

## Заказчик – Консультант – Интегратор

24.08.2009

*В связи с растущей актуальностью стандарта PCI DSS стоит обратить внимание на особенности взаимодействия участников процесса сертификации PCI. В данной статье рассмотрены основные вопросы, которые чаще всего возникают при подготовке и в процессе сертификации.*

*Александра Голик, заместитель директора компании Digital Security*

### **Введение**

С тех пор, как соответствие стандарту PCI DSS стало обязательным и обозначилось конкретными сроками, приобрели актуальность такие стороны вопроса прохождения сертификации, как:

- этапы работ, которые являются необходимыми при приведении платежной инфраструктуры организации в соответствие PCI;
- разделение работ по схеме «Заказчик – Консультант – Интегратор».

Путь к соответствию требованиям стандарта включает ряд этапов, для успешной реализации которых необходимо участие и сотрудничество трех сторон: Заказчика, Консультанта и Интегратора.

### **Проведение предварительного аудита**

Сначала необходимо выяснить, каков процент несоответствия требованиям стандарта PCI DSS. Для этого анализируется нормативно-распорядительная документация и проверяются существующие в платежной инфраструктуре технические решения. Проведенная работа позволяет составить перечень несоответствий требованиям, а также разработать рекомендации по их устранению, позволив тем самым компании-участнику индустрии платежных карт определиться с тем, как лучше организовать работу по устранению несоответствий и в каком порядке вносить изменения в инфраструктуру.

*По результатам проведенного аудита при наличии требований со статусом «Не выполнено», Заказчику необходимо подготовить «План мероприятий» (Action Plan) по приведению информационной инфраструктуры в соответствие требованиям PCI DSS с указанием сроков устранения несоответствий. Согласованный и утвержденный План мероприятий отправляется Консультантом в международные платежные системы.*

### **Планирование, разработка, внедрение**

По итогам проведения аудита, подготовки соответствующих заключений и разработки Консультантом рекомендаций начинается процесс приведения информационной инфраструктуры в соответствие требованиям стандарта.

При планировании работ рекомендуется руководствоваться концепцией приоритетного подхода к выполнению требований PCI DSS, разработанной Советом PCI SSC. Она заключается в том, что каждому требованию стандарта присвоен приоритет выполнения.

Основной комплекс работ по внедрению мер достижения соответствия PCI состоит из двух основных этапов:

- Разработка новой или рецензирование существующей документации

Для эффективного управления мерами по защите карточных данных необходимо наличие политик, регламентов и процедур, которые бы описывали процессы информационной безопасности. В случае если документация уже разработана, Консультанты проводят ее рецензирование. В ином случае Заказчику требуется решить задачу по разработке недостающих документов, которую, впрочем, он может поручить Консультанту.

*В данном вопросе следует учитывать, что даже если какой-либо процесс в платежной инфраструктуре Заказчика протекает в соответствии с требованиями стандарта, то факт отсутствия надлежащей регулирующей документации, сопровождаемой необходимыми записями, не позволит признать требование выполненным.*

- Планирование и внесение изменений в инфраструктуру

Пока Заказчик или Консультант работают над документацией, Интегратор формирует перечень необходимых с технической точки зрения изменений в инфраструктуру, согласно рекомендациям Консультанта. Интеграционный этап практической реализации этих изменений занимает наибольшее количество времени, отводимого на весь комплекс работ.

*Следует упомянуть про такой аспект, как компенсирующие меры. Существует распространенное, но, тем не менее, ложное убеждение, что разработка компенсирующих мер позволит сократить расходы на пути достижения соответствия. Компенсирующая мера разрабатывается только в случае невозможности реализации прямого требования стандарта вследствие наличия обоснованных технических или бизнес-ограничений, то есть, является исключением. Она должна обеспечивать аналогичный исходному требованию уровень снижения риска и, зачастую, требует гораздо больших финансовых вложений, чем выполнение прямого требования стандарта, так как ее внедрение может повлечь за собой применение целого комплекса организационных и технических мер. Таким образом, следует стремиться реализовать исходное требование стандарта, которое описывает самый прямой и наименее затратный путь снижения риска. При этом существует исключение, когда компенсирующая мера действительно может оказаться условно дешевле выполнения требования стандарта. Это тот случай, когда компанией уже были понесены затраты и уже применяющиеся решения закрывают определенные требования стандарта и могут быть признаны компенсирующими мерами.*

## **Проведение сертификационного аудита**

Проведение сертификационного аудита является заключающей стадией на пути организации к соответствию требованиям стандарта PCI DSS. В итоговом Отчете о Соответствии (Report on Compliance) не должно быть требований, статус которых отличается от «Выполнено».

