текст - комментарии Кабанова

### 1. Модели ценности информации: аддитивная модель, порядковая шкала.

(Википедия)

Аддитивная модель, порядковая шкала

**Аддитивная модель**:

Предположим, что имеется информация, которая представлена в виде конечного множества элементов (объектов), и задача заключается в оценке данной информации в денежном эквиваленте. При использовании аддитивной модели определение ценности базируется на экспертных оценках компонент данной информации, и при объективности денежных оценок её компонент подсчитывается искомая величина — их сумма в денежном эквиваленте. Основная проблема заключается в том, что количественная оценка компонент информации часто оценивается необъективно, даже при её оценке высококвалифицированными специалистами — причина заключается в неоднородности компонент информации в целом. Для решения этой проблемы принято использовать иерархическую относительную шкалу, которая представляет собой линейный порядок, с помощью которого сравниваются отдельные компоненты защищаемой информации по ценности одна относительно другой. Случай единой шкалы равносилен тому, что все компоненты, имеющие равную порядковую оценку, равноценны одна относительно другой.

Т.е. Пусть даны n объектов (элементов из которых состоит информация): O1, O2, . . . , On оценка производится по k-балльной шкале; результат оценки экспертами — вектор ценностей данных объектов для информации в целом: {a1, a2, ..., an}.

Исходя из этого, вычисляется стоимость одного балла для каждого объекта ti=Oi/ai ден.ед. Тогда сумма стоимостей компонент даёт сумму — стоимость всей информации T = t1 + … + tn.

Данный способ подсчета позволяет правильно соизмерить стоимость всей информации исходя из информации об ценности и стоимости ее компонент. А также позволяет решить обратную задачу – узнать стоимость компонента информации зная цену информации и оценку важности ее компонент

**Порядковая шкала**

Существуют случаи, когда не имеется необходимости или возможности установки соответствия ценности информации в денежных единицах (например, информация личного характера, военная или политическая информация, оценка которой в денежном эквиваленте может быть неразумной), но при этом может иметь смысл сравнительная оценка отдельных информационных компонент одной компоненты относительно другой. В качестве примера можно рассмотреть ситуацию в государственных структурах, где информация разбивается по грифам секретности. Чем выше класс грифа, тем большую ценность имеет защищаемая информация, в связи с чем по отношению к ней применяются более высокие требования по её защите от несанкционированного доступа.

Недостатком такой модели является то, что не всегда имеется возможность сравнить два компонента в принципе.

### 2. Классификация угроз безопасности информации. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров КС.

Кратко, тезисно

Классификация угроз информационной безопасности компьютерных систем может быть проведена по ряду базовых признаков.

1. По природе возникновения.
   1. Естественные угрозы, т.е. угрозы, вызванные воздействиями на КС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.
   2. Искусственные угрозы, т.е. угрозы, вызванные деятельностью человека.
2. По степени преднамеренности проявления.
   1. Случайные угрозы.
   2. Преднамеренные угрозы.
3. По непосредственному источнику угроз.
   1. Угрозы, непосредственным источником которых является природная среда (стихийные бедствия, магнитные бури, радиоактивное излучение и т.п.).
   2. Угрозы, непосредственным источником которых является человек.
   3. Угрозы, непосредственным источником которых являются санкционированные программно-аппаратные средства.
4. Угрозы, непосредственным источником которых являются несанкционированные программноаппаратные средства.
5. По положению источника угроз.
   1. Угрозы, источник которых расположен вне контролируемой зоны, территории (помещения), на которой находится КС.
6. Угрозы, источник которых расположен в пределах контролируемой зоны, территории (помещения), на которой находится КС.
7. Угрозы, источник которых имеет доступ к периферийным устройствам КС (терминалам).
8. Угрозы, источник которых непосредственно расположен в КС и связан либо с некорректным использованием ресурсов КС, либо с количественной или качественной недостаточностью этих ресурсов, которая была изначально заложена на стадии проектирования компьютерной системы.
9. По степени зависимости от активности КС.
   1. Угрозы, проявляемые независимо от активности КС, например, хищение носителей информации (магнитных дисков, лент, микросхем памяти и др.).
   2. Угрозы, которые могут проявляться только в процессе автоматизированной обработки данных, например, угрозы распространения программных вирусов.
10. По степени воздействия на КС.
    1. Пассивные угрозы, которые ничего не меняют в структуре и функциональной организации КС, например, угроза копирования данных.
    2. Активные угрозы, при реализации которых вносятся изменения в структурную и функциональную организацию КС, например, угроза внедрения аппаратных и программных спецвложений.
11. По этапам доступа пользователей или программ к ресурсам КС.
    1. Угрозы, которые могут проявляться на этапе доступа к ресурсам КС.
    2. Угрозы, которые после разрешения доступа реализуются в результате несанкционированного или некорректного использования ресурсов КС.
12. По способу доступа к ресурсам КС.
    1. Угрозы, использующие прямой стандартный путь доступа к ресурсам КС с помощью незаконно полученных паролей или путем несанкционированного использования терминалов законных пользователей.
    2. Угрозы, использующие скрытый нестандартный путь доступа к ресурсам КС в обход существующих средств защиты.
13. По текущему месту расположения информации, хранящейся и обрабатываемой в КС.
    1. Угроза доступа к информации на внешних запоминающих устройствах (например, путем копирования данных с жесткого диска).
    2. Угроза доступа к информации в основной памяти (например, путем несанкционированного обращения к памяти).
    3. Угроза доступа к информации, циркулирующей в линиях связи (например, путем незаконного подключения).
    4. Угроза доступа к информации, отображаемой на терминале или печатающем принтере (например, угроза записи отображаемой информации на скрытую видеокамеру).

