ЭКСПЕРТНЫЙ АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аудит информационной безопасности (ИБ) – независимая оценка текущего состояния системы информационной безопасности, устанавливающая уровень ее соответствия определенным критериям. Целью аудита может быть как комплексный аудит системы защиты информации компании-заказчика, так и аудит информационной безопасности отдельных узлов сети (серверов, сетей передачи данных, систем хранения данных и др.), критичных для работы компании-заказчика. Аудит безопасности отдельных узлов позволяет за счет снижения времени и стоимости аудита обеспечить безопасность критичных для бизнеса объектов за минимальное время.

Основными целями аудита информационной безопасности является:

- независимая оценка текущего состояния системы безопасности;
- идентификация, оценка опасности и ликвидация уязвимостей;
- технико-экономическое обоснование внедряемых механизмов безопасности;
- обеспечение соответствия требованиям действующего законодательства и международным стандартам;
- минимизация ущерба от инцидентов безопасности.

В последнее время, руководители многих компаний рассматривают получение сертификата, подтверждающего высокий уровень информационной безопасности, как «козырь» в борьбе за крупного клиента или делового партнера. В этом случае целесообразно проведение аудита существующей информационной системы компании и последующей сертификации на соответствие стандартов **ISO/IEC 27001:2005 и ISO 9001:2000**.

Аудит безопасности информационных систем позволяет:

1. получить полную и объективную оценку степени защищенности информационной системы;
2. выявить и описать имеющиеся проблемы;
3. выработать и обосновать требования к системе безопасности в рамках заданных критериев;
4. оценить уровень затрат на создание или модернизацию системы ИБ;
5. разработать эффективную программу создания или модернизации системы обеспечения информационной безопасности предприятия-заказчика до заданного уровня;
6. обеспечить предсказуемость результатов действий по обеспечению информационной безопасности и внедрить прозрачную плановую систему затрат.

Этапы аудита информационной безопасности

Работы выполняются в несколько этапов, программа аудита ИБ определяется по согласованию с заказчиком.

1. Постановка задачи и определение объекта аудита:

- определение задач, целей и объектов аудита информационной безопасности;
- формирование рабочей группы (включая специалистов заказчика);
- составление регламента проведения работ;
- разработка технического задания (ТЗ) на проведение работ.

2. Сбор, подготовка и анализ данных для проведения работ:

- изучение объекта исследования;
- анализ организационно-административных мер обеспечения ИБ;
- анализ программно-технических средств обеспечения ИБ;
- фиксация текущего состояния и характеристик объекта исследования;
- определение соответствия характеристик объекта исследования требованиям политики ИБ;
- выявление технических уязвимостей объекта исследования.

3. Подготовка аналитического отчета по выполненной работе, включая:

