Информационная безопасность

Обзорная лекция к междисциплинарному экзамену

(специализация «Информационная безопасность в коммерческих структурах»)

Классификация угроз информационной безопасности

- **Угроза информационной безопасности** (ИБ) – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.
- Попытка реализации угрозы называется **атакой.**
- Классификация угроз ИБ можно выполнить по нескольким критериям:
  - **по аспекту ИБ** (доступность, целостность, конфиденциальность);
  - **по компонентам ИС**, на которые угрозы нацелены (данные, программа, аппаратура, поддерживающая инфраструктура);
  - **по способу осуществления** (случайные или преднамеренные действия природного или техногенного характера);
  - **по расположению источника угроз** (внутри или вне рассматриваемой ИС).

Классификация угроз ИБ по базовым свойствам информации

- Вне зависимости от конкретных видов угроз информационная система должна обеспечивать базовые свойства информации и систем ее обработки. Для автоматизированных ИС рассматриваются три основных вида угроз:
  - **угроза нарушения конфиденциальности;**
  - **угроза нарушения целостности;**
  - **угроза отказа служб (отказа в доступе).**

Примеры реализации угроз (угроза нарушения конфиденциальности)

Часть информации, хранящейся и обрабатываемой в ИС, должна быть сокрыта от посторонних. Передача данной информации может нанести ущерб как организации, так и самой информационной системе.

Примеры реализации угроз (угроза нарушения конфиденциальности)

- Средствами атаки могут служить различные технические средства (подслушивание разговоров, сети), другие способы (несанкционированная передача паролей доступа и т.п.).
- Важный аспект при предотвращении угрозы конфиденциальности – непрерывность защиты данных на всем жизненном цикле ее хранения и обработки. Пример реализации угрозы – доступное хранение резервных копий данных.

Примеры реализации угроз (угроза нарушения целостности данных)

- Одними из наиболее часто реализуемых угроз ИБ являются кражи и подлоги. Целостность информации может быть разделена на **статическую** и **динамическую.**
- Примерами нарушения статической целостности являются:
  - ввод неверных данных;
  - несанкционированное изменение данных;
  - изменение программного модуля вирусом;
- Примеры нарушения динамической целостности:
  - нарушение атомарности транзакций;
  - дублирование данных;
  - внесение дополнительных пакетов в сетевой трафик.

Примеры реализации угроз (угроза отказа доступа)

- Отказ служб (отказа в доступе к ИС) относится к одним из наиболее часто реализуемых угроз ИБ. Относительно компонент ИС данный класс угроз может быть разбит на следующие типы:
  - отказ пользователей (нежелание, неумение работать с ИС);
  - внутренний отказ информационной системы (ошибки при переконфигурировании системы, отказы программного и аппаратного обеспечения, разрушение данных);
  - отказ поддерживающей инфраструктуры (нарушение работы систем связи, электропитания, разрушение и повреждение помещений).

Основные принципы обеспечения информационной безопасности

- Информационная безопасность может быть обеспечена при соблюдении следующих принципов:
  - Системности;
  - Комплексности;
  - Непрерывности защиты;
  - Разумной достаточности;
  - Гибкости управления и применения;
  - Открытости алгоритмов и механизмов защиты;
  - Простоты применения защитных мер и средств.

Понятие политики безопасности

- Политика безопасности – совокупность документированных решений, принимаемых на разных уровнях управления и направленных на защиту информации и ассоциированных с ней ресурсов.
- ИС предприятия и связанные с ней субъекты представляют собой сложную систему, для рассмотрения которой рекомендуют применять объектно-ориентированный подход и понятие уровней детализации.
- При формировании документированных решений разделяют несколько уровней управления:
  - **верхний** – выносится управление защитными ресурсами и координация использования данных ресурсов;
  - **средний** – выносятся вопросы, касающиеся отдельных аспектов информационной безопасности;
  - **нижний** – вопросы относящиеся к конкретным сервисам ИС.

Рекомендации к составу политики безопасности

- "Общие критерии оценки безопасности информационных технологий", версия 2.0 от 22 мая 1998 г. Британского стандарта BS7799:1995. рекомендует включать в документ, характеризующий политику информационной безопасности организации, следующие пункты:
  - вводный, подтверждающий заинтересованность высшего руководства проблемами информационной безопасности;
  - организационный, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности;
  - классификационный, описывающий имеющиеся на предприятии материальные и информационные ресурсы и необходимый уровень их защиты;
  - штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения, порядок реагирования на нарушение режима и т.д.);

Рекомендации к составу политики безопасности (продолжение)

- "Общие критерии оценки безопасности информационных технологий", версия 2.0 от 22 мая 1998 г. Британского стандарта BS7799:1995. рекомендует включать в документ, характеризующий политику информационной безопасности организации, следующие пункты:
  - раздел, освещающий вопросы физической защиты информации;
  - раздел управления, описывающий подход к управлению компьютерами и сетями передачи данных;
  - раздел, описывающий правила разграничения доступа к производственной информации;
  - раздел, описывающий порядок разработки и внедрения систем;
  - раздел, описывающий меры, направленные на обеспечение непрерывной работы организации (доступности информации);
  - юридический раздел, подтверждающий соответствие политики информационной безопасности текущему законодательству.

