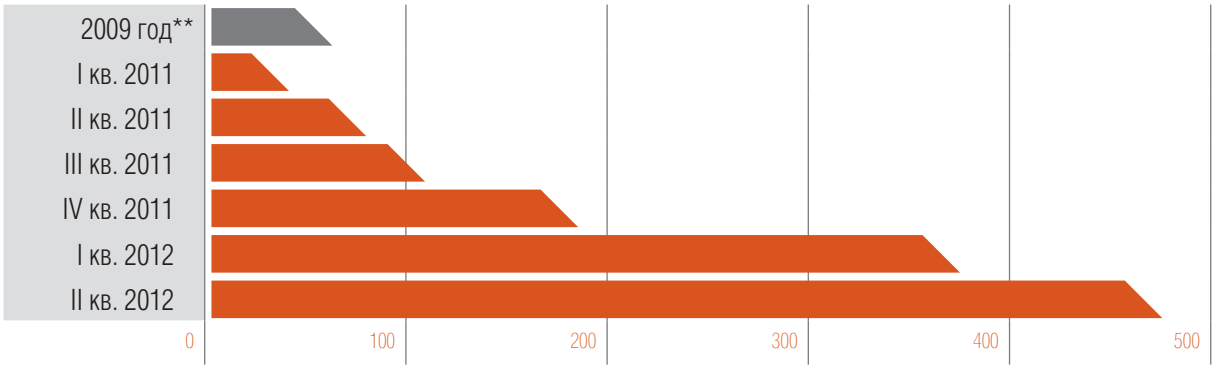
Устройство активного противодействия скиммингу

Cerber
MONEY SECURITY

Что такое скимминг и сложно ли стать его жертвой?

По официальным данным ассоциации European ATM Security Team (EAST), консолидирующей информацию о мошенничествах на устройствах финансового самообслуживания, в Европе наблюдается непрерывный рост числа преступлений, в которых фигурирует понятие «скимминга» — вида мошенничества, связанного с созданием дубликатов банковских карт за счет применения специальных устройств несанкционированного считывания данных магнитной полосы («скиммеров»), устанавливаемых на банкоматах и аналогичных по типу терминалах самообслуживания. Подобные тенденции отмечаются и в России:

Число зафиксированных случаев скимминга в Российской Федерации*



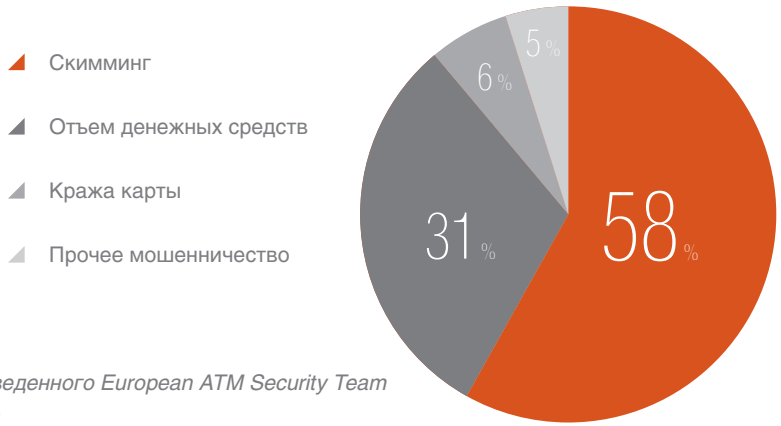
** По данным Ассоциации российских членов Europay*

*** Число случаев за весь год*

Рост преступлений данной категории в какой-то степени обусловлен стремительным развитием радиоэлектронной элементной базы, позволяющей постоянно уменьшать размеры скиммеров, что в сочетании с закамуфлированным внешним видом делает эти устройства незаметными не только для рядовых пользователей, но зачастую и для специалистов:

Таким образом, никто не застрахован от того, что, сняв наличные в банкомате или оплатив какие-либо услуги (пополнив счет мобильного телефона, оплатив интернет услуги, коммунальные платежи), копия использовавшейся при этом банковской карты не окажется у преступников, которые впоследствии смогут распоряжаться имеющимися на соответствующем счету денежными средствами. При этом стоит отметить, что такой копией смогут воспользоваться как через день, так и через неделю, месяц и даже год. Кроме того, электронный скан-образ карты за какие-то секунды может оказаться в любой точке мира. Владелец карты не всегда даже сможет установить — где и когда он стал жертвой скимминга. Также наивно полагать, что популярное в настоящее время смс-оповещение об операциях списания (зачисления) денежных средств на карту позволит вовремя принять необходимые меры (заблокировать карту). Сообщение придет после списания денег, а это могут оказаться все доступные средства, в том числе кредитные!