### 3. Понятие политики безопасности. Политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков.

Просто понятийно. Без целей, без примеров. Без информационных потоков. что такое дискр, мандатная, ролевое управление и изолир программ

Под **политикой безопасности** (ПБ) понимается: ∙

· интегральная (качественная) характеристика, описывающая свойства защищенности информации в компьютерной системе (КС) в заданном пространстве угроз;

· совокупность норм и правил, регламентирующих процесс обработки информации, обеспечивающих защиту от определенного множества угроз и составляющих.

1) **Дискреционная ПБ** - ПБ, основанная на дискреционном управлении доступом (DAC), которое определяется двумя свойствами:

· все субъекты и объекты должны быть идентифицированы;

· права доступа субъекта к объекту системы определяются на основании некоторого внешнего по отношению к системе правила.

2) **Мандатная ПБ** - ПБ, основанная на мандатном управлении доступом (MAC), которое подразумевает, что:

· все субъекты и объекты системы должны быть однозначно идентифицированы;

· задан линейно упорядоченный набор меток секретности;

· каждому объекту системы присвоена метка секретности, определяющая ценность содержащейся в нем информации - его уровень секретности в АС;

· каждому субъекту системы присвоена метка секретности, определяющая уровень доверия к нему в АС - максимальное значение метки секретности объектов, к которым субъект имеет доступ;

· метка секретности субъекта называется его уровнем доступа.

3) **Ролевое разграничение доступа (РРД)** представляет собой развитие политики дискреционного разграничения доступа; при этом права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли. Роль является совокупностью прав доступа на объекты системы.

4) **ПБ изолированной программной среды (ИПС)** - ПБ, которая реализуется путем изоляции субъектов системы друг от друга и путем контроля порождения новых субъектов таким образом, чтобы в системе могли активизироваться только субъекты из предопределенного списка.

### 4. Критерии безопасности компьютерных систем министерства обороны США («Оранжевая книга»).

Достоинства/недостатки, о каких системах (доверенных) речь, в рамках данного стандарта оценивается лишь степень доверия. Монитор обращений. Указать, что подразделяются на классы.

**Описание:**Критерии оценки доверенных компьютерных систем — стандарт Минобороны США, устанавливающий условия для оценки эффективности средств компьютерной безопасности, содержащихся в компьютерной системе. Первый в истории общедоступный оценочный стандарт в области ИБ.

Данный стандарт относится к оценочным стандартам (классификация информационных систем и средств защиты) и речь в нём идёт не о безопасных, а о **доверенных системах** - система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа. Каких-либо абсолютных систем (в том числе и безопасных) не существует. Поэтому и было предложено оценивать лишь степень доверия, которое можно оказать той или иной системе.

**Рассматриваются:**

1. Политики безопасности: мандатная (обязательные правила управления доступом напрямую, основанные на индивидуальном разрешении) и дискреционная (непротиворечивый набор правил для управления и ограничения доступа тем, кто хочет получить определенную информацию).
2. Подотчетности: аутентификация (распознавание пользователя), авторизация (проверка на доступ к информации) и аудит (информация должна избирательно храниться и защищаться).
3. Гарантии – механизмы гарантий и гарантии непрерывной защиты. Механизмы включают в себя операционную гарантию (уверенность в том, что реализация системы обеспечивает осуществление принятой стратегии защиты) и гарантия 1 2 жизненного цикла (уверенность в том, что система разработана и поддерживается в соответствии с формализованными и жёстко контролируемыми критериями).

**Классы защищенности в стандарте такие:**

1. группа D (минимальная защита) – те системы, которые не прошли испытания на более высокие группы;
2. группа C состоит из C1 (избирательная защита безопасности рассчитана на однопользовательские системы, в которых осуществляется совместная обработка данных одного уровня конфиденциальности) и C2 (защита контролируемого доступа, имеет индивидуальные учётные записи, вход возможен через процедуру авторизации, существует журнал контроля доступа к системе);
3. группа B состоит из B1 (меточная защита безопасности ), B2 (структурированная защита и B3 (домены безопасности);
4. группа А1 (проверяемая защита) – объединяет системы, функционально эквивалентные системам класса В3 и не требующие каких-либо дополнительных средств.

**Достоинства и недостатки:**

1. Устаревание, связанное с распространением распределённых вычислительных систем и сетей, особенности которых в «Оранжевой книге» никак не учитываются;
2. Неоправданно далеко отодвинуты такие требования, как извещение о нарушении защиты, конфигурационное управление, безопасный запуск и восстановление после сбоев;
3. Не нашли отражения в «Оранжевой книге» и вопросы обеспечения доступности информации;
4. Явная ориентация на производителя и оценщика, а не на покупателя систем. Стандарт не дает ответ на вопрос, как безопасным образом строить систему, как наращивать отдельные компоненты и конфигурацию в целом;
5. C усложнением систем всё больше стала проявляться принципиальная ограниченность «табличного» подхода к классификации систем по требованиям безопасности, когда система должна быть отнесена к одному из классов защищённости исходя из выполнения фиксированного набора требований к функциональным характеристикам – такой подход не позволяет учесть особенности системы и является недостаточно гибким.

### 5. Европейские критерии.

Что за документ, какие вводятся понятия (система, продукт), что такое объект оценки. Описать гарантированность (затрагивает корректность, эффективность средств безопасности) и показать уровни гарантированности.

