Лекция:
«Аудит безопасности предприятия (фирмы)»

Аудит безопасности *коммерческого предприятия (организации) желательно рассматривать как исключительно внутренний инструмент управления, исключающий в целях конспирации возможность предоставления информации о результатах его деятельности сторонним лицам и организациям.*

Последовательность действий проведения аудита безопасности фирмы:

1. Подготовка к проведению аудита безопасности:

- *выбор объекта аудита (фирма, отдельные здания и помещения, отдельные системы или их компоненты);*
- *составление команды аудиторов-экспертов;*
- *определение объема и масштаба аудита и установление конкретных сроков работы.*

2. Проведение аудита:

- *общий анализ состояния безопасности объекта аудита;*
- *регистрация, сбор и проверка статистических данных и результатов инструментальных измерений опасностей и угроз;*
- *оценка результатов проверки;*
- *составление отчета о результатах проверки по отдельным составляющим.*

3. Завершение аудита:

- *составление итогового отчета;*
- *разработка плана мероприятий по устранению узких мест и недостатков в обеспечении безопасности фирмы.*

Условиями успешного проведения аудита безопасности являются:

- активное участие руководства фирмы в его проведении;
- объективность и независимость аудиторов (экспертов), их компетентность и высокая профессиональность;
- четко структурированная процедура проверки;
- активная реализация предложенных мер обеспечения и усиления безопасности.

Аудит безопасности является действенным инструментом оценки безопасности и управления рисками. Предотвращение угроз безопасности означает, в том числе и защиту экономических, социальных и информационных интересов фирмы. Отсюда вывод, что аудит безопасности становится инструментом экономического менеджмента.

В зависимости от того, кто проводит аудит безопасности - сотрудники фирмы или независимая аудиторская компания, - его также можно разделить на ***внутренний и внешний****.*

Масштабы аудита:

аудит безопасности всей фирмы в комплексе;

аудит безопасности отдельных зданий и помещений (выделенные помещения);

аудит оборудования и технических средств конкретных типов и видов;

аудит отдельных видов и направлений деятельности: экономической, экологической, информационной, финансовой и т. д.

Внутренний аудит *позволяет оценить:*

соблюдение законодательных требований по безопасности;

выполнение требований стандартов и норм по безопасности;

наличие узких мест в системе безопасности фирмы и спланировать работу по их устранению;

