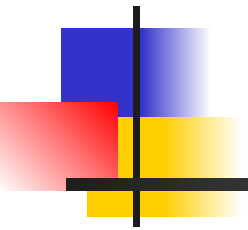

Информационная безопасность

Лекция

Законодательный уровень обеспечения ИБ

Меры законодательного уровня ИБ

- Меры законодательного уровня обеспечивают правовую поддержку мероприятий информационной безопасности. Выделяют две группы мер:
  - Меры, направленные на создание и поддержание в обществе негативного отношения к нарушениям и нарушителям информационной безопасности;
  - Направляющие и координирующие меры, способствующие повышению уровня знаний в области информационной безопасности, помогающие в разработке и распространении средств обеспечения безопасности;

Правовые акты общего назначения

- Основной закон Российской Федерации – Конституция. Статьи Конституции закрепляют ряд прав граждан на защиту и получение информации:
  - Ст. 24 – устанавливает право граждан на ознакомление с документами и нормативными актами, затрагивающими права и свободы;
  - Ст. 41 – гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья граждан, ст. 42 – право на получение информации о состоянии окружающей среды
  - Ст. 23 – гарантирует право на личную и семейную тайну
  - Ст. 29 – право искать, получать, производить и распространять информацию любым законным способом

Правовые акты общего назначения

- В Гражданском кодексе определяются понятия как банковская, коммерческая и служебная тайна:
  - Ст. 139 определяет, что для защиты информации, имеющей коммерческую ценность, ее обладатель имеет законные права по охране ее конфиденциальности.

Правовые акты общего назначения

- В Уголовном кодексе введен раздел, посвященный преступлениям в компьютерной сфере:
  - Ст. 272 – неправомерный доступ
  - Ст. 273 – создание, использование и распространение вредоносных программ для ЭВМ
  - Ст. 274 – нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сетей
- Статья 138 УК РФ предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений;
- Статья 183 УК РФ направлена на обеспечение защиты коммерческой и банковской тайны.

Закон «Об информации, информатизации и защите информации»

- Закон №24-ФЗ (принят 20.02.1995) является одним из основополагающих законов в области информационной безопасности.
- В законе юридически определены важные понятия, такие как **информация, документированная информация, информационная система, конфиденциальная информация, пользователь информации** и т.д.
- В законе выделены следующие цели защиты информации:
  - Предотвращение утечки, хищения, утраты, искажения информации
  - Предотвращения угроз безопасности личности, общества, государства
  - Предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима документированной информации
  - Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных
  - Сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством
  - Обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем

Закон «Об информации, информатизации и защите информации»

- В законе определены задачи защиты информации (прежде всего конфиденциальности данных):
  - «Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу»
- В качестве мер по обеспечению защиты информации в законе устанавливаются:
  - **лицензирование** организаций, занимающихся проектированием, производством средств защиты информации;
  - **сертификация** продуктов и услуг в области защиты информации.

Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ

О персональных данных

- Ст. 2. **Цель настоящего Федерального закона определяет** Цель обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.
- Ст. 8. С письменного согласия субъекта данные могут включаться фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные данных, которые могут быть в любое время исключены из общедоступных источников по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.
- Ст. 10. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается

Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ О персональных данных

- Ст. 14. Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных
- Ст.19. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Закон «О лицензировании отдельных видов деятельности»

- Закон №128-ФЗ от 8.08.2001 устанавливает требование к обязательному лицензированию некоторых видов деятельности, в том числе, относящихся к информационной безопасности:
  - Распространение шифровальных (криптографических) средств;
  - Техническое обслуживание шифровальных средств;
  - Предоставление услуг в области шифрования информации;
  - Разработка и производство шифровальных средств, защищенных с их помощью информационных систем и телекоммуникационных систем
  - Выдача сертификатов ключей ЭЦП, регистрация владельцев ЭЦП
  - Выявление электронных устройств, предназначенных для негласного получения информации
  - Разработка и производство средств защиты конфиденциальной информации
  - Техническая защита конфиденциальной информации

Закон «О лицензировании отдельных видов деятельности»

- В соответствии со статьей 1, действие данного закона не распространяется на следующие виды деятельности:
  - Деятельность, связанная с защитой государственной тайны;
  - Деятельность в области связи;
  - Образовательная деятельность.
- Основными лицензирующими органами в области защиты информации являются ФАПСИ (сейчас функции переданы ФСБ) и Гостехкомиссия РФ.
- Криптография и связанные с ней мероприятия лицензируются ФАПСИ.
- Гостехкомиссия лицензирует деятельность по защите конфиденциальной информации.
- Ввоз и вывоз средств криптографической защиты и нормативно-технической документации к ней осуществляется исключительно на основании лицензии МЭРТ, выданной на основании решения ФАПСИ.