Обеспокоенность населения данной проблемой подтверждают и результаты социологических исследований, периодически проводимых EAST:



** По данным опроса, проведенного European ATM Security Team в январе-марте 2012 года*

Кто же должен обеспечить безопасность?

Сложившаяся ситуация не позволяет населению в полном объеме использовать преимущества терминалов финансового самообслуживания, с одной стороны, а с другой — формирует отрицательный имидж банков, осуществляющих их эксплуатацию, — так как претензии в первую очередь предъявляются именно им. При этом в отдельных случаях банкам приходится компенсировать понесенный клиентами ущерб, а также постоянно увеличивать затраты на содержание подразделений, осуществляющих урегулирование, в том числе и судебное, подобных конфликтных ситуаций.

Понимание серьезности данной проблемы имеется и у органов государственной власти, в частности, Центральным банком Российской Федерации подготовлен проект новых рекомендаций банкам по повышению уровня безопасности использования терминалов финансового самообслуживания, в котором вопросам борьбы со скиммингом уделено особое внимание.

В этой связи обеспечение безопасности при использовании терминалов финансового самообслуживания становиться первоочередной задачей для организаций, предоставляющих подобного рода услуги, т.е. соответствующих банковских структур.

Так можно ли защититься от скимминга?

Учитывая, что проблема противодействия скимминг встала достаточно давно, то существуют различные средства и методы борьбы с ним.

Достаточны ли организационные меры?

Во-первых, это так называемые организационные меры, которые заключаются в размещении терминалов финансового самообслуживания в местах, где установку скиммеров на такие устройства произвести незаметно достаточно проблематично — это непосредственно отделения банков, помещения государственных учреждений и иные «доверительные» места. Организация непрерывного видеонаблюдения за функционированием терминалов самообслуживания и обеспечение физической охраны этих устройств, также относятся к данной категории мер.

Теоретически указанные действия могут обеспечить достаточный уровень безопасности. Однако на практике необходимо понимать, что выделить по отдельному охраннику или персональному оператору камеры видеонаблюдения для каждого терминала нереально, а существенное сужение мест размещения сети банкоматов сводит на нет преимущества ее использования. Кроме того, учитывая, что процедура установки скиммеров для профессионального злоумышленника занимает считанные секунды, то его размещение может в отдельных случаях произойти и «под носом» у не столь бдительной охраны, в том числе и непосредственно в «доверительных» местах. Все это делает данный комплекс мер с практической точки зрения не эффективным.

Обезопасит ли пассивное оборудование?

Ко второй категории относятся меры, основанные на использовании специального оборудования, физически препятствующего установке скимминговых устройств. Учитывая, что устройства-«шпионы» должны располагаться в непосредственной близости от карто-приемника, изготавливают всякого рода «накладки», которые устанавливаются на банкомате и не позволяют злоумышленнику прикрепить скиммер, чтобы он был незаметным для окружающих. Такие средства называют устройствами пассивного противодействия скимминг. Существенным плюсом такого решения является его низкая стоимость (около 1 тыс. рублей). Однако на этом плюсы заканчиваются, эффективность использования указанных средств весьма низкая, так как многие скимминговые устройства закамуфлированы под аналогичные

«накладки» и клиенту просто невозможно определить, что же все таки установлено на банкомате. Кроме того, многие скиммеры могут быть размещены непосредственно на средствах пассивной защиты и прекрасно при этом функционировать. В этой связи ориентироваться исключительно на такие средства защиты неправильно.

Реален ли быстрый переход на EMV-карты?

Следующим действием, которое могло бы полностью искоренить скимминг, является переход на EMV-карты — микропроцессорные карты без магнитной полосы. В Европе такие попытки постоянно предпринимаются и число используемых «чиппованых» карт постоянно увеличивается, но до полного отказа от «магнитной полосы» пока еще очень далеко — этот процесс может занять десятилетие! К тому же необходимо понимать, что такой переход сам по себе достаточно затратен – замена оборудования, перевыпуск карт, сертификация терминального оборудования и процессинга ведут к серьезным финансовым вложениям. Поэтому данный подход можно рассматривать только как перспективное направление.

