Соответствие нормативам PCI DSS и управление информационной безопасностью

Требование 10 стандарта защиты информации в индустрии платежных карт (PCI DSS) конкретно обязывает получателей платежей, банки и процессинговые системы «...отслеживать и контролировать все случаи доступа к сетевым ресурсам и данным владельцев карт». Стандарт защиты информации (DSS) в индустрии платежных карт (PCI) предъявляет многочисленные требования к отчетности, которые приобретают огромное значение при выполнении ежегодной аудиторской проверки соответствия требованиям PCI DSS.

Поскольку коммерческие предприятия соблюдают данные требования и признают необходимость выполнения условий PCI DSS в отношении мониторинга и подготовки отчетов, то возникают следующие вопросы: «Если соблюдение законодательных требований является важным условием, то каким образом моя организация может начать проявлять инициативу вместо простого следования тенденциям, и каким образом мы можем обеспечить выгодное расширение инвестиций своего времени и ресурсов за рамки нашей инициативы в сфере PCI DSS?»

Выгоды для клиента: соответствие нормативным требованиям и управление информационной безопасностью

Благодаря технологии RSA enVision Вы получите возможность:

- Отслеживать и контролировать доступ к данным владельцев карт и обслуживающим системам согласно требованиям PCI DSS;
- Быть уверенным в том, что в случае нарушения политики или безопасности Вы будете осведомлены об этом и сможете принять соответствующие меры;
- Вместо разбирательств с аудиторами сосредоточиться на развитии бизнеса – поскольку Ваша организация обладает инструментом, позволяющим оперативно подтвердить свое соответствие ключевым требованиям стандарта PCI DSS;
- Не ограничиваться простым соответствием нормативам, а за счет использования инвестиций в PCI DSS повысить общую защищенность вашей компании.

Выход за рамки простого соответствия нормативным требованиям за счет технологии RSA enVision®

Нарушения политики и безопасности происходят без предупреждения. Независимо от того, являлись ли они следствием непреднамеренных ошибок или попытками получения несанкционированного доступа к информации, Вам требуется постоянно быть в курсе этих событий для принятия соответствующих мер. Осведомленность и быстрота реакции являются важными условиями для обеспечения соответствия требованиям PCI DSS, и, в более широком смысле, они необходимы для обеспечения информационной безопасности всех отдельных предприятий, клиентов и партнеров Вашей организации.

Система RSA enVision преобразует необработанные и на первый взгляд не связанные между собой данные о событиях в системах безопасности и в сетях передачи данных, в понятную и поддающуюся интерпретации информацию, анализ которой позволяет предпринять соответствующие меры. По первоначально установленному базовому уровню активности всей сетевой среды, RSA enVision способен помочь определять случаи нештатного поведения и объявлять тревогу при обнаружении подобной активности. За счет сбора всех данных - от систем обеспечения безопасности, сетевых систем и корпоративных приложений до мэйнфреймов, настольных ПК и устройств хранения данных, RSA enVision дает Вам полную картину происходящего.

Помимо соблюдения требований PCI, RSA enVision позволяет избавиться от огромных хранилищ коммерческой информации, которая исторически накапливается в большинстве организаций. Система осуществляет сбор, анализ и управление всеми данными и предоставляет платформу, помогающую обеспечить требуемой информацией практически любого сотрудника Вашей организации. В результате не только аудиторы, отвечающие за соблюдение законодательных нормативов, будут иметь полный комплект сведений для решения вопросов соответствия им, но также и специалисты по управлению рисками и обеспечению безопасности получат возможность следить за угрозами безопасности в реальном времени. И любой персонал - от сотрудников службы поддержки, до служб управления приложениями и сетями сможет в любое время получить доступ ко всем необходимым отчетам.

Для сбора и анализа информации, относящейся к соблюдению нормативных требований и обеспечению безопасности, RSA enVision использует LogSmart Internet Protocol Database (IPDB). Данная технология отлична от большинства схем хранения данных, используемых в других решениях и основанных на системах управления реляционными базами данных (RDBMS). Для обеспечения эффективного хранения и целостности собранных данных в LogSmart IPDB применяются компрессия и шифрование.