Административный уровень защиты информации

- Под **административным уровнем** информационной безопасности относятся действия общего характера, предпринимаемые руководством организации к обеспечению защиты информации.
- Главная цель – **формирование политики безопасности**, отражающей подход организации к защите данных.
- Политика безопасности административного уровня – совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.
- Выработку политики безопасности и ее содержание рассматривают на трех горизонтальных уровнях детализации:
  - Верхний уровень, относящийся к организации в целом
  - Средний уровень – вопросы, касающиеся отдельных аспектов ИБ
  - Низкий уровень – вопросы относящиеся к конкретным сервисам

Политика безопасности (верхний уровень)

- Решения принимаемые на верхнем уровне определяют наиболее общие подходы к защите информации и исходят, как правило, от руководства организации.
- Типовой список решений:
  - Формирование или изменение комплексной программы обеспечения безопасности
  - Формулирование целей организации в области ИБ, определение направлений в достижении данных целей
  - Обеспечение документальной базы для соблюдения законов и правил
  - Формулирование административных решений по вопросам реализации программы безопасности
- В политике верхнего уровня определяются обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь.

Политика безопасности (средний уровень)

- К данному уровню относятся вопросы отдельных аспектов информационной безопасности, например, определение политики доступа к ресурсам Интернет, использование неофициального ПО.
- Политика среднего уровня для каждого аспекта определяет:
  - Описание аспекта
  - Область применения
  - Позиция организации по данному вопросу
  - Роли и обязанности
  - Законопослушность
  - Точки контакта

Политика безопасности (нижний уровень)

- Политика безопасности организации на нижнем уровне относится к конкретным информационным сервисам. Она включает два аспекта – цели и правила их достижения.
- На данном уровне политика безопасности должна быть прописана наиболее формально и детализировано.
- Формулирование целей политики безопасностей нижнего уровня исходят из соображений целостности, доступности и конфиденциальности данных.
- Из целей безопасности выводятся правила безопасности, описывающие условия, объекты и средства защиты.

Административный уровень защиты информации

- После формулирования политики безопасности, составляется программа обеспечения информационной безопасности.
- Программа безопасности также структурируется по уровням. В простом случае достаточно двух уровней:
  - верхнего (центрального) – охватывающего всю организацию;
  - нижнего (служебного) – относящегося к отдельным услугам или группам однородных сервисов.

Программа верхнего уровня

- Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. Цели такой программы:
  - Управление рисками (оценка рисков, выбор эффективных решений);
  - Координация деятельности в области информационной безопасности
  - Стратегическое планирование
  - Контроль деятельности в области информационной безопасности.
- Контроль деятельности в области ИБ должен гарантировать, во-первых, что действия организации не противоречат законам, во-вторых, что состояние безопасности в организации соответствует требованиям и реагировать на случаи нарушений.

Программы служебного уровня

- Цель программы нижнего уровня – обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов.
- На нижнем уровне осуществляется выбор механизмов защиты, технических и программных средств.
- Ответственность за реализацию программ нижнего уровня обычно несут администраторы соответствующих сервисов.

Синхронизация программы безопасности с жизненным циклом системы

- В жизненном цикле информационного сервиса можно выделить следующие этапы:
  - инициация, определяются потребности в новом сервисе, документируется его назначение;
  - приобретение (разработка), составляется спецификация, варианты приобретения или разработки, собственно приобретение;
  - установка (внедрение), сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию;
  - эксплуатация, работа в штатном и регламентном режиме;
  - утилизация (выведение из эксплуатации).
- Для обеспечения безопасной работы сервиса в рамках информационной системы на всех этапах жизненного цикла должны быть рассмотрены вопросы:
  - Какая информация предназначена для обслуживания?
  - Какие возможные последствия от реализации угроз ИБ а данном сервисе?
  - Каковы особенности данного сервиса?
  - Каковы характеристики персонала, имеющие отношения к информационной безопасности?

Управление доступом

- К числу мер обеспечения безопасности относится управление доступом.
- Управление доступом позволяет разграничить доступ субъектов к информационным объектам системы.

