

DeviceLock для соответствия стандарту PCI DSS



Оглавление:

- [Введение](#)
- [Структура стандарта и схема сертификации](#)
- [Ключевые положения PCI DSS](#)
- [Общий обзор решения DeviceLock от Смарт Лайн Инк](#)
- [Возможности DeviceLock и требования PCI DSS](#)
- [О компании Смарт Лайн Инк](#)
- [Контактная информация](#)

Введение

Платежные карты уже давно являются одним из самых популярных средств оплаты товаров и услуг физическим лицами. Они предоставляют своим держателям максимальное удобство, но, вместе с этим, использование платежных карт сопряжено с дополнительными рисками. Если информация, которая содержится на кредитной карте, попадает в руки злоумышленников – владелец карты рискует потерять деньги со своего банковского счета.

Не менее важно, что от утечек страдают не только владельцы, но и банки, а также платежные системы. В случае компрометации платежных сведений, банки вынуждены выпускать новые карты, а этот процесс сопровождается дополнительными расходами. В некоторых случаях банкам приходится восстанавливать материальный ущерб, который был нанесен держателю карты. Отметим, что кроме прямых потерь, финансовые институты терпят серьезные косвенные убытки, связанные с ухудшением репутации и снижением доверия к платежным картам.

Чтобы снизить риски утечки и нецелевого использования информации о кредитных картах, был разработан специальный стандарт PCI DSS (Payment Card Industry Data Security Standard). На сегодняшний день требования стандарта PCI DSS распространяются на все компании, осуществляющие обработку, хранение или передачу данных о держателях платежных карт (банки, процессинговые центры, поставщики услуг, розничные магазины, e-commerce и т.п.).

Первая версия стандарта была принята в начале 2005 года при участии ведущих платежных систем (VISA, MasterCard, American Express, Discover, Diner's Club и JCB.). Спустя полтора года была выпущена ее модификация (PCI DSS v. 1.1), которая с незначительными изменениями остается актуальной до сих пор.

Российские организации, осуществляющие обработку информации о кредитных картах, должны соответствовать PCI DSS с 2007 года. С 2008 года платежные системы планируют применять штрафные санкции к компаниям, не прошедшим процедуру сертификации.

В целом, PCI DSS является комплексным стандартом, содержащим более 100 четких требований по информационной безопасности организации. Несмотря на то, что многие организации уже имеют сложившуюся подсистему информационной безопасности, обеспечение совместимости с PCI DSS является достаточно сложной задачей, решение которой требует значительных инвестиций, а также временных и трудовых затрат.

В данном документе будут проанализированы требования стандарта PCI DSS. Кроме того, будут рассмотрены возможности продукта DeviceLock компании Смарт Лайн Инк, при помощи которого организация может гораздо эффективнее достичь соответствия данному стандарту.

Структура стандарта и схема сертификации

Стандарт различает два вида подотчетных организаций, которые, в свою очередь, делятся на несколько уровней, в зависимости от количества обрабатываемых транзакций.

Требованиям PCI DSS должны соответствовать:

- Торговые организации (мерчанты). Организации, которые занимаются торговлей с помощью платежных карт. Подразумевается, что торговые организации непосредственно участвуют в транзакциях.
- Поставщики услуг (например, процессинговые центры). Организации, которые занимаются обработкой транзакций, но не принимают в них непосредственного участия.

Для разных типов и уровней подотчетных организаций требования сертификации по PCI DSS могут отличаться. В качестве примера приведем требования, принятые для торговых организаций:

Таб. 1. Требования соответствия PCI DSS для торговых организаций			
Уровень	Определение уровня	Требования PCI DSS	Исполнитель
Первый	Торговые организации, обрабатывающие более 6 млн. транзакций в год. Организации, уже допускаявшие утечки данных.	Сертификационный аудит соответствия стандарту	Сертифицированный аудитор
		Ежеквартальный тест на проникновение	Сертифицированный вендор сканирования (Approved Scanning Vendor, ASV)
Второй	Торговые организации, обрабатывающие от 1 до 6 млн. транзакций в год.	Ежегодное самостоятельное заполнение опросного листа	сама организация
		Ежеквартальный тест на проникновение	ASV
Третий	Торговые организации, обрабатывающие от 20 тыс. до 1 млн. транзакций в год.	Ежегодное самостоятельное заполнение опросного листа	сама организация
		Ежеквартальный тест на проникновение	ASV
Четвертый	Торговые организации, обрабатывающие менее 20 тыс. транзакций в год.	Ежегодное самостоятельное заполнение опросного листа	сама организация
		Рекомендован ежеквартальный тест на проникновение	ASV

В целом, для соответствия стандарту необходимо выполнить два условия:

- Каждый квартал необходимо успешно проходить тест на проникновение (проводится авторизованной внешней организацией, Approved Scanning Vendor, ASV). Тест на проникновение, фактически, эквивалентен профессиональной хакерской атаке, которая проводится не ради преступного умысла, а исключительно с целью аудита.
- Каждая организация должна соответствовать списку требований, которые предъявляет стандарт. Проверка соответствия должна проводиться раз в год посредством внешнего сертификационного аудита.

