкоматы сделали услуги банка более удобными сегодня, чем когда-либо прежде.

БЕЗОПАСНОСТЬ АТМ В РОССИИ И В МИРЕ

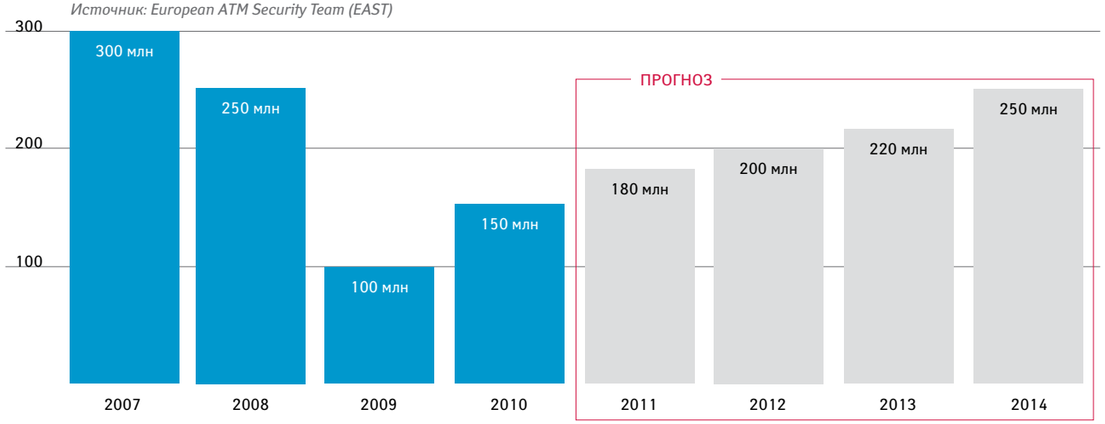
Скимминговые атаки происходят во всем мире, информация о случаях мошенничества была зафиксирована в Азиатско-Тихоокеанском регионе, США, Африке, Европе, Ближнем Востоке, Россия и страны СНГ не исключение. Развитие нестабильной финансовой обстановки в мире, рождает новые виды мошенничества.

Почти все убытки банков по статье мошенничество приходится на карточный скимминг. Прирост случаев карточного скимминга в 2008 году составил 129% и достиг уровня 10320, только официально зафиксированных случаев, увеличив убытки европейских банков до 1,37 миллионов евро на 1000 устройств финансового самообслуживания.

По официальным данным ассоциации European ATM Security Team (EAST), в течение 2008 года убытки европейских банков, связанные с мошенничеством на устройствах финансового самообслуживания, составили 485 миллионов евро, увеличившись по сравнению с 2007 годом на 11%, столь низкий процент роста потерь банков обусловлен активной банковской политикой безопасности по защите АТМ анти-скимминговыми системами и системами видеонаблюдения.

УБЫТКИ ОТ МОШЕННИЧЕСТВА НА УСТРОЙСТВАХ ФИНАНСОВОГО САМООБСЛУЖИВАНИЯ

Источник: European ATM Security Team (EAST)



По статистике в России установлено около 70 тысяч банкоматов и прогноз на ближайшие 5 лет — увеличение данного количества до 100 тысяч банкоматов, так же не стоит забывать о терминалах самообслуживания с возможностью приема международных пластиковых карт. В итоге общее количество к 2015 году легко достигнет планки в 150 тысяч единиц.

На первый взгляд эта цифра кажется внушительной. Однако на самом деле это означает, что в нашей стране на 1 млн. человек приходится всего 400 устройств. Для сравнения, в Европе это же количество человек обслуживает 600, в Великобритании — 800, а в США — 1000 банкоматов.

Это позволяет предположить, что в ближайшие годы количество АТМ-комплексов будет только увеличиваться. Но вместе с приростом числа банкоматов количество случаев несанкционированных транзакций может умножиться.

Безопасность клиента — ключевая задача любого банка

Системы персонализации по отпечаткам пальцев, радужной оболочке глаза пока крайне редко используются в России, — это связано, в основном, с большой стоимостью таких решений и несоответствия затраченных инвестиций и возможных потерь. Поэтому одним из наиболее распространенных вариантов мошенничества является получение денег через аппарат с использованием чужого ПИН-кода.

