Группа компаний **МАСКОМ**
Компания **Digital Security**

ТЕМА: Выполнение требований 152 ФЗ и PCI DSS в современных информационных системах - эффект синергии

Сергей Иванов, руководитель проекта Департамента безопасности информационных технологий, МАСКОМ

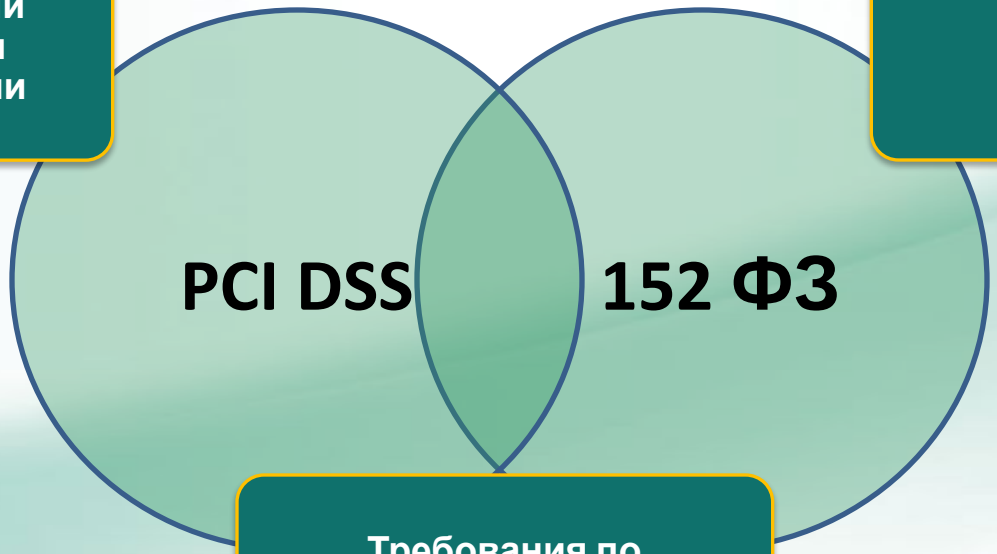
Алексей Синцов, Руководитель департамента аудита ИБ, Digital Security

CNews Forum 2011

Что общего между требованиями PCI DSS и требованиями по защите персональных данных

Количественные показатели, как основной критерий при определении уровня защиты или проверки

Обязательность выполнения требований



Требования по применению схожих средств защиты информации

Основные отличия требований PCI DSS и требований по защите персональных данных

PCI DSS

При увеличении риска ИБ требования одинаковы, изменяется глубина контроля выполнения требований

Аудит информационной безопасности проводит сертифицированный QSA-аудитор

Защищаемая информация – аутентификационные данные и данные о держателях карт

152 ФЗ

Требования по защите обусловлены количеством и составом персональных данных

Контроль за выполнением требований выполняют регуляторы: Роскомнадзор, ФСТЭК, ФСБ

Защищаемая информация – данные о субъекте персональных данных

Комплексный подход

1 этап — Обследование информационной системы

2 этап — Приведение в соответствие требованиям

3 этап — Оценка соответствия и сертификационный аудит

Обследование

PCI DSS

- Проведение предварительно аудита информационной безопасности
- Изучение организационно-распорядительной документации Компании
- Изучение инфраструктуры данных платежных карт

152

- Формирование опросных листов
- Интервью с руководителями подразделений и техническими специалистами
- Изучение процесса обработки персональных данных
- Разработка моделей угроз и нарушителя

Разработка рекомендаций по приведению в соответствие требований

Приведение в соответствие требованиям

PCI DSS

- Раздел технического проекта посвященный PCI DSS
- Разработка политик информационной безопасности
- Настройка соответствующего оборудования и программного обеспечения
- Проведение тестов на проникновение, ASV-сканирование

2 этап

152

- Раздел технического проекта посвященный защите персональных данных
- Разработка проектов организационно-распорядительной документации
- Настройка соответствующего оборудования и программного обеспечения
- Внедрение организационно-технических мер

Оценка соответствия и сертификационный аудит

PCI DSS

Проведение Сертификационного аудита

Выдача Сертификата Соответствия PCI DSS

152 ФЗ

Проведение оценки соответствия информационной системы персональных

Выдача заключения о соответствии…

3 этап

Заключение. Синергетический эффект

Возможность оптимизации процессов обеспечения информационной безопасности Заказчика

Сокращение сроков реализации проектов и снижение материальных затрат

Возможность оптимизации количества внедряемых технических решений

СПАСИБО ЗА ВНИМАНИЕ

www.mascom.ru