Д. Н. Макрушин

КОНЦЕПЦИЯ СИСТЕМЫ СБОРА И ОБРАБОТКИ ДАННЫХ ДЛЯ АУДИТА ПО СТАНДАРТУ PCI DSS

Введение

Оценка соответствия инфраструктуры, в которой хранятся, обрабатываются и передаются данные о держателях платежных карт, требованиям Стандарта безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard, PCI DSS) [1] позволяет выявить причины, создающие условия для нарушения свойств безопасности информационной системы и, как следствие, компрометации критичных данных [2].

Объективность оценки, качество и полнота полученной картины защищенности информационной среды зависят от методологии оценки соответствия требованиям стандарта PCI DSS, разработанной и применяемой компанией-консультантом в ходе сертификационного аудита, а также от программного обеспечения, которое используется для сбора и обработки информации, получаемой в процессе оценки. Автоматизация ряда методологических процессов позволит аудитору экономить временные ресурсы, затрачиваемые на выполнение рутинных действий по мере сбора и обработки исходных данных, сократить или рационализировать использование человеческих ресурсов при осуществлении аудиторских проверок, структурировать полученную информацию для последующего анализа и наглядной демонстрации результатов заказчику.

Разработка системы сбора и обработки данных, получаемых в ходе проведения оценки соответствия требованиям стандарта PCI DSS, предоставляет возможность осуществить автоматизацию действий аудитора, тем самым повышая качество процедуры аудита. Совместимость концептуального продукта с программным обеспечением от сторонних производителей, которое используется аудиторами в рамках уже разработанных методик, позволит использовать результаты внешних приложений в качестве входных данных проектируемой системы. Особенность архитектуры в виде подключаемых модулей обеспечит возможность расширения функциональности системы сбора и обработки данных, тем самым абстрагируя конечный продукт от стандарта безопасности, по которому осуществляется сертификационный аудит.

Классификация средств сбора

В процессе проведения оценки соответствия инфраструктуры, в которой хранятся, передаются и обрабатываются данные о держателях платежных карт, на соответствие требованиям стандарта «Payment Card Industry Data Security Standard» аудитор действует согласно разработанной им методике аудита сертификационного аудита. Данная методика позволяет за определенный период времени выделить основные компоненты исследуемой системы и соответствующим образом структурировать полученные результаты исследования. При этом сбор информации в ходе сертификационного аудита может осуществляться разными способами, в зависимости от типа источника исходных данных и параметров системы, которые подлежат проверке.

Методы сбора исходных данных для оценки соответствия тому или иному требованию зависят от типа источника исходных данных. Типы источников исходных данных, на основе которых осуществляется оценка соответствия:

1. объекты, являющиеся частью информационной системы, в отношении которых определены какие-либо параметры функционирования (конфигурационные файлы, политики безопасности, распорядительная документация, протоколы и т. п.), а также сущности, являющиеся результатом работы этих объектов (записи в журналах);

2. персонал организации, проходящий процедуру оценки соответствия;

3. статистические данные.

Для каждого из этих типов источников существуют свои методы сбора информации:

1. Сбор и обработка информации об объектах.

Накопление результатов реакции на внешнее воздействие (тест на проникновение) и инвентаризация ресурсов.

2. Сбор и обработка информации, содержащейся в объектах.

Представляет собой накопление информации из конфигурационных файлов, записей журналов (лог-файлов) целевой системы.

3. Анализ информации, содержащейся в объектах.

Осуществляется ручной или автоматизированный анализ политик безопасности, распорядительной документации и т. п. с целью последующей оценки соответствия требованиям стандарта.

4. Опрос персонала.

Проводится интервьюирование должностных лиц целевой организации с целью проверки полученной информации на соответствие требованиям стандарта.

5. Аккумуляция статистических данных.

Накапливаются статистические данные для проверки той или иной информации, полученной с помощью других методов, например при интервьюировании персонала.

В зависимости от описанных методов сбора исходных данных вводится классификация средств их сбора:

1. Обработчик — автоматическое или автоматизированное средство обработки входных данных по заданным параметрам, формирующее вывод результата в удобочитаемом для оператора виде. Соответствующий метод — сбор и обработка информации, содержащейся в объектах.

2. Аналитик. Лицо или автоматизированное средство обработки источника данных, которое осуществляет анализ некоторых объектов (политики информационной безопасности, распорядительной документации и т. п. документов). Соответствующий метод — анализ информации, содержащейся в объектах.

3. Опросный лист. Средство интервьюирования персонала исследуемой организации с целью последующего анализа на соответствие полученной информации требованиям стандарта. Соответствующий метод — опрос персонала.

В случае с методом аккумуляции статистических данных в качестве средства сбора может выступать одно из вышеперечисленных средств.

