**Взгляд на аудит сквозь призму стандарта PCI DSS**

Стремительно растет количество операций с использованием пластиковых карт: онлайн-платежи, безналичный расчет в торгово-сервисных предприятиях, манипуляции с банковским счетом в системах онлайн-банкинга и прочие платежные приложения от поставщиков услуг. Соответственно, расширяется инфраструктура, в которой циркулируют информация о держателях карт и критичные аутентификационные данные. В случае попадания этой информации или ее части в руки к злоумышленникам финансовые потери несут как банки-эмитенты, так и конечные пользователи.

С ростом масштабов системы, обрабатывающей элементы данных о держателях платежных карт, увеличивается и поле для мошенничества. В контексте рассматриваемой проблемы наиболее распространенными атаками, направленными на пользователя, по-прежнему остаются кража данных с использованием вредоносного программного обеспечения и хищение информации с использованием поддельных веб-ресурсов компании-вендора (фишинг). Атаки, направленные на самого вендора, в большинстве случаев осуществляются сотрудниками пострадавшей компании (инсайдинг). И если в первом случае со злоумышленниками можно бороться на уровне информирования пользователя и установки соответствующего клиентского программного обеспечения, то во втором случае нужен соответствующий организационный и технический подход к защите процессов системы, в которой хранятся, обрабатываются и передаются элементы данных пластиковых карт.

Совет по стандартам безопасности индустрии платежных карт (*Payment Card Industry Security Standards Council, PCI SSC*)[1], основанный ведущими международными платежными системами (*Visa, MasterCard, American Express, Discover, JCB*), разработал совокупность документов, в которых содержится регламент обеспечения безопасности данных о держателях карт – стандарт безопасности данных индустрии платежных карт (***Payment Card Industry Data Security Standard, PCI DSS***).

Стандарт **PCI DSS** выдвигает достаточно жесткие требования к защищенности компонентов инфраструктуры, в которой передается, обрабатывается или хранится информация о платежных картах. Проверка платежной инфраструктуры на соответствие этим требования позволяет выявить причины, которые значительно снижают уровень ее защищенности. Более того, грамотно построенная процедура аудита позволяет произвести структуризацию полученной информации в ходе мероприятий по оценке соответствия и составить рекомендации по повышению уровня информационной безопасности в приоритетном порядке. Таким образом, в распоряжении компании, заказавшей услугу оценки соответствия требованиям стандарта, в результате оказывается не только максимально полная картина защищенности платежной инфраструктуры в виде официального отчета, содержащего замечания по каждому требованию, но и план действий, представляющий собой совокупность основных шагов, которые необходимо выполнить для устранения проблем. Тесты на проникновение, которые входят в список обязательных мероприятий, регламентированных стандартом PCI DSS, способны продемонстрировать реальный уровень защищенности информационных ресурсов компании c как позиции злоумышленника, находящегося за пределами исследуемого периметра, так и с позиции внутреннего служащего компании.
Международные платежные системы (*МПС*) обязывает все банки, торгово-сервисные предприятия (*ТСП*), процессинги и другие компании, которые ведут бизнес в сфере платежных карт, соответствовать требованиям стандарта PCI DSS. Отсутствие штрафных санкций со стороны МПС за несоответствие требованиям стандарта является адаптационной мерой для инфраструктур и бизнес-процессов ТСП и сервис-провайдеров. Из вышесказанного следует тот факт, что не стоит воспринимать услугу проверки на соответствие требованиям стандарта PCI DSS исключительно как формальную процедуру для получения сертификата соответствия.

Компания-консультант, предоставляющая услугу проверки соответствия требованиям стандарта PCI DSS, должна иметь в своем распоряжении методологию проведения аудита по данному стандарту, которая позволит оценить состояние защищенности исследуемой инфраструктуры. В контексте требований PCI DSS, методология позволит за определенный период времени выделить основные компоненты исследуемой системы и соответствующим образом структурировать полученные результаты. Таким образом, задача консультанта состоит в обеспечении безопасности данных о держателях карт и, как следствие, осуществлении содействия в достижении соответствия требованиям стандарта PCI DSS компании-заказчика.

**Определения**

**ASV (Approved Scanning Vendor)** – поставщик услуг сканирования, имеющий официальный статус от Совета стандартов безопасности (PCI SSC).

