Digital Security

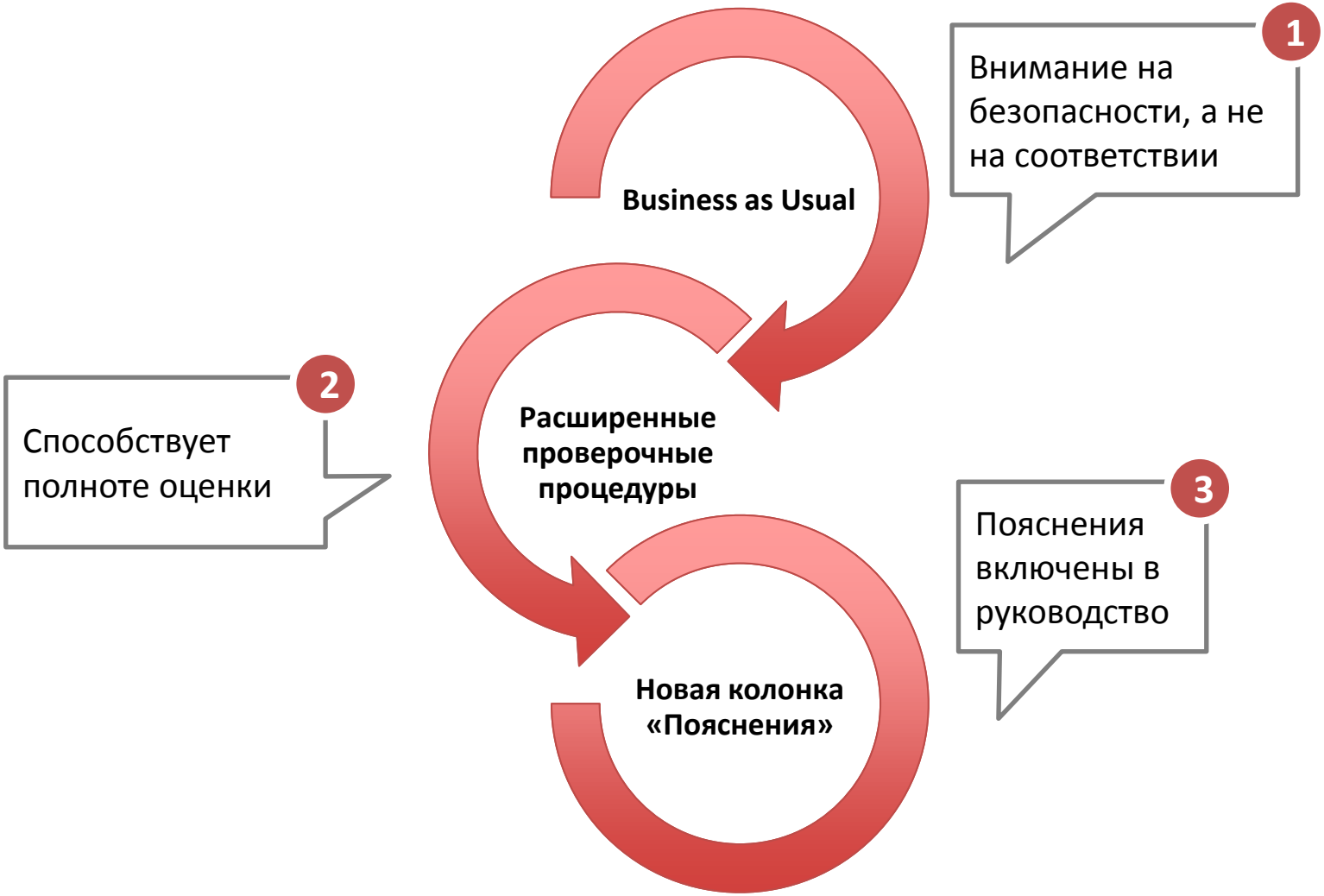
PCI DSS 3.0 – что нового?