Компоненты системы RSA PCI

> RSA®Access Manager. Система авторизации, разработанная компанией RSA, позволяет гарантировать получателям платежей, банкам и процессинговым системам платежей то, что доступ к данным владельцев карт через доступные в сети Веб-системы PCI могут получить только те пользователи, которые допущены к соответствующей служебной информации.

> RSA Data Security Solutions. Системы защиты данных, разработанные компанией RSA, позволяют предприятиям, деятельность которых регламентирована стандартом PCI, защищать данные владельцев карт на всех оконечных точках шифрования и осуществлять централизованное управление ключами шифрования в масштабе предприятия.

– RSA File Security Manager
– CipherOptics IP Security Gateway
– RSA DLP Suite
– RSA Key Manager

> RSA enVision®. Решение RSA по обеспечению соответствия нормативным требованиям и управлению безопасностью позволяет организациям, деятельность которых регламентирована стандартом PCI DSS, упростить процесс аудиторских проверок за счет централизованного отслеживания и контроля доступа к данным владельцев карт в среде PCI.

> EMC Storage Systems. Интеграция систем хранения EMC Symmetrix®, CLARiiON®, Celerra® и Centera™ с платформой RSA enVision предоставляет клиентам возможность экономного долговременного хранения всех важных сведений, необходимых для аудиторской проверки по PCI DSS.

> RSA SecurID®. Решения RSA по обеспечению безопасного доступа к корпоративным данным позволяют обеспечить строгую аутентификацию пользователей при доступе к системам хранения данных о владельцах карт и соответствующим сетям передачи данных.

> RSA Professional Services. RSA Professional Services предоставляет ряд возможностей, например: помощь клиентам в подготовке к аудиторской проверке PCI DSS, поддержка в установлении сведений о владельцах карт в масштабе всей организации и тп.

В то время как другие системы не могут в полном объеме собирать поступающие от контролируемых источников данные, поскольку обычные RDBMS просто не способны обеспечить их обработку, RSA enVision позволяет это сделать за счет использования технологии IPDB.
Преимущество данной технологии состоит в возможности выполнения анализа ситуации в реальном времени параллельно процессам шифрования , сжатия и записи поступающих данных. За счет этого Вы всегда будете обеспечены достоверной и своевременной информацией.
Преимущества от сбора данных без применения программ-агентов очевидны: отсутствие фильтрации данных на источнике, нет необходимости постоянного управления агентами, отсутствие дополнительных рисков безопасности и снижение стоимости владения за счет простоты конфигурирования и развертывания системы.

Кроме всего перечисленного, система RSA enVision позволяет Вашей организации быстро реагировать на нарушения установленных политик и безопасности, что помогает улучшить общее состояние информационной безопасности в Вашей компании и упростить процесс соблюдения законодательных нормативов.

В результате RSA enVision позволяет клиентам перенаправить свои финансовые и кадровые ресурсы на решение задач развития бизнеса вместо участия в постоянных аудиторских проверках на соответствие PCI DSS.
Для получения дополнительной информации о решениях RSA в области обеспечения соответствия требованиям PCI DSS, посетите сайт www.rsa.com/pci.

Требование 10 PCI DSS и RSA envision

Требование 10 PCI DSS конкретно обязывает компании «отслеживать и контролировать все случаи доступа к сетевым ресурсам и данным владельцев карт». Система RSA enVision позволяет клиентам облегчить процесс аудиторской проверки за счет централизации слежения и контроля доступа к данным владельцев карт в рамках инфраструктуры PCI. Специальные возможности RSA enVision обеспечивают соответствие стандартам PCI DSS, включая нижеследующие:

