ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ПОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ (ИБ) СЛЕДУЕТ ПОНИМАТЬ ЗАЩИТУ ИНТЕРЕСОВ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

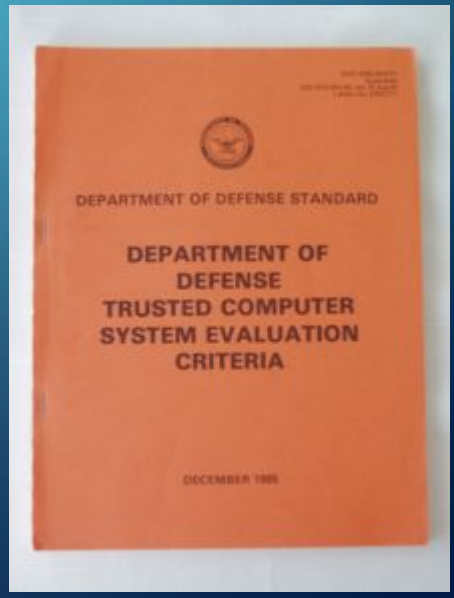
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

- Состояние защищенности информационной среды

- Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Защищенность информации, ресурсов и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений – производителям, владельцам, пользователям информации и поддерживающей инфраструктуре.



АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- **Законодательный** – федеральные и региональные законы, подзаконные и нормативные акты, международные отраслевые и корпоративные стандарты.
- **Административный** - действия общего и специального характера, предпринимаемые руководством организации.
- **Процедурный** – меры безопасности, закрепленные в соответствующих методологиях и реализуемые ответственными менеджерами и персоналом предприятия.
- **Научно-технический** – конкретные методики, программно-аппаратные, технологические и технические меры

ОСНОВНЫЕ СВОЙСТВА

Целостность

- Данные и информация, на основе которых принимаются решения, должны быть достоверными, точными и защищенными от возможных непреднамеренных и умышленных искажений

Доступность (готовность)

- Данные, информация и соответствующие службы, автоматизированные сервисы, средства взаимодействия и связи должны быть доступны и готовы к работе всегда, когда в них возникнет необходимость

Конфиденциальность

- Засекреченная информация должна быть доступна только тому, кому она предназначена

ОБЩАЯ СТРУКТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЗАДАЧИ ПОСТРОЕНИЯ СИСТЕМЫ ИБ

- Нормативно-законодательный аспект
  - Определить круг нормативных документов международного, федерального и отраслевого уровня, применение которых требуется при проектировании и реализации системы ИБ
  - Установить требования по категорированию информации на основе нормативных документов
  - Установить базовые требования к системе ИБ и ее компонентам на основе нормативных документов

Организационный аспект

- Установить соответствие защищаемой информации и информации по подсистемам и ресурсам ИС, в которых осуществляется хранение. Обработка и передача информации коечному пользователю (реестр ресурсов по критериям целостности, доступности, конфиденциальности)
- Определить набор служб, обеспечивающих доступ к ИР системы(типовые профили пользователей)
- Сформировать политику безопасности, которая включает описание границ и способов контроля безопасного состояния системы, условий и правил доступа различных пользователей к ресурсам системы, мониторинг деятельности пользователей

ЗАДАЧИ ПОСТРОЕНИЯ СИСТЕМЫ ИБ

- Процедурный аспект
  - Организовать физическую защиту по
    включая сети и телекоммуникацион
  - Обеспечит решение задач ИБ при у
  - Сформировать, утвердить и реализо
    нарушение режима ИБ
  - Внести дополнения, связанные со сп
    последствий несанкционированного д
    восстановительных работ.

Программно-технический аспект

- Обеспечить архитектурную и инфраструктурную полноту решений, связанных с хранением, обработкой и передачей конфиденциальной информации
- Гарантировать проектную и реализационную непротиворечивость механизмов безопасности по отношению к функционированию ИС в целом
- Выработать и реализовать проектные и программно-аппаратные решения по механизмам безопасности.

ФОРМИРОВАНИЕ ПОЛИТИКИ ИБ

Определение используемых руководящих документов и стандартов в области ИБ, а также основных положений политики (администрирование, контроль состояния, использование, защита, резервное копирование, ремонт-профилактика-восстановление, обучение персонала).

ФОРМИРОВАНИЕ ПОЛИТИКИ ИБ

- Разработка методологии выявления и оценки угроз и рисков их осуществления, определения подходов к управлению рисками.
- Является ли достаточным базовый уровень защищенности или требуется проводить полный вариант анализа рисков.

