ОБЗОР ЭЛЕМЕНТОВ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Элементы защиты

Службы, организующие ЗИ на уровне предприятия

Служба экономической безопасности	• Обеспечение политики экономической безопасности • Определение объекта защиты
Служба безопасности персонала	• Определение режима безопасности • Противодействие инсайдерам
Отдел кадров	• Защита персональных данных сотрудников в ИСПДН • Обеспечение режима безопасности
Служба информационной безопасности	• Организация и координация работ, связанных с защитой информации на предприятии; • Выявление и обезвреживание угроз.

Организационные меры. Организационные мероприятия

- Обучение сотрудников
- Организация рабочих мест в составе ИСПДн и мест хранения документов, отчуждаемых носителей информации
- Организация работы с обращениями граждан

Обучение сотрудников

- Цель: ознакомление с фактом и принципами работы с персональными данными, ответственность персонала
- Реализуется путем проведение общих инструктажей, разработки и ознакомления с инструкциями, проведением контроля в форме зачета или экзамена.
- Результат оформляется в виде подписанных листов ознакомления

Государственные контролирующие органы РФ

- Комитет Государственной думы по безопасности;
- Совет безопасности России
- Федеральная служба по техническому и экспортному контролю (ФСТЭК)
- Федеральная служба безопасности Российской Федерации (ФСБ России);
- Министерство внутренних дел Российской Федерации (МВД России);
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Государственный контроль

Средства вычислительной техники	Автоматизированная система	Лицензиат
		

Основные виды тайн

Государственная тайна

Конфиденциальная информация

Военная тайна

Банковская тайна

Тайна связи

Коммерческая тайна

Критически важные объекты

Правовое поле

Конституция РФ	• Право на доступ к информации (ст. 24,29,41,42) • Право на защиту данных (ст.23,24)
ГК РФ	• Банковская, служебная, коммерческая тайна
Доктрина ИБ	• совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации
УК РФ	• Статьи 138,272,273,274
ФЗ № 5485-1	• О государственной тайне от 21 июля 1993 года в редакции от 18.07.2009
ФЗ № 149	• Об информации, информационных технологиях и о защите информации от 27 июля 2006 года
Другие…	• О персональных Данных, ЭП, О инсайдерах, О лцензировании и д.р.

ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

Принцип минимальных привилегий

- каждая операция должна выполняться с наименьшим набором привилегий, требуемых для данной операции.

Принцип прозрачности

- СЗИ должна работать в фоновом режиме, быть незаметной и не мешать пользователям в основной работе, выполняя при этом все возложенные на нее функции.

Принцип превентивности

- последствия реализации угроз безопасности информации могут повлечь значительно большие финансовые, временные и материальные затрат по сравнению с затратами на создание комплексной системы защиты.

Принцип адекватности

- применяемые решения должны быть дифференцированы в зависимости от вероятности возникновения угроз безопасности, прогнозируемого ущерба от ее реализации, степени конфиденциальности информации и ее стоимости

Принцип системного подхода

- заключается во внесении комплексных мер по защите информации на стадии проектирования СЗИ, включая организационные и инженерно-технические мероприятия. Следует помнить оснащение средствами защиты изначально незащищенной АС является более дорогостоящим, чем оснащение средствами защиты проектируемой АС