Стандарт PCI DSS предполагает, что выполнение всех требований позволит успешно пройти и тест на проникновение, и проверку соответствия.

Требования PCI DSS имеют иерархическую структуру, которая изображена на рис. 1.

Основная масса положений стандарта связана с защитой информации о держателях банковских карт. Все требования к защите делятся на 6 контрольных задач, каждая из которых, в свою очередь, распадается на несколько главных требований (в общей сложности, стандарт предусматривает 12 главных требований). В списке положений PCI DSS также имеются требования к хранению платежных данных и специальные компенсирующие меры. Компенсирующая мера – это способ снизить риски утечки другим способом, нежели тот, что предлагает стандарт. Такие меры могут применяться только теми организациями, которые не могут соответствовать основным положениям PCI DSS в силу непреодолимых причин.



Рис. 1. Структура стандарта PCI DSS

Ключевые положения PCI DSS

Дать обзор всех требований PCI DSS в рамках данного документа не представляется возможным: ниже будут описаны только ключевые требования стандарта. Для более глубокого ознакомления с документом рекомендуется изучить оригинальный текст PCI DSS, который можно найти на сайте <https://www.pcisecuritystandards.org/>.

Важную роль в стандарте PCI DSS занимает вторая ключевая задача, которая содержит два главных требования (требования 3, 4). Для решения данной задачи организации требуется защитить платежную информацию в местах хранения и каналах передачи данных. Эта задача является одной из самых тяжелых для выполнения, поскольку в современной ИТ-инфраструктуре мест хранения и каналов передачи данных может быть очень много¹.

В частности, требование 3.4 стандарта PCI DSS явно указывает, что Personal Account Number (PAN, номер кредитной карты) «должен быть представлен в нечитаемом виде во всех местах хранения (включая данные на съемных носителях, резервных копиях и журналах протоколирования событий, а также данные, получаемые по беспроводным сетям)». На практике данное требование означает, что доступ к некоторым местам хранения (например, мобильным носителям) должен быть заблокирован, поскольку установить тотальную защиту на каждом из этих мест нереально (либо слишком дорого). С другой стороны, обойтись без специальных инструментов для защиты хранящихся данных никак нельзя, поскольку номера кредитных карт должны в любом случае где-то храниться и обрабатываться. PCI DSS рекомендует использовать для этих целей инструменты шифрования.

Требование 4 стандарта PCI DSS фактически эквивалентно предыдущему требованию с той разницей, что оно регламентирует защиту информации в момент ее передачи, а не хранения. Стандарт указывает, что «для защиты критичных данных о держателях карт во время их передачи [...], следует использовать только стойкие криптографические алгоритмы и протоколы». Таким образом, как и в случае предыдущего требования, часть каналов неизбежно придется заблокировать, а оставшиеся каналы – защитить.

Помимо второй ключевой задачи особую роль в стандарте играет пятая задача, которая также содержит два главных требования (требования 10 и 11). Несмотря на то, что оба обозначенных требования, по сути, являются вспомогательными, поскольку не влияют на информационную безопасность ИТ-инфраструктуры напрямую, пятая задача является одной из сложнейших в реализации.

В частности, пункт 10 стандарта PCI DSS требует протолировать все действия с платежной информацией. Стандарт явно указывает, что «для каждого системного компонента должен быть включен механизм протолирования событий», а для каждого события – «должны фиксироваться связанные с ним параметры». Кроме того, все журналы событий «должны просматриваться (анализироваться) не реже раза в день», «быть в оперативном доступе не менее трех месяцев» и «храниться не менее одного года». Другими словами, для соответствия PCI DSS необходимо не только сохранять разнообразные логи, но и оперативно анализировать их. Это означает, что все журналы протоколов необходимо структурировать и собрать в единую базу данных, поддерживающую различные аналитические запросы.