В этих случаях факт несанкционированной транзакции зачастую выявляется после списания денег со счета, а иногда — лишь в момент получения выписки клиентом. Таким образом, если не подключена услуга СМС-оповещения, промежуток времени получения информации клиентом о проведенных операциях может составить до полутора месяцев. Аналогичная ситуация возможна и при использовании поддельных (мошеннических) карт, полученных в результате скимминга.

Мошенничество основанное на невыдаче или неполной выдаче денег клиенту по его запросу участилась во время мирового кризиса. Недостача наличных в целом по кассе банкомата может объясняться, в частности, тем, что недобросовестный клиент извлёк часть из середины насчитанной пачки купюр.

ЧТО ТАКОЕ STOPSKIMMER?

StopSkimmer® противостоит любым скимминговым атакам на банкомат и терминалы финансового самообслуживания.

Постоянно работающее защитное поле, новейшая технология защитного поля StopSkimmer®, созданная высокотехнологичным излучателем с бесшумной технологией работы и увеличенным радиусом действия, не оставит злоумышленникам не единого шанса.

Контроллер детекторов позволит Вам обнаруживать, анализировать и незамедлительно сообщать об акте скиммига в службу безопасности банка. StopSkimmer® остановит Skimming и Scanning.

Возможности и преимущества

- Новейший запатентованный алгоритм защиты Банкоматов и Терминалов самообслуживания.
- Большой LCD позволяет осуществлять автономный мониторинг и анализ журнала атак с указанием даты и времени события.
- Запатентованная бесшумная технология защитного поля позволит максимально защитить клиентов банка, не отпугивая их.
- Сертификат Ростеста свидетельствует, что объект сертификации соответствует установленным для него стандартам и нормам, существующим в законодательстве Российской Федерации.
- Гарантийный срок 1 год, с возможность дальнейшего продления до 2 лет: вы можете точно спрогнозировать операционные расходы.
- Продукт запатентован №102416.
- Конкурентная цена.
- Отсутствие таможенных пошлин и сокращение сроков поставки.
- Возможность продажи небольшими партиями.
- Возможность предоставления дополнительных сервисов — русскоязычный и англоязычный вариант исполнения.
- Широкие и гибкие возможности закупки дополнительных опций защиты ATM и Терминалов самообслуживания, без замены основного блока.
- Доступен для установки на все известные банкоматы (NCR, Diebold, Wincor) и финансовых терминалов самообслуживания.
- Установка в течение 20 минут уменьшает время простоя банкомата, что является основной единицей измерения эффективности работы ATM.

Расширенный LCD экран позволяет осуществлять автономный мониторинг и анализ журнала атак с указанием даты и времени события

Лицевая панель

Индикация наличия атак на банкомат

Индикация наличия питания устройства и функционирования защитного поля

Какие существуют способы анализа и получения информации?

- Автономный мониторинг и анализ энергонезависимого журнала атак, с указанием даты и времени события.
- Мониторинг и программный анализ скимминговых угроз, с помощью ПК (ноутбука).*
- Он-лайн мониторинг и анализ энергонезависимого журнала атак на АТМ. С указанием даты и времени события. Сопряжение StopSkimmer® с ПО АТМ.
- Возможность просмотра информации со StopSkimmer® в привычном виде для просмотра атак и событий, со всех датчиков системы.
- Сопряжение журнала StopSkimmer® с видео информаци с системы видеонаблюдения Syvison.

** — требуется специализированное ПО для просмотра атак и событий, со всех датчиков системы.*

Мне необходима активная защита, с возможностью обнаружения скимминговых атак.

Все это легко выполнимо с помощью Контроллера датчиков StopSkimmer®, в состав которого входит:

- Детектор установки скиммера: Ливанская петля (Lebanese loops).
- Детектор открытия отсеков банкомата и внешнего модуля BoxVision.
- Старт записи видеорегистратора по сигналам от антискиммера.