**On-site аудит** – аудит инфраструктуры Заказчика, проводимый аудитором непосредственно на реально функционирующих компонентах.

**QSA (Qualified Security Assessor)** — компания, сотрудники которой индивидуально прошли тренинги и экзамены, проводимые Советом стандартов безопасности (PCI SSC).

**Аудитор (консультант)** — лицо, занимающееся аудитом по стандарту PCI DSS (проверкой соответствия требованиям стандарта) и консультационной деятельностью, связанной с оценкой соответствия требованиям стандарта PCI DSS.

**Заказчик** – юридическое лицо, заинтересованное в выполнении исполнителем услуги проверки на соответствие требованиям стандарта PCI DSS.

**Эквайер** – член ассоциации эмитентов банковских карт, который устанавливает и поддерживает взаимодействие с предприятиями торгово-сервисной сети, принимающей платежные карты. [2]

**Стандарт PCI DSS**

**Общие сведения о стандарте PCI DSS**

Стандарт безопасности данных индустрии платежных карт представляет собой совокупность 12 детализированных требований по обеспечению безопасности данных о держателях платежных карт, которые передаются, хранятся и обрабатываются в информационной инфраструктуре торгово-сервисных предприятий, сервис-провайдеров и других организаций. Принятие соответствующих мер по обеспечению соответствия требованиям стандарта подразумевает комплексный подход к обеспечению информационной безопасности данных платежных карт.

Состав [3] и описание официальных поддерживающих документов стандарта PCI DSS:

***1)*** *Стандарт безопасности данных индустрии платежных карт. Требования и процедуры аудита безопасности. Версия 2.0 (Payment Card Industry Data Security Standard. Requirements and Security Assessment Procedures v2.0).*
В документе детально описаны 12 требований стандарта, область их применимости, основные сведения по подготовке к аудиту соответствия требованиям стандарта и проведению аудита, а также сведения по написанию отчетных материалов. Документ разработан преимущественно для использования аудиторами, проводящими onsite-аудит на соответствие требованиям стандарта.

***2)*** *Глоссарий. Версия 2.0 (Glossary v2.0).*
Перечень терминов и сокращений, используемых в нормативной документации PCI DSS. Предназначен для понимания терминов, используемых в других поддерживающих документах и поэтому рекомендуется Заказчику для ознакомления.

***3)*** *Ориентирование в PCI DSS. Версия 2.0 (Navigating the PCI DSS. Version 2.0).*
Документ, в котором описываются 12 требований стандарта с пояснением их значений в целях улучшения понимания требований стандарта предприятиями торгово-сервисной сети, сервис-провайдерами и другими финансовыми учреждениями.

***4)*** *Приоритезированный подход к достижению соответствия PCI DSS. Версия 1.2 (Prioritized Approach for PCI DSS v1.2).*
Правила работ для уменьшения рисков на ранних стадиях мероприятий по достижению соответствия стандарту. Приоритезированный подход состоит из 6 этапов, которые в порядке приоритета помогут распределить усилия по достижению соответствия, снизят риск компрометации данных о платежных картах в процессе выполнения. Подход не заменяет требования стандарта PCI DSS v2.0.

***5)*** *Требования, предъявляемые к квалифицированным экспертам безопасности (PCI DSS Validation Requirements for Qualified Security Assessors).*
Приложение, в котором содержатся требования, предъявляемые Советом по стандартам безопасности платежных карт экспертам безопасности, получающим или уже имеющим статус квалифицированного эксперта безопасности (QSA).

***6)*** *Требования, предъявляемые к поставщикам услуг сканирования (PCI DSS Validation Requirements for Approved Scanning Vendors).*
Приложение, в котором содержатся требования, предъявляемые Советом по стандартам безопасности платежных карт экспертам безопасности, получающим или уже имеющим поставщика услуг сканирования (ASV).

***7)*** *Листы самооценки. Версия 2.0 (PCI DSS Self-Assessment Questionnaire v2.0).*
Листы самооценки предназначены для организации проведения самооценки торгово-сервисными предприятиями и сервис-провайдерами их соответствия стандарту и представляют собой средства проверки соответствия финансовой организации стандарту PCI DSS согласно документу «Стандарт безопасности данных индустрии платежных карт. Требования и процедуры аудита безопасности. Версия 2.0» («Payment Card Industry Data Security Standard. Requirements and Security Assessment Procedures v2.0»). Существуют несколько вариантов листа самоооценки, которые используются в том или ином случае.