В контексте проектирования системы сбора и обработки информации наибольший интерес представляют средства, не требующие вмешательства аналитика, т. е. пункты «Обработчик» и «Опросный лист». Данная выборка позволяет выявить пункты процедур проверки, которые можно полностью или частично автоматизировать.

Архитектура системы

В архитектуре системы сбора и обработки информации присутствует условное разделение среды, в которой циркулирует информация, на внешнюю и внутреннюю. К внешней среде относятся вспомогательные приложения, которые используются в ходе сертификационного аудита. В качестве примера вспомогательных приложений, составляющих внешнюю среду разрабатываемой системы, взяты система контроля защищенности и соответствия стандартам MaxPatrol [3], разработанная компанией Positive Technologies, и свободная утилита Nmap, предназначенная для настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети.

Одной из ключевых особенностей указанных приложений является возможность экспорта полученных данных в формат XML (Extensible Markup Language) – расширяемого языка разметки, предназначенного для хранения структурированных данных и обмена информацией между программами. Таким образом, структурированные данные легко поддаются дальнейшей обработке, что упрощает обмен информацией между компонентами системы. Архитектура проектируемой системы схематично изображена на рис. 1.

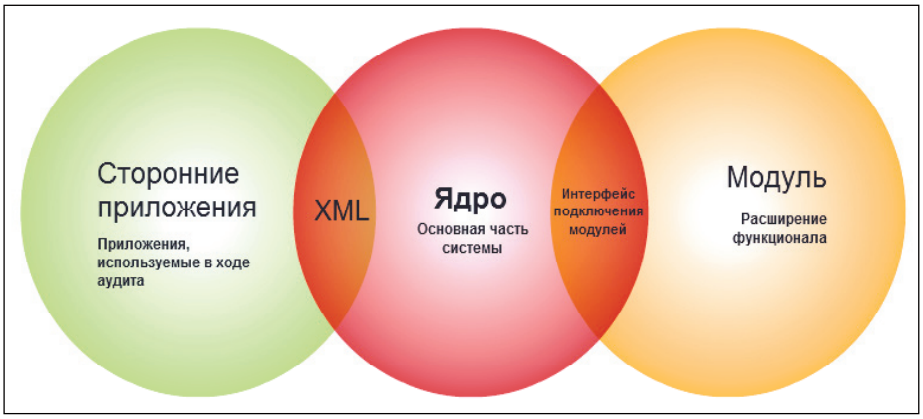

Рис. 1. Общая схема системы сбора и обработки информации

Ядро системы осуществляет преобразование данных, полученных от опросных листов и внешней среды, к которой принадлежат все вспомогательные приложения. На рис. 2 изображена структура ядра системы.