Основные типы политики управления доступом.

- Одним из сужений политики безопасности является политика безопасности при управлении доступом к информационным объектам.
- Политика безопасности на уровне управления доступом включает:
  - Множество объектов системы O_j – пассивных сущностей и субъектов системы S_j – активных сущностей
  - Множество возможных действий над объектами R
  - Для каждой пары «объект, субъект» (S_j, O_j) множество разрешенных операций, являющееся подмножеством множества возможных операций.

Модель произвольного доступа (дискреционная модель)

- В основе дискреционной модели управления доступом лежат следующие положения:
  - Все субъекты и объекты должны быть идентифицированы;
  - Права доступа субъекта к объекту системы определяются на основании некоторого внешнего правила.
- Отношения «субъекты-объекты» можно представить в виде матрицы доступа, в строках которой перечислены субъекты, в столбцах объекты ИС, а в клетках, на пересечении строк и столбцов, записаны дополнительные условия и разрешенные виды доступа.
- **Достоинство** модели — относительно простая реализация соответствующих механизмов защиты.
- **Недостаток** — статичность модели. Кроме того, возникает вопрос определения правил распространения прав доступа и анализа их влияния на безопасность ИС.

Модель принудительного доступа (мандатная модель)

- Мандатное управление доступом, включает следующие требования:
  - Все субъекты и объекты ИС должны быть однозначны идентифицированы;
  - Задан линейно упорядоченный набор меток секретности;
  - Каждому объекту системы присвоена метка секретности, определяющая ценность содержащей в ней информации — *уровень секретности*;
  - Каждому субъекту системы присвоена метка секретности, определяющая уровень к нему ИС — максимальное значение метки секретности объектов, к которым субъект имеет доступ; метка секретности субъекта называется его уровнем доступа.

Модель принудительного доступа (мандатная модель)

- Основная цель мандатной политики — предотвращение утечки информации от объектов с высоким доступа к объектам низким уровнем доступа.
- Важное достоинство мандатной модели – формальное доказательство утверждения: *если начальное состояние системы безопасно, и все переходы системы из состояния в состояние не нарушает ограничений, сформулированных политикой безопасности, то любое состояние системы безопасно.*
- Недостаток мандатной модели – сложность реализации. Множество операций ограничивается операциями чтения (поток данных направлен от объекта к субъекту) и записи (поток направлен от субъекта к объекту).

Контроль прав доступа

- При реализации политики безопасности на уровне доступа в информационной системе должен существовать модуль, обеспечивающий выполнение операций доступа на основе построенной политики безопасности – монитор безопасности.
- Задача монитора безопасности – контролировать выполнение операций в соответствии с определенной политикой безопасности.

Процедурный уровень информационной безопасности

- совокупность организационных мер безопасности, ориентированных на людей и направленных на обеспечение заданного уровня информационной безопасности

Основные классы мер процедурного уровня

- Управление персоналом
- Физическая защита
- Поддержание работоспособности ИС
- Реагирование на нарушения режима безопасности
- Планирование восстановительных работ

Управление персоналом

- Комплекс мер, направленных на взаимодействие с сотрудниками организации, обеспечивающее заданный уровень безопасности.
- Основные принципы:
  - Разделение обязанностей
  - Минимизация привилегий

Управление персоналом

- **Принцип разделения обязанностей** предписывает распределить роли и ответственности между участниками таким образом, чтобы один человек не мог нарушить критически важный процесс. Разделение выполнения критически важных действий позволяет уменьшить вероятность ошибок и злоупотреблений
- **Минимизация привилегий** предполагает выделение пользователю только тех прав, что необходимы ему для выполнения служебных обязанностей. Задача данного принципа уменьшить ущерб от случайных или умышленных некорректных операций

Физическая защита

- Основной принцип физической защиты – ее непрерывность в пространстве и во времени. Для физической защиты не должно существовать «окон опасности»
- Включает в себя несколько направлений:
  - Физическое управление доступом
  - Противопожарные меры
  - Защита поддерживающей инфраструктуры
  - Защита от перехвата данных
  - Защита мобильных систем

Физическая защита

- Меры физического управления доступом позволяют контролировать и при необходимости ограничивать вход и выход сотрудников и посетителей.
- Противопожарные меры позволяют избежать потерь при предупреждении, возникновении и ликвидации пожаров
- Поддерживающая инфраструктура – электро-, водо- и теплоснабжение, кондиционеры и средства коммуникаций. К данным системам применимы те же требования целостности и доступности, что и для информационных систем

