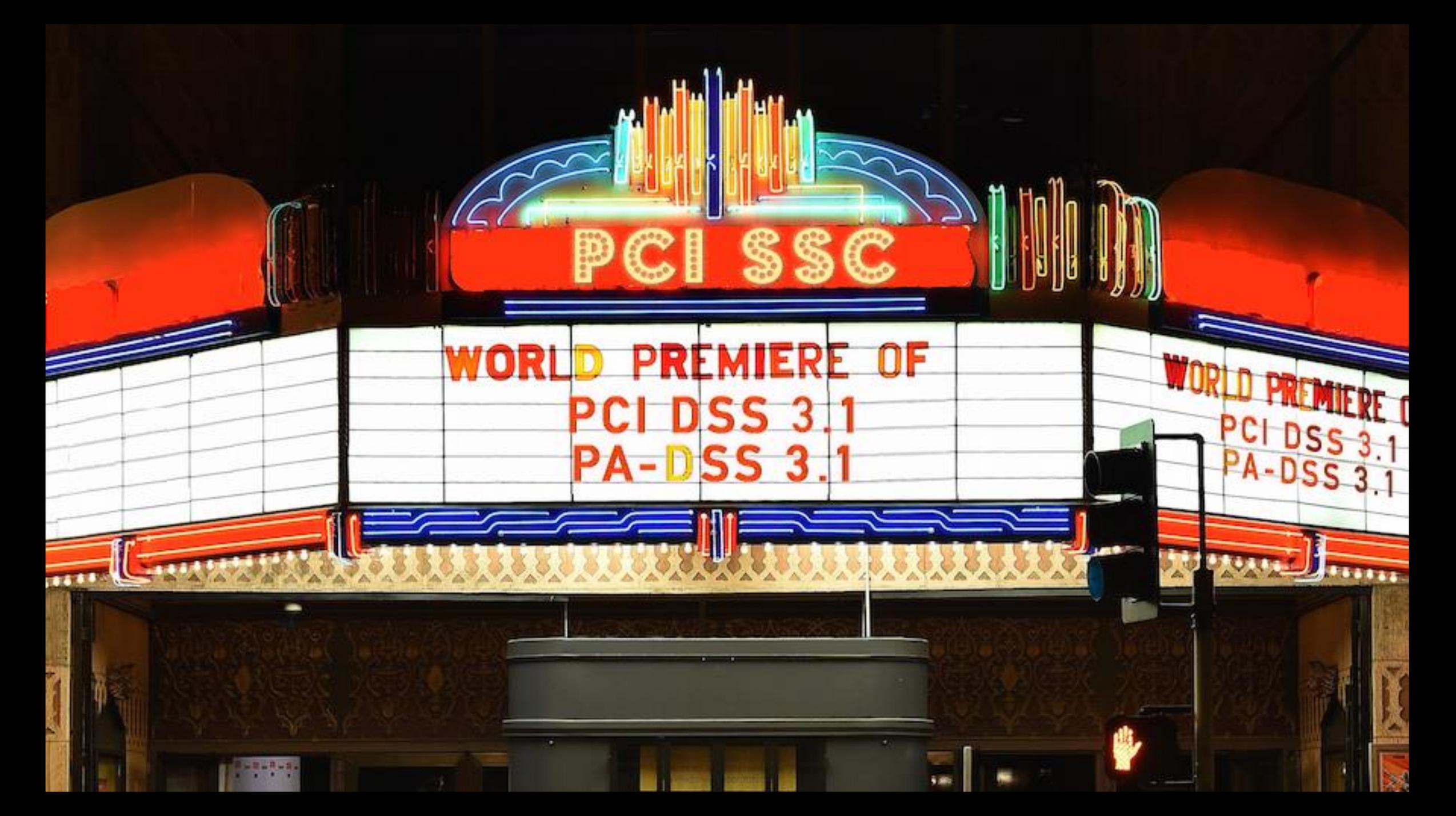




Последние изменения в стандартах безопасности платежных карт

Андрей Гайко,
QSA



PCI SSC

WORLD PREMIERE OF
PCI DSS 3.1
PA-DSS 3.1

WORLD PREMIERE OF
PCI DSS 3.1
PA-DSS 3.1



PCI DSS 3.1

- **2.2.3.c, 2.3.f, 4.1.i** Компании, использующие уязвимые протоколы, должны составить план миграции на новые протоколы (такие планы должны быть в наличии и при аудите они будут проверяться), разработать и выполнять процедуры по мониторингу новостей об уязвимостях в используемых протоколах
- **2.2.3.b, 2.3.e, 4.1.h.** POS (POI), использующие SSL или TLS 1.0 и которые могут быть проверены на предмет невозможности их компрометации, могут и дальше использовать эти протоколы после 30 июня 2016 года
- Разрабатывая или внедряя новые системы необходимо исключить использование SSL всех версий и TLS версии 1.0
- После 30 июня 2016 года все компании обязаны отказаться от использования протокола SSL и TLS 1.0 и закончить миграцию на более безопасные

Обязателен к применению с 1 июля 2015 года



PA-DSS 3.1

