



Курс "PCI-DSS: специалист по внедрению"

Ориентирован на:

специалистов, аналитиков и руководителей подразделений ИТ и ИБ, связанных с карточными системами, заинтересованных в получении знаний и требований стандарта PCI DSS. Также курс ориентирован на аудиторов (специалистов по оценке соответствия).

Формат и продолжительность:

Семинар, 5 дней 40 часов (80% теория, 20% практика)

Методические материалы:

Учебные материалы в электронном виде

Документ об окончании курса:

Сертификат учебного центра о прослушивании курса

Программа курса:

Модуль 1. Обзор стандарта PCI DSS

- История стандарта
- Сфера действия стандарта
- Риски, связанные с дискредитацией карточных данных
- Схемы монетизации карточных данных

Модуль 2. Методы и средства обеспечения безопасности и оценки защищенности данных платежных карт

- Содержимое платежной карты
- Содержимое платежной полосы



- Критичные аутентификационные данные
- Платежная карта: EMV-чип: общие сведения
- Корректная утилизация платежной карты
- Выпуск платежной карты
- PAN как минимальная единица защиты
- Алгоритм Луна
- Анализ схемы корпоративной сети, принципов сегментации и разделения информационных потоков.
- Анализ конфигурации межсетевых экранов, корректности и актуальности списков контроля доступа.
- Проверка наличия беспроводных сетей стандарта 802.11X и анализ их защищенности.
- Анализ используемых сетевых протоколов с точки зрения безопасности. Анализ принятых в информационной системе политик безопасности (политики контроля доступа, парольной политики, политики физической безопасности и т.д.) Анализ принципов и технологий обработки критической информации о платежных картах.
- Проверка наличия процедуры своевременного обновления системных компонентов и антивирусного ПО на серверах и рабочих станциях.
- Проверка наличия механизмов регулярного мониторинга сети и информационных ресурсов.
- Приведение критичных данных к нечитаемому виду.
- Однонаправленное хеширование.
- Шифрование.
- Урезание.
- Понятие компенсационных мер на примере выполнения требований п. 3.4.1 PCI DSS Понятие строгой криптографии PSI DSS.
- Сканирование информационной сети на наличие уязвимостей (ASV)
- Проведение теста на проникновение на уровне приложений (Application-layer penetration tests)
- Анализ защищенности беспроводных сетей

Модуль 3. PCI DSS. Индустрия платежных карт. Базовая терминология

- Инфраструктура стандартов группы PCI
- Стандарт PCI DSS - история
- PCI DSS. Эмиссия платежных карт МПС Visa и MasterCard
- PCI DSS. Две стадии эквайринга платёжных карт МПС Visa и MasterCard PCI DSS. Этапы авторизации.
- PCI DSS. Этапы клиринга и взаимного расчета.
- Платежная инфраструктура
- PCI DSS. Распределение ответственности за безопасность данных.
- PCI DSS. Стандарты безопасности данных индустрии платежных карт.
- Виды отчетности



- Путь к соответствию
- Банкомат как специфический объект PCI DSS

Модуль 4. Стандарт PCI DSS 4.0. Что нового?

- проведение анализа достаточности уровня информационной безопасности;
- идентификация текущих рисков несоответствия требованиям законодательства и регуляторов в области защиты информации;
- формирование экспертного заключения о соответствии и рекомендаций по устранению несоответствий.

Итоговый тест.

Подведение итогов, ответы на вопросы.

Требования к оборудованию учебного класса:

На каждого студента выделенный ПЭВМ с доступом в сеть Интернет, установленной ОС Windows и пакетом программ Office