Следующее (одиннадцатое) требование предписывает проводить регулярное тестирование сетей инфраструктуры на проблемы с безопасностью. Данное требование,

¹ Например, данные могут лежать на файл-серверах, храниться в различных информационных системах, на локальных рабочих станциях или на мобильных носителях. Данные могут передаваться через такие каналы, как электронная почта, локальные порты, беспроводные интерфейсы и т. д.

по сути, дублирует схему сертификации по стандарту, которая предписывает проводить тест на проникновение не реже одного раза в три месяца.

Добавим, что кроме «тактических» требований, стандарт PCI DSS содержит несколько «стратегических» положений, регламентирующих общие принципы обеспечения информационной безопасности. В частности, шестое требование стандарта обязывает проводить разработку информационных систем «в соответствии с руководствами по безопасному программированию», а двенадцатое требование – «поддерживать политику, определяющую правила информационной безопасности».

Общий обзор решения DeviceLock от Смарт Лайн Инк

Продукт DeviceLock разработан российской компанией ЗАО «Смарт Лайн Инк» и предназначен для использования в корпоративных информационных системах. С помощью DeviceLock предприятия любого масштаба могут обеспечить всесторонний контроль над данными, покидающими корпоративную сеть через порты рабочих станций, внешние накопители, принтеры и беспроводные сети. Кроме того, DeviceLock включает в себя защиту от аппаратных клавиатурных шпионов, использующихся для кражи ценной информации с рабочих станций сотрудника. Злоумышленник может подключить такое устройство между компьютером и клавиатурой служащего и тем самым обмануть антивирус и другое защитное программное обеспечение. Однако DeviceLock выявит подмену, блокирует работу «шпиона», предупредит пользователя и сделает запись в журнал событий.

Ключевой особенностью продукта является не только контроль над фактом передачи данных в соответствии с заданными политиками, но еще и полное теневое копирование всей исходящей информации. Хотя сегодня существует огромное количество решений для хранения почтовой корреспонденции, только DeviceLock позволяет собирать и анализировать информацию, покинувшую корпоративную сеть через локальные порты рабочей станции.

Когда речь заходит о контроле над информационным обменом между корпоративными рабочими станциями и персональными карманными компьютерами работников, смартфонами и различными коммуникаторами, то DeviceLock не просто поддерживает теневое копирование всех данных, передаваемых на мобильное устройство, но позволяет также реализовать гибкие политики безопасности и проследить за их исполнением. Например, продукт может разрешить синхронизировать контакты и календарь, но запретить копирование файлов или синхронизацию электронной почты с вложениями.

Это крайне полезная функциональность, особенно, в свете постоянного роста популярности мобильных устройств в корпоративном секторе. Кроме того, нельзя сбрасывать со счетов приближающуюся консьюмеризацию корпоративных IT-систем. Авторитетные исследовательские агентства Yankee Group и CSC Research утверждают, что менеджеры IT-департаментов не могут игнорировать либо запретить то обилие портативных устройств, которыми постоянно пользуются служащие. Они вынуждены обеспечить поддержку мобильных компьютеров сотрудников, поскольку в противном случае компания рискует потерять инновационный потенциал, снизить производительность труда своих работников, а, следом, и ослабить свою конкурентоспособность. Между тем, массовая консьюмеризация чревата новыми серьезными рисками в области информационной безопасности, так как мобильные устройства могут быть использованы для осуществления мошенничества, утечки и других внутренних нарушений. Решить эту проблему, в существенной степени, позволяет DeviceLock.

Таким образом, продукт защищает компанию от утечки цифровых активов, попадания во внутреннюю сеть нежелательных типов данных, предоставляет инструментарий для ретроспективного анализа всей информации, которую сотрудники компании скопировали

на внешние носители и забрали с собой, а также придает необходимую компании гибкость при работе с мобильными устройствами.

Следует отметить, что DeviceLock позволяет контролировать весь спектр потенциально опасных устройств: USB-порты, дисководы, CD/DVD-приводы, а также FireWire, инфракрасные, параллельные и последовательные порты, Wi-Fi и Bluetooth-адаптеры, ленточные накопители, КПК, любые внутренние и внешние сменные накопители и жесткие диски. DeviceLock осуществляет детальный аудит действий пользователей с устройствами и данными.

Отдельно стоит выделить возможности DeviceLock по гранулированному контролю доступа пользователей к принтерам, в том числе локальным, сетевым и виртуальным. Продукт не только обеспечивает выполнение корпоративной политики информационной безопасности посредством разграничения доступа пользователей к принтерам, тем самым минимизируя риск несанкционированной утечки данных, но также ведет событийное протоколирование и оставляет теневые копии распечатываемых документов, которые впоследствии можно проанализировать и просмотреть в графическом формате с помощью встроенного инструментария.