Эффективны ли активные средства противодействия?

Последним, наиболее эффективным с практической точки зрения методом борьбы со скимминго, является использование специальных радиоэлектронных средств, так называемых активных средств противодействия, которые создают различные электромагнитные поля и тем самым не позволяют никакому другому устройству, кроме банкомата, считать данные с карты.

Изделия такого типа хорошо себя зарекомендовали в ряде европейских стран и бесспорно являются основным средством борьбы со скимминго. В проекте рекомендаций по повышению уровня безопасности использования терминалов финансового самообслуживания Центральный банк Российской Федерации настаивает на применении банками именно активных средств защиты!

Однако и здесь есть свои сложности — это, с одной стороны, высокая стоимость устройств данного типа (1–2 тыс.$ за комплект), а с другой — распространены случаи, когда заявленные производителем устройств характеристики не соответствуют действительности, и установка на банкомат таких средств защиты проблемы скимминга не решает. Таким образом, выстраивая комплексную систему безопасности терминальной сети, нужно очень серьезно подходить к выбору средств защиты и делать выводы об эффективности тех или иных изделий на основании анализа результатов их испытаний, экспертных заключений и квалификации производителей.

Что такое изделие «Cerber» и как оно работает?

Изделие «Cerber» (условное обозначение — АЕРВ.468200.053), производимое Обществом с ограниченной ответственностью «АНСЕР ПРО», является устройством активного противодействия несанкционированному считыванию данных магнитной полосы пластиковых карт при их пользовании в банкоматах и прочих терминалах финансового самообслуживания.

Принцип работы изделия заключается в создании направленных электромагнитных импульсных помех в районе картридера терминала, препятствующих доступу к карте всех несанкционированных устройств. Отличительной особенностью изделия является то, что «защитное поле» генерируется постоянно, а при входе (выходе) карты в (из) картридер(-а) терминала — в наиболее уязвимый момент, мощность силового поля усиливается в несколько раз. Немаловажную роль играет и алгоритм формирования «защитного поля», который основан на многолетних исследованиях лаборатории компании — разработчика в области обеспечения безопасности и разработке собственных инновационных подходов к решению данной проблемы. Именно таким образом и достигается максимально возможный уровень защиты, при котором совершенно неважно когда, куда и каким образом злоумышленник установит скиммер — своей цели он уже никогда не добьется!

Действительно ли изделие «Cerber» эффективно борется со скимингом?

Изделие «Cerber» ни в чем не уступает, а по основным целевым параметрам превосходит лучшие зарубежные и отечественные аналоги. И это не голословное заявление. По результатам тестирования функциональных характеристик устройств активного противодействия скиммингу, проводимого ОАО «Сбербанк России» в июне 2012 г., изделие «Cerber» признано победителем в данном классе устройств. При этом стоит отметить, что суть тестирования заключалась в следующем: каждый из ведущих производителей устройств антискимминга пытался скомпрометировать надежность защиты средств «чужого» производства. Действительно, ни одна комиссия не сможет так досконально выявить слабые стороны продукции, как смогут это сделать конкуренты, которые всеми силами и средствами стремятся показать недееспособность «чужого» бренда. По результатам многодневных испытаний, единственным изделием, преодолеть защитный барьер которого не удалось никому, была продукция ООО «АНСЕР ПРО».

Что может лучше свидетельствовать об эффективности защиты, обеспечиваемой устройством?


ON
Cerber

Какие функциональные возможности предоставляет устройство активного противодействия скиммингу «Cerber»?

Помимо основного назначения по блокированию скимминговых атак «Cerber» реализует следующий набор «полезных» функций:

- отключение терминала финансового самообслуживания при неисправности антискимминговой защиты, т.е. в случае, если по каким-либо причинам защитное устройство вышло из строя (в том числе под воздействием злоумышленника), операции с банковскими картами будут прекращены — клиент не сможет вставить карту в картридер, а соответственно ее копия не будет сделана преступником;

- аудит событий в энергонезависимой памяти, предусматривающий учет фактов установки скиммеров на терминал, т.е. служба эксплуатации (безопасности) сможет получить информацию о том, предпринимались ли в принципе попытки скимминговых атак на конкретном месте, а также количество таких атак с фиксацией даты и времени их проведения;

- отправка тревожных сообщений в случае выявления фактов установки скимминговых устройств;