Андрей Гайко
QSA-аудитор

Главные новости

- Опубликован официальный перевод стандарта
- Опубликованы сопровождающие документы
- Выпущен шаблон ROC для PCI DSS 3.0
- Добавили новые типы SAQ

Изменения в новой версии PCI DSS



Изменения в новой версии PCI DSS: Business-as-usual

Изменения в новой версии PCI DSS: Изменение в таблице требований

«PCI DSS 2.0 Требования и процедуры аудита безопасности»

Требования PCI DSS	Проверочные процедуры

«Понимание назначения требований»

Пояснение

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
3.4 PAN должен быть представлен в нечитаемом виде во всех местах хранения (включая данные на съемных носителях, в резервных копиях и журналах протоколирования событий). Для этого следует использовать любой из следующих методов: • функция стойкого однонаправленного хеширования	**3.4.a** Изучить документацию о системе, используемой для защиты основного номера держателя карты, в том числе информацию о ее производителе, типе системы, применяемых алгоритмах шифрования (если они используются), и убедиться, что основной номер держателя карты приводится к нечитаемому виду с помощью одного из следующих методов: • функция стойкого однонаправленного хеширования; • усечение (truncation);	все номера PAN, которые хранятся в основных хранилищах (базах данных, неструктурированных файлах, таких как текстовые файлы, таблицы и т.д.), а также во вспомогательных хранилищах (резервных копиях, журналах регистрации событий, журналах исключений и устранения неисправностей и т.д.), должны быть защищены.

«PCI DSS 3.0 Требования и процедуры аудита безопасности»

Изменения в SAQ

- Изменилась структура всех SAQ
- Добавили два новых SAQ:

SAQ A-EP – предназначен ТОЛЬКО для e-commerce мерчантов, которые принимают платежи на своем сайте, но проводят их через стороннюю сертифицированную по PCI DSS организацию. Мерчанты не должны хранить, обрабатывать или передавать ДДК в какие-либо иные свои системы.

SAQ B-IP – предназначен для мерчантов, использующих отдельностоящие POI-терминалы (сертифицированные по PCI PTS), подключенные к платежному шлюзу, и не хранящие ДДК в электронном виде. Не предназначен для e-commerce. Мерчант должен использоваться только PCI PTS-устройства (любого класса кроме SCR)

Изменения в новой версии PCI DSS: Хранение критичных данных

Запрещается хранить критичные аутентификационные данные после авторизации, даже в зашифрованном виде. Данное требование действует, даже если PAN отсутствует в среде.

Организации должны напрямую связаться со своими эквайерами или МПС, чтобы узнать, разрешается ли хранить критичные аутентификационные данные до авторизации и в течение какого срока, а также получить информацию о других требованиях к использованию и защите данных.