Необходима ли замена дорогостоящего устройства при появлении новых скимминговых атак?

Философия и архитектура StopSkimmer® позволяет противостоять будущим атакам путем обновления ПО и добавления новых датчиков в Контроллер Датчиков StopSkimmer®, без замены основного блока управления устройства.

Мне необходимо, получить изображение и проанализировать с данными StopSkimmer® для полной защиты.

Установка StopSkimmer® в защитном боксе BoxVision™ позволяет осуществить легкий доступ к чтению и анализу информации, не открывая банкомат.

Решение спорных ситуаций с невыдачей денег клиенту по его запросу — это сложная и неприятная процедура, тем более во время мирового кризиса.

Система видеонаблюдения для банкоматови финансовых терминалов — Syvision™ позволяет вести видеоконтроль видеозапись и осуществлять последующий поиск видео по событиям, что повышает эффективность использования видеоархива.

Компоненты Syvision™ могут располагаться внутри банкомата при наличии видеоподготовки.

Для установки камер на банкоматы не предусматривающее установку системы видеонаблюдения, PBF Group разработал накладные декоративные панели собственного дизайна.

- Надежное исполнение панелей и креплений на банкомат.
- Возможность изготовления декоративных панелей под заказ, любых форм и цветов.
- Возможность нанесения символики банка.
- Легкая система установки.

Компоненты Syvision™ могут располагаться вне банкомата, в верхнем защитном боксе BoxVision™:

- Уникальный дизайн, качественные материалы надежное исполнение.
- Окраска BoxVision™ соответствует вариантам окраски банкоматов, декоративная вентиляционная перфорация совпадает с перфорацией банкомата, что легко вписывается в дизайн банкомата и воспринимается клиентом как единое целое.
- Тонированное внешнее стекло с возможностью установки портретной камеры по всей длине стекла, с внешней системой крепления, которая не позволяет выдавить стекло.
- Гибкое исполнение внутреннего наполнения и креплений.
- Усиленные петли, расположенные по всей длине BoxVision™, с защитой от выбивания.

** — Если злоумышленники попытаются нейтрализовать защитное поле StopSkimmer®?*
Благодаря созданию запатентованной технологии защитного поля заглушить защитное поле StopSkimmer будет невозможно.

Если злоумышленник отрежет антенну или попытается сделать короткое замыкание антенны излучателя? Он сможет считать данные? Нет, данные с карт клиентов будут сохранены. При обрыве, или при попытке закоротить излучатель защитного поля, StopSkimmer® незамедлительно отреагирует и отключит питание от кардридера банкомата или терминала финансового самообслуживания

Как обезопасить процесс считывания карт клиентов банка? Ведь при наличии и развитии сервисов оплаты мобильной связи и коммунальных платежей, прием и отдача карты происходит многократно, и в каждый момент злоумышленник может украсть данные.

Новейшая запатентованная технология защитного поля StopSkimmer®, созданная инновационным излучателем, с бесшумной технологией работы и увеличенным радиусом действия, надежно защитит вам АТМ и финансовый терминал самообслуживания.

Если злоумышленники обесточат банкомат?

Журнал событий атак с указанием точного времени и даты атаки, надежно защищен и имеет автономное питание.

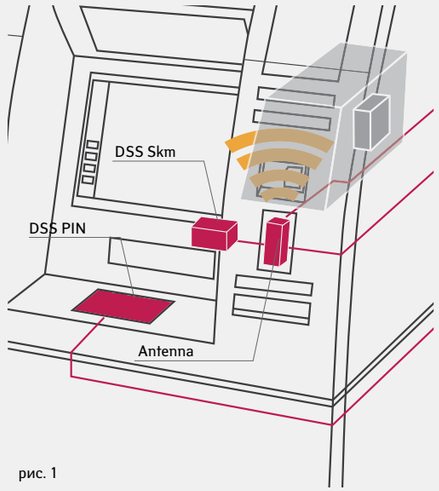


рис. 1

Какие скиммеры остановит StopSkimmer®?