- **8.2, 11.1, 12.1-12.2.** Из примеров безопасных протоколов удалены SSL и TLS 1.0
- Сертификация по PA-DSS v3.0 возможна до 31 августа 2015 г.
- После 1 сентября все приложения должны проходить оценку соответствия по PA-DSS v3.1
- Приложения, находящиеся в процессе сертификации, должны быть сертифицированы до 30 ноября 2015 г.

Обязателен к применению с 1 июля 2015 года



«На основании статистики по расследованию инцидентов (собранный за 10 лет), связанным с компрометацией ДДК, на момент инцидента ни одна компания, не соответствовала требованиям PCI DSS»

*согласно данным, представленным в отчете VERIZON 2015 PCI COMPLIANCE REPORT





PCI DSS Designated Entities Supplemental Validation

Что это?

- Дополнительные обязательные к исполнению требования для отдельных организаций, постоянное соответствие (BAU)

Для кого?

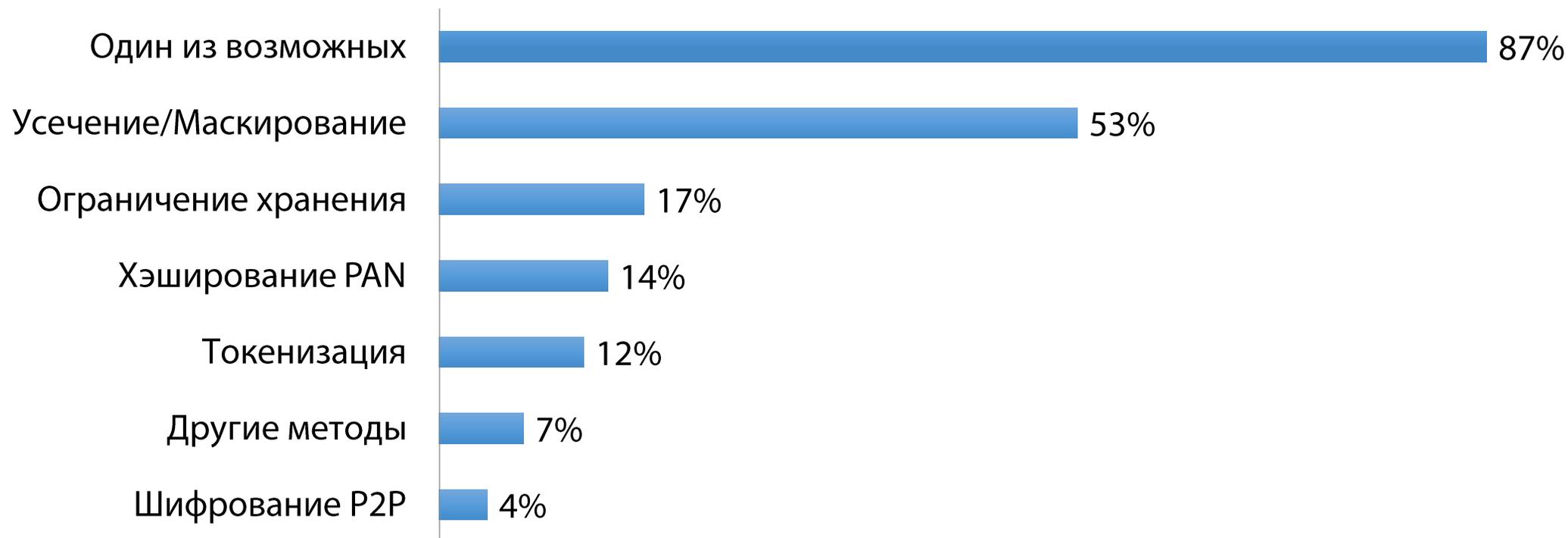
- Для компаний с высоким риском компрометации данных (например, обрабатывающих большое количество ДДК) или часто подвергающимся атакам

Требования PCI DSS DESV обязательны к исполнению для всех компаний?

