

Основным достоинством нового течеискателя является возможность выполнения бесконтактных измерений температуры грунта одновременно с измерением уровня вибрации. Опытной эксплуатацией подтверждена возможность выявления утечек в теплосетях и возможность отслеживания прокладки теплотрасс с помощью теплотрических измерений. Таким образом достигается существенное повышение достоверности выявления местоположения утечек на трубопроводах теплосетей.

1. *Владимирский А.А.* Принципы построения акустического течеискателя "А-10". // Зб. наук. пр. ПІМЕ НАНУ. Вип. 19, Київ, 2003р. - С.122-128.
2. *Владимирский А.А., Владимирский И.А.* Разработка термо-акустического течеискателя А-20Т. // Зб. наук. пр. ПІМЕ НАНУ. Вип. 52, Київ, 2009р. - С.54-56.

Поступила 11.10.2010р.

УДК 004.056.32

Д.П. Галата, НАУ, г. Киев

Б.Я. Корниенко, к.т.н., НАУ, г. Киев

Л.П. Галата, НАУ, г.Киев

СЕРТИФИКАЦИЯ ПО СТАНДАРТУ PCI DSS

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. Compliance to PCI DSS standards is truly a mandatory rule for business merchants who opt to accept payments through the use of plastic cards such debit and credit cards.

В Украине с 2006 г. сертификация информационных систем по стандарту PCI DSS (Payment Card Industry Data Security Standard) является обязательной для финансовых компаний [1]. В случае несоответствия его требованиям для партнеров крупнейших платежных систем (VISA, MasterCard и др.) вводятся жесткие штрафные санкции.

Повышенный интерес к стандарту сегодня – не просто боязнь попасть под штрафные санкции платежных систем, но и естественное желание чувствовать себя защищенными и обеспечить безопасность своих клиентов.

Постановка задачи

Целью данной статьи является исследование использования стандарта PCI DSS для сертификации информационных систем.

Процедура сертификации

При подготовке к сертификации на соответствие PCI DSS необходимо

принимать во внимание ряд важных моментов. Аудит и разработка плана, учитывая определение границ проекта, занимает от одного до четырех месяцев. Сроки устранения несоответствий стандарту напрямую зависят от выявленных недостатков, развитости ИТ-инфраструктуры и текущей загрузки ИТ-систем финансового учреждения другими проектами. Поэтому на данную процедуру может потребоваться от двух месяцев до двух лет. Основными же сложностями на этапе аудита может стать отсутствие документации, регламентирующей деятельность ИТ [2-4].

Проект по сертификации – это интерес всей компании, поэтому и подходить к нему надо со всей ответственностью: с поддержкой со стороны руководства и действиями со стороны функциональных департаментов.

Этапы подготовки к сертификации:

На первом этапе производятся:

- Анализ, систематизация и уточнение полученных от Заказчика исходных данных о компонентах информационной системы, в которых хранится или обрабатывается критичная информация о платежных картах [5].

- Анализ нормативно-распорядительной документации по информационной безопасности (политик, регламентов и инструкций), необходимой в соответствии с требованиями стандарта PCI DSS.

- Анализ топологии сети, состава и характеристик аппаратных и программных средств передачи информации.

- Анализ характера внутренних и внешних связей информационной системы, информационных потоков и принципов обработки критичной информации о платежных картах в информационной системе.

- Определение и утверждение области применения стандарта (области сертификации) на основании результатов работы по предыдущим пунктам.

На втором этапе подготовки к сертификации по PCI DSS производятся:

- Оценка соответствия информационной системы Заказчика требованиям стандарта PCI DSS.

- Подготовка отчета о результатах предварительного аудита.

На третьем этапе подготовки к сертификации по PCI DSS производятся:

- Выработка предложений и рекомендаций по устранению выявленных несоответствий требованиям стандарта PCI DSS.

- Консультационные услуги по внедрению новых или доработке существующих компонентов информационной системы с целью соответствия требованиям стандарта PCI DSS.

SRC Security Research & Consulting GmbH - единственный официальный аудитор, осуществляющий сертификацию процессинговых компаний на соответствие всем требованиям безопасности (MasterCard Site Data Protection (SDP) и VISA Account Information Security, установленным основными платежными системами VISA и MasterCard соответственно, и предъявляемым к компаниям, обрабатывающим банковские карты в сети Интернет). Со времени своего появления в Германской банковской системе, SRC Security Research & Consulting GmbH является основным связующим

звеном между исследованиями и готовыми продуктами в сфере безопасности международных платежных систем.

При оценке уровня защиты данных платежных карт, в первую очередь, специалистами берутся во внимание такие основные требования PCI DSS:

- защищенность сети
- степень защиты данных держателей карт
- наличие программы мероприятий по управлению уязвимостями и контролю доступа
- регулярный мониторинг и тестирование сети
- внедрение политик информационной безопасности.

Получение такого сертификата – это не гарантия того, что вы обеспечили информационную безопасность своей компании на целый год до проведения следующей сертификации. Обеспечение безопасности – это циклический процесс, который никогда не останавливается. Любые изменения в ваших информационных системах и процессах, приобретение новых аппаратных или программных средств, появление новых сотрудников и даже рутинная ежедневная операционная деятельность – требуют постоянного внимания. Безопасностью надо заниматься постоянно. А что касается сертификации, то получение сертификата также бывает разным. Если пойти по легкому пути и получить сертификат, проведя сканирование и заполнив опросник, то не стоит думать, что ваши системы защищены и соответствуют требованиям стандарта и есть вероятность, что в случае инцидента будут наложены штрафные санкции. А если провести полный цикл аудита, реализовать проекты по устранению несоответствий требованиям стандарта в информационных системах, то можно с уверенностью сказать, что получая сертификат соответствия, вы также выполнили львиную долю работ по обеспечению информационной безопасности организации. Большую часть, но и это не все.

Вывод

PCI DSS – это набор норм, соответствие которым не решает всех проблем в области информационной безопасности. Однако если в вашей организации уделяется достаточно внимания вопросам информационной безопасности, то это создает дополнительное преимущество. Процесс постоянного совершенствования с каждым годом сокращает сроки и стоимость проекта по сертификации на соответствие требованиям стандарта PCI DSS.

Успешно проведенный аудит и получение сертификата PCI DSS бесспорно подчеркивают ответственный и профессиональный подход любой компании к вопросам безопасности

1. <http://www.dsec.ru>
2. <http://www.infosec.ru>
3. <https://www.pcidss.ru>
4. <http://www.twirpx.com>
5. <http://www.paysystems.org.ua>

Поступила 4.10.2010г.