Конфигурация сканирования:

– OpenVAS (версия 9) запускался в режиме сканирования «Full and fast»;

– Nessus (версия 7.0.0) запускался в режиме «Advanced Scan»;

– Rapid7 Nexpose (версия 6.5) запускался в режиме «Full audit»;

– сканирование производилось с использованием атрибутов доступа.

Результаты сканирования:

– OpenVAS: обнаружил 352 уязвимости, из них: High (высокий уровень) – 126, Medium (средний уровень) – 127, Low (низкий уровень) – 21, Log (информативный уровень) – 78;

– Nessus: обнаружил 397 уязвимостей, из них: Critical (критичный уровень) – 26, High (высокий уровень) – 92, Medium (средний уровень) – 129, Low (низкий уровень) – 13, Log (информативный уровень) – 137;

– Rapid7 Nexpose: обнаружил 307 уязвимостей, из них: Critical (критичный уровень) - 80, Severe (серьезный уровень) – 197, Moderate (средний уровень) – 30.

На основании проведенного тестирования, лучшее качество сканирования по количеству опасных (Critical/High/Medium/Severe) уязвимостей показал сканер Rapid7 Nexpose (277). Наибольшее количество информативных (Low/Log/Moderate) уязвимостей обнаружил сканер Nessus (150).

Литература

1. Metasploitable // sourceforge.net [Электронный ресурс]. – URL: https://sourceforge.net/ projects/ metasploitable/?source=typ_redirect (дата обращения: 02.05.2018).

МЕТОДЫ ОРГАНИЗАЦИИ КОНТРОЛЯ ДОСТУПА ПРИ ОЦЕНКЕ СЕБЕСТОИМОСТИ ИТ-ПРОЕКТОВ

А.Д. Зайков

Рассмотрим процесс разработки ИТ-проекта. В упрощенном виде проекты выглядят так: заказчик высылает задание, программисты оценивают, сколько уйдет на выполнение задания времени и средств, далее согласуют это с заказчиком и получают необходимое финансирование, затем приступают к выполнению проекта. Данный процесс чаще всего можно встретить в небольших командах разработки или небольших проектах, где каждый новый релиз выходит регулярно [1].

В больших проектах, в которых участвует сразу несколько команд разработки, обнаружить внутренние проблемы не так просто. Эффективность и качество разработки зависят от ряда факторов: продуктивность разработчиков, стабильность релизов, гибкость проекта, уровень и способы взаимодействия между заказчиком и разработчиками. Использование инструментов управления и грамотной методики расчета себестоимости ИТ-проекта позволяет руководству компании и клиенту держать руку на пульсе проекта и иметь всегда достоверную информацию о том, как справляется команда с задачами на проекте, а также оценить степень готовности продукта.

Разработка и применение новой методики расчета себестоимости ИТ-проекта позволит оптимизировать техническую базу, подготовить оценку сроков и затрат, произвести качественную и количественную оценку рисков, создать план проекта, своевременно отслеживать эффективность производимых работ. Но полученные данные должны быть видны только руководящим лицам компании, т.к. являются конфиденциальными и не должны быть обнародованы рядовым сотрудникам компании. Система Atlassian JIRA позволяет организовать контроль доступа, подсчитать данные о себестоимости и трудозатратах на ИТ-проектах, а также ограничить видимость этих данных при помощи кастомизации прав доступа пользователей, создании дополнительных экранов для определенных групп пользователей, а также с помощью заскриптованных полей.

Литература

1. Репин В.В., Елиферов В.Г. Процессный подход к управлению. Моделирование бизнес-процессов. М.: Манн, Иванов и Фербер, 2013. 544 с.