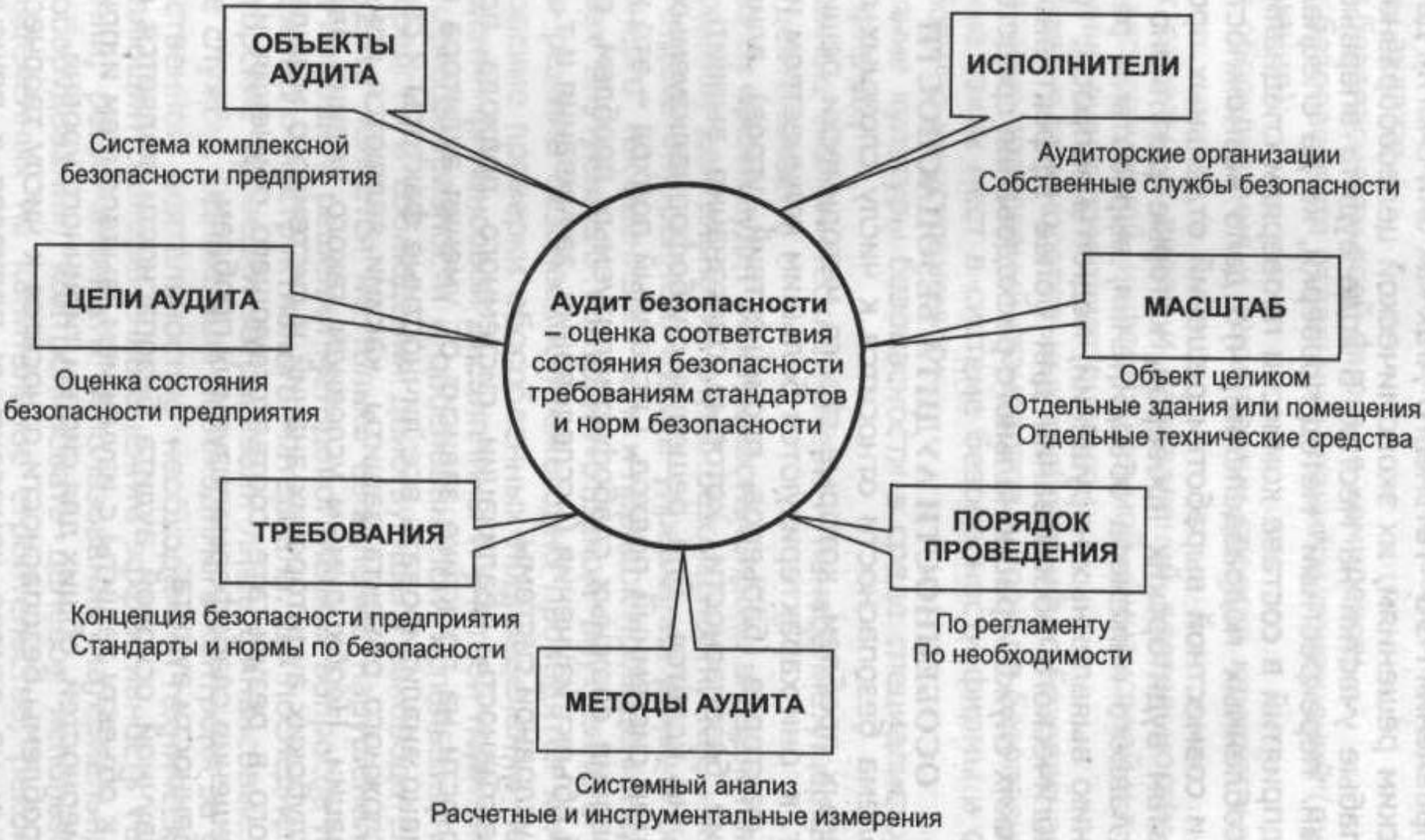
состояние культуры безопасности в среде специалистов и сотрудников фирмы;

возможные экономические потери и нанесение ущерба в любой сфере деятельности.

Особенности аудита:

1. *Научной основой аудита безопасности является системный подход к объекту защиты с изучением, выявлением и применением закономерностей, общих для систем типичного уровня.*
2. *Проблемы безопасности относятся к числу творческих задач, решаемых на основе комплексных подходов к решению слабоструктурированных задач в социально-экономических системах.*
3. *Результативность и качество аудита безопасности зависят от человека, решающего эти задачи, от его мыслительной деятельности. Процесс решения слабоструктурированной задачи - это сложный субъективный процесс.*
4. *Результатом аудита безопасности является оценка соответствия безопасности требованиям, установленным на объекте защиты.*
5. *Основой решения слабоформализованных задач является соответствие формализованной модели требований безопасности реальному формализованному состоянию.*
6. *Объектом исследования аудита безопасности является фирма (организация, предприятие).*

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ АУДИТА БЕЗОПАСНОСТИ



Варианты аудита информационной безопасности:

1. Комплексный анализ ИС предприятия и подсистемы информационной безопасности на методологическом, организационно-управленческом, технологическом и техническом уровнях. Анализ рисков.

1.1. Исследование и оценка состояния информационной безопасности ИС и подсистемы информационной безопасности предприятия.

Комплексная оценка соответствия типовым требованиям РД ФСТЭК РФ к системе информационной безопасности предприятия.

Комплексная оценка соответствия типовым требованиям международных стандартов ISO к системе информационной безопасности предприятия.

Комплексная оценка соответствия специальных требований заказчика к системе информационной безопасности предприятия.

1.2. Работы на основе анализа рисков.

Уровень управления рисками на основе качественных оценок рисков.

Уровень управления рисками на основе количественных оценок рисков.

1.3. Инструментальные исследования.

Инструментальное исследование элементов инфраструктуры компьютерной сети и корпоративной информационной системы на наличие уязвимостей.

Инструментальное исследование защищенности точек доступа предприятия в Internet.

1.4. Анализ документооборота предприятия.