Закон №1-ФЗ «Об электронной цифровой подписи»

- Закон «Об электронной цифровой подписи» обеспечивает правовые условия использования электронной цифровой подписи в электронных документах. Действие данного закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок.
- ЭЦП равнозначна собственноручной подписи при соблюдении следующих условий:
  - Сертификат подписи, относящийся к ЭЦП, не утратил силы на момент подписания документа;
  - Подтверждена подлинность ЭЦП в электронном документе;
  - ЭЦП используется в соответствии со сведениями, указанными в сертификате ключа 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 об ЭЦП

- **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);

Основные понятия закона об ЭЦП

- **средства электронной цифровой подписи** - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной;
- **сертификат средств электронной цифровой подписи –** документ на бумажном носителе, выданный в соответствии с правилами сертификации;
- **закрытый ключ электронной цифровой подписи –** уникальная последовательность символов, известная владельцу сертификата ключа подписи;
- **открытый ключ электронной цифровой подписи**;
- **сертификат ключа подписи -** документ на бумажном носителе или в электронном виде, включающие открытый ключ ЭЦП;
- **подтверждение подлинности электронной цифровой подписи в электронном документе** – положительный результат проверки;
- **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 –** ИС, доступная для использования всем физическим и юридическим лицам;
- **корпоративная информационная система –** ИС, пользователями которой может быть ограниченный круг лиц.

Сертификат ключа электронной цифровой подписи

- По закону сертификат ключа подписи включает в себя:
  - Уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
  - Фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца;
  - Открытый ключ ЭЦП;
  - Наименование средств ЭЦП, с которыми используется данный открытый ключ ЭЦП;
  - Наименование и местонахождение удостоверяющего центра, выдавшего сертификат ключа подписи;
  - Сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

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.

Оценочные стандарты в области информационной безопасности

- Оценочные стандарты направлены на классификацию информационных систем и средств защиты по требованиям безопасности.
- Первым оценочным стандартом, получившим широкое распространение, стал стандарт Министерство обороны США «Критерии оценки доверенных компьютерных систем» («Оранжевая книга») – 1983 г.
- В данном стандарте рассматриваются вопросы управления доступа к данным (т.е. обеспечение конфиденциальности и целостности информации).
- Степень доверия оценивается по двум критериям:
  - **Политика безопасности** – набор правил, определяющих как обрабатывается, защищается и распространяется информация
  - **Уровень гарантированности** – меры доверия, которая может быть оказана архитектуре и реализации ИС.

Положения «Оранжевой книги»

- В «Оранжевой книге» определены три категории требований безопасности:
  - **Политика безопасности**:
    - Система должна поддерживать точно определенную политику безопасности. Возможность доступа субъектов к объектам должна определяться на основании их идентификации и набора правил управления доступа;
    - С объектами должны быть ассоциированы метки безопасности, используемые в качестве исходной информации для процедур контроля.
  - **Подотчетность**:
    - Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификации (аутентификация) и правил разграничения доступа.
    - Для определения степени ответственности пользователей за действия в системе, все происходящие события должны отслеживаться и регистрироваться в защищенном протоколе. Система регистрации должна осуществлять анализ общего потока событий и выделять те события, которые оказывают влияние на безопасность.

Положения «Оранжевой книги»

- В «Оранжевой книге» определены три категории требований безопасности:
  - **Гарантии**:
    - Средства защиты должны содержать независимые аппаратные и/или программные компоненты, обеспечивающие работоспособность функций защиты. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.
    - Все средства защиты должны быть защищены от несанкционированного вмешательства и отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты.