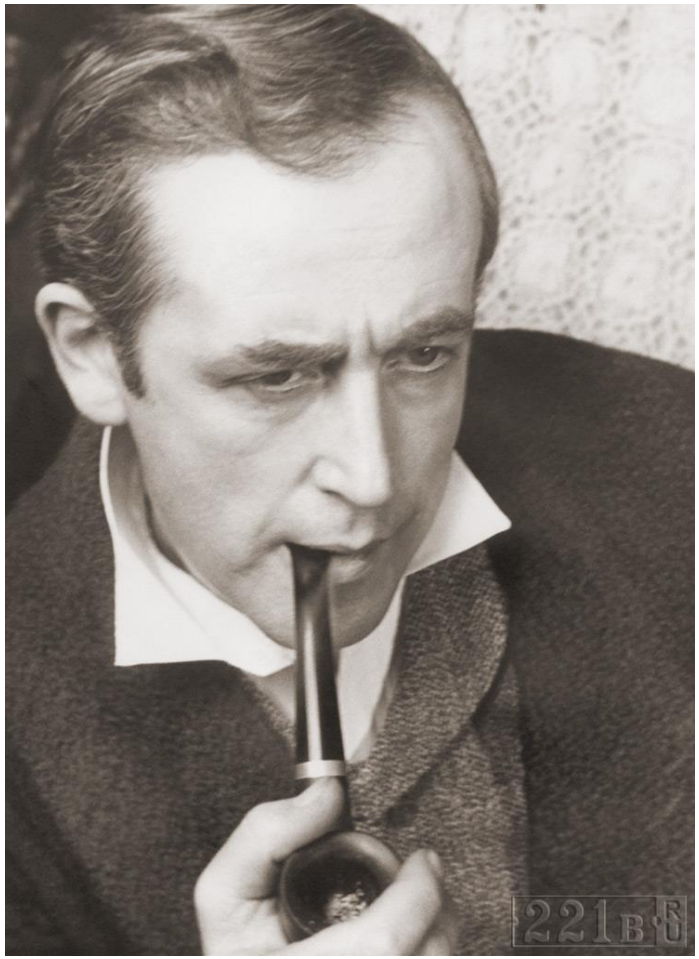
Принцип непрерывности защиты

- функционирование системы защиты не должно быть периодическим. Защитные мероприятия должны проводиться непрерывно и в объеме предусмотренном политикой безопасности

Принцип адаптивности

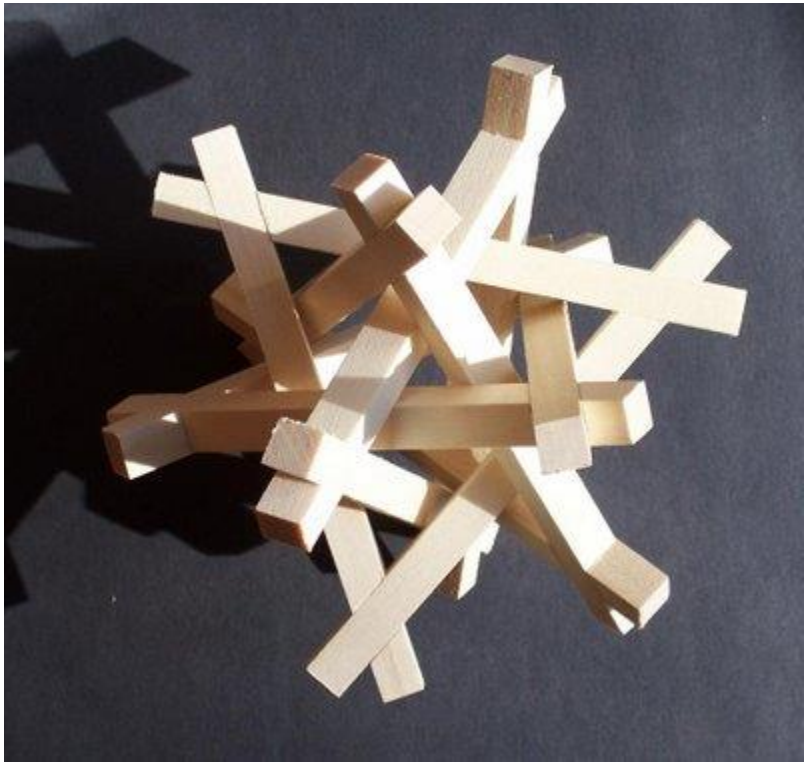
- система защиты должна строиться с учетом возможного изменения конфигурации АС, числа пользователей, степени конфиденциальности и ценности информации. Введение новых элементов АС не должно приводить к снижению достигнутого уровня защищенности

Принцип доказательности



- Результаты работы СЗИ не должны зависеть от субъекта.
- Используются:
  - Только известные формальные модели
  - Применение систем аутоинтефикации
  - Сертифицированных элементов
  - Требование сертификации СЗИ в целом

Принцип унификации решений



- Разрабатываемые решения должны быть единообразными в схожих ситуациях.
- Следствием принципа является использование:
  - Типовых проектов
  - Типовой классификации ресурсов
  - Типовых конфигурации