StopSkimmer® защищает банкомат или терминал финансового самообслуживания от всех известных на данный момент видов скиммеров, а именно:

- Аудио скиммер
- Цифровой скиммер
- Цифро-аналоговый скиммер

С любым видом хранения и передачи данных (рис.1).

Как обнаружить скиммингговые устройства, которые способны украсть PIN-код клиента?

Датчик системы активного детектирования установки накладной клавиатуры и накладной скиммингговой видеокамеры позволит Вам детектировать данный вид скимминга (рис.1).

Как защититься от новых перспективных скиммингговых атак?

Мы советуем применять конфигурацию StopSkimmer® Base с системой активного детектирования установки скиммингговых атак DSS. Философия и архитектура StopSkimmer® позволяет противостоять будущим атакам путем обновления ПО и добавления новых датчиков в Контроллер Датчиков StopSkimmer®, без замены основного блока управления устройства (рис.1).

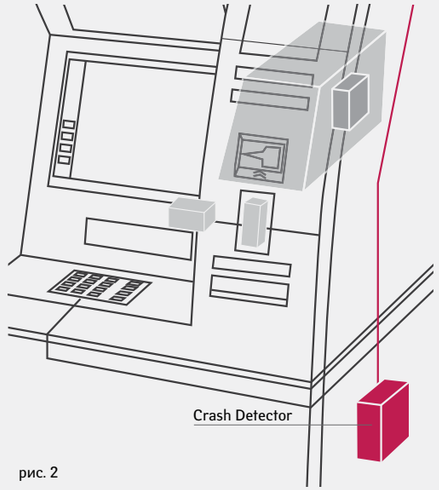


рис. 2

Если злоумышленник попытается высверлить антенну StopSkimmer® и совершить акт вандализма на банкомат?

В этом случае актуально применение вибродатчика Crash Detector. StopSkimmer® незамедлительно зафиксирует акт вандализма в энергонезависимый журнал событий и пошлет тревожное сообщение (рис. 2).

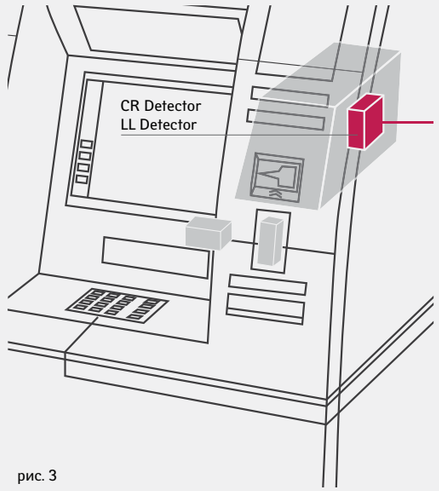


рис. 3

Как бороться против альтернативного вида скимминга - Ливанская петля (Lebanese Loops)?

Детектировать данный вид скимминга можно с помощью датчика LL - StopSkimmer® незамедлительно зафиксирует скимминг, запишет в энергонезависимый журнал событий и пошлет тревожное сообщение (рис.3).

Как защитить CardReader банкомата от актов вандализма?

Вам поможет датчик блокировки шторки CardReader банкомата. StopSkimmer® незамедлительно зафиксирует акт вандализма и пошлет тревожное сообщение (рис.3).

Как узнать, кто установил скиммер?

Вам необходимо установить систему видеонаблюдения на банкомат или терминал финансового самообслуживания SyVision и синхронизировать его с системой StopSkimmer® с датчиком определения скиммера и системой он-лайн мониторинга (рис.4).