ФОРМИРОВАНИЕ ПОЛИТИКИ ИБ

- Структуризация контр мер по уровням требований к безопасности.

ФОРМИРОВАНИЕ ПОЛИТИКИ ИБ

- Порядок сертификации на соответствие стандартам в области информационной безопасности. Периодичность проведения совещаний на уровне руководства, порядок обучения всех категорий пользователей информационных систем по вопросам ИБ.

ТРИ УРОВНЯ ПОЛИТИКИ ИБ

ВЕРХНИЙ УРОВЕНЬ

Решения общего характера для организации
Формулирование целей, которые преследует в области ИБ,

- Определение общих направлений и средств достижения целей
- Формирование или пересмотр общей программы ИБ, определение ответственных за реализацию и сопровождение программы
- Обеспечение правовой базы для соблюдения государственных законов и корпоративных правил
- Формулировка общих управленческих решений по вопросам реализации программы ИБ, для организации в целом.

АСПЕКТЫ ИБ

- Описание аспекта
- Позиция организации
- Роли, обязанности, ответственность
- Законопослушность
- Точки контакта

ТРИ УРОВНЯ ПОЛИТИКИ ИБ

СРЕДНИЙ УРОВЕНЬ

КОНКРЕТНЫЕ СЕРВИСЫ

Включает в себя конкретные цели и задачи, правила и способы их достижения.
Более детальна.
Кто имеет право доступа к объектам, поддерживаемым сервисом?
При каких условиях можно читать и модифицировать данные?
Как организовать удаленный доступ к сервису?

ТРИ УРОВНЯ ПОЛИТИКИ ИБ
НИЖНИЙ УРОВЕНЬ

МОДЕЛИ, ОПИСЫВАЮЩИЕ ПРОЦЕСС ЗАЩИТЫ ИНФОРМАЦИИ. ТЕРМИНЫ

- Ресурс – все, что представляет ценность с точки зрения организации и является объектом защиты.
- Угроза – совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности.
- Уязвимость – слабость в системе защиты, которая дает возможность реализации угрозы.
- Анализ рисков – процесс определения угроз, уязвимостей, возможного ущерба, контрмер
- Полный анализ рисков -

МОДЕЛИ, ОПИСЫВАЮЩИЕ ПРОЦЕСС ЗАЩИТЫ ИНФОРМАЦИИ. ТЕРМИНЫ

- Полный анализ рисков – анализ рисков для информационных систем, предъявляющих повышенные требования в области ИБ.
- Риск нарушения ИБ – возможность реализации угрозы.
- Оценка рисков – идентификация рисков, выбор параметров для их описания и получение оценок по этим параметрам.
- Управление рисками – процесс определения контрмер в соответствии с оценкой рисков.
- Система управления рисками ИБ – комплекс мер, направленных на обеспечение режима ИБ на всех стадиях жизненного цикла ИС.
- Класс рисков – множество угроз ИБ, выделенных по определенномк признаку

КЛАССИФИКАЦИЯ УГРОЗ ИБ

- Происшествия, связанные с техническими причинами
- Происшествия , связанные со стихийными бедствиями
- Происшествия, связанные с ненамеренными действиями людей
- Злоумышленные действия людей

ПРИМЕРЫ УГРОЗ ИБ

- Физическая безопасность и безопасность окружающей среды
- Управление коммуникациями и операциями
- Аспекты ИБ в управлении непрерывностью бизнеса
- Соответствие (требованиям законодательства, соответствие политикам и стандартам ИБ организации)

Угрозы - потенциальные источники нежелательных событий, которые могут нанести ущерб ресурсами

ПРИМЕРЫ УЯЗВИМОСТЕЙ

- Среда и инфраструктура
- Аппаратное обеспечения
- Программное обеспечение
- Коммуникации
- Документы
- Персонал
- Общие уязвимые места

Уязвимости – слабые места в защите, которые способствуют реализации угроз.

