# СТАНДАРТ PCI DSS 3.2

ДиалогНаука

# Информация о PCI DSS

- **Выпущен:** 30 июня 2005 года
- **Разработку инициировали:** MasterCard Worldwide, Visa International, American Express, Discover Financial Services, JCB
- **Цель:** Обеспечить защиту электронных платежных систем в свете участившихся случаев хищений информации о держателях платежных карт
- **Обязателен для внедрения:** Во всех организациях, хранящих, обрабатывающих и передающих данные о держателях платежных карт: процессинговые компании, банки, Интернет-магазины и др.
- **Актуальная версия:** 3.1 и 3.2

# Кому необходим PCI DSS

Требования стандарта PCI DSS распространяется на организации, обрабатывающие, хранящие или передающие информацию о держателях платежных карт, например:

- Процессинговые компании
- Банки, имеющие собственный процессинг
- Крупные розничные сети
- Операторы сотовой связи
- Интернет-магазины
- Коммерческие ЦОД

# Терминология PCI DSS

**Merchat (Торгово-сервисное предприятие)**

- Принимают платежные карты для оплаты товаров или услуг (розничные сети, рестораны, Интернет-магазины и т.д.)

**Сервис-провайдер (Поставщик услуг)**

- Оказывают различные услуги, необходимые для осуществления оплаты (банки, процессинги и т.д.)

**Транзакция**

- Операция с картой по оплате, снятию или переводу денежных средств

**QSA (Qualified Security Assessor)**

- Компания имеющая право проводить аудиты по PCI DSS

**ASV (Approved Scanning Vendor)**

- Компания, имеющая право проводить внешние сканирования уязвимостей

# Процедуры подтверждения соответствия сервис-провайдеров

## Уровни сервис-провайдеров

- Level 1 > 300 тыс. транзакций в год
- Level 2 < 300 тыс. транзакций в год

## Процедуры подтверждения соответствия

- Ежегодный сертификационный аудит, выполняемый QSA (Level 1)
- Ежегодное заполнение самоопросника Self-Assessment (Level 2)
- Ежеквартальное внешнее сканирование уязвимостей, проводимое ASV (Level 1, 2)
- Ежеквартальное внутреннее сканирование уязвимостей (Level 1, 2)
- Ежегодное выполнение внутренних и внешних тестов на проникновение (Level 1, 2)
- Ежегодное выполнение анализа рисков (Level 1, 2)

# Последствия несоответствия

- Ущерб от действий злоумышленников (финансовый и репутационный)
- Отказ в повышении статуса в платежных системах
- Штрафные санкции (размеры штрафов конфиденциальны)
- Отказ международных платежных систем в предоставлении услуг

# Состав услуг PCI DSS

Услуги по сертификации включают три этапа:

- Обследование ИС заказчика и разработка рекомендаций по приведению в соответствие
- Реализация требований стандарта
- Сертификация

# Состав услуг PCI DSS

Обследование ИС заказчика и разработка рекомендаций по приведению в соответствие

- Сбор и анализ исходной информации
- Разработка плана мероприятий по приведению в соответствие

# Состав услуг по PCI DSS

**Реализация требований стандарта**

- Разработка политик, стандартов и процедур
- Проектирование СОИБ
- Внедрение СОИБ

# Состав услуг PCI DSS

**Услуги по сертификации**

- Анализ рисков ИБ
- Ежеквартальные ASV-сканирования
- Ежеквартальные сканирования уязвимостей из ЛВС
- Тестирование на проникновение из сети Интернет и ЛВС
- Сертификационный аудит

# Наши преимущества

- Необходимые компетенции
- Большой опыт выполнения работ по внедрению PCI DSS и проведению сертификации по PCI DSS
- Гибкость при приведении в соответствие и сертификации
- Возможность выполнения комплексных проектов вместе с НПС и СТО БР

# PCI DSS v3.2

- Опубликован 28 апреля 2016г.
- Обязателен с 1 ноября 2016г.
- До 31 октября действуют обе версии
- Виза принимает отчеты по PCI DSS v3.1 до 31 декабря 2016г. (по аудитам завершенным до 31 октября 2016г.)

# PCI DSS v3.2 / основные изменения

- Уточнения и дополнительные руководства
- Срок перехода на TLS 1.1 или TLS 1.2 продлен
- Многофакторная аутентификация для администраторов (обязательно с 1 февраля 2018г.)

## PCI DSS v3.2 изменения для сервис-провайдеров

- Документирование криптографической архитектуры
- Выполнение требований PCI DSS и актуализация документации должно являться частью проводимого изменения
- Обеспечение непрерывности функционирования средств ЗИ
- Тестирование на проникновение каждые 6 месяцев для проверки механизмов сегментации
- Назначение ответственного за соответствие PCI DSS
- Ежеквартальная проверка выполнения процессов ИБ

# Вопросы?

**Александр Крупчик**
Тел.:  +7 (495) 980-67-76,164
Факс: +7 (495) 980-67-75
Моб.: +7 (916) 147-08-20
E-mail: krupchik@dialognauka.ru

ДиалОгНаука