2. Разработка комплексных рекомендаций по методологическому, организационно-управленческому, технологическому, общетехническому и программно-аппаратному обеспечению режима информационной безопасности предприятия.

1. Разработка концепции обеспечения информационной безопасности предприятия.
2. Разработка корпоративной политики обеспечения информационной безопасности предприятия на организационно-управленческом, правовом, технологическом и техническом уровнях.
3. Разработка плана защиты предприятия заказчика.
4. Дополнительные работы по анализу и созданию методологического, организационно-управленческого, технологического, инфраструктурного и технического обеспечения режима информационной безопасности предприятия заказчика.

3. Организационно-технологический анализ ИС предприятия.

3.1. Организационно-технологический анализ ИС предприятия.

Оценка соответствия типовым требованиям руководящих документов РФ к системе информационной безопасности предприятия в области организационно-технологических норм.

Анализ документооборота предприятия категории «конфиденциально» на соответствие требованиям концепции информационной безопасности, положению о коммерческой тайны, прочим внутренним требованиям предприятия по обеспечению конфиденциальности информации.

Дополнительные работы по исследованию и оценке информационной безопасности объекта.

3.2. Разработка рекомендации по организационно-управленческому, технологическому, общетехническому обеспечению режима информационной безопасности предприятия.

- *Разработка элементов концепции обеспечения информационной безопасности предприятия.*
- *Разработка элементов корпоративной политики обеспечения информационной безопасности предприятия на организационно-правленческом, правовом и технологическом уровнях.*

4. Экспертиза решений и проектов.

4.1. Экспертиза решений и проектов автоматизации на соответствие требованиям по обеспечению информационной безопасности экспертно-документальным методом.

4.2. Экспертиза проектов подсистем информационной безопасности на соответствие требованиям по безопасности экспертно-документальным методом.

5. Работы по анализу документооборота и поставке типовых комплектов организационно-распорядительной документации.

5.1. Анализ документооборота предприятия категории «конфиденциально» на соответствие требованиям концепции информационной безопасности, положению о коммерческой тайне, прочим внутренним требованиям предприятия по обеспечению конфиденциальности информации.

5.2. Поставка комплекта типовой организационно-распорядительной документации в соответствии с рекомендациями корпоративной политики ИБ предприятия на организационно-управленческом и правовом уровнях

6. Работы, поддерживающие практическую реализацию плана защиты.

1. Разработка технического проекта модернизации средств защиты ИС, установленных у заказчика по результатам проведенного комплексного аналитического исследования корпоративной сети.

2. Разработка системы поддержки принятия решений на предприятии заказчика по обеспечению информационной безопасности предприятия на основе системных и программных средств.

3. Подготовка предприятия к аттестации.

- *Подготовка «под ключ» предприятия к аттестации объектов информатизации заказчика на соответствие требованиям РД РФ.*
- *Подготовка предприятия к аттестации ИС на соответствие требованиям по безопасности международных стандартов ISO при обеспечении требований информационной безопасности предприятия.*

4. Разработка организационно-распорядительной и технологической документации.

- *Разработка расширенного перечня сведений ограниченного распространения как части политики безопасности.*
- *Разработка пакета организационно-распорядительной документации (ОРД) в соответствии с рекомендациями корпоративной политики ИБ предприятия на организационно-управленческом и правовом уровнях.*
- *Поставка комплекта типовой организационно-распорядительной документации в соответствии с рекомендациями корпоративной политики ИБ предприятия на организационно-управленческом и правовом уровнях.*

7. Повышение квалификации и переподготовка специалистов.

1. Тренинги в области организационно-правовой составляющей защиты информации.

2. Обучение основам экономической безопасности.

3. Тренинги в области технологии защиты информации.

4. Тренинги по применению продуктов (технических средств) защиты информации.

5. Обучение действиям при попытке взлома информационных систем.

6. Обучение и тренинги по восстановлению работоспособности системы после нарушения штатного режима ее функционирования, а также по восстановлению данных и программ из резервных копий.

8. Сопровождение системы информационной безопасности после проведенного комплексного анализа или анализа элементов системы ИБ предприятия.

9. Ежегодная переоценка состояния ИБ.