Требование 10 PCI DSS и RSA enVision

Требование PCI DSS	Возможности RSA enVision
Требование 10.1 Установить процесс привязки любых попыток доступа к компонентам системы (особенно выполненных с использованием административных прав, например, уровня «root») к конкретному пользователю	RSA enVision позволяет отслеживать деятельность пользователя-с административными правами и контролировать тот факт, что он действует в соответствии с установленной политикой. Кроме того, данная система может направлять предупреждения диспетчеру в том случае, если его деятельность нарушает политику. RSA enVision уже содержит готовые формы отчетов, в которых фиксируются все случаи получения административных прав в контролируемых системах UNIX и Linux. Отчет: «PCI – Administrative Privilege Escalation – UNIX/Linux» («PCI – Расширение административных прав – UNIX/Linux»)
Требование 10.2 Автоматически вести регистрационные журналы для всех компонент системы для того, чтобы получить возможность восстановить последовательность событий	Система RSA enVision помогает компаниям реализовать автоматическое ведение регистрационных журналов, детализирующих процесс доступа пользователей к данным владельцев карт, меры, принятые пользователями, имеющими администраивные/root права, процесс доступа к регистрационным журналам, неудачные попытки доступа, использование механизмов идентификации/аутентификации, инициализацию журнала аудита , создание/удаление объектов системного уровня.
Требование 10.2.1 Все попытки доступа отдельного пользователя к данным владельца карты	Система отчетности RSA enVision предоставляет встроенные возможности, которые отражают все успешные попытки доступа к файловым объектам в группе устройств «данные владельца карт»; эта группа является подгруппой группы устройств PCI и должна включать в себя только серверы, которые используются для хранения данных владельцев карт. Отчет: «PCI – Individual User Accesses to Cardholder Data – Windows» («PCI – Попытки доступа отдельного пользователя к данным владельцев карт – Windows»)
Требование 10.2.2 Все действия, совершенные пользователем с правами администратора или root-правами	RSA enVision позволяет клиентам получать отчет обо всех действиях, совершенных пользователями, вошедшими в систему с правами доступа «root» . Кроме того, в эти отчеты можно дополнительно включать имена пользователей, которым ранее были предоставлены административные права в Вашей инфраструктуре. Report: «PCI – All Actions by Individuals with Root or Administrative Privileges– UNIX/Linux» («PCI – Все действия отдельных пользователей, имеющих права администратора или права доступа «root» – UNIX/Linux») Функция подготовки отчетов RSA enVision позволяет следить за всеми действиями, совершенными пользователями, вошедшими в систему с именем “Administrator”. Можно ужесточить режим безопасности за счет включения в список дополнительных имен пользователей, которые ранее имели административный доступ к Вашей информационной среде. Отчет: «PCI – All Actions by Individuals with Root or Administrative Privileges – Windows» («PCI – Все действия отдельных пользователей, имеющих права администратора или права доступа «root» – Windows»)
Требование 10.2.3 Доступ ко всем регистрационным журналам	RSA enVision имеет встроенные отчеты, которые позволяют пользователям легко отслеживать все успешные подключения к RSA enVision. Отчет: «PCI – Access to All Audit Trails» («PCI – Доступ к любым регистрационным журналам»)
Требование 10.2.4 Неудачные попытки логического доступа	RSA enVision позволяет клиентам легко получать отчет обо всех попытках доступа, которые были отклонены согласно ограничениям списка контроля доступа. Отчет: «PCI – Invalid Logical Access Attempts – ACL Denied Summary» («PCI – Неудачные попытки логического доступа – отчет о попытках, отклоненных согласно списку контроля доступа»)
Требование 10.2.5 Использование механизмов идентификации и аутентификации	RSA enVision может позволить организациям легко просматривать отчет с подробным описанием всех попыток доступа пользователей к группе устройств PCI, при которых аутентификация выполнялась с помощью серверов RSA Authentication Manager. Отчет: «PCI–Use of Identification and Authentication Systems–RSA» («PCI – Использование систем идентификации и аутентификации – RSA»)
Требование 10.2.6 Инициализация регистрационных журналов	RSA enVision имеет встроенную функцию подготовки отчетов, которые позволяют контролировать инициализацию регистрационных журналов в операционных системах Windows, UNIX, Linux, AIX и HPUX. Отчет: «PCI–Initialization of Audit Logs» («PCI –Инициализация регистрационных журналов»)
Требование 10.2.7 Создание и удаление объектов системного уровня	Возможности RSA enVision по подготовке отчетов позволяют клиентам следить за удалением всех объектов системного уровня в контролируемых системах на базе Windows, взаимодействующих с группой устройств PCI. Отчет: «PCI–Deletion of System-level Objects–Windows» («PCI – Удаление объектов системного уровня – Windows»)