**что за документ**:

Европейские критерии безопасности информационных технологий опубликованы от имени органов безопасности 4 стран – Франции, Германии, Нидерландов и Великобритании. Принципиально важной чертой Европейских критериев является отсутствие требований к условиям, в которых должна работать Информационная Система . Организация, запрашивающая сертификационные услуги, формулирует цель оценки, то есть описывает условия, в которых должна работать система, возможные угрозы её безопасности и предоставляемые ею защитные функции. Задача органа сертификации – оценить, насколько корректны и эффективны архитектура и реализация механизмов безопасности в описанных заказчиком условиях. В терминологии «Оранжевой книги» ЕК относятся к гарантированности безопасной работы системы. Требования к политикам безопасности и наличию защитных механизмов не являются составной частью ЕК.

**Система** – конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении.

**Продукт** – это аппаратно-программный «пакет», который можно купить и по своему усмотрению встроить в ту или иную систему.

**Объект оценки** - Из практических соображений важно обеспечить единство критериев оценки продуктов и систем – например, чтобы облегчить оценку систему, составленную из ранее сертифицированных продуктов. По этой причине для систем и продуктов вводится единый термин – объект оценки

**Гарантированность** затрагивает два аспекта – эффективность и корректность средств безопасности.

При проверк**е эффективности** анализируется соответствие между целями, сформулированными для объекта оценки, и имеющимся набором функций безопасности. Т.е, рассматриваются вопросы адекватности функциональности, взаимной согласованности функций, простоты их использования, а также возможные последствия эксплуатации известных слабых мест защиты.

**корректность** средств защиты, которая определяет правильность средств защиты и надежность реализации функций безопасности. При проверке корректности анализируется весь жизненный цикл объекта оценки – от проектирования до эксплуатации и сопровождения.

Кроме того, в понятие **эффективность** входит способность механизмов защиты противостоять прямым атакам. Определяются три градации мощности – базовая, средняя и высокая. Под корректностью понимается правильность реализации функций и механизмов безопасности. В ЕК определяется семь уровней гарантированности корректности – **от Е0 до Е6** .

E0 - Определяет минимальную адекватность.

E1-Анализируется общая архитектура система, а адекватность средств защиты подтверждается функциональным тестированием.

E2 -Уровень Е2 включает требования уровня Е1, а также неформальное описание конкретной реализации, данные функционального тестирования должны быть подсчитаны, ОО должен включать в себя систему управления конфигурацией и одобренную процедуру распространения.

E3 -Уровень Е3 представляет собой уровень Е2 с включением в него оценки исходного кода и\или набросков аппаратных средств соответствующих механизмам безопасности, также данные тестирования этих механизмов должны быть оценены.

E4 -В дополнении к требованиям Е3 должны быть представлены основополагающая формальная модель политики безопасности поддерживающая цель защиты. Функции обеспечения безопасности, дизайн архитектуры и подобный план должны быть указаны в полуформальной форме.

E5 -В дополнении к требованиям уровня Е4 должны быть показаны соответствия исходного кода и\или аппаратных чертежей с подробным планом.

E6-дополнении к требованиям уровня Е5 должны быть формально описаны функции обеспечения безопасности и архитектурный дизайн в соответствии с определённой основополагающей политикой безопасности.

### 6. Федеральные критерии.

Выделенное маркером. Вводится понятие профиля защиты, его состав. Функциональные требования. Ранжируются по уровням по четырем критериям.

**Профиль защиты** -- это нормативный документ, который регламентирует все аспекты безопасности ИТ-продукта в виде требований к его проектированию, технологии разработки и квалификационному анализу.

*Как правило, один профиль защиты описывает несколько близких по структуре и назначению ИТ-продуктов. Основное внимание в профиле защиты уделяется требованиям к составу средств защиты и качеству их реализации, а также к адекватности предполагаемым угрозам безопасности.*

**Профиль защиты состоит** **из следующих пяти разделов**: описание, обоснование, функциональные требования к ИТ-продукту, требования к технологии разработки ИТпродукта, требования к процессу квалификационного аналза ИТ-продукта.

**Описание профиля** содержит классификационную информацию, необходимую для его идентификации в специальной картотеке. Федеральные критерии предлагают поддерживать такую картотеку на общегосударственном уровне.

*Это позволит любой организации воспользоваться созданными ранее профилями защиты непосредственно или использовать их в качестве прототипов при разработке новых.*

**Обоснование** содержит описание среды эксплуатации, предполагаемых угроз безопасности и методов использования ИТ-продукта. Кроме того, этот раздел содержит подробный перечень задач по обеспечению безопасности, решаемых с помощью данного профиля.

Раздел **функциональных требований к ИТ-продукту** содержит описание функциональных возможностей средств защиты ИТ-продукта и определяет условия, в которых обеспечивается безопасность в виде перечня угроз, которым успешно противостоят предложенные средства защиты. Угрозы, лежащие вне этого диапазона, должны быть устранены с помощью дополнительных, не входящих в состав продукта, средств обеспечения безопасности.

Раздел **требований к технологии разработки ИТ-продукта** охватывает все этапы его создания, начиная от разработки проекта и заканчивая вводом готовой системы в эксплуатацию. Раздел содержит требования, как к самому процессу разработки, так и к условиям, в которых она проводится, к используемым технологическим средствам, а также к документированию этого процесса. Выполнение требований этого раздела является непременным условием для проведения квалификационного анализа и сертификации ИТ-продукта.