***8)*** *Аттестация соответствия PCI DSS – торговые организации. Версия 2.0 (PCI DSS Attestation of Compliance – Merchants v2.0).*
Шаблон документа, который заполняется QSA или торговой организацией (в случае, если торговая организация осуществляет внутренний аудит), и в результате является официальным документом о соответствии данной организации стандарту PCI DSS.

***9)*** *Аттестация соответствия PCI DSS – сервис-провайдеры. Версия 2.0 (PCI DSS Attestation of Compliance – Service Providers v2.0).*
Шаблон документа, который должны заполнить QSA и сервис-провайдер в качестве официального документа о соответствии данного сервис-провайдера стандарту PCI DSS.

Дополнительная документация:

*1) Дополнительные документы – ASV (Additional Documents — ASV).*
Набор документации для поставщиков услуг сканирования (ASV): руководство по программе ASV, список требований ASV, проверка соответствия статусу ASV.

*2) Дополнительные документы – QSA (Additional Documents — QSA).*
Набор документации для квалифицированных экспертов безопасности (QSA): соглашение QSA, список требований QSA.

*3) Дополнительные документы – PFI (Additional Documents — PFI).*
Набор документации для экспертов-криминалистов в индустрии платежных карт (PFI): руководство по программе PFI, список требований PFI, проверка соответствия статусу PFI. Статус эксперта-криминалиста в платежной индустрии введен Советом PCI SSC со второй версией стандарта PCI DSS.

*4) Требование 11.3 Тестирование на проникновение (Requirement 11.3 Penetration Testing).*
Подробное описание требования 11.3 стандарта PCI DSS к проведению тестирований на проникновение.

*5) Требование 6.6 Защита веб-приложений (Requirement 6.6 Application Reviews and Web Application Firewalls Clarified).*
Уточнение к требованию 6.6 стандарта PCI DSS к обеспечению защиты веб-приложений.

*6) Руководство по беспроводным сетям. Версия 1.2 (Wireless Guidelines v1.2)*
Документ содержит предложения и рекомендации для развертывания и тестирования беспроводных сетей в контексте требований стандарта PCI DSS.

Разработчик стандарта не уделяет внимание процедуре структуризации своей документационной базы. Консультант должен определить взаимосвязь официальных документов с целью разработки методологической базы проведения аудита. Рисунок 1 содержит схему, отражающую подчиненность официальных документов стандарта PCI DSS.



*Рисунок 1* – Подчиненность официальных документов стандарта PCI DSS

**Ключевые требования по организации защиты данных**

Ключевые требования по организации защиты данных о держателях платежных карт сформулированы в документе «Стандарт безопасности данных индустрии платежных карт. Требования и процедуры аудита безопасности. Версия 2.0» («Payment Card Industry Data Security Standard. Requirements and Security Assessment Procedures v2.0») и сгруппированы таким образом, чтобы упростить процедуру аудита безопасности. Ниже приведен список 12 требований, находящихся в основе стандарта PCI DSS и объединенных в группы по типам процедур аудита и и их краткий анализ.[4]

*1) Требование 1. «Установить и обеспечить функционирование межсетевых экранов для защиты данных о держателях карт».
2) Требование 2. «Не использовать пароли и другие системные параметры, заданные производителем по умолчанию».*

Первая группа носит название *«Построение и обслуживание защищенной сети»* (требования 1 и 2). С первого требования становится понятно, насколько важен процесс сегментации целевой инфраструктуры и на основе каких средств строится этот процесс. *Межсетевой экран* – основа обеспечения безопасности. Грамотное проектирование циркулируемого траффика приводит в порядок всю инфраструктуру в целом. Тем не менее, в последней версии стандарта все же делается некоторое смягчение формулировки первого требования и подразумевается факт фильтрации и блокировки траффика не только средствами межсетевого экрана.

Помимо осуществления блокирования и фильтрации сетевого траффика на основных компонентах рассматриваемой системы (что в контексте поддерживающих документов означает сервера в исследуемой сети), первое требование содержит пункт 1.4, который подразумевает персональные межсетевые экраны на рабочих станциях сотрудников компании с должной конфигурацией (пользователь не может изменять параметры работы файрволла) – это самая трудноконтролируемая процедура со стороны администратора организации. Второе требование напоминает администраторам сети об обязательном изменении системных параметров, заданных производителем по умолчанию.