Классы защищенности компьютерных систем по «Оранжевой книге»

- «Оранжевая книга» предусматривает 4 группы критериев, соответствующие различной степени защищенности: от минимальной (группа D) до формально доказанной (группа A). Каждая группа содержит по одному или несколько классов. Уровень защищенности возрастает от группы D к группе A, а внутри группы с увеличением класса:
  - Группа D. Минимальная защита.
  - Группа C. Дискреционная защита.
  - Группа B. Мандатное управление доступом.
  - Группа A. Верифицированная защита.

Структура требований «Оранжевой книги»

- В Оранжевой книге вводятся три категории требований безопасности:
  - Политика безопасности
  - Аудит
  - Корректность
- В рамках этих категорий введены шесть требований: четыре из них направлены на обеспечение безопасности непосредственно, две – на оценку качества средств защиты.

Структура требований «Оранжевой книги»

- **Политика безопасности**
  - **Требование 1. Политика безопасности.** Система должна поддерживать точно определенную политику безопасности. Возможность доступа субъектов к объектам определяется на основе их идентификаторов и набора правил управления доступом.
  - **Требование 2. Метки.** С объектами должны быть ассоциированы метки безопасности, используемые в качестве исходной информации для процедур контроля доступа. Система должна обеспечивать возможность присвоения каждому объекту метку, определяющую степень конфиденциальности и режимы доступа к объекту.

Структура требований «Оранжевой книги»

- **Подотчетность**
  - **Требование 3. Идентификация и аутентификация.** Все объекты должны иметь универсальные идентификаторы. Контроль доступа осуществляется на основе идентификации субъектов и объектов и правил разграничения. Средства идентификации и аутентификации должны быть защищены от НСД.
  - **Требование 4. Регистрация и учет**. Для определения ответственности пользователей, все происходящие в системе события, имеющие значение для безопасности, должны отслеживаться и регистрироваться в защищенном протоколе.

Структура требований «Оранжевой книги»

- **Гарантии (корректность)**
  - **Требование 5. Контроль корректности функционирования средств защиты.** Средства защиты должны содержать независимые аппаратные или программные компоненты, обеспечивающие работоспособность функций защиты. Основной принцип контроля корректности состоит в том, что средства контроля независимы от средств защиты.
  - **Требование 6. Непрерывность защиты.** Все средства должны быть защищены от несанкционированного вмешательства или отключения. Данное свойство должно соблюдаться в любом режиме функционирования системы защиты и компьютерной системы в целом.

Механизмы безопасности «Оранжевой книги»

- Политика безопасности должна включать следующие элементы:
  - **Произвольное управление доступом** – метод разграничения доступа к объектам, основанный на учете личности субъекта;
  - **Безопасность повторного использования объектов** – средство управления доступом, предохраняющее от случайного или преднамеренного извлечения информации из областей оперативной или дисковой памяти;
  - **Метки безопасности** – специальные идентификаторы определяющие уровни секретности объектов и субъектов;
  - **Принудительное управление доступом** – управление доступом к объектам основанное на сопоставлении меток безопасности субъектов и объектов.

Классы безопасности «Оранжевой книги»

- Различие между классами безопасности вычислительных систем в «Оранжевой книги» коротко может быть сформулировано в терминах управления доступом:
  - Уровень С – произвольное управление доступом;
  - Уровень В – принудительное управление доступом;
  - Уровень А – верификационное управление доступом.

Гарантированность безопасности

- «Оранжевая книга» рассматривает два вида гарантированности – операционная и технологическая.
- **Операционная гарантированность** относится к архитектурным решениям и включает проверку следующих элементов:
  - Архитектура системы;
  - Целостность системы;
  - Проверка скрытых каналов передачи информации;
  - Доверенное администрирование;
  - Доверенное восстановление после сбоев.

Гарантированность безопасности

- Технологическая гарантированность относится к методам построения и сопровождения системы. Она должна охватывать весь жизненный цикл системы, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения.
- Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы исключить утечку информации и «закладки» в системе.

Руководящие документы Гостехкомиссии РФ

- Показатели защищенности средств вычислительной техники (СВТ) от несанкционированного доступа (НСД):
  - В руководящих документах ГТК устанавливается классификация СВТ по уровню защищенности от НСД. Показатели защищенности содержат требования защищенности СВТ от НСД к информации. Конкретные перечни показателей определяют классы защищенности и описываются совокупностью требований.
  - Установлено семь классов защищенности СВТ от НСД. Самый низкий класс – седьмой, самый высокий – первый.

