Лекция 4

**Виды и цели аудита ИБ**

Различают внешний и внутренний аудит.

Внешний аудит — это, как правило, разовое мероприятие, проводимое по инициативе руководства организации или акционеров. Внешний аудит рекомендуется (а для ряда финансовых учреждений и акционерных обществ требуется) проводить регулярно.

Внутренний аудит – непрерывную деятельность, которая осуществляется на основании документа, обычно носящего название «Положение о внутреннем аудите», и в соответствии с планом, подготовка которого осуществляется подразделением внутреннего аудита и утверждается руководством организации. Аудит безопасности информационных систем является одной из составляющих ИТ—аудита.

**Целями проведения аудита безопасности являются:**

— получение объективных доказательств, анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС; — оценка текущего уровня защищенности ИС;

— локализация узких мест в системе защиты ИС;

— оценка соответствия ИС существующим стандартам в области информационной безопасности;

— выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

Представленные Аудитору рапорты о инцидентах СИБ должны содержать документацию о т. н. «слабых точках» СИБ.

В число дополнительных задач, стоящих перед внутренним аудитором, помимо оказания помощи внешним аудиторам, могут также входить:

— разработка политик безопасности и других организационно—распорядительных документов по защите информации и участие в их внедрении в работу организации;

— постановка задач для [ИТ](https://ru.wikipedia.org/wiki/%D0%98%D0%A2)—персонала, касающихся обеспечения защиты информации;

— участие в обучении пользователей и обслуживающего персонала ИС вопросам обеспечения информационной безопасности;

— участие в разборе инцидентов, связанных с нарушением информационной безопасности;

— прочие задачи.

**Основные направления АИБ:**

1. **Аттестация** объектов информатизации по требованиям безопасности информации:
   * аттестация автоматизированных систем, средств связи, обработки и передачи [информации](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F);
   * аттестация помещений, предназначенных для ведения конфиденциальных переговоров;
   * аттестация технических средств, установленных в выделенных помещениях.
2. **Контроль** защищенности информации ограниченного доступа:
   * выявление технических [каналов утечки информации](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D1%8B_%D1%83%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) и способов [несанкционированного доступа](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D1%81%D0%B0%D0%BD%D0%BA%D1%86%D0%B8%D0%BE%D0%BD%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF) к ней;
   * контроль эффективности применяемых средств защиты информации.
3. **Специальные исследования** технических средств на наличие побочных [электромагнитных излучений](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BC%D0%B0%D0%B3%D0%BD%D0%B8%D1%82%D0%BD%D1%8B%D0%B5_%D0%B8%D0%B7%D0%BB%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D1%8F) и наводок (ПЭМИН):
   * персональные ЭВМ, средства связи и обработки информации;
   * локальные вычислительные системы;
   * оформления результатов исследований в соответствии с требованиями ФСБ и ФСТЭК (Федеральная служба по техническому и экспортному контролю).
4. **Проектирование объектов в защищенном исполнении**:
   * разработка концепции информационной безопасности;
   * проектирование автоматизированных систем, средств связи, обработки и передачи информации в защищенном исполнении;
   * проектирование помещений, предназначенных для ведения конфиденциальных переговоров.