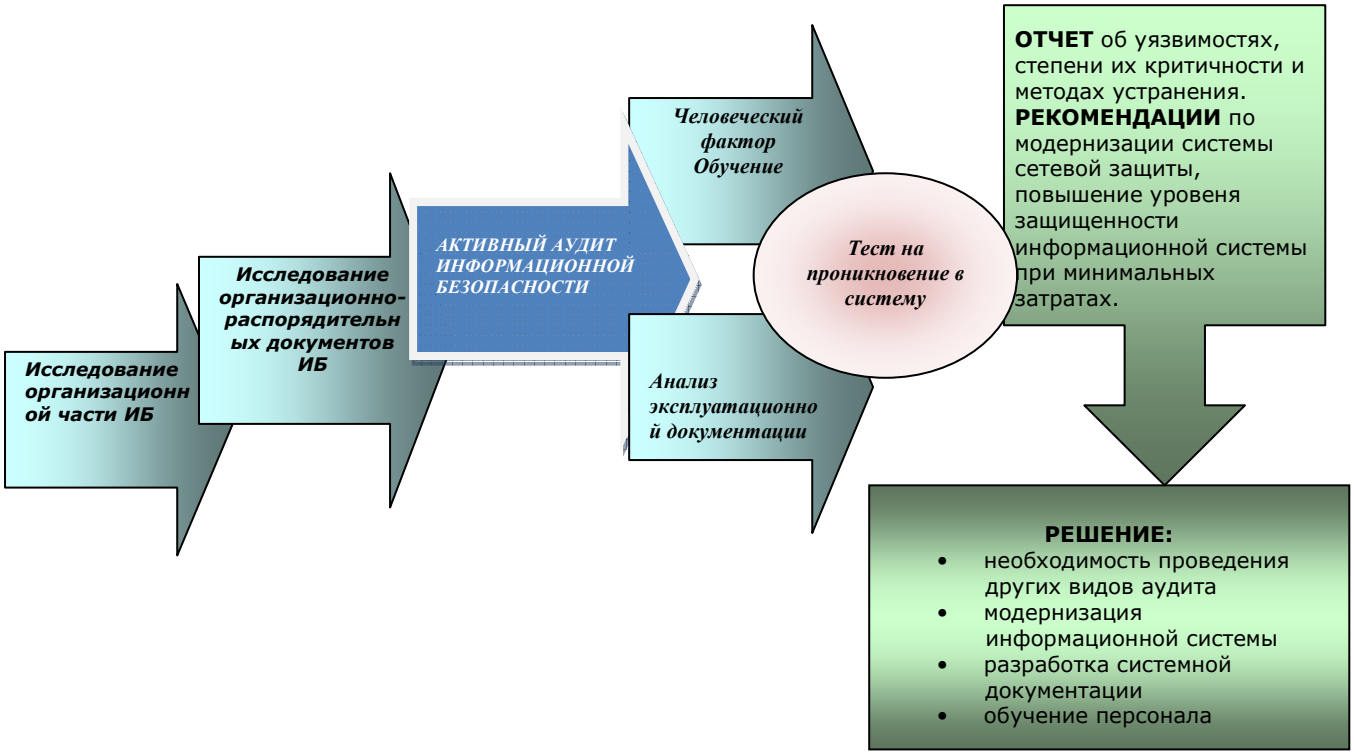
- моделирование процессов нарушения системы безопасности;
- определение угроз нарушения ИБ;
- анализ уязвимостей и и оценка рисков;
- определение устойчивости объекта в соответствии с требованиями по обеспечению ИБ;
- разработка организационных мер обеспечения ИБ;
- разработка предложения по развитию программно-технических средств обеспечения ИБ;
- разработка рекомендаций по совершенствованию структуры информационной системы заказчика;
- разработка рекомендаций по повышению квалификации штатного персонала.

4. Завершение работы:

- ознакомление уполномоченных представителей заказчика с результатами работы;
- консультирование персонала заказчика (проведение семинара);
- передача полученных материалов и документации заказчику и сдача отчета;
- оформление акта выполненных работ.

Детализация этапов аудита проводится рабочей группой экспертов SI BIS и представителей заказчика на этапе подготовки технического задания. Подробный перечень объектов аудита, их характеристики, сроки работ, согласование промежуточных результатов, предотвращение выявленных критических ситуаций и прочие условия выполнения работ предусматриваются в ТЗ, утверждаемом сторонами до начала последующих этапов.

Методика проведения экспертного аудита ИБ



Составляющей частью экспертного аудита ИБ, является **активный аудит**, который также может рассматриваться как отдельное решение.

Цель активного аудита - с помощью специального программного обеспечения и специальных методов исследования, осуществить сбор информации о состоянии системы сетевой защиты. Под состоянием системы сетевой защиты понимают, лишь те параметры и настройки, использование которых помогает злоумышленнику проникнуть в сети и нанести вред предприятию. При осуществлении данного вида аудита, моделируется как можно большее количество сетевых атак, которые может реализовать злоумышленник.

Методика проведения активного аудита ИБ