Поддержка работоспособности ИС

- Выделяется несколько направлений работы системных администраторов для поддержания работоспособности ИС:
  - Поддержка пользователей
  - Поддержка программного обеспечения
  - Конфигурационное управление
  - Резервное копирование
  - Управление носителями
  - Документирование
  - Регламентные работы

Поддержка работоспособности

- **Поддержка пользователей** – консультирование и помощь пользователям в процессе выполнения работы
- **Поддержка программного обеспечения** – организация работ по контролю за используемым ПО, его своевременное обновление, контроль за неавторизованным изменением ПО и доступа к ним
- **Конфигурационное управление –** контроль за изменениями вносимыми в программную конфигурацию

Поддержка работоспособности

- **Резервное копирование –** необходимо для восстановления данных в случае аварии или другой причины
- **Управление носителями** – обеспечивает физической защиты и учета дискет, лент, выдачи печатных форм и т.п. Обеспечивает конфиденциальность, целостность и доступность информации. Управление носителями должно охватывать весь жизненный цикл.

Поддержка работоспособности

- **Документирование** – описание выполняемых процедурных, административных или иных мер по обеспечению ИБ.
- **Регламентные работы** – одна из возможных угроз ИБ. Сотрудник, выполняющий регламентные работы, получает исключительный доступ к ИС. Проведение регламентных работ должно выполняться под контролем со стороны службы ИБ.

Планирование восстановительных работ

- В любой организации возможны аварии, вызванные естественными причинами, халатностью или некомпетентностью персонала или действиями злоумышленника. В любой организации существуют критически важные процессы, которые должны быть восстановлены в первую очередь.
- В организации должен существовать план выполнения восстановительных работ при реализации угроз, препятствующих выполнению критически важных функций

Планирование восстановительных работ

- Этапы планирования восстановительных работ:
  - Выявление критически важных функций организации, выставление приоритетов
  - Идентификация ресурсов, для выполнения критически важных функций
  - Определение перечня возможных аварий
  - Разработка стратегии восстановительных работ
  - Подготовка к реализации выбранной стратегии
  - Проверка стратегии

Идентификация и аутентификация пользователей

- *Идентификация субъекта в ИС* — установление соответствия между множеством сущностей системы и множеством *идентификаторов*.
- *Аутентификации* — процесс проверки подлинности предъявленного идентификатора.
- Аутентификация бывает односторонней и двусторонней (взаимной).
- При двусторонней аутентификации выделяют:
  - *Аутентификации субъекта* решает задачу установления подлинности идентификатора, предъявляемого субъектом взаимодействия и используется при доступе к ресурсам.
  - *Аутентификация объекта* устанавливает подлинность идентификатора некоторого объекта. В качестве доказательства подлинности обычно используется подтверждением того, что источником данного объекта является владелец указанного идентификатора.

Системы аутентификации

- Различают три группы методов аутентификации:
  - Индивидуального объекта заданного типа (удостоверения, пропуска, магнитные карты, токены и т. п.);
  - Знание некоторой известной только ему и проверяющей стороне информации (**парольные схемы**);
  - Индивидуальных биометрических характеристик пользователя (использование отпечатков пальцев, радужной оболочки глаза и т.п.).
- Если в процедуре аутентификации участвуют две стороны, то такая схема называется *непосредственной аутентификацией*. Если же в процессе участвуют вспомогательные стороны, говорят об *аутентификации с участием доверенной стороны*. Третью сторону называют сервером аутентификации.

Парольные схемы аутентификации

- Классическое средство аутентификации субъекта — *парольные схемы*. В данной схеме *претендент* предъявляет пароль, а *верификатор* сравнивает этот пароль с имеющимся у него множеством паролей.
- Достоинство парольной аутентификации – простота применения и понятность для пользователя.
- Недостаток парольной схемы — возможность несанкционированного доступа к паролям, хранимым в памяти компьютера и большая вероятность подбора пароля.
- Один из способов защиты при передаче пароля — криптографическое преобразование перед передачей, например, с помощью *хэш-фукнции*.

Основные компоненты парольной схемы

- Основными компонентами парольной схемы являются:
  - Интерфейс пользователя;
  - Интерфейс администратора;
  - Модуль сопряжения с другими подсистемами безопасности;
  - База данных учетных записей.
- Хранение паролей может быть осуществлено в виде:
  - В открытом виде;
  - В виде сверток (хеширование)
  - Зашифрованном на некотором ключе.