Стандарт PCI DSS 3.0, стр.8

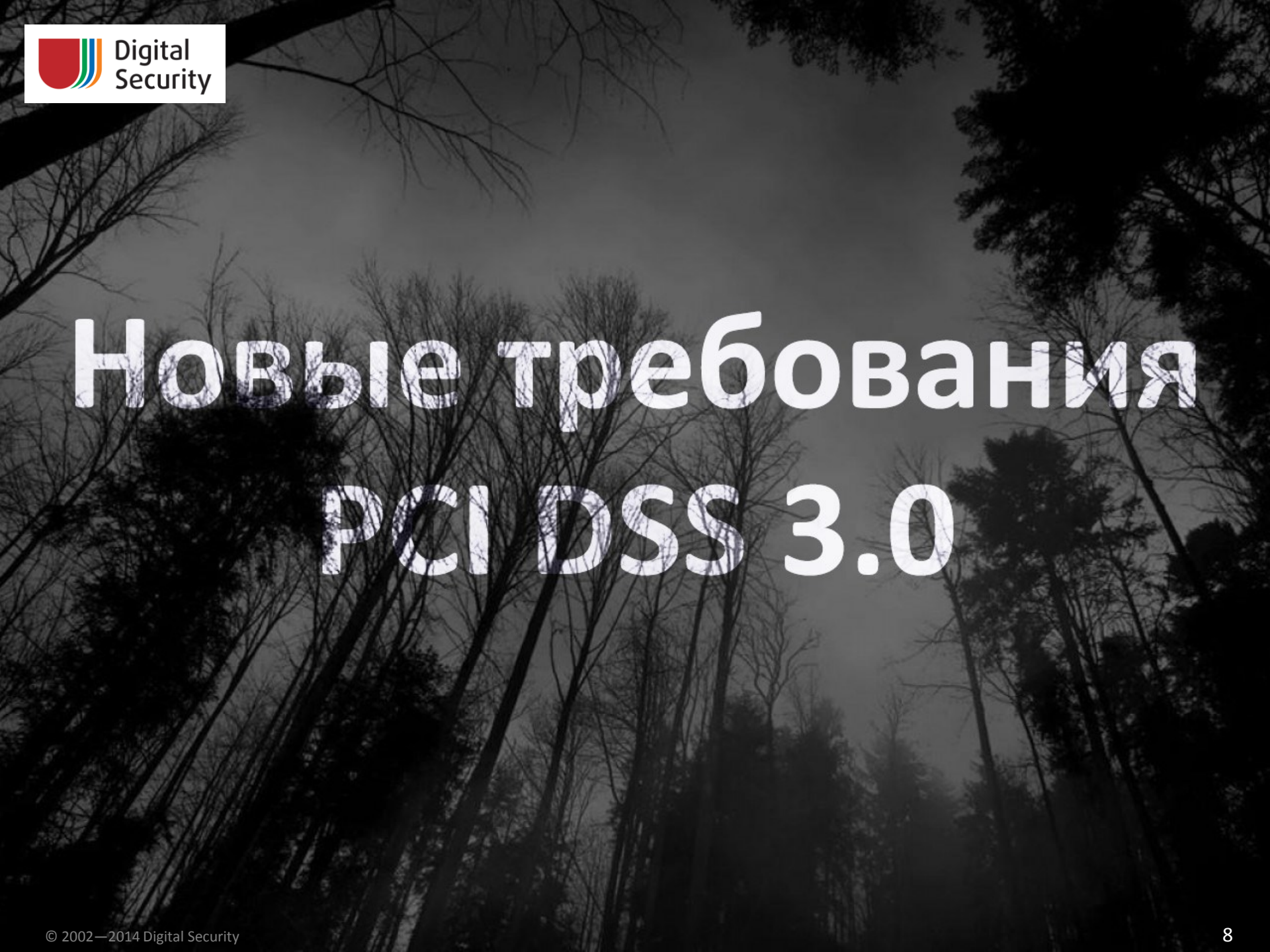
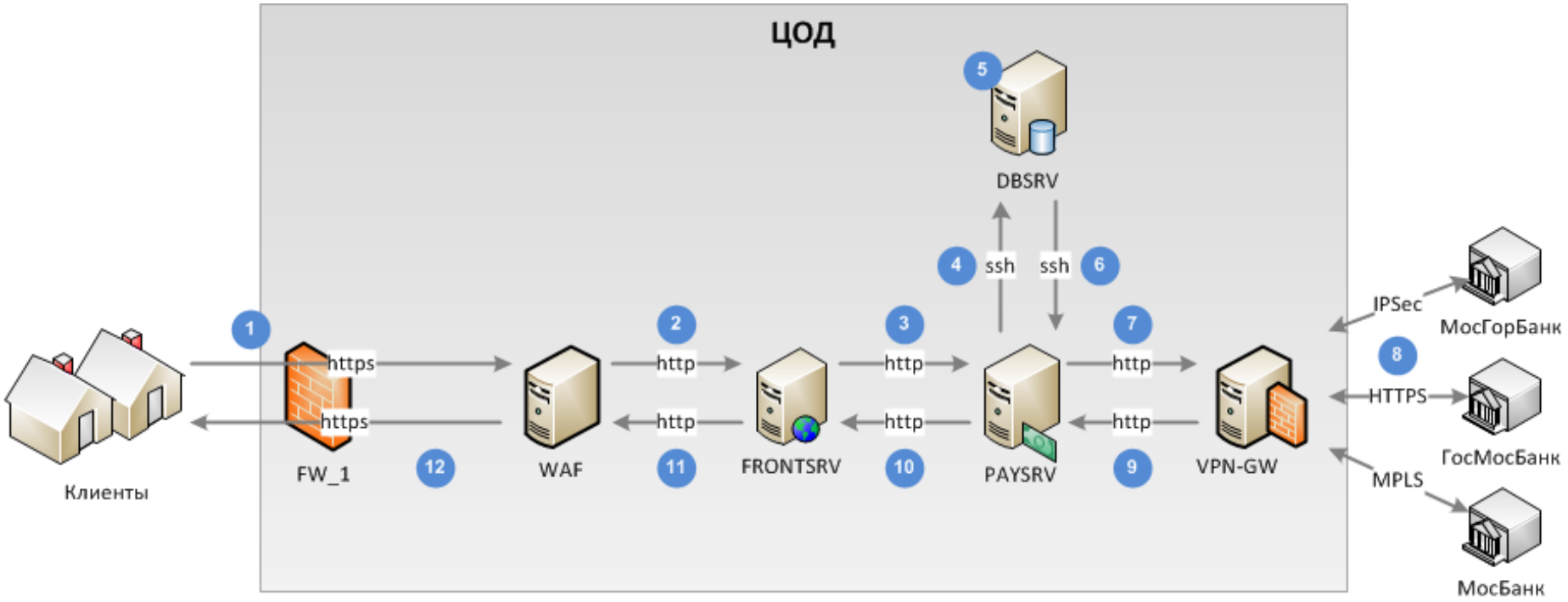