Оценка состояния защищенности предприятия (фирмы)

Для оценки состояния защищенности фирмы выбраны основные направления обеспечения безопасности:

1. *Состав и структура службы безопасности.*
2. *Правовое обеспечение безопасности.*
3. *Организационные меры защиты.*
4. *Инженерно-техническое обеспечение безопасности.*
5. *Управление безопасностью.*

В каждом направлении выделены функционально ориентированные классы мер защиты и обеспечения безопасности, каждый из которых наделяется условной количественной оценкой по 6-балльной шкале.

0 - полное отсутствие каких-либо мероприятий обеспечения безопасности;

1 - отдельные несистематизированные мероприятия;

2 - отдельные мероприятия, проводимые по единому плану обеспечения безопасности;

3 - минимальный объем мероприятий по единому плану;

4 - расширенные мероприятия по отражению вероятных угроз;

5 - полный набор мероприятий, увязанный с наращиванием мер по отражению непредвиденных опасностей угроз.

Матрица комплексной оценки состояния безопасности

Классы	0	1	2	3	4	5
1. СТРУКТУРА СЛУЖБЫ БЕЗОПАСНОСТИ						
1.1. Подразделение охраны						
1.2. Подразделение режима						
1.3. Выделенное подразделение по подбору и расстановке кадров, допущенных к конфиденциальной информации						
1.4. Подразделение специальных документов и коммерческих секретов						
1.5. Подразделение инженерно-технического обеспечения безопасности						
1.6. Подразделение информационно-аналитической работы						
2. ПРАВОВАЯ ЗАЩИТА						
2.1. Наличие требований по обеспечению безопасности в уставе предприятия						
2.2. Регламентация мер по безопасности в коллективном договоре						
2.3. Регламентация мер по безопасности в правилах внутреннего трудового распорядка						
2.4. Регламентация мер безопасности в трудовом договоре						
2.5. Регламентация мер безопасности в положениях структурных подразделений						
2.6. Регламентация мер безопасности в функциональных обязанностях сотрудников						
2.7. Перечень сведений, составляющих коммерческую тайну						
3. ОРГАНИЗАЦИОННАЯ ЗАЩИТА						
3.1. Охрана персонала						

3.2. Охрана материальных ценностей						
3.3. Охрана финансовых ресурсов						
3.4. Защита информации						
3.5. Охрана зданий и помещений						
3.6. Режим допуска и пребывания на объекте						
3.7. Режим допуска к коммерческим секретам						
3.8. Режим подбора и расстановки кадров						
3.9. Мониторинг сотрудников						
3.10. Мониторинг конкурентов						
4. ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА						
4.1. Используются физические средства охраны						
4.2. Используются технические средства контроля доступа в помещения, здания						
4.3. Используются технические средства защиты информации						
4.4. Используются средства мониторинга лояльности персонала						
4.5. Используются средства активного противодействия электронному шпионажу						
5. УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ						
5.1. Наличие совета по безопасности						
5.2. Текущее планирование деятельности СБ						
5.3. Планы по обеспечению безопасности в кризисных ситуациях						
5.4. Взаимодействие с другими СБ и органами МВД						

КЛАССИФИКАТОР ОБЕСПЕЧЕННОСТИ:

Правовая:

1. Положение
2. Инструкция
3. Руководство
4. Наставление
5. Рекомендации

Организационно-функциональная 1:

1. Система охранной и пожарной сигнализации
2. Система телевидения и наблюдения
3. Система ограничения доступа
4. Система информационной безопасности
5. Система сбора, накопления и обработки информации
6. Система детективной и аналитической работы
7. Система противодействия промышленному шпионажу
8. Система связи и оповещения
9. Система бесперебойного питания
10. Система вспомогательного обеспечения
11. Система дежурного освещения

Организационно-функциональная 2:

1. Средства охраны
2. Средства телевизионного наблюдения
3. Средства контроля доступа
4. Средства связи
5. Средства защиты документов
6. Средства акустического контроля
7. Средства радиоконтроля
8. Аппаратура поиска каналов утечки информации
9. Оборудование защиты переговоров
10. Средства защиты информации от разглашения
11. Средства защиты информации от утечки
12. Средства защиты информации от НСД
13. Средства криптографической защиты информации
14. Антитеррористические средства
15. Досмотровое оборудование