**Лекция 6**

Методы Аудита ИБ

На сегодняшний день существует три основных метода аудита информационной безопасности, они представлены на рисунке 1.



Рисунок 1 – Методы АИБ

Активный аудит ИБ – это исследование состояния защищенности ИС с точки зрения злоумышленника, обладающего высокой квалификацией в области информационных технологий. При его осуществлении моделируется как можно большее количество атак на систему сетевой защиты. При этом аудитору предоставляется только та информация, которую можно найти в открытых источниках. Результатом активного аудита является информация обо всех уязвимостях, степени их критичности и методах устранения.

В рамках активного аудита проводится пентест.

**pentest** (penetration test – «тест на проникновение») — метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника.

В ходе пентеста аудитор имитирует действия злоумышленника: пытается взломать сайт, сделать некорректный заказ, использовать уязвимости CMS, имитирует DDoS-атаку. Во время этого теста проверяются открытые порты, сетевые сервисы с неправильной настройкой, через которые можно получить данные из внутренней сети компании. Также разрабатываются методы противодействия DDoS-атакам

Экспертный аудит – это сравнение состояния информационной безопасности с описанием состояния информационной безопасности, которое базируется:

на требованиях, предъявленных руководством компании;

на аккумулированном в компании-аудиторе мировом и частном опыте.

Для экспертного аудита берется некий эталонный комплекс мер, которые должны быть применены на предприятии с точки зрения начальства, отдела безопасности, других экспертов. Аудитор сравнивает имеющуюся степень защиты с идеальной и выносит вердикт.

Аудит на соответствие стандартам (сертификация) нацелен на получения сертификата PCI DSS (Payment Card Industry Data Security Standard, Стандарт безопасности данных индустрии платежных карт) или ГОСТ Р ИСО/МЭК 27001 (Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования).

Сертификация PCI DSS — это обязательное требование Международных Платежных Систем (Visa, MasterCard, МИР, American Express, Discover, JCB) для компаний, которые обрабатывают, передают или хранят данные платежных карт. Все эти организации обязаны выполнять требования стандарта, PCI DSS, подтверждением этого факта является ежегодный сертификационный аудит – представитель службы проверки оценивает, насколько решения в компании соответствуют стандартам PCI DSS. В итоге фирма получает рекомендации, что именно нужно сделать, чтобы пройти сертификацию без проблем.

Комплексный аудит. Он позволяет оценить уровень защиты системы в компании с использованием всех перечисленных методов или их комбинаций. Считается наиболее эффективным, так как позволяет дать наиболее полную оценку ситуации.

При проведении комплексного аудита информационной безопасности группой экспертов оцениваются следующие процессы обеспечения информационной безопасности, в том числе указываются потенциальные уязвимости, как процессов, так и технической реализации путем применения инструментальных средств аудита:

процесс назначения и распределения ролей в области информационной безопасности;

процесс антивирусной защиты;

процесс использования ресурсов сети Интернет;

процесс криптографической защиты информационных активов;

процессы системы управления информационной безопасностью;

процессы аудита и мониторинга информационной безопасности;

процесс управления информационными активами;

процесс управления рисками информационной безопасности;

процесс обеспечения физической безопасности;

процесс управления и контроля доступа;

процесс обеспечения информационной безопасности на стадиях жизненного цикла информационных систем;

процессы обеспечения непрерывности деятельности;

процессы управления документацией и записями;

процессы управления инцидентами информационной безопасности и др.

При проведении комплексного аудита информационной безопасности дополнительно могут быть проведены следующие работы:

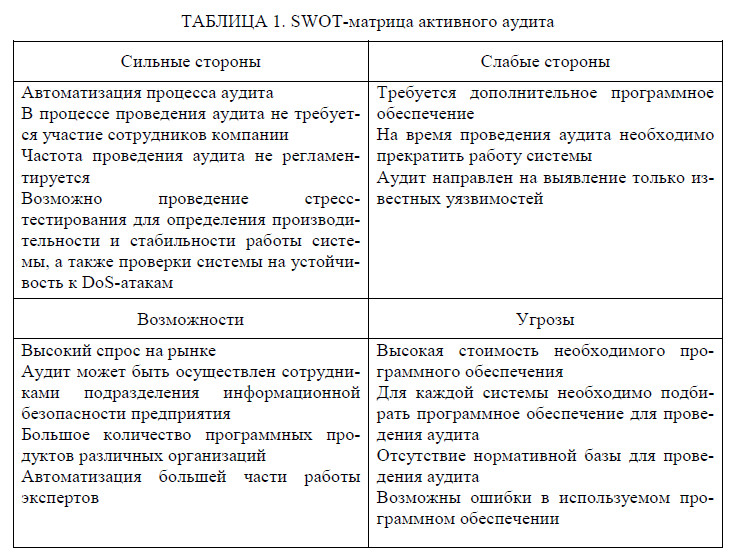
инструментальное сканирование;

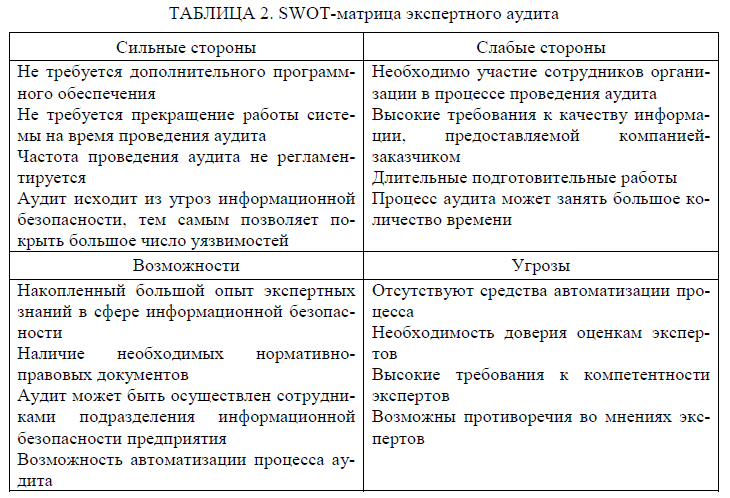
тест на проникновение;

анализ рисков информационной безопасности.

Результаты комплексного аудита информационной безопасности оформляются в виде отчета, содержащего, как рекомендации для специалистов по информационной безопасности и информационным технологиям Компании, так и высокоуровневое описание возможных направлений развития системы обеспечения информационной безопасности, с учетом актуальных проблем, связанных с обеспечением информационной безопасности, и отраслевой специфики Компании для руководства

Примеры таблиц SWOT-анализа для АИБ



****

****