*3) Требование 3. «Обеспечить безопасное хранение данных о держателях карт».
4) Требование 4. «Обеспечить шифрование данных о держателях карт при их передаче через сети общего пользования».*

Группа требований *«Защита данных о держателях карт»* (требования 3 и 4) рассматривает критичные методы защиты данных (шифрование, политики ключей безопасности и т.п.) и область их применения, в то время как остальные методы защиты информации, описанные в других требованиях, позиционируются в качестве средств снижения рисков компрометации. Данная совокупность требований описывает политику и жизненный цикл ключей безопасности. В связи с тем, что хранение данных о владельцах пластиковых карт в зашифрованном виде позволяет исключить факт их незаконного использования злоумышленником (если тот каким-либо образом он преодолел остальные рубежи защиты), пункты этой группы носят довольно жесткую формулировку, что позволяет однозначно ее интерпретировать объектом и субъектом аудита. Полезной техникой при хранении данных о держателях пластиковых карт, относящихся к персональным данным (информация, относящаяся к определенному физическому лицу), является их «обезличивание» — процедура удаления или независимого хранения фрагментов этих данных, которые сами по себе не могут однозначно идентифицировать своего владельца.

*5) Требование 5. «Использовать и регулярно обновлять антивирусное программное обеспечение».
6) Требование 6. «Разрабатывать и поддерживать безопасные системы и приложения».*

Группа, объединяющая в себе требования 5 и 6, называется *«Управление уязвимостями»*. Под управлением уязвимостями понимается своевременная установка актуальных обновлений, в том числе и на антивирусное программное обеспечение, разработка, поддерживание и использование безопасных приложений, в том числе и веб-ориентированных.

*7) Требование 7. «Ограничить доступ к данным о держателях карт в соответствии со служебной необходимостью».
8) Требование 8. «Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре».
9) Требование 9. «Ограничить физический доступ к данным о держателях карт».*

Требования 7, 8, 9 объединены в группу *«Внедрение строгих мер контроля доступа»* и носят организационно-технический характер обеспечения защиты информации с использованием как организационных мер обеспечения безопасности, так и механизмов физического доступа и мониторинга.

*10) Требование 10. «Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт».
11) Требование 11. «Регулярно выполнять тестирование систем и процессов обеспечения безопасности».*

Примечательной для аудитора является группа требований *«Регулярные мониторинг и тестирование сети»* (требования 10, 11). Не каждое торгово-сервисное предприятие может позволить себе содержание внутренней службы информационной безопасности и своими силами регулярно выполнять профилактические тесты на проникновение и мониторинг процессов обеспечения безопасности. Потребность в осуществлении этих систематических процедур рождает на рынке информационной безопасности спектр услуг в виде внутренних и внешних тестов на проникновение, сканирования инфраструктуры на уязвимости от совершенно разных поставщиков. Аудитор в процессе оценки соответствия требованиям стандарта PCI DSS, должен ознакомиться с результатами последнего профилактического теста на проникновение и ASV-сканирования (подпункты 11.2 «Ежеквартальное сканирование на уязвимости» и 11.3 «Ежегодные тесты на проникновение») и убедиться, что все выявленные уязвимости устранены. Тот факт, что результаты эти могут быть получены в результате услуг тестов на проникновение и сканирования на уязвимости, предоставленных третьей организацией и, как следствие, вывод аудитора строится на доверии к данным, полученным в ходе оказания этой услуги третьей стороной.

*12) Требование 12. «Разработать и поддерживать политику информационной безопасности».*

Требование 12 по масштабам своей реализации является одним из самых трудных в плане адаптации к инфраструктуре Заказчика. Пункт 12.1.1 требует создания такой политики, которая учитывает все требования PCI DSS. Торгово-сервисные предприятия и сервис-провайдеры, которые проходят сертификацию, должны разработать свою политику безопасности или пересмотреть текущую в соответствии с требованиями стандарта.

**Программы обеспечения безопасности Visa и MasterCard**

Стандарт PCI DSS разработан ведущими международными платежными системами и объединяет в себе требования программ обеспечения безопасности Visa и MasterCard.