- дистанционное обновление программного обеспечения изделия, т.е. в случае расширения функциональных возможностей «Cerber» не обязательно ехать и осуществлять «перепрошивку» устройства — эту операцию можно сделать удаленно;

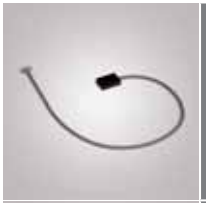
- световая индикация работоспособности элементов устройства, наличия зафиксированных атак, фактов внепланового отключения изделия, позволяющая эксплуатационным службам, просто взглянув на изделие, понять — были ли какие-либо проблемы или нет;

- доступ к параметрам изделия с использование персональных ЭВМ, в том числе ноутбуков с использованием USB-кабеля;

- количество сервисов может быть значительно шире, т.е. решение позволяет осуществить подключение разнородных датчиков (имеется достаточное количество входных разъемов), отвечающих за мониторинг отдельных характеристик терминалов самообслуживания, а также окружающей среды, и определить те или иные действия в зависимости от значений фиксируемых параметров. Реализация данного подхода не требует доработки аппаратной части изделия, необходимо изменение только отдельной составляющей программного обеспечения, которое может быть произведено в кратчайшие сроки.

Что входит в состав устройства активного противодействия скиммингу «Cerber»?

	Базовое устройство, реализует основные алгоритмы и функциональные возможности изделия
	Силовой кабель, необходим для организации электропитаний базового устройства *(зависит от модели банкомата)*
	Трансмиттер, создает «защитное поле»
	Удлинительный кабель, позволяет разместить базовое устройство в требуемом месте в зависимости от типа терминала финансового самообслуживания *(зависит от модели банкомата)*
	Датчик проверки наличия «защитного поля», позволяет изделию контролировать поля в окрестности картридера, т.е. если злоумышленнику каким-либо образом удастся вывести из строя трансмиттер («сбить», «высверлить») или подвергнуть его атаке (например, путем излучения в противофазе), то средство защиты узнает об этом и примет соответствующие меры — отключит картридер терминала и пошлет тревожный сигнал

	Датчик поиска скиммеров, позволяет изделию обнаруживать присутствие посторонних устройств (принцип действия – датчик «объема») *(дополнительная опция)*
	Коммуникационный кабель USB, позволяет подключить устройство к терминалу финансового самообслуживания или внешней ПЭВМ для настройки и получения дополнительной информации *(дополнительная опция)*
	Датчик открытия банкомата, позволяет зафиксировать факт вскрытия дверцы терминала финансового самообслуживания *(дополнительная опция)*
	*Устройство тестирования уровня сигнала защитного поля, позволяет специалисту службы эксплуатации проверить защитные характеристики функционирующего устройства* *(дополнительная опция)*

Как осуществляется установка устройства активного противодействия скиммингу «Cerber»?

Все компоненты «Cerber» устанавливаются внутри корпуса терминала финансового самообслуживания, благодаря чему злоумышленники не имеют возможности узнать — оборудован банкомат средствами активного антискимминга или нет. Кроме того, это минимизирует возможность вывода изделия из строя путем физического воздействия, а так же полностью защищает устройство от актов вандализма.

Схематичное расположение элементов изделия приведено на рисунке — так излучающая антенна помещается в районе картридера, блок центрального управления может быть установлен в любом доступном месте, при необходимости подключается датчик объема. Питание изделия осуществляется от сетевого кабеля картридера.

Суммарное время монтажа изделия занимает от 15 до 30 минут!

Не испортит ли устройство активного противодействия скимминг «Cerber» терминал финансового самообслуживания, на котором оно установлено, или используемые клиентами карты?

Изделие «Cerber» прошло испытания в специализированном сервисном центре (ЛАН АТМсервис) на терминалах финансового самообслуживания различных типов и марок, в результате которых не было выявлено ни одного случая нарушения работоспособности узлов банкоматов, порчи банковских карт, а также иных факторов, препятствующих установке и последующему использованию данных средств безопасности.

В настоящее время завершаются испытания у официальных представителей производителей терминалов финансового самообслуживания ведущих мировых брендов. В частности уже сделаны выводы, что монтаж изделия не противоречит документации по эксплуатации банкоматов в части, касающейся геометрических и механических требований, а установка «Cerber» не ведет к потере гарантии на терминалы финансового самообслуживания.

Возможна ли интеграция устройства активного противодействия скимминг «Cerber» в единую систему мониторинга функционирования терминалов финансового самообслуживания?