Раздел **требований к процессу квалификационного анализа ИТ-продукта** регламентирует порядок проведения квалификационного анализа в виде методики исследований и тестирования ИТ-продукта. Объем и глубина требуемых исследований зависят от наиболее вероятных типов угроз, среды применения в планируемой технологии эксплуатации.

**Функциональные требования:**

Функциональные требования ФК разделены на восемь классов и определяют все аспекты функционирования ядра безопасности. Под ядром безопасности понимается совокупность аппаратных, программных и специальных компонент вычислительной системы, реализующих функции защиты и обеспечения безопасности.

Состав и содержание включенных в профиль защиты функциональных требований 8 определяются средой эксплуатации ИТ-продукта. Чтобы обосновать выбор тех или иных требований и не вступать в противоречие с существующими стандартами в области безопасности ИТ-продуктов, функциональные требования приведенные в ФК, ранжируются по уровням с помощью следующих **четырех критериев**: широта сферы применения, степень детализации, функциональный состав средств защиты, обеспечиваемый уровень безопасности.

### 

### 7. Общие критерии оценки безопасности информационных технологий.

Про сертификаты необязательно. Универсальность общих критериев. Центральное звено -- объект оценки. Что такое система, продукт. Среда безопасности в рамках стандарта. Структуризация пространства. Функциональные и требования доверия. Задание по безопасности и функциональные пакеты. Структура стандарта (3 части).

**Информационная Система** – специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации

**Аппаратно-программный Продукт** – совокупность средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы

**Среда безопасности:**

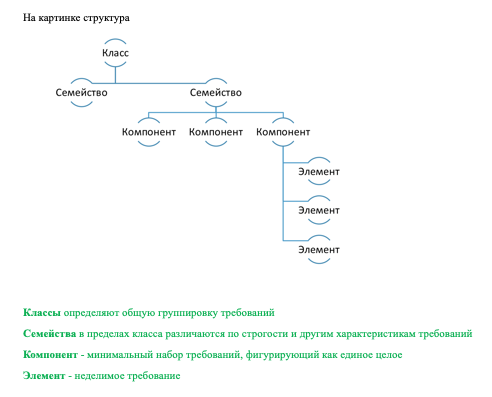
* законодательная среда
* административная среда
* процедурная среда
* программно-техническая среда

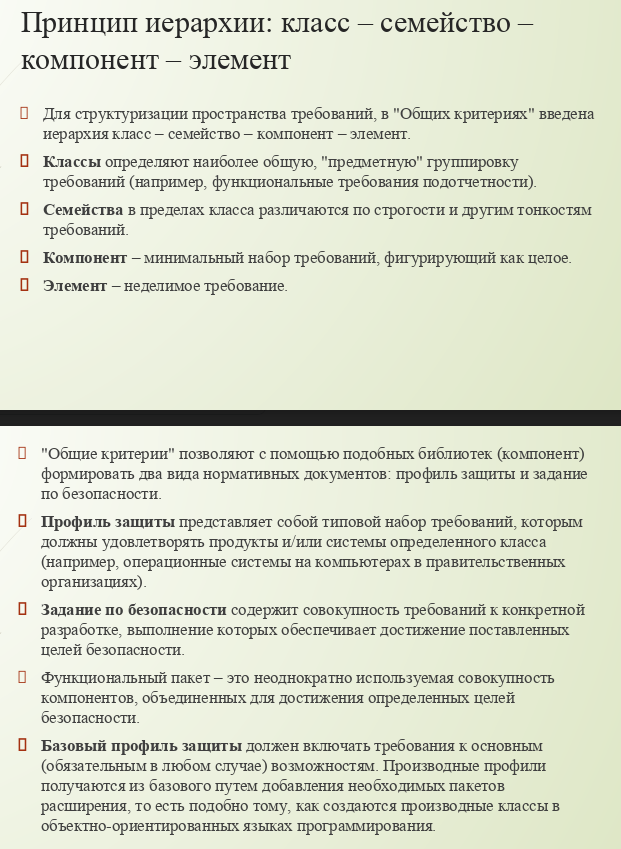
**Аспекты среды ОО:**

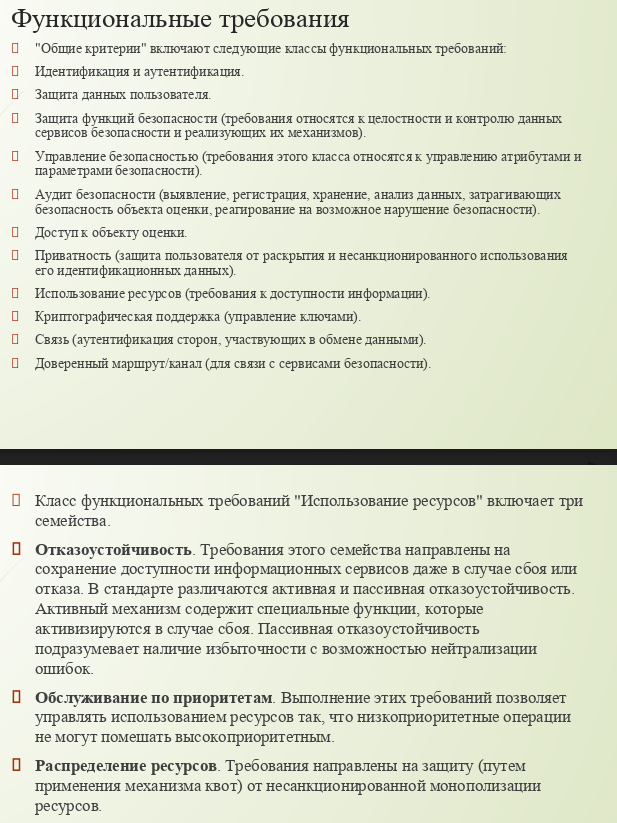
* предположения безопасности
* угрозы безопасности
* положения политик безопасности