**Программа Visa AIS**

Программа безопасности учетной записи (Visa Account Information Security, AIS) разработана Visa для Европы (аналогичная программа Visa для США — Cardholder Information Security Program) с целью помочь торгово-сервисным предприятиям и сервис-провайдерам улучшить свои меры обеспечения безопасности данных держателей платежных карт Visa и информации о транзакциях.

Требования программы Visa AIS, которые должны быть выполнены организацией, зависят от числа ежегодно хранимых, обрабатываемых и передаваемых ею учетных данных Visa.В соответствии с этими данными эквайер присваивает определенный уровень торгово-сервисному предприятию. Ниже представлен список требований программы для торгово-сервисных предприятий и сервис провайдеров.

Требования к торгово-сервисным предприятиям (merchants):

1) ежегодный аудит на соответствие требованиям PCI DSS (любое ТСП, обрабатывающее более 6 млн. транзакций по Visa в год или интернациональные ТСП, которым был присвоен 1 уровень Visa в другом регионе или стране);

2) ежегодное самостоятельное заполнение опросного листа (SAQ) (ТСП, обрабатывающие от 1 млн. до 6 млн. транзакций по Visa в год по всем платежным каналам или ТСП, обрабатывающие от 20 000 до 1 млн. транзакций электронной торговли по Visa в год);

3) ежеквартальное сканирование сети поставщиком услуг сканирования (ASV);

4) наличие аттестата соответствия (для всех уровне ТСП);

5) проверка соответствия требованиям, выполняемая эквайером (ТСП, обрабатывающие менее 20 000 транзакций электронной торговли по Visa в год, или все другие ТСП, обрабатывающие до 1 млн. транзакций в год).

Требования, предъявляемые Visa к сервис-провайдерам (Service Providers):

1) ежегодный аудит на соответствие требованиям PCI DSS;

2) ежегодное заполнение SAQ (любой поставщик услуг, обрабатывающий менее 300 000 транзакций по Visa в год);

3) ежеквартальное сканирование сети в соответствии со стандартом PCI DSS;

4) наличие аттестата соответствия.

**Программа MasterCard SDP**

Программа MasterCard Site Data Protection (SDP), утвержденная MasterCard, предназначена для обеспечения безопасного хранения ТСП и сервис-провайдерами данных учетных записей MasterCard в соответствии со стандартом PCI DSS. Ниже представлен список требований программы для торгово-сервисных предприятий и сервис провайдеров.

Требования, предъявляемые MasterCard торгово-сервисным предприятиям (merchants):

а) ТСП уровня 1 (все ТСП, с ежегодным оборотом более 6 миллионов транзакций ежегодно по картам MasterCard и Maestro; все ТСП, пострадавшие от взлома или атаки, результатом которого была утечка данных; любое ТСП, которое было отнесено к уровню 1, по усмотрению MasterCard) должны выполнять следующие требования:

1) ежегодный аудит, выполняемый QSA;
2) ежеквартальное сканирование сети, выполняемое ASV;
3) обязательное выполнение процедур подтверждения соответствия.

б) ТСП уровня 2 (все ТСП с оборотом более 1 миллиона, но менее либо равным 6 миллионам транзакций ежегодно по картам MasterCard и Maestro; все ТСП, соответствующие уровню 2 другой платежной системы) должны выполнять следующие требования:

1) ежегодный аудит, проводимый QSA;
2) ежегодное заполнение опросного листа SAQ (до 31 декабря 2010 года);
3) ежеквартальное сканирование сети, проводимое ASV;
4) выполнение начальных процедур проверки соответствия (до 31 декабря 2010 года).

в) ТСП уровня 3 (все ТСП, количество транзакций электронной торговли по MasterCard и Maestro превышает 20 000 в год, но общее количество транзакций электронной торговли по MasterCard и Maestro не превышает 1 миллиона; все ТСП, соответствующие уровню 3 другой платежной системы) должны выполнять следующие требования:

1) ежегодное заполнение опросного листа SAQ;
2) ежеквартальное сканирование сети, проводимое ASV;
3) обязательное выполнение процедур подтверждения соответствия.

г) ТСП уровня 4 (все ТСП, не относящиеся к первым трем уровням) должны выполнять следующие требования:

1) ежегодное заполнение опросного листа SAQ;
2) ежеквартальное сканирование сети, проводимое ASV;
3) консультация с эквайером о дате выполнения процедур проверки соответствия.