Требование 10 PCI DSS и RSA envision - *продолжение*

Требование PCI DSS	Возможности RSA enVision
> **Требование 10.3** Регистрация последовательных записей регистрационного журнала для всех компонентов системы для каждого события	RSA enVision будет регистрировать события по мере поступления сообщений от подключенных устройств. Кроме того, RSA enVision сохраняет метаданные событий, которые могут анализироваться и проверяться с целью определения типа события.
Требование 10.3.1 Идентификация пользователя	RSA enVision позволяет организациям регистрировать идентификационную информацию пользователя для каждого события, связанного с группой устройств PCI.
Требование 10.3.2 Тип события	RSA enVision позволяет организациям идентифицировать сведения о типе каждого события, связанного с группой устройств PCI. Если устройство не сообщило о типе события, RSA enVision тем не менее поддерживает функцию подготовки отчетов путем сохранения метаданных, которые могут анализироваться и проверяться для определения типа события.
Требование 10.3.3 Дата и время	RSA enVision позволяет организациям регистрировать дату и время для каждого события, связанного с группой устройств PCI.
Требование 10.3.4 Идентификация успешного или неудачного действия	RSA enVision позволяет организациям регистрировать сведения об успешном/неудачном выполнении каждого события, связанного с группой устройств PCI.
Требование 10.3.5 Происхождение события	RSA enVision позволяет организациям регистрировать сведения об источнике каждого события, связанного с группой устройств PCI
Требование 10.3.6 Обозначение или наименование соответствующих данных, компонента системы или источника	RSA enVision позволяет организациям регистрировать наименование или другие идентифицирующие признаки систем, данных, компонентов или прочих источников PCI.
> **Требование 10.5** Защитить журналы для аудита таким образом, чтобы они не могли быть изменены	Нефильтрованные данные в полном объеме хранятся в базе данных RSA enVision в исходном виде. Более того, режим «однократной записи, многократного считывания» позволяет обеспечить работоспособность зеркальной копии даже в случае нарушения целостности исходных данных. Журналы регистрации событий, сведения в которые заносятся приложением RSA enVision, хранятся в защищенной операционной системе в сжатом виде, их безопасность обеспечивает упрощенная система шифрования.
Требование 10.5.1 Ограничить аудиторию просмотра журналов для аудита только теми пользователями, которым это необходимо для выполнения работы	RSA enVision позволяет организациям назначать права доступа к информации таким образом, чтобы только уполномоченные пользователи могли просматривать журнал для аудита.
Требование 10.5.2 Защитить журнальные файлы для аудита от несанкционированных изменений	Журналы RSA enVision не могут быть изменены с помощью графического интерфейса пользователя (GUI); изменения могут быть внесены только пользователем с правами административного доступа непосредственно к АПК RSA enVision. Кроме того, доступ к данным RSA enVision, а также работа архивных прикладных интерфейсов осуществляется в режиме «только для чтения», поэтому в системе журналы не могут быть изменены.
Требование 10.5.3 Оперативно осуществлять резервное копирование файлов журналов для аудита на централизованный сервер журналов или на носитель, изменение данных на котором затруднено	RSA enVision позволяет задавать график резервного копирования файлов журналов для аудита на централизованный сервер журналов или на другой носитель с нужной периодичностью, например, каждые 10 минут или ежечасно, в зависимости от запросов клиента. RSA enVision использует прикладной интерфейс «поддержки библиотечного сервера», который позволяет пользователям задавать график резервного копирования на устройство или группу устройств (например, группу устройств PCI). Клиент получит возможность, например, задавать копирование на устройство PCI через каждые 10 минут, а на устройства, не входящие в группу PCI – один раз в день.