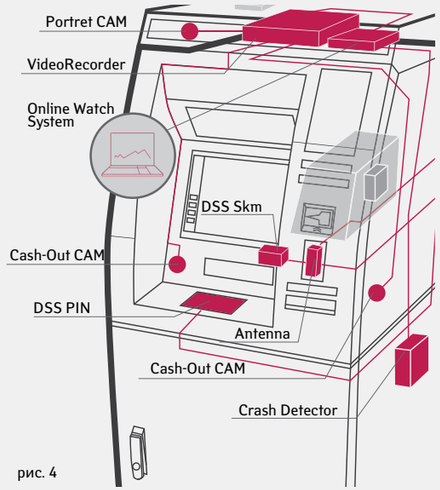


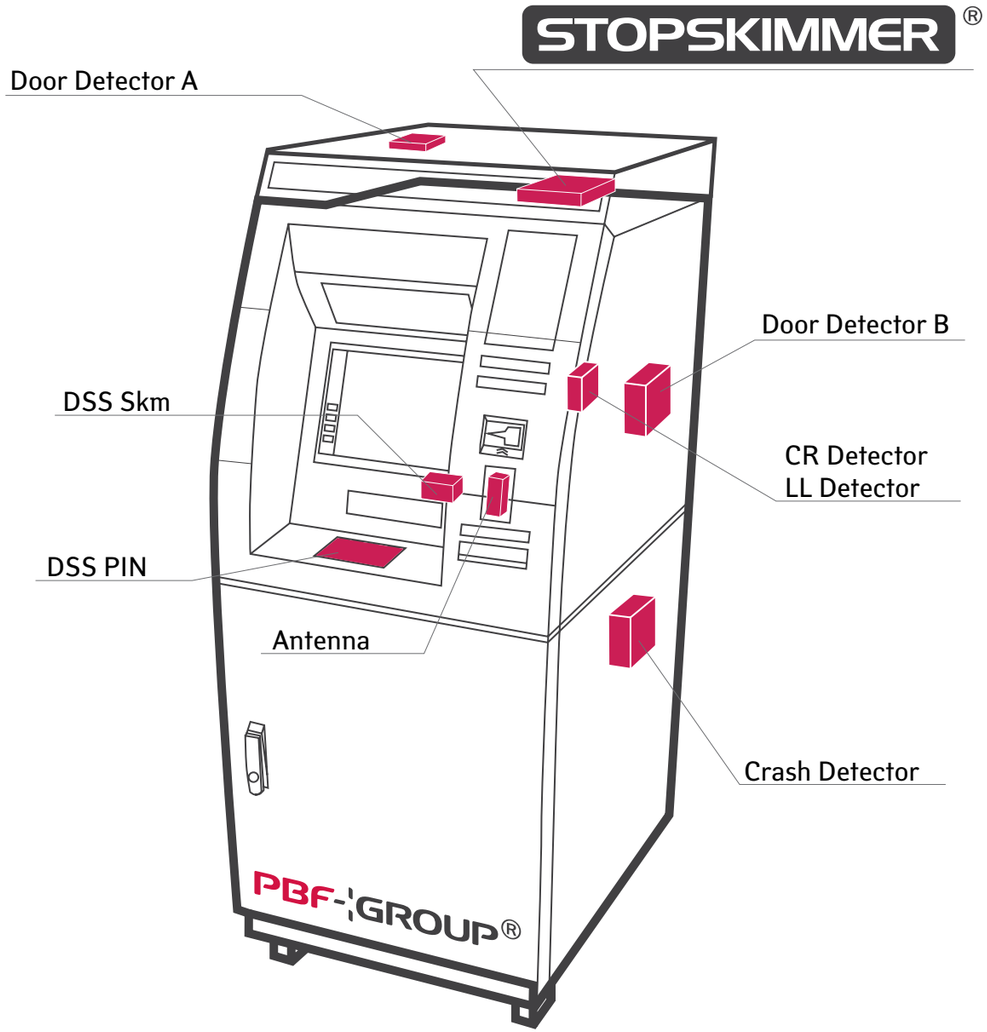
рис. 4

Как получать актуальную информацию о степени защищенности банкомата или терминала финансового самообслуживания в реальном времени?

Вам поможет система он-лайн мониторинга датчиков StopSkimmer®, вы будете иметь полную информацию о Вашем банкомате в реальном времени (рис.4).

Что делать если злоумышленник попадет внутрь отсека банкомата ,поставит скиммер неизвестной модификации, отрежет антенну, а если...?

