Лекция 5

**Основные этапы проведения комплексного АИБ**

* инициирование процедуры аудита;
* сбор информации аудита;
* [анализ данных](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) аудита;
* выработку рекомендаций;
* подготовку аудиторского отчета.

На этапе ***инициирования процедуры аудита*** должны быть решены следующие организационные вопросы:

1. права и обязанности аудитора должны быть четко определены и документально закреплены в его должностных инструкциях, а также в положении о внутреннем (внешнем) аудите;
2. аудитором должен быть подготовлен и согласован с руководством план проведения аудита;
3. в положении о внутреннем аудите должно быть закреплено, в частности, что сотрудники компании обязаны оказывать содействие аудитору и предоставлять всю необходимую для проведения аудита информацию.

На этапе инициирования процедуры аудита должны быть определены границы проведения обследования. План и границы проведения аудита обсуждаются на рабочем собрании, в котором участвуют аудиторы, руководство компании и руководители структурных подразделений.

Этап ***сбора информации аудита*** является наиболее сложным и длительным, что связано в основном с отсутствием необходимой документации на информационную систему и с необходимостью плотного взаимодействия аудитора со многими должностными лицами организации.

Компетентные выводы относительно положения дел в компании с информационной безопасностью могут быть сделаны аудитором только при условии наличия всех необходимых исходных данных для анализа. Первый пункт аудиторского обследования начинается с получения информации об организационной структуре пользователей ИС и обслуживающих подразделений. Назначение и принципы функционирования ИС во многом определяют существующие риски и требования безопасности, предъявляемые к системе. Далее, аудитору требуется более детальная информация о структуре ИС. Это позволит уяснить, каким образом осуществляется распределение механизмов безопасности по структурным элементам и уровням функционирования ИС.

На **этапе**[**анализа данных**](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) определяются с методами анализа. Здесь возможно несколько подходов.

*Первый подход*, самый сложный, базируется на анализе рисков. Опираясь на методы анализа рисков, аудитор определяет для обследуемой ИС индивидуальный набор требований безопасности, в наибольшей степени учитывающий особенности данной ИС, среды её функционирования и существующие в данной среде угрозы безопасности.

*Второй подход*, самый практичный, опирается на использование стандартов информационной безопасности. Стандарты определяют базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики. Стандарты могут определять разные наборы требований безопасности, в зависимости от уровня защищенности ИС, который требуется обеспечить, её принадлежности (коммерческая организация либо государственное учреждение), а также назначения (финансы, промышленность, связь и т. п.). От аудитора в данном случае требуется правильно определить набор требований стандарта, соответствие которым нужно обеспечить.

*Третий подход*, наиболее эффективный, предполагает комбинирование первых двух. Базовый набор требований безопасности, предъявляемых к ИС, определяется стандартом. Дополнительные требования, в максимальной степени учитывающие особенности функционирования данной ИС, формируются на основе анализа рисков.

На этапе выработки рекомендаций, выдаваемых аудитором по результатам анализа состояния ИС, определяются используемым подходом, особенностями обследуемой ИС, состоянием дел с информационной безопасностью и степенью детализации, используемой при проведении аудита. В любом случае, рекомендации аудитора должны быть конкретными и применимыми к данной ИС, экономически обоснованными, аргументированными (подкрепленными результатами анализа) и отсортированными по степени важности. При этом мероприятия по обеспечению защиты организационного уровня практически всегда имеют приоритет над конкретными программно—техническими методами защиты. В то же время наивно ожидать от аудитора, в качестве результата проведения аудита, выдачи технического проекта подсистемы информационной безопасности, либо детальных рекомендаций по внедрению конкретных программно—технических средств защиты информации. Это требует более детальной проработки конкретных вопросов организации защиты, хотя внутренние аудиторы могут принимать в этих работах самое активное участие.

***Аудиторский отчет*** является основным результатом проведения аудита. Его качество характеризует качество работы аудитора. Он должен, по крайней мере, содержать описание целей проведения аудита, характеристику обследуемой ИС, указание границ проведения аудита и используемых методов, результаты анализа данных аудита, выводы, обобщающие эти результаты и содержащие оценку уровня защищенности АС или соответствие её требованиям стандартов, и, конечно, рекомендации аудитора по устранению существующих недостатков и совершенствованию системы защиты.