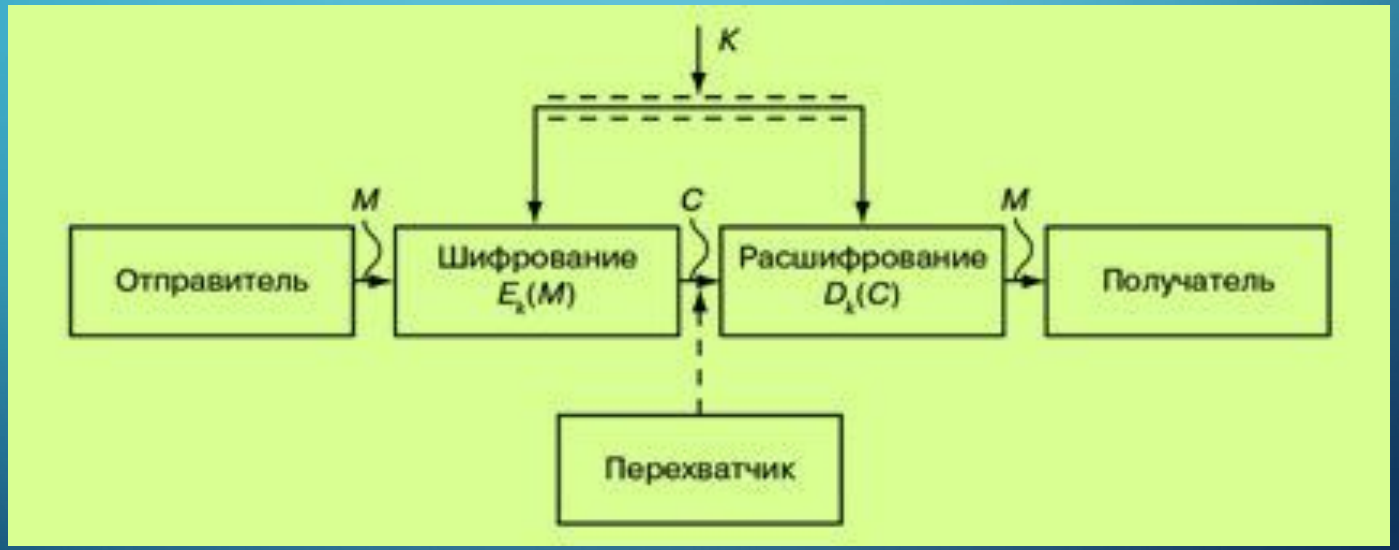
ТЕХНОЛОГИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

- **Криптография** - это совокупность технических, математических, алгоритмических и программных методов преобразования данных (шифрование данных), которая делает их бесполезными для любого пользователя, у которого нет ключа для расшифровки. Криптографические преобразования обеспечивают **конфиденциальность и целостность**

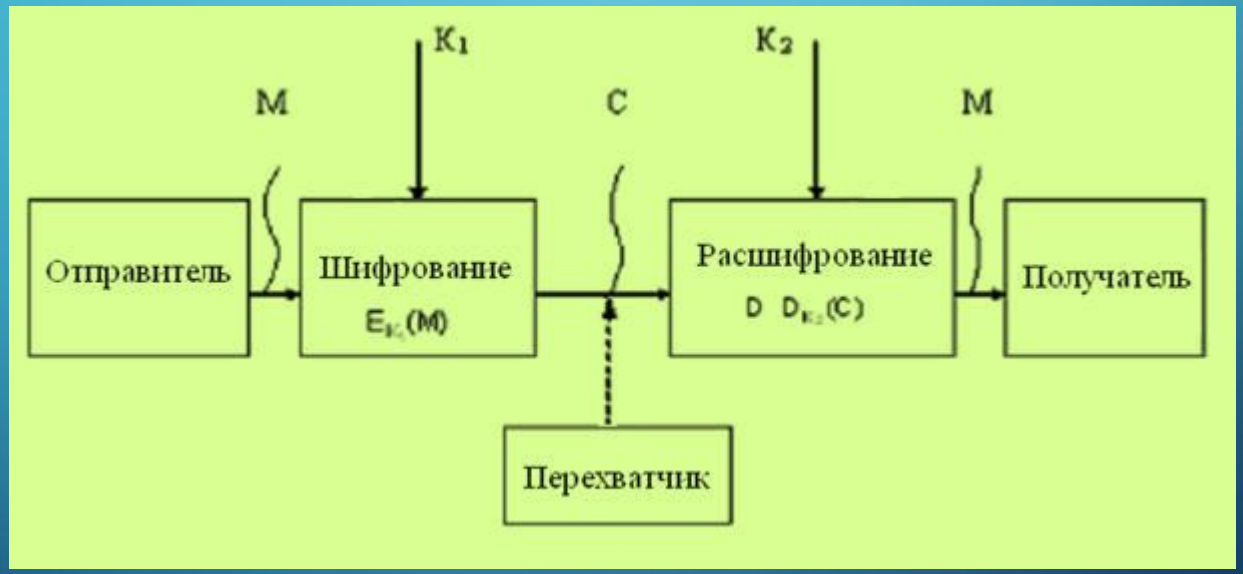
- **идентификация**
  - Отождествление
- **аутентификация**
  - Проверка подлинности
- **контроль**
- **целостность**
  - Обеспечение и контроль целостности данных