Продукт может управляться через групповые политики Windows в домене Active Directory, благодаря чему легко интегрируется в существующую ИТ-инфраструктуру организации любого масштаба. Предприятия могут легко защищать десятки и сотни тысяч удаленных компьютеров при помощи DeviceLock, используя управление через групповые политики Active Directory.

С функциональной точки зрения, DeviceLock состоит из трех частей (рис. 2):

1. DeviceLock Service – это агент, устанавливаемый на каждый компьютер, который автоматически запускается и обеспечивает защиту устройств на машине-клиенте, в то же время оставаясь невидимым для локального пользователя.
2. DeviceLock Enterprise Server – это дополнительный компонент, используемый для централизованного сбора и хранения данных теневого копирования и журналов аудита. DeviceLock Enterprise Server использует MS SQL Server для хранения данных.
3. Консоль управления – это интерфейс контроля, используемый администратором для управления системой, на которой установлен агент. DeviceLock поставляется с тремя консолями управления: DeviceLock Management Console, DeviceLock Enterprise Manager и DeviceLock Group Policy Manager.

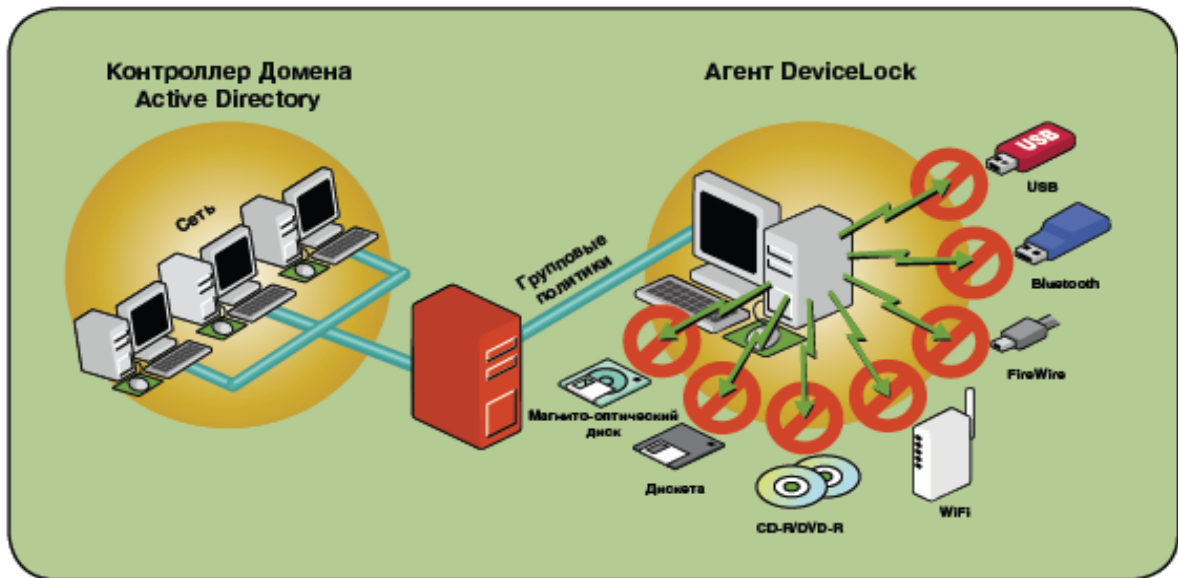


Рис. 2. Схема работы DeviceLock

Возможности DeviceLock и требования PCI DSS

Продукт DeviceLock осуществляет контроль над перемещением данных через локальные порты рабочей станции, беспроводные сети и съемные носители на основе гибких политик. Каждый раз решение о том, чтобы разрешить или запретить доступ к внешнему устройству принимается автоматически. Таким образом, настройки и политики DeviceLock легко подвержены аудиту, а сам продукт не создает дополнительных рисков информационной безопасности.

Использование DeviceLock в корпоративной среде позволяет обеспечить соответствие двум ключевым требованиям стандарта PCI DSS:

- **Контроль над информацией во время передачи.** В требованиях PCI DSS отражена основная задача стандарта – не допустить утечку платежных сведений за пределы обрабатывающей их организации. Продукт DeviceLock обеспечивает контроль над использованием локальных портов корпоративных компьютеров, принтеров, беспроводных сетей и мобильных устройств, что позволяет минимизировать риск несанкционированной утечки платежных сведений.
- **Обеспечение аудита.** Требование 10 стандарта PCI DSS посвящено механизму протоколирования событий с целью их дальнейшего анализа. В этой связи DeviceLock предлагает уникальную функциональность – теневое копирование данных, покидающих корпоративную сеть через локальные порты рабочих станций, сменные носители, беспроводные сети и мобильные устройства. Все сведения автоматически передаются в специальную центральную базу данных и доступны для последующего аудита и ретроспективного анализа.