Руководящие документы Гостехкомиссии РФ

- Классы защищенности автоматизированных систем:
  - Установлено девять классов защищенности АС от НСД, распределенных по трем группам. Каждый класс отвечает совокупностью требований к средствам защиты. В пределах группы соблюдается иерархия классов защищенности АС.
  - Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС. В группе два класса – 3Б и 3А.
  - Вторая группа включает АС, в которых пользователи имеют одинаковые полномочия доступа ко всей информации, обрабатываемой и хранимой в АС на носителях разного уровня конфиденциальности. В группе два класса – 2Б и 2А.
  - Первая группа включает многопользовательские АС, где одновременно обрабатывается и хранится информация разных уровней конфиденциальности. Различные пользователи имеют различные права. В группе пять классов – 1Д, 1Г, 1В, 1Б, 1А.
  - При выполнении классификации рассматриваются подсистемы защиты и требования к ним:
    - Подсистема управления доступом
    - Подсистема регистрации и учета
    - Криптографическая подсистема
    - Подсистема обеспечения целостности

Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»

- Стандарт ISO/IEC 15408 является международным оценочным стандартом в области информационной безопасности. Выпущен в 1999 г. Часто для его обозначения используется именование «Общие критерии».
- «Общие критерии» являются метастандартом, определяющим инструменты для оценки безопасности информационных систем и порядок их использования.
- В отличие от «Оранжевой книги» и других подобных стандартов, Общие критерии не содержат предопределенных классов безопасности. Данные классы могут быть построены для конкретной организации или информационной системы.

Виды требований информационной безопасности

- В данном стандарте введены два основных вида требований безопасности:
  - **Функциональные требования**, соответствующие активному аспекту защиты и предъявляемые к функциям безопасности и реализующим их механизмам.
  - **Требования доверия**, соответствующие пассивному аспекту защиты, предъявляемые к технологии и процессу разработки и эксплуатации ИС.
- Требования безопасности предъявляются для определенного программно-аппаратного продукта, а их выполнение проверяется с целью оценки уровня информационной безопасности.

Угрозы информационной безопасности

- Общие критерии рассматривают объект оценки в контексте некоторой среды безопасности, характеризующейся определенными *условиями* и *угрозами.*
- Для характеристики угрозы информационной безопасности используются следующие параметры:
  - Источник угрозы;
  - Метод воздействия на объект оценки;
  - Уязвимости, которые могут быть использованы;
  - Ресурсы, которые могут пострадать от реализации.

Профиль защиты

- Одним из основных нормативных документов, определяемых в Общих критериях является профиль защиты.
- **Профиль защиты** – документ, включающий в себя типовой набор требований, которым должны удовлетворять системы определенного класса.
- **Задание по безопасности (проект защиты)** – содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей.

Функциональные требования

- Функциональные требования сгруппированы в Общих критериях на основе выполнения определенной роли.
- Всего в Общих критериях определено 11 функциональных классов, 66 семейств и 135 компонентов.
- Классы функциональных требований:
  - Идентификация и аутентификация
  - Защита данных пользователя
  - Защита функций безопасности (относится к целостности и контролю сервисов и механизмов безопасности)
  - Управление безопасностью (требования к управлению атрибутами и параметрами безопасности)
  - Аудит безопасности
  - Доступ к объекту оценки
  - Приватность (защита пользователя от раскрытия и использования его идентификационных данных)
  - Использование ресурсов (требование доступности информации)
  - Криптографическая поддержка
  - Связь (аутентификация сторон при обмене данными)
  - Доверенный маршрут/канал (для связи с сервисами безопасности)

Требования доверия безопасности

- Установление доверия безопасности основывается на исследовании объекта оценки.
- Всего определено 10 классов, 44 семейства и 93 компонента требований доверия.
- Классы требований доверия безопасности:
  - Требования к разработке системы (поэтапная детализация функций безопасности)
  - Поддержка жизненного цикла (требование к модели жизненного цикла)
  - Тестирование
  - Оценка уязвимостей (включая оценку стойкости функций безопасности)
  - Поставка и эксплуатация
  - Управление конфигурацией
  - Руководства (требования к эксплуатационной документации)
  - Поддержка доверия
  - Оценка профиля защиты
  - Оценка задания на безопасность