**Виды требований безопасности:**

* **Функциональные** – соответствуют активному аспекту защиты
* **Требования доверия** – соответствуют пассивному аспекту защиты (предъявляются к технологии и процессу разработки ПО)







**Функциональные требования:**

11 классов, 66 семейств, 135 компонентов

Классы

**Группа элементарных классов:**

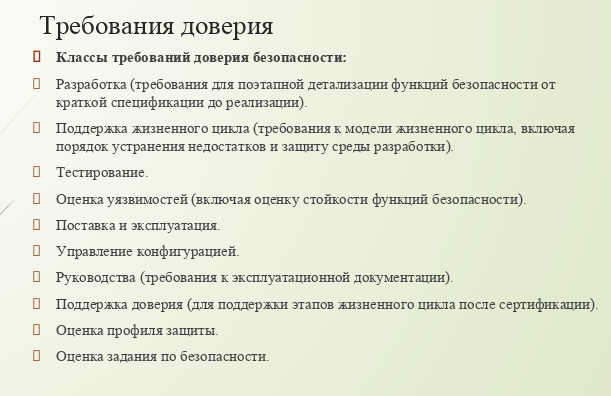
* FAU – аудит безопасности. Класс FAU включает шесть семейств (FAU\_GEN, FAU\_SEL, FAU\_STG, FAU\_SAR, FAU\_SAA и FAU\_ARP), причём каждое семейство может содержать разное число компонентов.Назначение компонентов данного класса следующее. FAU\_GEN — генерация данных аудита безопасности. Содержит два элемента FAU\_GEN.1 (генерация данных аудита) и FAU\_GEN.2 (ассоциация идентификатора пользователя).
* FIA – идентификация/аутентификация
* FRU – использование ресурсов (обеспечение доступности)

**Производные сервисы, реализованные на базе элементарных:**

* FCO — связь (безопасность коммуникаций отправитель-получатель);
* FPR — приватность;
* FDP — защита данных пользователя;
* FPT — защита функций безопасности объекта оценки.

**Классы инфраструктуры объекта оценки:**

* FCS — криптографическая поддержка (обеспечивает управление криптоключами и крипто- операциями);
* FMT — управление безопасностью
* FTA — доступ к объекту оценки (управление сеансами работы пользователей);
* FTP — доверенный маршрут/канал;



**Требования доверия:**

10 классов, 44 семейства, 93 компонента

Группы классов:

Первая группа содержит классы требований, предшествующих разработке и оценке объекта:

Вторая группа связана с этапами жизненного цикла объекта аттестации:

* APE — оценка профиля защиты;
* ASE — оценка задания по безопасности.
* ADV — разработка, проектирование объекта;
* ALC — поддержка жизненного цикла;
* ACM — управление конфигурацией;
* AGD — руководство администратора и пользователя;
* ATE — тестирование;
* AVA — оценка уязвимостей;
* ADO — требования к поставке и эксплуатации;
* АMA — поддержка доверия-требования, применяется после сертификации объекта на соответствие общим критериям.

**Каждое требование(элемент) доверия принадлежит одному из трёх типов:**

1. Элементы действий разработчика(подтверждаются свидетельствами)

2. Элементы представления и содержания свидетельств

3. Элементы действий оценщика



### 8. Руководящие документы ФСТЭК России.

Основные: автоматизированные системы защиты от нсд (три группы), средства вычислит.техники защиты от нсд (классы защищенности, показатели защищенности), межсетевые экраны.

По свд :Класс защищенности, сколько их, иерархичность, как меняется от класса к классу. Выжимка из таблицы с парой показателей

Достоинства/недостатки, перспективы(?)

РД играют роль национальных оценочных стандартов в области ИБ. Все эти документы обязательны в гос. учреждениях.

Приведем некоторые РД:

1. *«Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»*

Документ устанавливает классификацию автоматизированных систем,

подлежащих защите от несанкционированного доступа к информации, и

требования по защите информации в автоматизированных системах

различных классов.

Руководящим документом устанавливает девять классов защищенности

автоматизированной системы от несанкционированного доступа,

распределенных по трем группам. В пределах

каждой группы соблюдается иерархия классов защищенности

автоматизированной системы.

**Третья группа** включает автоматизированные системы, в которых работает один пользователь, допущенный ко всей информации, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

**Вторая группа** включает автоматизированные системы, в которых пользователи имеют одинаковые полномочия доступа ко всей информации, обрабатываемой и хранимой в автоматизированной системе на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

**Первая группа** включает многопользовательские автоматизированные системы, в которых одновременно обрабатывается и хранится информация разных уровней конфиденциальности. Не все пользователи имеют равные права доступа. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

/\*длиннющая табличка, которую вряд ли имеет смысл перерисовывать\*/

1. *«Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».*

Данный документ устанавливает классификацию межсетевых экранов по

уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Установлено семь классов защищенности средств вычислительной техники от несанкционированного доступа к информации. Самый низкий класс – седьмой, самый высокий – первый.



**К недостаткам** Руководящих документов относят:

* ориентацию на противодействие несанкционированному доступу;
* отсутствие требований к адекватности реализации политики безопасности.