В «Cerber» есть все необходимое для организации централизованного мониторинга функционирования сети терминалов, когда в режиме on-line на экране монитора или видеостене отображается комплексная информация о том, какие устройства работоспособны, а какие нет, на каких устройствах предпринимаются попытки скимминговых атак, а какие работают в штатном режиме, и многое другое.

Для этого достаточно подключить изделие непосредственно к терминалу с использованием USB-кабеля, который можно опционально включить в комплект поставки либо приобрести самостоятельно. Далее возможны два варианта. Первый предполагает, что в банке уже функционирует собственная система мониторинга. Для такого случая имеется набор библиотек, содержащий полную комбинацию API-функций, позволяющих на программном уровне организовать взаимодействие с изделием «Cerber» — получать от каждого устройства информацию о текущем

состоянии и отображать ее с использованием существующих интерфейсов. Если в банке такой системы пока нет, то можно приобрести программное обеспечение ООО «АНСЕР ПРО», которое решает перечисленные выше интеграционные задачи.

Более того, интеграционные решения ООО «АНСЕР ПРО» предоставляют возможность централизованного обновления программного обеспечения «Cerber» на всех терминалах, что значительно упрощает процесс эксплуатации этих устройств.

Почему необходимо использовать именно устройство активного противодействия скиммингу «Cerber»?

«Cerber» имеет следующие конкурентные преимущества:

- эффективная защита от всех видов скимминга *(аудио, цифрового, цифро-аналогового и др.);*
- возможность установки на терминалы финансового самообслуживания любых типов и марок;
- быстрая и простая процедура установки;
- большой набор вспомогательных функций;
- возможность расширения функциональных возможностей;
- возможность интеграции решения в централизованную систему мониторинга функционирования терминалов финансового самообслуживания;
- отсутствие возможности у злоумышленника увидеть и демонтировать устройство;
- адекватная стоимость;
- короткие сроки поставки;
- соответствие действующим в Российской Федерации стандартам и нормам по электробезопасности;
- устойчивость к актам вандализма за счет скрытия всех узлов в корпусе терминала.

Who is «АНСЕР ПРО»?

ООО «АНСЕР ПРО» — компания, которая уже более шести лет занимается вопросами обеспечения информационной безопасности. Основу компании составляют выпускники ведущих ВУЗов страны, в том числе уникальные специалисты — в прошлом сотрудники профильных подразделений органов государственной безопасности, обладающие бесценным опытом разработки средств защиты информации.

Квалификация организации подтверждается многочисленными лицензиями ФСБ России и ФСТЭК России на деятельность по разработке и (или) производству средств защиты конфиденциальной информации, технической защите конфиденциальной информации, на проведение работ, связанных с созданием средств защиты информации, и др. ООО «АНСЕР ПРО» аккредитовано ФСБ России в качестве испытательной лаборатории, которая осуществляет проверку средств защиты информации на соответствие жестким требованиям по обеспечению безопасности информации.

Основной принцип, которого придерживается компания, заключается в том, что в вопросах защиты информации не бывает вероятностей, безопасность либо гарантируется, либо не обеспечивается!

Исходя из этого постулата разрабатывается вся продукция ООО «АНСЕР ПРО». Поэтому можно с уверенность утверждать, что, принимая решение в пользу «Cerber», Вы делаете правильный выбор!

Как посмотреть работу устройства активного противодействия скиммингу «Cerber» на практике и приобрести его?

Специалисты компании всегда готовы подъехать к Вам, установить образец «Cerber» на любой терминал финансового самообслуживания, продемонстрировать работу изделия* и обсудить условия поставки. При необходимости устройство может быть предоставлено для проведения тестовой эксплуатации.

Для этого достаточно просто позвонить по указанному ниже телефону (написать письмо по электронной почте), договорится о встрече и задать интересующие вопросы!

Контактные данные:
Общество с ограниченной ответственностью «АНСЕР ПРО»
Центральный офис: 115569, г. Москва, ул. Маршала Захарова, дом 6, корп. 3,
тел.: +7 (499) 703-41-50, e-mail: anti-skimming@answerpro.ru.

---

* Демонстрация возможна в г. Москве и Московской области.

ООО «АНСЕР ПРО»
Центральный офис: 115569, г. Москва,
ул. Маршала Захарова, дом 6, корп. 3,

тел.: +7 (499) 703-41-50,
e-mail: anti-skimming@answerpro.ru.