Использование одноразовых паролей

- В современных распределенных системах требуется передача пароля по сети. Если информация не будет защищена, то возникает угроза ее перехвата и использования злоумышленником.
- Один из вариантов защиты – использование **одноразовых паролей** (схема S/Key):
  - В процессе аутентификации используется односторонняя функция *f,* данная функция известна пользователю и серверу аутентификации
  - Задан ключ K, известный только пользователю
  - На этапе начального администрирования функция *f* применяется к ключу K n раз, результат сохраняется на сервер
  - Во время аутентификации сервер присылает на пользовательскую систему число (n-1)
  - Пользователь применяет функцию *f* к секретному числу (n-1) раз и отправляет результат серверу
  - Сервер применяет функцию *f* к полученному от пользователя значению и сравнивает с ранее сохраненной величиной. В случае совпадения подлинность считается установленной, сервер запоминает присланное значение и уменьшает на единицу счетчик.

Схемы аутентификации с третьей доверенной стороной

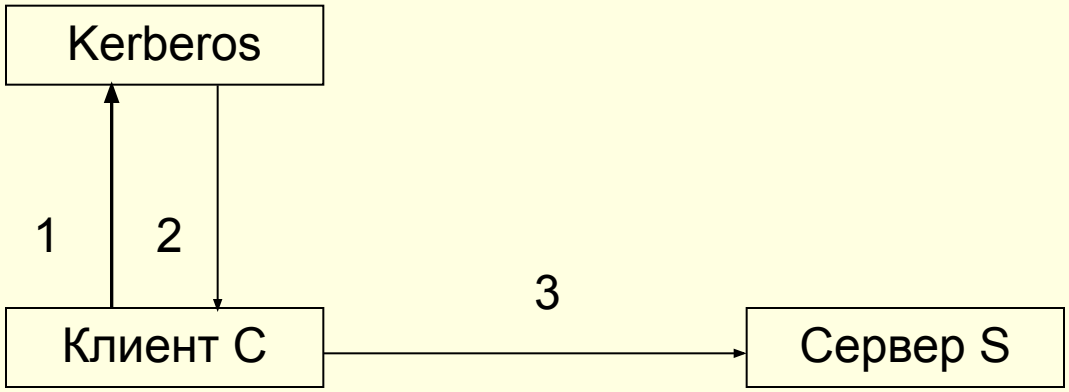
- В распределенных многопользовательских ИС использование криптографических методов при аутентификации субъектов затруднено в силу того, что каждый верификатор (сервер, хост и т.д.) должен иметь копию ключа и информацию о пользователе данного ключа.
- Эта проблема устраняется за счет использования специального сервера аутентификации – третьей доверенной стороны, с которой разделяют ключи шифрования каждый пользователь и каждый верификатор.
- Пример схемы аутентификации с третьей доверенной стороной – **схема Kerberos**.

Аутентификация Kerberos

- Схема Kerberos предназначена для решения задачи аутентификации в открытой сети с использованием третьей доверенной стороны.
- Чтобы получить доступ к серверу S, клиент C посылает Kerberos запрос, содержащий сведения о клиенте и запрашиваемой услуге. В ответ Kerberos возвращает так называемый **билет**, зашифрованный секретным ключом сервера и копию части информации из билета, зашифрованного секретным ключом клиента. Клиент расшифровывает вторую порцию данных и пересылает ее вместе с билетом серверу. Сервер, расшифровав билет, сравнивает с дополнительной информацией, присланной клиентом. Совпадение будет свидетельствовать о том, что клиент смог расшифровать данные присланные ему Kerberos и тем подтверждает знание секретного ключа и свою подлинность.
- В схеме Kerberos сами секретные ключи не передаются по сети, они используются только в процессе шифрования.

Аутентификация Kerberos

1. Клиент C -> Kerberos: c, s, … клиент направляет Kerberos сведения о себе и запрашиваемом сервере
2. Kerberos -> клиент C: {d1}Kc, {Tc.s} Ks Kerberos возвращает билет, зашифрованный ключом сервера и дополнительную информацию, зашифрованную ключом клиента
3. Клиент C -> сервер S: d2, {Tc.s} Ks клиент направляет на сервер билет и дополнительную информацию



Аудит в информационных системах

- Для обеспечения защиты данных ИС используются подходы, основанные на фиксации и анализе событий, происходящих в информационной системе.
- **Протоколирование** – сбор и накопление информации о событиях ИС (внешних, внутренних, клиентских)
- **Аудит** – анализ накопленной информации, проводимый оперативно или периодически.

Функции и назначение аудита

- Аудит в ИС позволяет решить следующие задачи:
  - Обеспечение подотчетности пользователей и администраторов ИС;
  - Обеспечение реконструкции последовательности событий;
  - Обнаружение попыток нарушений ИБ;
  - Предоставление информации для выявления и анализа проблем.