Требование 10 PCI DSS и RSA envision - *продолжение*

Требование PCI DSS	Возможности RSA enVision
Требование 10.5.5 Использовать функцию мониторинга целостности файла и ПО для обнаружения изменений журналов, чтобы невозможно было внести изменения в существующие данные журнала без генерации предупреждений (вновь вносимые данные не должны вызывать появления предупреждения)	RSA enVision способен генерировать предупреждения, оповещающие аудиторов и прочих сотрудников о внесении любых изменений в журналы. Кроме того, в программно-аппаратном комплексе RSA enVision используется защищенная операционая система, что гарантирует повышенную безопасность.
> **Требование 10.7** Сохранять архив журналов для аудита не менее одного года; период доступности в интерактивном режиме должен быть не менее трех месяцев	АПК RSA enVision NAS3500 включает предварительно сконфигурированные, протестированные и смонтированные в стойке защищенные кожухами устройства EMC Celerra, которые позволяют клиентам использовать от 3,5 Тб до 7 Тб объема хранения, что особенно удобно для хранения файлов журналов, доступ к которым должен быть обеспечен в интерактивном режиме. Кроме того, поскольку RSA enVision имеет встроенные функции интеграции с сетевыми архивными платформами, например, EMC Symmetric®, CLARiiON, EMC® Centera™ и EMC Celerra®, клиенты получают возможность сохранения важной информации в соответствии с требованиями стандартов. Подключаемые к сети системы хранения данных EMC Celerra отличаются оптимальным соотношением цена/качество при отсутствии сбоев в работе системы. Последнее означает, что приложения продолжают функционировать с сохранением прежних характеристик и уровня сервиса даже при возникновении отказа. Система Celerra удовлетворяет данным условиям благодаря активно-пассивной групповой архитектуре, построенной по схеме N+1, а также благодаря исключению любого уязвимого звена от сети до дискового накопителя. Подключаемые к сети передачи данных системы хранения данных EMC Celerra реализуют функцию, называемую «Сохранение на уровне файла», гарантирующую защиту путем однократной записи и многократного считывания файлов, хранимых на диске. Данная функция Celerra позволяет защитить файлы и каталоги от удаления, изменения, переименования или перезаписи в течение заданного периода хранения. Функция сохранения уровня файла Celerra защищает целостность доступных в интерактивном режиме журналов для аудита в течение установленного в организации периода хранения (например, 3 месяца).

Требования PCI DSS к подготовке отчетов и проведению аудиторской проверки и RSA enVision

Помимо своей ключевой функции по оказанию помощи клиентам в достижении соответствия Требованию 10 PCI DSS, RSA enVision является мощной технологией, предоставляющей доступ к широкому диапазону систем PCI от межсетевых экранов до беспроводных сетей передачи данных и устройств аутентификации и пр. с целью сбора, сопоставления и проверки данных. Данная технология помогает клиентам удовлетворять основным требованиям PCI DSS благодаря нижеследующему:

- Создание адекватного набора отчетов о деятельности межсетевых экранов для быстрой проверки соответствия Требованию 1 («Установить и поддерживать архитектуру межсетевых экранов для защиты данных владельцев карт»);
- Соблюдение основных положений Требования 2 («Не использовать параметры, заданные поставщиком по умолчанию, для системных паролей и других параметров системы безопасности»), обеспеченное постоянным контролем за изменениями конфигурации беспроводной среды;
- Облегчение процесса подготовки отчетов по обновлениям антивирусных систем предприятия с целью соответствия Требованию 5 («Использовать и регулярно обновлять антивирусное программное обеспечение»);
- Подтверждение соответствия Требованию 6 («Разрабатывать и поддерживать системы и приложения для обеспечения безопасности») путем составления отчетов по патчам и служебным приложениям.

Требования PCI DSS к подготовке отчетов и проведению аудиторской проверки и RSA enVision