В этом случае, мы рекомендуем поставить полный набор охранных датчиков StopSkimmer® с видеозаписью по поступающим событиям от них, а так же внедрить систему он-лайн мониторинга. При постоянном контроле, вы будете надежно защищены (рис.4).



Какие антискиммеры производит компания PBF Group?

Компания PBF Group предлагает следующие модели антискиммеров:

StopSkimmer® Base
Базовая модель антискиммеров для защиты банкоматов, с бесшумной технологией защитного поля. Дисплей для автономного анализа атак. Возможность подключения всех датчиков, система он-лайн мониторинга через PC банкомата.

StopSkimmer® Eth
Расширенная модель антискиммера для защиты банкоматов, с бесшумной технологией защитного поля. Дисплей для автономного анализа атак. Возможность подключения всех датчиков, система он-лайн мониторинга не используя PC банкомата.

StopSkimmer® Light
Доступное решение для защиты киосков финансового самообслуживания, с бесшумной технологией защитного поля. Подключение и анализ датчиков невозможен.

За чем ставить StopSkimmer®, если в течение 5 лет пройдет миграция на EVM?

Европейские банки и международные платежные системы начали миграцию на EMV более 10 лет назад, результат на данный момент не утешительный.

Америка пока не спешит переходить на Чип-карты, а это серьезный аргумент.

Так же по данным Euopean ATM Security Team(EAST)

There is still a risk of EMV cards being skimmed as long as they have an active mag-stripe on them.

Пока на EMV картах будет магнитная полоса, данные карты находятся в зоне риска.

«Anti-skimming devices will always have a part to play as long as there are cards with magnetic stripes on them. In some European countries, such devices are mandatory for all ATMs, or for ATMs that have been attacked by fraudsters,» Gunn said.

PBF-GROUP®

ФАДЕЕВ
Евгений Павлович

Основатель
и исполнительный директор
Компании PBF Group

Окончил Московский Авиационный институт в 1970 году
по специальности «Радиоэлектронные устройства».

Создавал различные конструкции радиоэлектронных устройств.

В середине 80-х годов увлекся Микропроцессорной техникой. Увлечение микропроцессорной тематикой привело к смещению акцентов в сторону работ по автоматизации
в банковской сфере.

В 1994 году участвовал в установке и адаптации программного обеспечения
одно из первых банкоматов NCR в России.

В 1996 году компания Hypercom, одна из ведущих мировых фирм по производству банковских решений, решает открыть инженерный офис в Москве. Евгений Фадеев принят на должность технического директора.

Работа в Hypercom продолжалась до 2002 года. За это время было внедрено много технических решений. Последние 3 года работы в Хайперком занимал должность генерального директора.

После ухода из Hypercom им была создана компания PBF Group.

Компания PBF GROUP была образованна в 2002 г. для оказания профессиональных услуг банкам и околобанковским организациям. Диапазон возможностей нашей компании и квалификация наших специалистов позволяют нам подключаться к этим работам на любом этапе, начиная от постановки задачи и кончая гарантийным обслуживанием всех поставленных компонентов мы не используем стандартные решения: вся наша продукция — результат оригинальных разработок профессионального коллектива компании. Вы можете быть уверенными в качестве нашей продукции: каждое устройство в процессе сборки проходит многоступенчатый контроль.

В 2002 г. Компания PBF Group выпускает линейку коммуникационного оборудования ConnecTR для маршрутизации транзакций POS-Терминалов компании Hypercom.

В 2005 г. Компания PBF Group получает статус официального дилера компании Hypercom, лидера в области технологий обеспечения безопасности электронных платежей.

В 2006 г. совместно с банком «Райффайзенбанк Австрия» осуществляет переход на POS-терминальное оборудование нового поколения компании Hypercom.

С 2006 г. Компания анализирует методы защиты Банкоматов и финансовых терминалов обслуживания, разрабатывая индивидуальную систему видеонаблюдения для банкоматов Opteva Diebold, не имеющих штатных мест для установки видеонаблюдения.

В 2010 мы представляем вам StopSkimmer®.

PBF GROUP®

www.pbfgroup.ru + info@pbfgroup.ru + 7(495) 792-11-59