Протоколирование и аудит

- При выполнении протоколирования рекомендуется фиксировать следующие события (согласно «Оранжевой книге»):
  - Вход в систему
  - Выход из системы
  - Обращение к удаленной системе
  - Операции с файлами
  - Смена привилегий или иных атрибутов безопасности
- В базу данных фиксируемых событий записывается следующая информация:
  - Дата и время события
  - Уникальный идентификатор субъекта – инициатора события
  - Результат события
  - Источник запроса
  - Имена объектов
  - Описание изменений, внесенных в базу данных защиты

Активный аудит

- Выделяют **активный аудит** – выявление подозрительной активности и управление средствами автоматического реагирования на нее
- Активность противоречащую политике безопасности разделяют:
  - Атаки, направленные на незаконное получение полномочий
  - Действия, выполняемые в рамках полномочий, но нарушающие политику безопасности (злоупотребление полномочиями)

Активный аудит

- Разделяют ошибки активного аудита первого и второго рода:
  - Ошибки первого рода – пропуск атак
  - Ошибки второго рода – ложные срабатывания
- Методы активного аудита:
  - Сигнатурный – на основе определения сигнатуры атаки (совокупность условий при которых считается, что атака имеет место) – велики ошибки первого рода (неумение обнаруживать неизвестные атаки)
  - Статистический – на основе анализа выполняемых действий субъектов – велики ошибки второго рода

Понятие цифровой подписи

- Использование цифровой подписи в электронных документах призвано обеспечить ей ту же роль, что и обычная подпись на бумажных документах – подтверждение подлинности и актуальности передаваемых сообщений.
- Получатель сообщения (или третья доверенная сторона) с помощью существующего ключа может удостоверится в подлинности автора сообщений.
- При разработке алгоритма цифровой подписи решаются две основных задачи:
  - механизм формирования подпись должна гарантировать невозможность подделки;
  - должен существовать механизм проверки принадлежности подписи указанному владельцу.

Механизм формирования электронной цифровой подписи

- Электронная цифровая подпись (ЭЦП) выполняет роль обычной подписи в электронных документах для подтверждения подлинности сообщений – данные присоединяются к передаваемому сообщению, подтверждая подлинность отправителя сообщения
- При формировании цифровой подписи по классической схеме отправитель:
  - Применяет к исходному тексту хэш-функцию
  - Дополняет хэш-образ до длины, требуемой в алгоритме создания ЭЦП
  - Вычисляет ЭЦП по хэш-образу с использованием секретного ключа создания подписи
- Получатель, получив подписанное сообщение, отделяет цифровую подпись от основного текста и выполняет проверку:
  - Применяет к тексту полученного сообщения хэш-функцию
  - Дополняет хэш-образ до требуемой длины
  - Проверяет соответствие хэш-образа сообщения полученной цифровой подписи с использованием открытого ключа проверки подписи

Законодательный уровень применения цифровой подписи

- 10 января 2002 года был подписан закон «Об электронной цифровой подписи».
- Статья 1. **Цель и сфера применения** настоящего Федерального закона
  - 1. Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.
  - 2. Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско - правовых сделок и в других предусмотренных законодательством Российской Федерации случаях.
- Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Основные понятия закона

- электронный документ - документ, в котором информация представлена в электронно - цифровой форме;
- электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;
- владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);
- средства электронной цифровой подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной;
- сертификат средств электронной цифровой подписи ;
- закрытый ключ электронной цифровой подписи;
- открытый ключ электронной цифровой подписи;
- сертификат ключа подписи;
- подтверждение подлинности электронной цифровой подписи в электронном документе;
- пользователь сертификата ключа подписи - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;
- информационная система общего пользования;
- корпоративная информационная система.

Условия использования электронной цифровой подписи

- В законе определены условия равнозначности ЭЦП в электронных документах собственноручной подписи на бумажном носителе, содержание сертификата ЭЦП, сроки и порядок хранения сертификатов.
- Закон определяет задачи и функции удостоверяющих центров, требования к их функционированию.
- В законе определены особенности использования ЭЦП в сфере государственного управления, в корпоративных информационных системах.

Основные этапы разработки защищенной системы

- Процесс разработки защищенной информационной системы включает в себя следующие этапы:
  - определение политики безопасности;
  - проектирование модели ИС;
  - разработка кода ИС;
  - обеспечение гарантий соответствия реализации заданной политике безопасности.

Определение политики безопасности

- При разработке защищенной информационной системы в соответствии с требованиями «Единых критериев безопасности информационных технологий» необходимо формирование следующих документов:
  - Задачи защиты – потребности потребителей ИТ-продукта в противостоянии к заданному множеству угроз безопасности;
  - Профиль защиты – специальный нормативный документ, представляющий собой совокупность задач защиты, функциональных требований, требований адекватности и их обоснование;
  - Проект защиты – специальный нормативный документ, представляющий собой совокупность задач защиты, функциональных требований, общих спецификаций средств защиты и их обоснование.