Разграничение доступа

ОБОБЩЕННАЯ СХЕМА СИММЕТРИЧНОЙ КРИПТОСИСТЕМЫ С ЗАКРЫТЫМ КЛЮЧОМ



ОБОБЩЕННАЯ СХЕМА АССИМЕТРИЧНОЙ КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ



КОМПЬЮТЕРНАЯ ПРОГРАММА ПОТЕНЦИАЛЬНО ОПАСНА, ЕСЛИ…

1. Может скрыть признаки своего присутствия в среде
2. Может реализовать самодублирование
3. Может разрушить код других программ
4. Может перенести фрагменты информации
5. Имеет потенциальную возможность исказить, подменить массив информации

КЛАССИФИКАЦИЯ ВРЕДОНОСНЫХ ПРОГРАММ

- Вирусы и черви
- Троянские программы
- Подозрительные упаковщики
- Вредоносные утилиты

ВРЕДОНОСНЫЕ УТИЛИТЫ

- Вредоносные программы , разработанные для автоматизации создания других вирусов, червей или троянских программ, взломов др. программ и т.п.
- Riskware, Pornware, программные закладки

ОСНОВНЫЕ МОДЕЛИ ВЗАИМОДЕЙСТВИЯ ПРОКЛАДНОЙ ПРОГРАММЫ И ПРОГРАММНОЙ ЗАКЛАДКИ

Перехват	Троянский конь	Наблюдатель
Компроментация	Инициатор ошибок/ искажение	Уборка мусора

ПРИМЕРНАЯ ПРОГРАММА АУДИТА ВОПРОСОВ УПРАВЛЕНИЯ НЕПРЕРЫВНОСТЬЮ БИЗНЕСА

ISO/IEC 27004:2009 И

ГОСТ Р ИСО/МЭК 27004-2011

- Получение предварительной информации (общее представление об организации, ее бизнесе, организационной структуре и используемых ИТ; политики и планы восстановления после сбоев)
- Проверка анализа рисков ИБ (проводился или нет анализ рисков; предварительная оценка рисков)
- Проверка ответственных лиц (определение ответственных лиц за разработку плана, вовлеченность в разработку ключевых пользователей; ответственных за координацию/управление в рамках плана; определение ответственных в нештатных ситуациях; поддерживается ли план в актуальном состоянии; документированы ли обязанности; актуальность контактной информации; где хранятся планы)
- Оценка планов обеспечения непрерывности бизнеса и восстановления после сбоев (проверить актуальность и полноту планов, их адекватность, наличие приоритета восстановления, определить какие системы не рассмотрены в планах почему)
- Проверка процедур резервного копирования и восстановления данных (существуют ли формальные процедуры резервного копирования, следует ли им организация, проводилось ли обучение персонала по данным процедурам, проводилось ли тестирование процедур)
- Проверка удаленного хранения резервных данных (определить, где находится внешний центр резервного хранения данных, посетить объект удаленного хранения резервных данных, убедиться в эффективности процедур проверки полноты получения отправленных данных)
- Проверка резервной площадки(резервная площадка не должна быть подвержена тем же рискам, что и основная площадка. Как использовалась площадка во время последнего теста, оценить состояние резервной площадки, определить периодичность и адекватность проверки журналов на предмет полноты)
- Тестирование планов (наличие бюджет на восстановление сбоев; процедура пересмотра планов; расписание тестирования планов; результаты тестов; адекватность тестов; мероприятия по устранению недостатков)
- Проверка обучения персонала (определить проходили ли пользователи и ИТ-персонал обучение действиям в случае нештатных ситуаций или прерываний. Включала ли программа обучения раздел связи со сторонними организациями, оросить ИТ-персонал на предмет обучения/знаний в смежных областях, случай отсутствия основного сотрудника)