Несмотря на указанные недостатки, Руководящие документы заполнили «правовой вакуум» в области стандартов информационной безопасности в Российской Федерации и оперативно решили проблему проектирования и оценки качества защищенных автоматизированных систем. Развитием нормативной базы в этом направлении является разработка «профилей защиты» для различных классов средств вычислительной техники, автоматизированных систем и межсетевых экранов на базе «Общих критериев».

### 9. Рекомендации X.500.

Что такое X500-9. Что такое сертификат, структура, удостоверяющие центры.

Рекомендации семейства X.500 описывают службу директории.

Служба директорий – это сетевой сервис, предоставляющий централизованные средства управления ресурсами автоматизированной системы (пользователи, файлы, устройства и т.д.).

Для доступа к службе директорий используется протокол LDAP.

Директория – комплекс открытых систем, взаимодействующих с целью предоставления услуг службы директорий.

Информация, доступ к которой возможен посредством Директории, называется Информационной базой директории (ИБД).

Записи в ИБД располагаются в виде дерева, называемая Информационным Деревом Директории (ИДД).

Вершинами ИДД являются элементы, хранящие информации об объектах. Природа этих объектов может быть произвольной, главное, чтобы они были идентифицируемы. Элементы директории могут быть составные, объединять подэлементы, содержащие информацию об отдельных аспектах защиты. Каждый элемент состоит из атрибутов, имеющих тип и одно или несколько значений.

Для работы с услугами Директории имеются 2 группы операций: модификации и опроса.

Рекомендация X.501 описывает описывают 3 возможные схемы управления доступом с использованием метод безопасности: базовая, упрощенная и основанная на правилах.

В рекомендации X.509 регламентируются следующие аспекты: сертификаты открытых ключей, сертификаты атрибутов и сервисы аутентификации.

Сертификат открытого ключа – это структура данных, обеспечивающая ассоциирование открытого ключа и его владельца. Надежность ассоциации и подлинность сертификата подтверждается удостоверяющем центром (УЦ).

Сертификаты открытых ключей подразделяется на 2 основных вида: сертификаты

оконечных сущностей и сертификаты УЦ. Оконечные сущности не имеют права заниматься выпуском и аннулированием сертификатом, этим занимается только УЦ. При процессе получения и проверки пользователем A открытого ключа пользователя B, сначала проверяется, выпускает ли УЦ пользователя A сертификаты открытых ключей и для B, если да то процесс завершается (полное доверие к УЦ), если нет, то строится сертификационный маршрут, в котором выпускаются промежуточные сертификаты для промежуточных УЦ, и, таким образом строится маршрут к B. В сертификационном маршруте проверяются согласованность политик безопасности, содержащаяся в сертификатах.

Сертификат атрибутов – это структура данных, снабженная цифровой подписью соответствующего УЦ и связывающая значения некоторых атрибутов с идентификационной информацией держателя сертификата. Сертификаты атрибутов имеют универсальный характер, но в X.509 они используются как основа инфраструктуры управления привилегиями.

В контексте управления привилегиями УЦ называется центром авторизации. Выделяется главный центр авторизации, который может делегировать другим центрам права делегирования и наделение привилегиями.

На протяжение маршрута должно действовать правило доминирования: промежуточный центр не вправе делегировать больше привилегий, чем сам имеет.

В X.509 включены такие сервисы безопасности как простая и сильная аутентификация.

/\* +Следующее, если хватит время \*/

В простой аутентификации данные могут вырабатываться и передаваться 3 способами:

· Имя и пароль в открытом виде

· Имя, пароль, случайное число и временной штамп подаются на вход односторонней функции, результат которой передается получателю для проверки

· К описанному выше результату добавляется случайное число и/или временной штамп и еще раз подвергается односторонней функции (возможно той же самой)

Например, во втором способе происходит примерно следующе:

· Генерируется токен безопасности с помощью данных пользователя и функции

· Токен безопасности и другие данные, кроме пароля, передаются другому пользователю, этот переданный набор есть токен аутентификации.

· Пользователя, принявший токен аутентификации, запрашивает пароль у службы директории (или его локальную копию), реконструирует свой токен безопасности и сравнивает с полученным.

Сильная аутентификация основана на применении ассиметричных методов шифрования, пригодных для генерации электронной подписи. Подлинность пользователя A считается установленной, если он продемонстрирует владение секретным ключом, ассоциированным с хранящимся в сертификате на имя A открытым ключом.

### 10. Рекомендации X.800.

Рекомендации X800 нужны для сопоставление уровням в семиуровневой модели ВОС(взаимодействия открытых систем) и механизмов безопасности со свойствами информации, которые ЦЕЛЕСООБРАЗНО обеспечить на данном уровне.

Уровни и свойства безопасности:



Для реализации функций безопасности могут использоваться следующие ***механизмы защиты*** и их комбинации:

При ***управлении доступом*** могут использоваться следующие виды и источники информации:

· базы данных управления доступом (списки доступа и др.);

· пароли или иная аутентифицирующая информация;

· электронные ключи или иные удостоверения, предъявление которых свидетельствует о наличии прав доступа;

· метки безопасности, ассоциированные с субъектами и объектами доступа;

· время запрашиваемого доступа;

· маршрут запрашиваемого доступа;

· длительность запрашиваемого доступа.