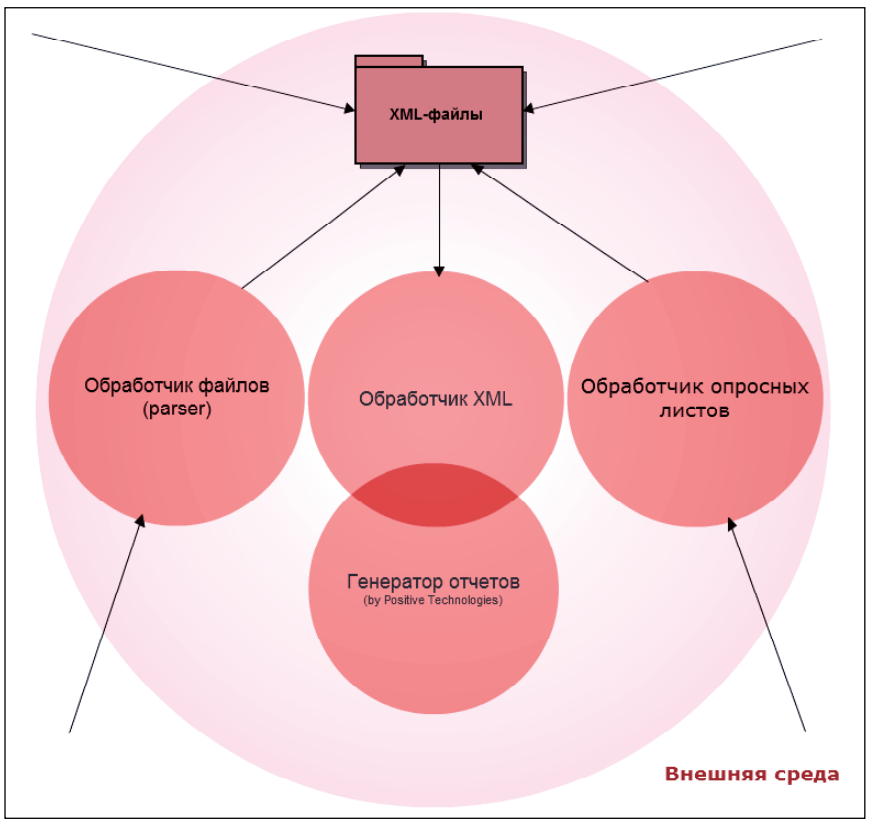

Рис. 2. Структура ядра системы сбора и обработки информации

Ядро аккумулирует все XML-файлы, являющиеся результатами работы вспомогательных приложений, обработчика файлов и обработчика опросных листов. Далее обработчик XML выбирает нужные данные из этих файлов, соотносит результаты с соответствующими контролями PCI DSS и экспортирует полученную информацию в результирующий XML-файл, формат которого позволяет впоследствии на его основе сгенерировать отчет о результатах оценки соответствия требованиям стандарта как с помощью генератора отчетов, разработанного сотрудниками компании Positive Technologies, так и с помощью внутреннего генератора отчетов.

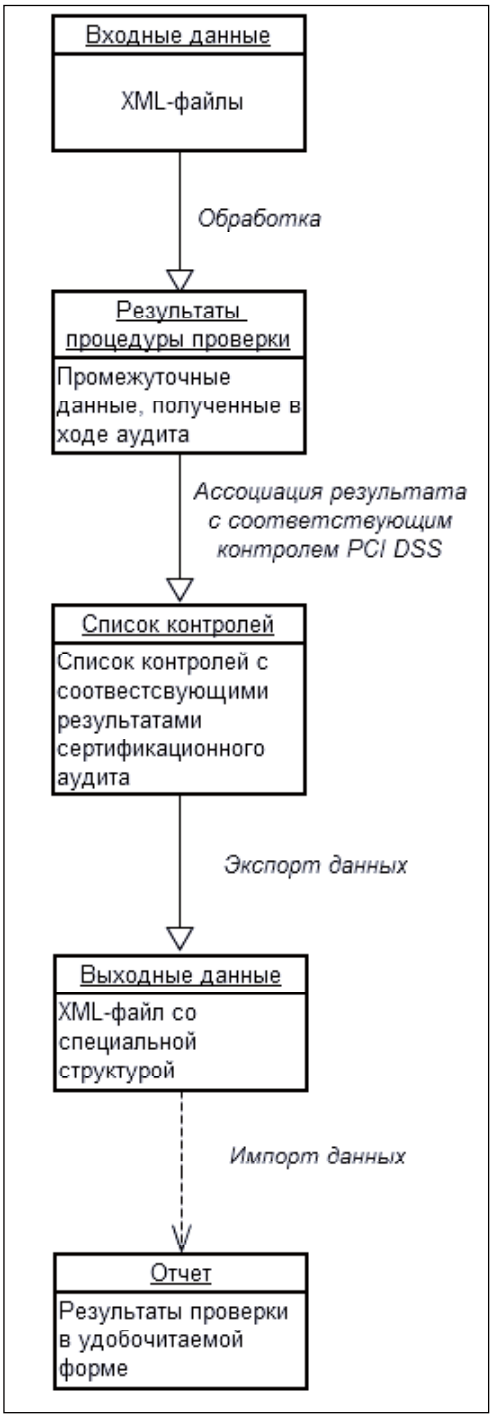

Рис. 3. Алгоритм работы приложения

Обработчик опросных листов представляет собой веб-приложение, которое может быть реализовано с использованием распространенных технологий. В данном случае опросный лист — это веб-ресурс, который содержит список вопросов с вариантами ответа. На основе введенных интервьюируемым лицом вариантов ответа после завершения опроса генерируется XML-файл, который содержит результат оценки соответствия тому или иному требованию стандарта.

Заключение

Анализ и систематизация требований стандарта PCI DSS по типу сбора информации в ходе оценки соответствия позволили определить пункты процедур проверки, которые могут быть автоматизированы. На основе результатов интервьюирования персонала и данных, полученных с помощью сторонних приложений в ходе аудита, разработан алгоритм работы приложения, реализующего функционал ядра системы сбора и обработки информации (рис. 3). Данный алгоритм может быть использован для создания программного обеспечения системы сбора и обработки информации, полученной в ходе проведения оценки соответствия требованиям стандарта PCI DSS.

СПИСОК ЛИТЕРАТУРЫ:

1. Стандарт безопасности данных индустрии платежных карт. Требования и процедуры аудита безопасности (версия 2.0) PCI SSC.
2. PCI DSS Glossary (версия 2.0) PCI SSC.
3. Официальный веб-ресурс компании Positive Technologies. URL: www.ptsecurity.ru.