Требования, предъявляемые MasterCard сервис-провайдерам (Service Providers):

а) Сервис-провайдеры уровня 1 (все сторонние процессинги; все организации хранения данных, которые хранят, передают или обрабатывают ежегодно более 300 000 транзакций MasterCard и Maestro) должны выполнять следующие требования:

1) ежегодный аудит, проводимый QSA;
2) ежеквартальное сканирование сети, проводимое ASV.

б) Сервис-провайдеры уровня 2 (все организации хранения данных, которые хранят, передают или обрабатывают ежегодно менее 300 000 транзакций MasterCard и Maestro) должны выполнять следующие требования:

1) ежегодное заполнение опросного листа SAQ;
2) ежеквартальное сканирование сети, проводимое ASV.

**Ответственность за неисполнение требований МПС**

Уровень ТСП определяется непосредственно эквайером, к которому подключено ТСП. В свою очередь, МПС два раза в год требует от эквайеров предоставление отчетов о соответствии ТСП уровней 1, 2 и 3 требованиям стандарта PCI DSS. Таким образом, эквайер выполняет роль посредника между торгово-сервисными предприятиями и МПС. В случае нарушения торгово-сервисными предприятиями правил МПС, Visa применит соответствующие меры по контролю рисков, которые могут выражаться в наложении штрафов на эквайеров [5].

Сервис-провайдеры, которые удовлетворяют критерию Уровня 1 проходят необходимые процедуры соответствия и включаются в список PCI DSS Compliant Service Providers. Сервис-провайдеры Уровня 2 не включаются в указанный список и контролируются соответствующими эквайерами (контроль представляет собой мониторинг результатов самоопросника).

*Рисунок 2* – Схема взаимодействия МПС с финансовыми организациями

**Аудит ИБ по стандарту PCI DSS**

**Услуги в рамках стандарта PCI DSS**

Ниже перечислен спектр услуг, которые могут быть предоставлены в рамках стандарта PCI DSS.

*1) Аудит на соответствие требованиям стандарта PCI DSS*

Проводится аудиторами, имеющими статус QSA (Qualified Security Assessor) и включает в себя следующие общие этапы:
а) работы по подготовке и планированию аудита на соответствие стандарту PCI DSS;
б) проведение мероприятий согласно процедуре аудита;
в) анализ полученных результатов;
г) формирование Отчета о проведении аудита на соответствие стандарту PCI DSS.

*2) Подготовка инфраструктуры Заказчика для проведения аудита на соответствие требованиям стандарта PCI DSS*
Проводится с целью подготовить инфраструктуру Заказчика к мероприятиям по сертификации на соответствие стандарту PCI DSS и представляет собой предварительный аудит на соответствие требованиям стандарта.

*3) Сканирование уязвимостей в соответствии с требованиями стандарта PCI DSS*
Проводится компанией, имеющий статус ASV (Approved Scanning Vendor) и, в соответствии с требованием 11.3 стандарта PCI DSS, является обязательной процедурой, которая подробно отражена в официальном документе PCI DSS Security Scanning Procedures.

*4) Тест на проникновение в соответствии с требованиями стандарта PCI DSS*
Тест на проникновения является обязательной процедурой для достижения соответствия стандарту, которая проводится минимум раз в год (требование 11.3 стандарта PCI DSS) и включает в себя:

а) внешний тест на проникновение;
б) внутренний аудит.

*5) Курсы повышения квалификации в области информационной безопасности сотрудников организации-заказчика*
Проводится с целью повышения уровня осведомленности сотрудников Заказчика и опционально включает в себя:

а) тренинги и семинары, посвященные тем или иным аспектам информационной безопасности;
б) демонстрация тематических презентаций;
г) проведение вебинаров.

Стандарт PCI DSS объединяет требования программ по защите информации, разработанных Visa и MasterCard (Visa AIS, MasterCard SDP), которые распространяется на все организации, работающие с указанными платежными системами.

Действия стандарта обязательны для региона CEMEA (центральная и восточная Европа, Ближний Восток и Африка), где стандарт PCI DSS является обязательным, поэтому все ТСП и сервис-провайдеры, входящие в этот регион, должны в обязательном порядке пройти процедуру соответствия требованиям стандарта. Таким образом, российские финансовые организации, которые сотрудничают с вышеуказанными МПС, в обязательном порядке должны проходить процедуру оценки соответствия требованиям стандарта PCI DSS.