Требование PCI DSS	Возможности RSA enVision
> Требование 1.1 Установить стандарты конфигурации межсетевых экранов, которые включают следующее:	
Требование 1.1.1 Формальный процесс для подтверждения и тестирования всех соединений с внешней сетью передачи данных и изменений конфигурации межсетевых экранов	RSA enVision обеспечивает соответствие требованиям благодаря встроенной функции подготовки отчетов, отражающих все изменения конфигурации межсетевых экранов, произведенные в рамках группы устройств PCI. Отчет: «PCI – Firewall Configuration Changes» («PCI – Изменения конфигурации межсетевых экранов»)
Требование 1.1.5 Документированный список сервисов и портов, необходимых для осуществления деятельности	RSA enVision имеет встроенные функции подготовки отчетов, суммирующих весь трафик на портах устройств группы PCI через межсетевой экран. Отчет: «PCI – Traffic by Port – PCI Device Group» («PCI – Трафик через порт – группа устройств PCI»)
Требование 1.1.6 Обоснование и документирование применения любого протокола, помимо протокола передачи гипертекста (HTTP), протокола безопасных соединений (SSL), протоколов SSH и VPN	RSA enVision предоставляет готовые к работе шаблоны отчетов, в которых описан весь трафик, проходящий через порты межсетевых экранов, не регламентированные требованиями PCI, на внутренние IP-адреса Отчет: «PCI – Traffic to Nonstandard Ports – Detail» («PCI – Трафик через нестандартные порты – подробная информация») В отчетах RSA enVision суммирован весь трафик через не регламентированный PCI порт принимающего компьютера. Отчет: «PCI – Traffic to Non-standard Ports – Summary» («PCI – Трафик через нестандартные порты – обзор»)
Требование 1.1.8 Квартальная проверка наборов правил межсетевого экрана и маршрутизатора	Система подготовки отчетов RSA enVision помогает соответствовать требованиям благодаря наличию готовых шаблонов отчетов, отражающих все изменения конфигурации межсетевых экранов, сделанных в рамках группы устройств PCI. Отчет: «PCI – Firewall Configuration Changes» («PCI – Изменения конфигурации межсетевых экранов»)
Требование 1.1.9 Стандарты конфигурации для маршрутизаторов	Шаблоны RSA enVision позволяют клиентам легко отображать все изменения конфигурации маршрутизаторов в пределах группы устройств PCI. Отчет: «PCI – Router Configuration Changes» («PCI – Изменения конфигурации маршрутизаторов»)

Требования PCI DSS к подготовке отчетов и проведению аудиторской проверки и RSA enVision - *продолжение*

Требование PCI DSS	Возможности RSA enVision
> Требование 1.3 Создать конфигурацию межсетевых экранов, ограничивающую соединения между общедоступными серверами и любыми компонентами системы, хранящими данные владельцев карт, включая любые соединения по беспроводным сетям передачи данных. Такая конфигурация межсетевых экранов должна обеспечивать следующее:	
Требование 1.3.1 Ограничение входящего Интернет-трафика для IP-адресов в пределах демилитаризованной зоны (входные фильтры)	Возможности RSA enVision по подготовке отчетов позволяют клиентам автоматически регистрировать весь входящий по нестандартным портам Интернет-трафик в пределах группы устройств PCI в подробной либо сокращенной форме. Отчет: «PCI – Inbound Internet Traffic on Non-standard Ports – Detail» («PCI – Входящий Интернет-трафик через нестандартные порты – подробная информация»)
Требование 1.3.2 Запрет пропуска внутренних адресов через сеть Интернет в демилитаризованную зону	Встроенные шаблоны RSA enVision позволяют клиентам легко создавать отчеты в подробной и краткой форме по всему входящему по нестандартным портам Интернет-трафику в пределах группы устройств PCI. Отчет: «PCI – Inbound Internet Traffic on Non-standard Ports – Detail» («PCI – Входящий Интернет-трафик через нестандартные порты – подробная информация»)
Требование 1.3.6 Защита и синхронизация файлов конфигурации маршрутизатора. Например, рабочие файлы конфигурации (для штатного функционирования маршрутизаторов) и загрузочные файлы конфигурации (действующие при перезагрузке машин) должны иметь аналогичную защитную конфигурацию.	RSA enVision имеет встроенные функции подготовки отчетов, в которых суммирована информация обо всем исходящем трафике по адресам назначения. Отчет: «PCI – Outbound Traffic Summary» («PCI – Обзор исходящего трафика») RSA enVision генерирует отчет по всему исходящему трафику для конкретного внутреннего IP-адреса. Отчет: «PCI – Outbound Traffic Detail by Source Address» («PCI – Подробные сведения об исходящем трафике по адресу источника»)
Требование 2.1.1 Для беспроводных сред изменить параметры, установленные поставщиком по умолчанию, включая, помимо прочего, ключи протокола защиты данных (WEP), идентификатор беспроводной сети (SSID), пароли и строки имен и паролей SNMP. Отключить трансляции SSID. Включить защищенный доступ WiFi (WPA и WPA2) для шифрования и аутентификации при их наличии.	RSA enVision имеет встроенные функции подготовки отчетов, которые отражают все изменения конфигурации беспроводных маршрутизаторов, что позволяет клиентам легко демонстрировать аудиторам тот факт, что установки поставщика, включая ключи WEP, идентификаторы SSID, пароль, строки имен и паролей SNMP, а также параметры отключения трансляций SSID, были изменены до того, как беспроводной маршрутизатор был введен в эксплуатацию в среде обработки платежных карт. Отчет: «PCI – Wireless Environment Configuration Changes» («PCI – Изменения конфигурации беспроводного оборудования»)
> Требование 3.6 Полностью документировать и внедрять все процессы и процедуры управления ключами защиты, применяемыми для шифрования данных владельцев карт.	RSA enVision имеет встроенные функции подготовки отчетов, которые позволяют клиентам получать подробную информацию обо всех первоначальных и периодических изменениях ключей шифрования, использованных для безопасного хранения и передачи данных владельцев карт, а также информацию об управлении доступом, например, сведения об успешных и неудачных процедурах входа пользователя в систему, соблюдении политик и регулярном составлении отчетности.
> Требование 4.1 Использовать строгие протоколы криптографии и обеспечения безопасности, например, протокол безопасных соединений (SSL) / протокол транспортного уровня (TLS) и протокол безопасности IP (IPSec) для защиты важных данных владельцев карт в процессе их передачи по открытым, общедоступным сетям передачи данных. Примерами открытых, общедоступных сетей, в которых действует PCI DSS, являются Интернет, WiFi (IEEE 802.11x), глобальная система мобильной связи (GSM) и система пакетной радиосвязи общего пользования (GPRS).	Функция подготовки отчетов RSA enVision позволяет клиентам получать доступ ко всем операциям шифрования в тех случаях, когда использование криптографии было неудачным или когда пользователь отказался от ее применения. Отчет: «PCI – Encrypted Transmission Failures» («PCI – Сбой при передаче зашифрованных данных»)