*Если по каким-либо причинам требование стандарта является неприменимым к платежной инфраструктуре компании, Консультант обозначает его статус «Выполнено», пометчая в комментарии, что оно не применимо.*

Неотъемлемой частью сертификационного аудита является проверка наличия Отчета о тестировании на проникновение (внутреннем и внешнем). Согласно требованию 11.3 подобное тестирование должно проводиться не реже одного раза в год. Кроме того стандарт PCI DSS в рамках требования 11.2 обязывает выполнять ежеквартальное ASV-сканирование.

*В рамках сертификационного аудита Консультанту (в данном случае находящемуся в роли аудитора) достаточно проверить отчеты о проведенном тестировании на проникновение (внутреннем и внешнем) и ASV-сканировании. При этом стоит обратить особое внимание на то, что отчет о тестах на проникновение не должен являться простым отчетом сканера уязвимостей (как это, к сожалению, очень часто бывает) – на это QSA-аудитор всегда обращает самое пристальное внимание. Тест на проникновение и сканирование – это совершенно разные работы.*

## Результаты

При успешном прохождении сертификационного аудита Заказчик получает Сертификат Соответствия, а в международные платежные системы отправляется Отчет о Соответствии (Report on Compliance) и Свидетельство о Соответствии (Attestation of Compliance).

## Взаимодействие сторон

*Немаловажную роль при организации процесса подготовки и прохождения сертификации играет выбор различных компаний в качестве Консультанта и Интегратора:*

- 1. Независимый от Интегратора Консультант не заинтересован в навязывании Заказчику дорогостоящего программного обеспечения и оборудования для устранения найденных в процессе аудита несоответствий.*
- 2. Консультант, не являющийся Интегратором, ориентирован именно на приведение системы в соответствие и итоговую сертификацию с минимальными для Заказчика затратами.*

В общем виде, достижение желаемого результата – соответствия всем требованиям стандарта PCI DSS – возможно только в случае скоординированной работы всех участников процесса – Заказчика, Консультанта и Интегратора.

*Таблица 1. Взаимодействие сторон*

Этап	Консультант	Интегратор	Заказчик
1	Предварительный аудит на соответствие требованиям PCI DSS		Предоставление запрашиваемой Консультантом информации

Этап	Консультант	Интегратор	Заказчик
2	Разработка детальных рекомендаций по приведению инфраструктуры Заказчика в соответствие требованиям PCI DSS		
3	Согласование перечня программного обеспечения и оборудования	Выбор программного обеспечения и оборудования, необходимого для приведения инфраструктуры Заказчика в соответствие требованиям PCI DSS	Согласование перечня программного обеспечения и оборудования
4	Консультации по внедрению	Поставка, установка и настройка программного обеспечения и оборудования	Внедрение рекомендаций, не связанных с установкой и настройкой программного обеспечения и оборудования
5	Разработка системы менеджмента информационной безопасности в соответствии с PCI DSS	Документирование настроек ОС и оборудования (выполняется или Интегратором или Заказчиком)	Внедрение системы менеджмента информационной безопасности
6	Тест на проникновение из сети Интернет	Устранение выявленных несоответствий	Устранение выявленных несоответствий
7	Внутренний тест на проникновение	Устранение выявленных несоответствий	Устранение выявленных несоответствий
8	Ежеквартальное ASV-сканирование	Устранение выявленных несоответствий	Устранение выявленных несоответствий
9	Сертификационный аудит, отправка отчетных документов в международные платежные системы, выдача Сертификата соответствия		

## Об авторе

Александра Голик - заместитель директора компании Digital Security. На протяжении нескольких лет является менеджером проектов компании по оказанию консалтинговых услуг в области информационной безопасности.

## О стандарте PCI DSS

Стандарт PCI DSS (Payment Card Industry Data Security Standard) предназначен для обеспечения безопасности обработки, хранения и передачи данных о держателях платежных карт в информационных системах компаний, работающих с международными платежными системами Visa, MasterCard и другими. Стандарт разработан сообществом PCI Security Standards Council, в которое входят мировые лидеры на рынке платежных карт, такие как American Express, Discover Financial Services, JCB, MasterCard Worldwide и Visa International.

Под действие требований стандарта попадают банки, процессинговые центры, поставщики ИТ-услуг, торгово-сервисные предприятия, и иные организации, обрабатывающие транзакции по международным платежным картам. К части этих компаний международные платежные системы предъявляют требование о прохождении обязательного ежегодного аудита компанией, обладающей статусом QSA.

Текущая версия стандарта 1.2 выпущена 1 октября 2008 года.