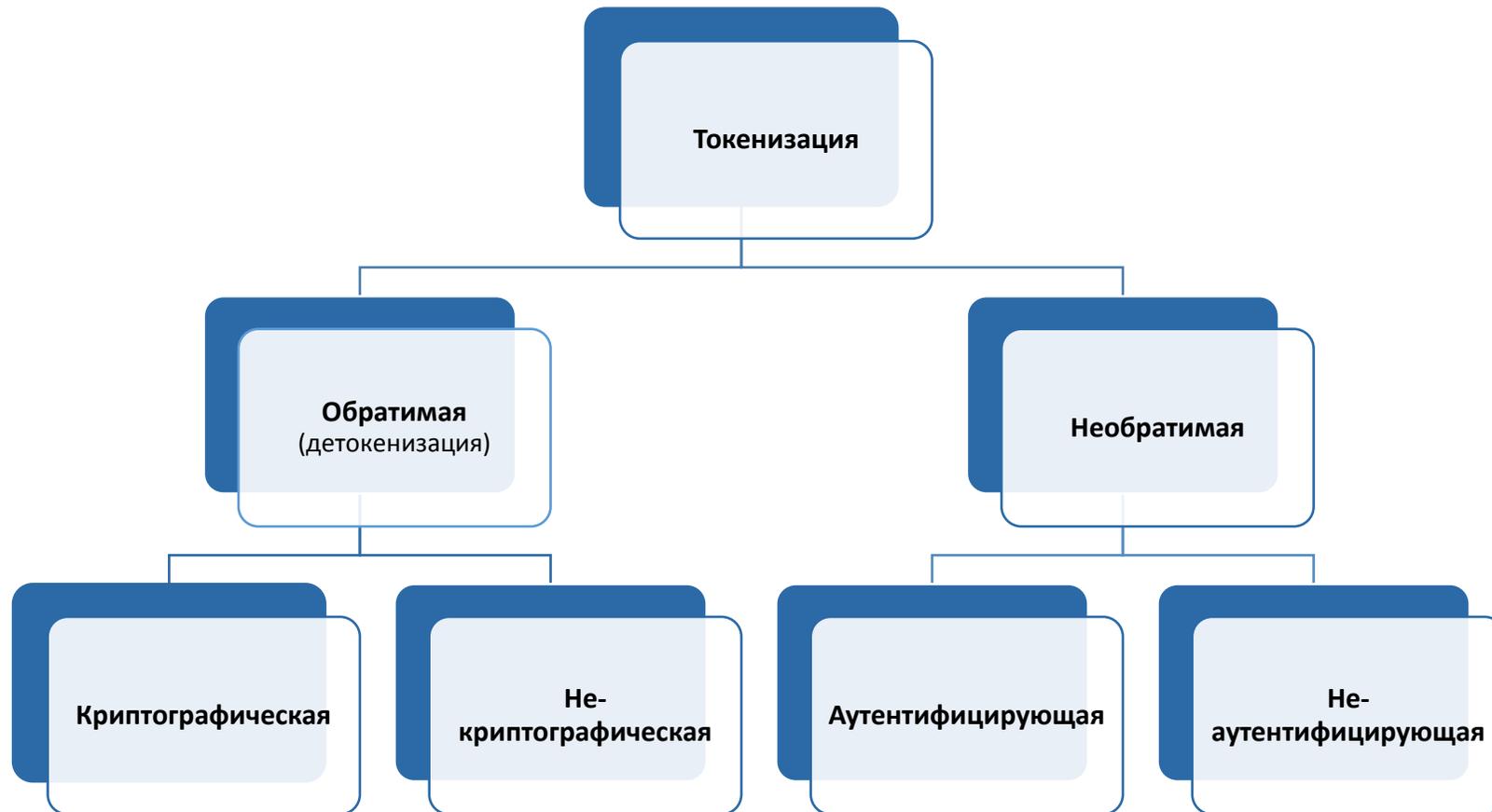
- Только если об этом попросит эквайер или МПС

У меня есть сертификат PCI DSS. Мне надо сертифицироваться еще раз?