Требования PCI DSS к подготовке отчетов и проведению аудита и RSA enVision - *продолжение*

Требование PCI DSS	Возможности RSA enVision
> **Требование 5.2** Организовать своевременное обновление антивирусных систем, их эффективную работу, а также возможность генерировать журналы для аудита	RSA enVision предоставляет шаблоны отчетов, которые позволяют администраторам и аудиторам легко просматривать информацию о процедурах обновления антивирусных систем. Отчет: «PCI – Anti-virus Update Procedures» («PCI – Процедуры обновления антивирусных систем»)
> **Требование 6.1** Организовать установку для всех компонентов системы и ПО последних версий патчей, разработанных производителями и относящихся к обеспечению безопасности. Установить соответствующие патчи в течение месяца со дня их выпуска	RSA enVision имеет встроенные функции подготовки отчетов, которые отражают обзоры всех патчей и пакетов обновлений в системах на базе Microsoft Windows. Отчет: «PCI – Vendor-supplied Patch Application» («PCI – Патч, разработанный производителем»)

RSA – это Ваш проверенный партнер

Компания RSA, входящая в состав корпорации EMC, - ведущий разработчик систем безопасности для повышения эффективности бизнеса. RSA помогает лидерам глобального рынка решать сложнейшие задачи в сфере безопасности. Решения RSA построены вокруг информации. Они обеспечивают ее целостность и конфиденциальность на протяжении всего жизненного цикла, независимо от того, где она находится, кто с ней работает и каким образом она используется.

RSA предлагает уникальные решения в сфере идентификации пользователей, управления доступом к данным, предотвращения утечки данных, шифрования, управления защищенными инфраструктурами, соответствия законодательным требованиям и предотвращения несанкционированных действий. Эти решения применяются для защиты личных данных миллионов пользователей, сведений о выполняемых ими операциях и данных, создаваемых в результате выполнения этих операций. Дополнительные сведения приведены на сайтах www.RSA.com и www.EMC.com.

RSA®
The Security Division of EMC
RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com