Проектирование модели ИС

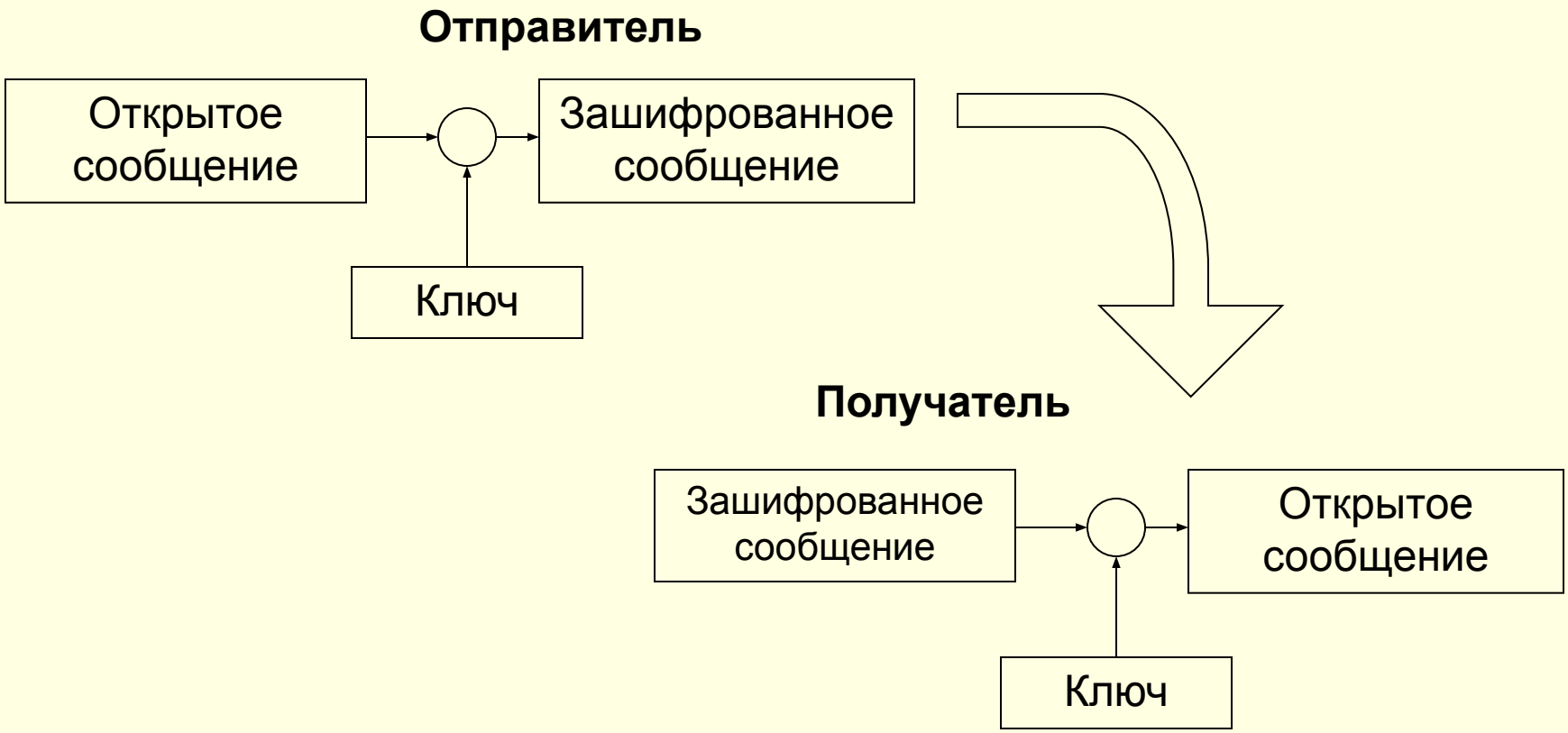
- При проектировании ИС можно выделить следующие методологии построения ИС:
  - Иерархический метод разработки;
  - Исследование корректности и верификации.
- Иерархический метод разработки на основе принципа абстракции предполагает ведение разработки двумя путями:
  - «Снизу-вверх» - проектирование от аппаратуры к виртуальной машине;
  - «сверху - вниз» - проектирование от виртуальной машины, представляющей ИС, с требуемыми свойствами, и последовательно разрабатываются слои виртуальной системы вплоть до аппаратуры.
- Структурный принцип
- Принцип модульного проектирования заключается в разделении программ на функционально самостоятельные части, обеспечивающие заменяемость, кодификацию и т.д.