**Общий подход к проведению аудита соответствия**

Среди общего перечня услуг, которые могут быть предоставлены в рамках стандарта PCI DSS, получение общей картины защищенности инфраструктуры Заказчика и выдачу ему сертификата соответствия может обеспечить услуга аудита на соответствие его требованиям, которая проводится компанией, получившей статус QSA.

Среди подходов к проведению аудитов ИБ различают два принципиально разных методики:

1) тесты на проникновение;
2) технологический аудит информационной безопасности.

На первых стадиях процедуры проверки соответствия аудитор выделяет область аудита – набор компонент, проверка которых, по его мнению, достаточна для получения полной информации о степени защищенности данных платежных карт.

В процесс проведения аудита на соответствие требованиям стандарта PCI DSS выполняется анализ требований и принятие соответствующих мер, описанных в официальном документе «Стандарт безопасности данных индустрии платежных карт. Требования и процедуры аудита безопасности» («Payment Card Industry Data Security Standard. Requirements and Security Assessment Procedures»). Результаты определения области аудита и выборок подтверждаются аудитором и заносятся в Отчет. Далее аудитор определяет общее количество компонентов (офисы компании, ТСП, действующие лица компании и другое) [6]. Полученные данные используются в качестве исходных на этапе оценки соответствия.

Согласно разработанной методике проведения оценки соответствия аудитор производит анализ полученной информации на этапе сбора исходных данных. Результаты заносит в таблицу требований. В случае выявления несоответствия требований составляется перечень компенсирующих мер [6], если невыполненные требования подразумевают такие меры. По окончанию процедуры оценки соответствия аудитором заполняет Отчет (AOC, Свидетельство о соответствии).

**Основные этапы проведения аудита**

Нижеперечисленные пункты представляют собой совокупность этапов работ, на основе которых построены аудиторские практики ведущих российских консалтинговых компаний.
***1)*** *Этап первый. Анализ и систематизация.*
*Исходные данные*:
а) информация о компонентах системы Заказчика, в которой хранится или обрабатывается критичная информация о держателях платежных карт;
б) нормативно-распорядительная документация Заказчика, связанная с информационной безопасностью (политика информационной безопасности, регламенты, инструкции и другая документация, необходимая в соответствии с требованиями PCI DSS);
в) состав и характеристика аппаратных и программных средств передачи информации, топология сети;
г) характер внутренней и внешней связи информационной системы, принципы обработки критичной информации в информационной системе.
*Состав работ:*
а) анализ исходных данных;
б) выделение области аудита на основе анализа исходных данных.
Выходные данные:
а) топология (список и характеристика устройств обработки информации) области аудита;
б) информация об объеме работ по проведению и определение необходимых технических средств аудита.

***2)*** *Этап второй. Оценка соответствия требованиям стандарта.*
*Исходные данные*: выходные данные, полученные на предыдущем этапе.
*Состав работ* (определяется особенностями выделенной сертификационной области Заказчика):
а) анализ корпоративной сети и проверка ее защищенности;
б) анализ беспроводных сетей и проверка их защищенности;
в) анализ конфигурации межсетевых экранов;
г) анализ списков контроля доступа;
д) анализ парольной политики;
е) анализ технологий обработки критичной информации;
ж) проверка наличия ПО мониторинга сети и логирования действий пользователя;
з) проверка политик обновления ПО (в том числе защитного ПО).
*Выходные данные:*
а) итоговый вывод о соответствии инфраструктуры заказчика требованиям стандарта PCI DSS;
б) получение Заказчиком картины защищенности его инфраструктуры, имеющихся уязвимостей и ошибок в проектировании политики безопасности.

***3)*** *Этап третий. Формирование отчета.*
*Исходные данные*: выходные данные, полученные на предыдущем этапе.
*Состав работ:* подготовка отчета о результатах сертификационного аудита.
*Выходные данные:* отчет о результатах проведения сертификационного аудита на соответствие инфраструктуры Заказчика требованиям стандарта PCI DSS.