В таблице далее (таб. 2.) просуммирована функциональность DeviceLock в соответствии с требованиями стандарта PCI DSS:

Таб. 2. Функциональность DeviceLock применительно к требованиям PCI DSS	
Требования PCI DSS	Возможности DeviceLock
<p>3.1. Должна быть разработана политика хранения и обращения с данными о держателях карт.</p>	<p>Одной из основных целей внутренней политики безопасности является защита конфиденциальной информации (в том числе, и данных о держателях карт) от возможной утечки. Очевидно, что наибольшими возможностями для кражи информации обладают сотрудники компании, поскольку они, в отличие от внешних злоумышленников, имеют легальный доступ к этой информации. Решение DeviceLock позволяет минимизировать риски, связанные с утечкой конфиденциальных сведений через локальные порты компьютеров, принтеры, беспроводные сети и персональные мобильные устройства. Продукт помогает защитить организацию не только от спланированных краж, но и от случайных действий персонала.</p>
<p>12.1. Должна быть разработана, опубликована и распространена поддерживаемая в актуальном состоянии политика безопасности.</p>	
<p>9.1. Следует использовать средства контроля доступа [...] чтобы ограничить и отслеживать физический доступ к системам, которые хранят, обрабатывают или передают данные о держателях карт. В частности [требование 9.1.2], следует ограничить доступ к сетевым разъемам компьютеров, содержащих платежную информацию.</p>	<p>С помощью агента DeviceLock Service администратор системы может ограничить доступ к локальным портам компьютеров корпоративной сети. Программное ограничение в данном случае эквивалентно аппаратному, поскольку доступ к агенту могут получить только специально авторизованные администраторы (члены локальной группы Administrators операционных систем защищенных DeviceLock компьютеров не являются автоматически авторизованными).</p>
<p>10.2. Для каждого системного компонента должен быть включен механизм протоколирования событий.</p>	<p>Продукт DeviceLock имеет развитую функцию теневого копирования, которая не только протоколирует все попытки передачи данных на внешние устройства, но и копирует переданную информацию в специальную базу данных. Вместе с каждым событием в базе сохраняется подробная информация о нем (время события, тип канала передачи, идентификатор пользователя и другие параметры). Таким образом, с помощью DeviceLock администратор системы всегда будет иметь исчерпывающую событийную информацию о перемещении данных компании через локальные порты и интерфейсы рабочих станций, удобную для аудита, а также анализа и сбора доказательной базы при проведении расследований инцидентов информационной безопасности.</p>
<p>10.3. Для каждого события должны фиксироваться связанные с ним параметры (тип события, дата и время и т. д.)</p>	

О компании Смарт Лайн Инк

Разработчик DeviceLock – ЗАО “Смарт Лайн Инк”. Основанная в 1996 году, российская компания Смарт Лайн Инк (SmartLine Inc) занимается разработкой программного обеспечения для администрирования компьютерных сетей. Качество и надежность продуктов Смарт Лайн Инк подтверждают более 55 тысяч клиентов в 80-ти странах мира – государственные, военные, медицинские, образовательные, крупнейшие финансовые и

коммерческие учреждения, а также компании малого и среднего бизнеса. Программное обеспечение Smart Лайн Инк установлено на более чем 3 000 000 компьютерах. В число клиентов компании входят Центральный Банк РФ, Сбербанк России, ОАО "Силловые машины", ВТБ 24, Российская государственная библиотека, BAE SYSTEMS, AEROTEC Engineering GmbH, HSBC Bank, Barclays Bank, Chase Manhattan Bank. Smart Лайн Инк – международная компания с офисами в Лондоне, Милане, Москве, Ратингене (Германия) и Сан Рамоне (штат Калифорния, США). Основной офис разработки программных продуктов Smart Лайн Инк находится в Москве.

Контактная информация

ЗАО "Смарт Лайн Инк"

Москва, Б. Семеновская ул., д. 40, офис 301

Телефон: +7 (495) 967-99-60, +7 (495) 366-21-93 (контактное лицо – Анастасия Дементьева)

Отдел продаж: sales@devicelock.com

Тех. поддержка: support@devicelock.com