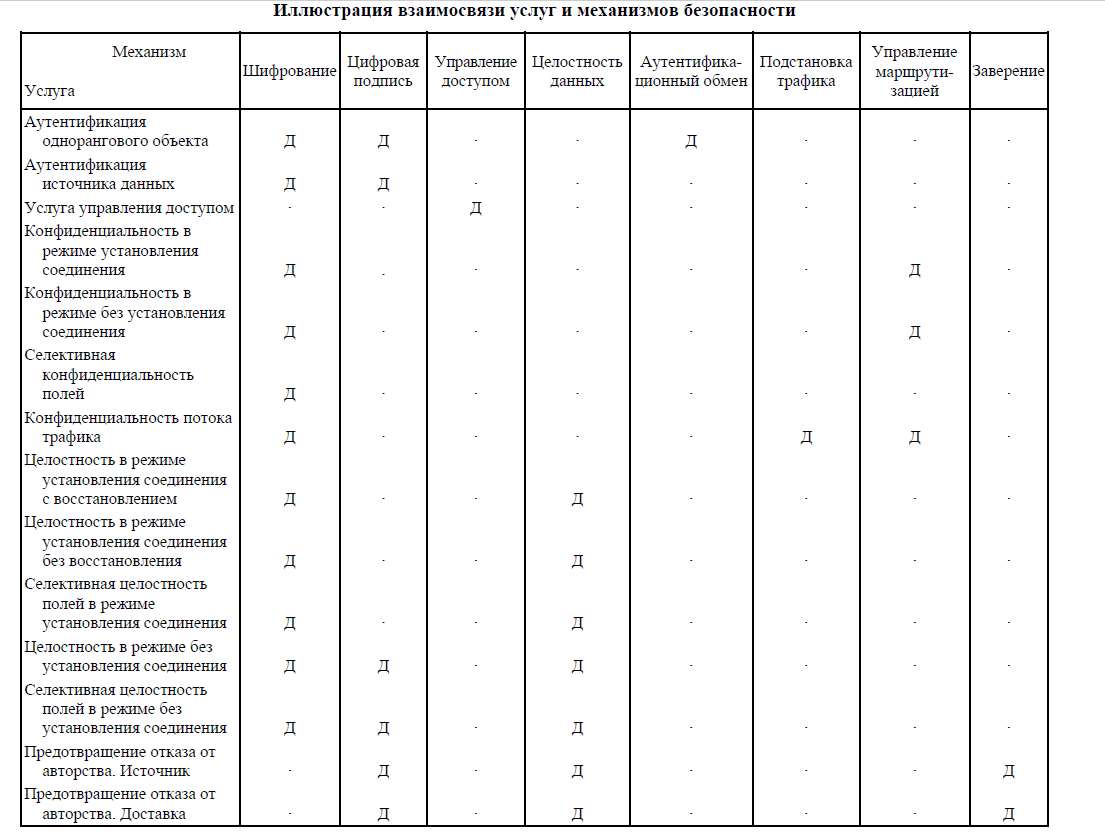
***Механизмы дополнения трафика(подстановка трафика в таблице)*** эффективны только в сочетании со средствами обеспечения конфиденциальности, поскольку в противном случае злоумышленнику будет очевиден фиктивный характер дополнительных сообщений.

***Управление маршрутизацией. Маршруты*** могут быть статическими или динамическими. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять метка безопасности, ассоциированная с передаваемыми данными.

Механизм ***нотаризации(заверение в таблице)*** служит для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателя. Заверение обеспечивается надежной третьей стороной, которая обладает достаточной информацией, чтобы ее заверениям можно было доверять. Обычно нотаризация опирается на механизм цифровой подписи.

***Администрирование средств безопасности()*** включает в себя распространение информации, необходимой для работы функций и механизмов безопасности, а также сбор и анализ информации об их функционировании.

Взаимосвязь свойств(на картинке “Услуга”) и механизмов:



Для чего нужны. табличка с 7-ур. моделью. Показать, на каких уровнях обеспечивается механизм ИБ.

Наиболее экономически целесообразные модели защиты…

### 11. Стандарты серии ISO 27000.

Сказать для чего существует эта линейка стандартов. Что такое серия стандартов, какие осн стандарты входят (27000-1, 2 (базирование на рисках, *последний абзац из материалов*), 5(отвечает за *управление рисками*, структурирует этот процесс, основан на модели pdca(?..)), 35), кратко о них.

Менеджмент информ без. Цикл шухарда деминга. Фокус стандарта.

ISO/IEC 27000 – серия международных стандартов, которая включает стандарты информационной безопасности, опубликованные совместно Международной организацией по стандартизации (International Organization for Standardization, ISO) и Международной электротехнической комиссией (International Electrotechnical Commission, IEC).

Кратко рассмотрим основополагающие стандарты серии ISO/IEC 27000.

Стандарт **ISO/IEC 27001** содержит требования в области информационной безопасности для создания, развития и поддержания системы менеджмента информационной безопасности. В нем собраны описания лучших мировых практик в области менеджмента информационной безопасности.

Основная философия **ISO/IEC 27002** базируется на управлении рисками: выяснить, где находятся риски, а затем систематически обрабатывать их. Стандарт ISO/IEC 27002 предоставляет лучшие практические советы по менеджменту информационной безопасности для тех, кто отвечает за создание, реализацию или обслуживание системы менеджмента информационной безопасности.

Стандарт **ISO/IEC 27005:** «Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности». Описывает процесс управления рисками в системе менеджмента информационной безопасности. Цель стандарта – помочь организациям всех типов лучше управлять информационными рисками.