**Поле битвы — сегмент**

Если оптимистично смотреть на область применения PCI DSS, то по своей сути требования распространяются на систему, в которой происходит манипуляция с номером карты (PAN). Однако понятие «система» на практике довольно растяжимое и номера карт могут обрабатываться во множестве компонентов, которые и определяют систему. Кстати говоря, помимо данных о держателях карт, куда относится PAN и другая информация, есть еще и критичные аутентификационные данные, хранение которых недопустимо даже в зашифрованном виде.

*Рисунок 3* — Таблица, иллюстрирующая элементы данных и соответствующие им меры

Если взглянуть на таблицу, которая иллюстрирует элементы данных пластиковых карт и соответствующие им меры защиты, то можно заметить, что такие элементы как **CVV2** (*Card Verification Value 2* — код проверки подлинности карты платёжной системы Visa) и **CVC2** (аналогичный код платежной системы MasterCard) относятся к критичным аутентификационным данным, а значит не подлежат хранению. Тем не менее, в пользовательской практике встречаются случаи, когда торгово-сервисное предприятие с целью упрощения жизни своим клиентам не требует повторного ввода этого кода на своем веб-ресурсе. Таким организациям приходится выбирать между сертификатом PCI DSS (и, как следствие, безопасностью своих бизнес-процессов) и излишней псевдозаботой о своих пользователях, ведь CVC2 и CVV2 являются одним из ключевых звеньев при совершении финансовых online-операций.

Оптимизация структуры целевой системы с последующим выделением среды, в которой происходит манипуляция с данными о держателях карт, позволяет сузить область влияния PCI DSS, сфокусировать внимание аудитора на более конкретном объекте и, как следствие, сократить затраты на проведение оценки соответствия. Только вот процесс сегментации требует понимания и, возможно, реструктуризации бизнес-процессов рассматриваемой организации, что может оказаться куда дороже, чем неоптимизированный аудит. В таком случае под область аудита попадает вся сеть. Тут уже каждая организация должна сама решить, стоит ли ей пересматривать свою текущую практику ведения бизнеса или проще подвергнуться проверке в режиме «как есть».

Если каким-либо образом беспроводные сети используются в качестве среды передачи данных о держателях карт, то этот факт является следствием некорректной сегментации или ее отсутствием. В данном случае в силу вступают требования PCI DSS для беспроводных сетей, что нехорошо ни для проверяемой стороны (в силу «дотошности» требований) ни для стороны проверяющей (специалисты по безопасности беспроводных сетей «на дороге валяются»).

Еще одним «паразитом» в исследуемом сегменте выступают сторонние организации, которые предоставляют услуги обработки, хранения или передачи данных о держателях карт исследуемой организации. Каждой из третьих сторон необходимо представить аудитору сертификат соответствия PCI DSS или, в противном случае, пройти процедуру оценки соответствия.

*Делаем выводы:*

**1)** грамотная сегментация способна сократить временные и, в некоторых случаях, финансовые расходы на проведение оценки соответствия;
**2)** наличие в системе беспроводных сетей, как средств обработки данных о держателях – результат некорректной процедуры сегментации или же ее отсутствия;
**3)** привлечение третьих сторон в бизнес-процесс влечет к дополнительным временным затратам на проверку этих сторон аудитором, который должен отчетливо понимать роль исследуемой компании и ее поставщиков услуг (третьих сторон) в платежной индустрии.

**Список использованных источников**

1. Глоссарий (версия 2.0) — PCI SSC, 2010 — 16 стр.
2. PCI Security Standards Council – PCI SSC, 2010 – [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).
3. Библиотека документов PCI DSS – PCI SSC, 2010 – [www.pcisecuritystandards.org/security\_standards/documents.php?category=supporting](http://www.pcisecuritystandards.org/security_standards/documents.php?category=supporting)
4. Документ «Стандарт безопасности данных индустрии платежных карт. Требования и процедуры аудита безопасности» (версия 2.0) — PCI SSC, 2010 – 84 стр.
5. PCI DSS Compliance Management – «Информзащита», 2010 – [www.pcisecurity.ru](http://www.pcisecurity.ru).
6. Приложения B, С, F документа «Стандарт безопасности данных индустрии платежных карт. Требования и процедуры аудита безопасности» (версия 2.0) — PCI SSC, 2010 – 84 стр.

Некоторые материалы данной аналитической работы опубликованы в журнале «Хакер»(#144) за январь 2011 г.