МЕТОДИКА АУДИТА БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Морозов Р.Н., Губенко Н.Е.
Донецкий национальный технический университет

Комплексный аудит информационной безопасности

Аудит информационной безопасности (ИБ) – независимая оценка текущего состояния системы информационной безопасности, устанавливающая уровень ее соответствия определенным критериям, и предоставление результатов в виде рекомендаций [1].

Комплексный аудит безопасности информационных систем позволяет получить наиболее полную и объективную оценку защищенности информационной системы, локализовать имеющиеся проблемы и разработать эффективную программу построения системы обеспечения информационной безопасности организации.

Этапы комплексного аудита

Аудит безопасности проводят, решая следующие задачи:

- Повышение уровня защиты информации до приемлемого;
- Оптимизация и планирование затрат на обеспечение информационной безопасности;
- Обоснование инвестиций в системы защиты;
- Получение максимальной отдачи от инвестиций, вкладываемых в системы защиты информации;
- Подтверждение того, что используемые внутренние средства контроля соответствуют задачам организации и позволяют обеспечить эффективность и непрерывность бизнеса.

Проведение аудита безопасности корпоративной информационной системы заказчика осуществляется в четыре этапа:

1. Постановка задачи и уточнение границ работ
2. Сбор и анализ информации
3. Проведение анализа рисков
4. Разработка рекомендаций

Постановка задачи и уточнение границ работ

На данном этапе проводятся сбор исходных данных от заказчика, их предварительный анализ, а также организационные мероприятия по подготовке проведения аудита:

- Уточняются цели и задачи аудита
- Формируется рабочая группа
- Подготавливается и согласовывается техническое задание на проведение аудита

Целью аудита может быть как комплексный аудит системы защиты информации компании-заказчика, так и аудит информационной безопасности отдельных ИТ-систем (сетей передачи данных, вычислительных систем и систем хранения данных, и др.). На этом этапе цели проведения аудита уточняются и планируются все последующие шаги.

В состав рабочей группы должны входить специалисты компании исполнителя (компании проводящей аудит) и сотрудники компании заказчика. Сотрудники заказчика обеспечивают представление всей необходимой информации, контролируют процессы проведения обследования, а также участвуют в согласовании его результатов (промежуточных и конечных) [1]. Специалисты исполнителя отвечают за квалифицированное проведение работ по обследованию предметных областей в соответствии с определенными целями и задачами проекта, согласуют процессы и результаты проведения обследования.

Этап постановки задачи завершается разработкой, согласованием и утверждением технического задания (ТЗ). В ТЗ на аудит фиксируется состав и содержание работ по аудиту и требования к разрабатываемым документам. Кроме того, в ТЗ вносят сроки проведения работ, а при необходимости — план-график.

Параллельно с ТЗ разрабатывается соглашение о конфиденциальности и организуется взаимодействие со службой безопасности заказчика.

Сбор и анализ информации

На этом этапе собирается информация и дается оценка следующих мер и средств:

- организационных мер в области информационной безопасности;
- программно-технических средств защиты информации;
- обеспечения физической безопасности.

Анализируются следующие характеристики построения и функционирования корпоративной информационной системы:

- Организационные характеристики
- Организационно-технические характеристики
- Технические характеристики, связанные с архитектурой ИС
- Технические характеристики, связанные с конфигурацией сетевых устройств и серверов ИС
- Технические характеристики, связанные с использованием встроенных механизмов информационной безопасности

После получения исходных данных готовится отчет об обследовании. Отчет об обследовании является основой для последующих этапов аудита: анализа рисков и разработки рекомендаций.

Проведение анализа рисков

Проведение данного этапа является важной стадией при аудите информационной безопасности. Анализ рисков проводится для оценки реальных угроз нарушения информационной безопасности и разработки рекомендаций, выполнение которых позволит минимизировать эти угрозы.

Исходной информацией для анализа рисков является согласованный с заказчиком отчет о проведенном обследовании.

Анализ рисков дает возможность:

- адекватно оценить существующие угрозы;
- идентифицировать критичные ресурсы ИС;

- выработать адекватные требования по защите информации;
- сформировать перечень наиболее опасных уязвимых мест, угроз и потенциальных злоумышленников;
- получить определенный уровень гарантий, основанный на объективном экспертном заключении.

При анализе рисков осуществляется:

- классификация информационных ресурсов;
- анализ уязвимостей;
- составление модели потенциального злоумышленника;
- оценка рисков нарушения информационной безопасности.

В процессе анализа рисков проводится оценка критичности идентифицированных уязвимых мест и возможности их использования потенциальным злоумышленником для осуществления несанкционированных действий.

Разработка рекомендаций

На основании информации, полученной в ходе обследования информационной инфраструктуры заказчика и результатов анализа рисков, разрабатываются рекомендации по совершенствованию системы защиты информации, применение которых позволит минимизировать риски, с приложением списка конкретных уязвимостей активного сетевого оборудования, серверов, межсетевых экранов и др.

По завершении аудита подготавливается итоговый отчет, содержащий оценку текущего уровня безопасности ИТ-инфраструктуры, информацию об обнаруженных проблемах, анализ соответствующих рисков и рекомендации по их устранению [1].

Результат

Результатом аудита безопасности внешнего периметра корпоративной сети является аудиторский отчет. Общая структура отчета:

- Оценка текущего уровня защищенности информационной системы:
  - Описание и оценка текущего уровня защищенности информационной системы;
  - Анализ конфигурации конфигурационной информации, найденные уязвимости;
  - Анализ рисков, связанных с возможностью осуществления внутренних и внешних угроз в отношении ресурсов информационной системы;
- Рекомендации по технической составляющей ИБ:
  - по изменению конфигурации существующих сетевых устройств и серверов;
  - по изменению конфигурации существующих средств защиты;
  - по активации дополнительных штатных механизмов безопасности на уровне системного программного обеспечения;
  - по использованию дополнительных средств защиты;
- Рекомендации по организационной составляющей ИБ:
  - по разработке политики информационной безопасности;
  - по организации службы ИБ;
  - по разработке организационно-распорядительных и нормативно-технических документов;
  - по пересмотру ролевых функций персонала и зон ответственности;
  - по разработке программы осведомленности сотрудников в части информационной безопасности;
  - по поддержке и повышению квалификации персонала.

Литература

1. А. П. Курило. Аудит информационной безопасности. - БДЦ-пресс. 2006. - 304 с.