- Аудит по требованиям PCI DSS DESV выполняется в ходе аудита по PCI DSS

**% компаний, использующих метод**

*по результатам анализа RoC за 2012 – 2014 год (Verizon)



Алгоритм	3DES	AES	RSA	Эллиптические кривые	DSA/D-H
Минимальная длина ключа в битах	Использование не допускается	128	3072	256	3072/256

Алгоритм хэширования

SHA-256

SHA3-256

SHA3-384

SHA-512

SHA3-512

Вероятность угадывания PAN из токена должна быть не менее 1 в 10^6 (как и вероятность угадывания усеченного PAN)





Оглавление

1	Принятые обозначения и сокращения	3
2	Общие сведения	5
2.1	Цель документа	5
2.2	Положение о конфиденциальности	5
2.3	Используемая литература	5
2.4	Принятая шкала оценки критичности уязвимостей (Assigning a Severity Score)	5
2.5	Этапы работ по тестированию на проникновение	6
3	Перед проведением работ	8
3.1	Область аудита	8
3.2	Время проведения аудита	8
3.3	Цель выполнения работ	8
3.4	Место проведения аудита	8
3.5	Проверка ранее выявленных уязвимостей и угроз	9
3.6	Требования к окружению	9
3.7	Методы взаимодействия и передачи информации	9
3.8	Реагирование на инциденты	10
3.9	Ограничения	10
4	Выполнение работ	11
4.1	Тестирование на уровне сети	11
4.2	Тестирование на уровне приложений	11
4.3	Модель нарушителя и угроз	12
4.4	Сбор информации о системе и ее анализ	12
4.5	Проверка корректности сегментации сети	13
4.6	Идентификация/обнаружение уязвимостей	13
4.7	Эксплуатация уязвимостей	14
4.8	Пост-эксплуатация	15
4.9	Получение доступа к ДДК	15
5	После выполнения работ	16
5.1	Повторное тестирование	16
5.2	Восстановление информационных систем Заказчика после аудита	16
6	Отчетность	17

Методика

Последние изменения в стандартах безопасности платежных карт

Оглавление

1	Принятые обозначения и сокращения	3
2	Общие сведения	5
2.1	Информация об исполнителе	5
2.2	Дата проведения аудита	5
2.3	Описание выполненных работ	6
2.4	Область аудита	7
2.4.1	Перечень проверенных подсетей	8
2.4.2	Перечень проверенных компонентов CDE	9
2.4.3	Перечень не проверенных компонентов CDE	10
2.4.4	Перечень проверенных компонентов вне CDE	12
2.4.5	Сведения о «глубине» теста на проникновение	13
2.5	Модель нарушителя	14
2.5.1	Внутренний нарушитель	14
2.5.2	Внешний нарушитель	14
2.6	Методология тестирования	14
2.7	Ограничения	15
3	Сведения о тестировании	16
3.1	Результаты проверки сегментации	17
3.2	Результаты тестирования	19
3.2.1	Найденные уязвимости	20
3.2.2	Возможные риски компрометации CDE	24
3.3	Используемые средства	25
3.4	Выводы	26
4	Восстановление информационной системы после аудита	27

Отчет



Чего ожидать в 2015 году

Ежедневный анализ журналов событий

- Руководство по анализу событий и выявлении потенциальных проблем безопасности
- Руководство по инструментам/техникам агрегации и просмотра событий

Разделение ответственности между компанией и поставщиками услуг

- Руководство по предоставлению отчетности
- Руководство по разделению области ответственности, сервисов



Information Supplement: Penetration Testing Guidance	https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf
Tokenization Product Security Guidelines: Irreversible and Reversible Tokens	https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf
PCI DSS Designated Entities Supplemental Validation	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_DESV.pdf
Verizon 2015 PCI Compliance Report	http://www.verizonenterprise.com/resources/report/rp_pci-report-2015_en_xg.pdf



Спасибо за внимание!

115054, Россия,
Москва, Партийный пер.,
д. 1, корп. 57, стр. 3

197046, Россия,
Санкт-Петербург,
Петроградская наб., 16 А

+7 (812) 703-15-47
+7 (495) 223-07-86
info@digitalcompliance.ru