Схема информационных потоков. Требование 1

Для каждого платежного процесса необходима схема информационных потоков.

Пример: Процесс приема платежей с веб-страниц клиентов



Учет всех компонентов. Требование 2

Должен вестись перечень всех программных и аппаратных средств, входящих в область оценки:

- серверы (физические, виртуальные);
- АРМ, ноутбуки;
- сетевое оборудование;
- системное и прикладное ПО;
- СЗИ;
- т.д.

Применение антивирусной защиты. Требование 5

- Раньше нужно было защищать только системы «подверженные вирусным атакам»

  Теперь необходимо периодически оценивать риски заражения всех используемых операционных систем

- Отключение или изменение настроек антивируса разрешается только после согласования с руководством

Разделение полномочий. Требование 7

Необходимо внедрить, реализовать и поддерживать процесс Разделения полномочий (Separation/Segregation of Duties, SoD).

Парольные политики. Требование 8

- Уход от направленности на пароли, как на основное средство аутентификации
- Ввод понятия парольной фразы
- Даны рекомендации по использованию иных механизмов аутентификации
- Необходимо разработать инструкции для пользователей по каждому методу аутентификации

Физический доступ. Требование 9

- Бейджи больше не являются обязательными, достаточно эффективного метода отличия сотрудников от посетителей
- Физический доступ должен администрироваться

Учет считывающих устройств. Требование 9

- Контроль и учет устройств считывания карт (вступит в силу с 1 июля 2015 г.): POS, банкоматы, кард-ридеры для доступа в помещения с банкоматами и т.д.
- Обучение сотрудников методам распознавания взлома и подмены устройств. Разработка обучающих материалов

Журналы регистрации событий. Требование 10

Уточнены требования по фиксации событий:

- факты любого вида доступа каждого пользователя к ДДК;
- расширение полномочий;
- изменения учетных записей с правами суперпользователя и администратора;
- инициализации журналов, остановка или приостановка ведения журналов.

Период проверки журналов можно увеличить, основываясь на оценке рисков.

Тест на проникновение. Требование 11

- Необходимо внедрить методологию проведения теста на проникновение (с июля 2015)
- Тест на проникновение, кроме остальных задач, должен проверять эффективность сегментации

Реагирование на изменения. Требование 11

- Термин «мониторинг целостности файлов» заменен на «механизм обнаружения изменений», то есть суть – в фиксации любых изменений в инфраструктуре
- Надо реагировать на любые срабатывания этого механизма. Надо фиксировать все изменения в инфраструктуре и на каждое реагировать

Разделение ответственности за выполнение требований. Требование 12

Разделение ответственность за выполнение требований между компанией и поставщиком услуг.

Поставщик услуг дает письменные обязательства о соответствии (с июля 2015) и безопасность передаваемых ему ДДК.

Проверка выполнения требований поставщиком услуг:

- либо в рамках аудита компании;
- либо проверка результатов прохождения поставщиком услуг аудита по PCI DSS.

Примеры схем и таблиц

Примеры схем в формате Visio	http://goo.gl/D9OYPr
Описание требований к схемам	http://goo.gl/q57qYf
Перечни сведений об инфраструктуре	http://goo.gl/PDwGBY

В случае вопросов или предложений по улучшению схем и таблиц пишите: a.gaiko@dsec.ru

Спасибо за внимание!

Спасибо за внимание!

Полная версия презентации доступна по ссылке: http://goo.gl/8JdP94

Андрей Гайко

QSA-аудитор

a.gaiko@dsec.ru