Системы криптографической защиты информации

- Задача средств криптографической защиты информации — преобразование информационных объектов с помощью некоторого обратимого математического алгоритма.
- Процесс **шифрования** использует в качестве входных параметров объект – открытый текст и объект – ключ, а результат преобразования — объект – зашифрованный текст. При **дешифровании** выполняется обратный процесс.
- Криптографическому методу в ИС соответствует некоторый специальный алгоритм. При выполнении данного алгоритма используется уникальное числовое значение – **ключ**.
- Знание ключа позволяет выполнить обратное преобразование и получить открытое сообщения.
- Стойкость криптографической системы определяется используемыми алгоритмами и степенью секретности ключа.

Криптографические средства защиты данных

- Для обеспечения защиты информации в распределенных информационных системах активно применяются криптографические средства защиты информации.
- Сущность криптографических методов заключается в следующем:



Использование средств криптографической защиты для предотвращения угроз ИБ

- **Обеспечение конфиденциальности данных**. Использование криптографических алгоритмов позволяет предотвратить утечку информации. Отсутствие ключа у «злоумышленника» не позволяет раскрыть зашифрованную информацию;
- **Обеспечение целостности данных**. Использование алгоритмов несимметричного шифрования и хэширования делает возможным создание способа контроля целостности информации.
- **Электронная цифровая подпись.** Позволяет решить задачу отказа от информации.
- **Обеспечение аутентификации**. Криптографические методы используются в различных схемах аутентификации в распределенных системах (Kerberos, S/Key и др.).

Требования к системам криптографической защиты

- ***Криптографические требования***
  - Эффективность применения злоумышленником определяется **средней долей дешифрованной информации**, являющейся средним значением отношения количества дешифрованной информации к общему количеству шифрованной информации, подлежащей дешифрованию, и трудоемкостью дешифрования единицы информации, измеряемой Q числом элементарных опробований.
  - Под **элементарными опробованиями** понимается операция над двумя n-разрядными двоичными числами. При реализации алгоритма дешифрования может быть использован гипотетический вычислитель, объем памяти которого не превышает M двоичных разрядов. За одно обращение к памяти может быть записано по некоторому адресу или извлечено не более n бит информации. Обращение к памяти по трудоемкости приравнивается к элементарному опробованию.
  - За единицу информации принимается общий объем информации обработанной на одном средстве криптографической защиты в течении единицы времени. Атака злоумышленника является успешной, если объем полученной открытой информации больше некоторого заданного объема V.

Требования к системам криптографической защиты

- ***Требования надежности***.
  - Средства защиты должны обеспечивать заданный уровень надежности применяемых криптографических преобразований информации, определяемый значением допустимой вероятности неисправностей или сбоев, приводящих к получению злоумышленником дополнительной информации о криптографических преобразованиях.
  - Ремонт и сервисное обслуживание средств криптографической защиты не должно приводить к ухудшению свойств средств в части параметров надежности.

Требования к системам криптографической защиты

- ***Требование по защите от несанкционированного доступа для средств криптографической информации в составе информационных систем.***
- В автоматизированных информационных системах, для которых реализованы программные или аппаратные средства криптографических защиты информации, при хранении и обработке информации должны быть предусмотрены следующие основные механизмы защиты:
  - идентификация и аутентификация пользователей и субъектов доступа;
  - управление доступом;
  - обеспечения целостности;
  - регистрация и учет.

Требования к системам криптографической защиты

- ***Требование по защите от несанкционированного доступа для средств криптографической информации в составе информационных систем.***
- В автоматизированных информационных системах, для которых реализованы программные или аппаратные средства криптографических защиты информации, при хранении и обработке информации должны быть предусмотрены следующие основные механизмы защиты:
  - идентификация и аутентификация пользователей и субъектов доступа;
  - управление доступом;
  - обеспечения целостности;
  - регистрация и учет.

Требования к системам криптографической защиты

- ***Требования к средствам разработки, изготовления и изготовления и функционирования средств криптографической защиты информации.***
- Аппаратные и программные средства, на которых ведется разработка систем криптографической защиты информации, не должны содержать явных или скрытых функциональных возможностей, позволяющих:
  - модифицировать или изменять алгоритм работы средств защиты информации в процессе их разработки, изготовления и эксплуатации;
  - модифицировать или изменять информационные или управляющие потоки, связанные с функционированием средств;
  - осуществлять доступ посторонних лиц к ключам идентификационной и аутентификационной информации;
  - получать доступ к конфиденциальной информации средств криптографической защиты информации.