Основан на модели PDCA:

На этапе:

* **планирования** (Plan) системы менеджмента информационной безопасности осуществляются установление контекста, оценка риска, разработка плана обработки риска и принятие риска;
* **реализации** (Do) системы менеджмента информационной безопасности осуществляются действия по снижению риска до приемлемого уровня в соответствии с планом обработки риска;
* **проверки** (Check) системы менеджмента информационной безопасности осуществляются мониторинг и пересмотр обработки риска по результатам обработки инцидентов и изменений обстоятельств;
* **улучшения** (Act) системы менеджмента информационной безопасности осуществляются любые корректирующие действия по усовершенствованию, включая повторное инициирование процесса управления рисками информационной безопасности.

Стандарт **ISO/IEC 27035** «Информационная технология. Методы обеспечения безопасности. Менеджмент инцидентов информационной безопасности» является руководством по выявлению, регистрации и оценке случаев нарушения безопасности и уязвимостей.

Состоит из двух частей:

* **ISO/IЕС 27035-1** «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Часть 1. Принципы менеджмента инцидентов»;
* **ISO/IЕС 27035-2** «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Часть 2: Руководство по планированию и подготовке реагирования на инцидент».

### 12. Парольные системы.

Требования не надо.

Что такое пароль. Как хранятся пароли, сверки, в открытом виде, как осуществляется аутентификация. Параметры оценки стойкости, формула Андерсена, хранение паролей, передача пароля по сети.

Под **парольной системой** будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многоразовых паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

**Пароль пользователя** – некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно.

Возможны следующие виды хранения паролей:

* в открытом виде (ключ генерируется программно и хранится в системе, обеспечивая возможность ее автоматической перезагрузки);
* в виде сверток (хеширование);
* зашифрованными на некотором ключе.

Про свертки:

Хеширование не обеспечивает защиту от подбора паролей по словарю в случае получения базы данных злоумышленником. При выборе алгоритма хеширования, который будет использован для вычисления сверток паролей, необходимо гарантировать несовпадение значений сверток, полученных на основе различных паролей пользователей. Кроме того, следует предусмотреть механизм, обеспечивающий уникальность сверток в том случае, если два пользователя выбирают одинаковые пароли. Для этого при вычислении каждой свертки обычно используют некоторое количество «случайной» информации, например, выдаваемой генератором псевдослучайных чисел.

Способы аутентификации:

* *по хранимой копии пароля или его свёртке (plaintext-equivalent):*

В первую разновидность способов входят системы аутентификации,

предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Их слабой стороной является то, что получение злоумышленником этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя.

* *по некоторому проверочному значению (verifier-based):*

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации.

* *без непосредственной передачи информации о пароле проверяющей стороне (zero-knowledge):*

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен "троянский конь").

* *с использованием пароля для получения криптографического ключа (cryptographic):*

Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств задействованных в них математических и криптографических преобразований и может быть строго доказана.

**Передача по сети**

В большинстве случаев аутентификация происходит в распределённых системах и связана с передачей по сети информации о параметрах учетных записей пользователей. Если передаваемая по сети в процессе аутентификации информация не защищена надлежащим образом, возникает угроза ее перехвата злоумышленником и использования для нарушения защиты парольной системы. Известно, что многие компьютерные системы позволяют переключать сетевой адаптер в режим прослушивания адресованного другим получателям сетевого трафика в сети, основанной на широковещательной передаче пакетов данных.

Способы передачи паролей по сети:

* в открытом виде
* в зашифрованном виде
* в виде сверток
* без непосредственной передачи информации о пароле («доказательство с нулевым разглашением»)

Виды защиты сетевого трафика:

* физическая защита сети
* оконечное шифрование
* шифрование пакетов

Угрозы безопасности парольной системы:

* перехват и повторное использование информации
* перехват и восстановление паролей
* модификация передаваемой информации с целью введения в заблуждение принимающей стороны
* имитация злоумышленником действий проверяющей стороны для введения в заблуждение пользователя

**Параметры оценки стойкости**

|  |  |
| --- | --- |
| **Параметр** | **Способ определения** |
| Мощность алфавита паролей **A** | Могут варьироваться для для обеспечения заданного значения **S** () |
| Длина пароля **L** |
| Мощность пространства паролей **S** | Вычисляется на основе заданных параметров **P**, **T** или **V.** |
| Скорость подбора паролей **V** | Может быть искусственно увеличена для защиты от данной угрозы. Задается используемым алгоритмом вычисления свертки. Алгоритм, имеющий медленные реализации, повышает стойкость по отношению к данной угрозе. |
| Срок действия пароля (задает промежуток времени, по истечении которого пароль должен быть обязательно сменен) **Т** | Определяется исходя из заданной вероятности **Р**, или полагается заданным для дальнейшего определения **S**. |
| Вероятность подбора пароля в течение его срока действия (подбор продолжается непрерывно в течение всего срока действия пароля) **Р** | Выбирается заранее для дальнейшего определения **S** или **T.** |

ВАЖНО!!! Параметры **S**, **V**, **T** и **P** связаны соотношением:

**Формула Андерсона**

**,**

где:

* k – число опробований в единицу времени;
* T – срок действия пароля (число единиц времени, в течение которого происходит опробование);
* P – вероятность подбора пароля в течение срока его действия;
* S – мощность пространства паролей.

Формулу можно переписать для минут и месяцев:

,

где:

* k – число опробований в минуту;
* M – количество месяцев, в течение которых происходит опробование
* P – вероятность подбора пароля в течение срока его действия
* S – мощность пространства паролей