Лекция 1

3.09.2024

Информация

Свойства информации:

1. *Неограниченное тиражирование*;
2. *Возможность внесения изменений* (целенаправленных или случайных);
3. *Достоверность*;
4. *Полнота*;
5. *Своевременность*;
6. *Субъективная стоимость*;
7. *Идеальность*;
8. *Соотношение себестоимости и рыночной цены*.

Системы защиты:

- СКУД (система управления контроля доступа)
- СОТ (система телеметрии)
- Физические (двери, решетки)

Базовые принципы защиты информации:

- конфиденциальность;
- целостность;
- доступность.

Основные проблемы обладания информацией:

- качество;
- достоверность;
- своевременность;

Предпосылки:

1. Мощность компьютеров увеличивается, квалификация падает.

2. **Безопасность системы определяется самым слабым ее элементом.**
3. 80% потерь и утечек – из-за сотрудников.
4. Любая система строится по принципу «латания дыр».

ИБС:

- безопасность функционирования (БФ);
- защита информации (ЗИ);

Защита информации:

1. Предотвращение утечек и возможных последствий от несанкционированных действий;
2. Обнаружение воздействий, направленных на разрушение системы;
3. Локализация мест воздействия;
4. Ликвидация последствий и восстановление функциональности;

Задача системы защиты решается в сочетании априорных (обнаружение) и апостериорных (ликвидация).

Все современные системы защиты должны учитывать все возможные целенаправленные действия пользователя.

Концептуальная модель информации:

источник информации (ИИ) – люди, документы, отходы и т.д.;

объекты угроз (ОУ) – сведения о составе, состоянии или деятельности;

угрозы (У) – угрозы целостности, конфиденциальности и/или отказа в доступе;

источники угроз (ИУ) – сотрудники, конкуренты, спец органы;

цели угроз (ЦУ) – ознакомление, модификация, уничтожение;

способы доступа (СД) – разглашение, утечка, НСД (несанкционированный доступ);

направления защиты (НЗ) – законодательные, организационные, технические (программно-аппаратные);

способы защиты (СЗ) – упреждение, предотвращение, пресечение, противодействие;

средства защиты (СрЗ) – физические, системные, программные, криптографические;

Угроза безопасности компьютерной системы – потенциально возможное происшествие, преднамеренное или нет, которое может оказать нежелательное воздействие на систему и на хранящуюся или передаваемую в ней информацию.

Уязвимость – некая неудачная характеристика системы, которая делает возможным возникновение угрозы.

Атака – преднамеренное действие, которое заключается в поиске и исправлении уязвимостей.

Виды угроз:

- угроза конфиденциальности (доступ у того, кому он не предназначался);
- угроза целостности;
- угроза отказа в обслуживании;

Угрозы по характеру воздействия:

- целенаправленные (атаки, вирусы и т.д.);
- случайные (сбои);

Взаимосвязь основных понятий, связанных с угрозой

ИСО/МЭК 15408

ИУ – источники угроз

У – угрозы

1. *Оценка имеющихся ресурсов*;
2. *Определение потенциально возможных угроз*;

Специфические характеристики информации:

1. *Статичность* (может ли информация изменяться во времени);
2. *Единица защищаемой информации* (бит, блок, система и т.д.);
3. *Время жизни информации* (как долго информация должна быть закрыта);
4. *Стоимость скрытого нарушения целостности* (выражает убытки, которые могут быть нанесены вследствие несвоевременной ликвидации);
5. *Стоимость ущерба*;

Задачи информационной безопасности:

1. *Секретность* (сводится к тому, чтобы при передаче и хранении информации, чтобы противник, получив доступ к носителю, не смог получить доступ к самой информации);
2. *Идентификация и аутентификация*

   Идентификация + аутентификация = авторизация

   Идентификация – подтверждение личности.

   Аутентификация – подтверждение наличия прав доступа.
3. *Целостность* (задача заключается в том, чтобы утвердить отсутствие модификаций данных или определить их наличие);
4. *Контроль доступа* (совокупность средств и методов, предназначенных для ограничения доступа к ресурсу);
5. *Неотказуемость* (свойство, при котором существуют математические доказательство того, что никто, кроме автора, не может воспроизвести информацию (сигнатура, отпечаток).

Валидация – сверка выставленных требований с необходимыми для достижения определенных целей.

Верификация – подтверждение соответствия конечного продукта неким предопределенным эталонным значениям.

6.09.2024

Электронная подпись (ЭП) решает задачи:

- подтверждение авторства;
- контроль целостности;
- датирование.

В основе ЭП лежат ассиметричные криптоалгоритмы и функции контроля целостности (функция хеширования).

Алгоритмы шифрования делятся на:

- симметричные;
- ассиметричные.

Каждый абонент генерирует себе пару ***взаимозаменяемых*** и ***взаимодополняющих*** (свойства) ключей. Одна половина такого ключа будет считаться открытой, вторая – закрытой. Та часть, которая считается открытой, может быть переслана вашим партнером или выложена в общий доступ, например, на сервер открытых ключей. Таким образом, у каждого абонента сети получается своя пара и открытые ключи тех, с кем он собирается общается. После передачи ключей можно осуществить шифрованную переписку. Тогда абонент шифрует текст на открытом ключе получателя. Абонент Б со своей стороны дешифрует на своей стороне на взаимодополняющей половине (закрытой абонента Б).

А собирается отправить Б подписанный документ.

1. На текст накладывается хеш-функция. Получается ее некий дайджест, отпечаток, хеш-значения.
2. Полученный отпечаток шифруется на своем закрытом элементе. Это и будет ЭП абонента А для текста Т. Т.о в ЭП заложен и механизм контроля целостности, и авторства.
3. Зашифровываем текст с приложенной подписью на открытом чужом ключе – шифрованный и подписанный текст.
4. На своем конце абонент Б дешифрует полученное на дополняющей половине своим закрытым ключом. Получает некий текст и абракадабру. Предполагая, что абра – подпись, ее нужно проверить. Предполагая, что это подпись, дешифруем ее на открытом ключе абонента А и получаем некоторое дешифрованное сообщение. Получили отпечаток. Теперь нужно проверить на целостность. Нужно хешировать, получаем отпечаток и сравниваем то, что дещифровали и посчитали. Если совпало, то все ОК, если нет, то ошиблись.

Лекция 2

Способы и механизмы обеспечения защиты

10.09.2024

Направления защиты:

- Законодательные;
- Информационные;
- Физические;
- Программные (аппаратные).

Законодательные наб

Организационные касаются методов организации допуска на предприятии.

Физические – что-то конкретное (забор, проволока)

Программные (аппаратные) – все, что с программной начинкой

Люди, участвующие в процессе должны подписать соответствующие документы: договор о конфиденциальности, коммерческая тайна.

Существуют системы типа ***черный ящик***.

Технические и программно-технические средства направленны на минимизирование человеческого влияния и обеспечение безопасности.

Метод защиты (способ защиты) – совокупность приемов и операций, реализующих функции защиты (методы шифрования).

Средства защиты – некие устройства или ПО для реализации метода защиты (ПО, обеспечивающее криптоалгоритмы).

Механизм защиты – совокупность средств защиты, функционирующих совместно для выполнения определённой защиты (крипто протокол).

Система обеспечения безопасности данных – совокупность средств и методов защиты.

Основные группы механизмов защиты

Четыре базовые группы:

1. ***Подсистема управления доступом***

   Включает идентификацию и аутентификацию пользователей и ресурсов, и проверку их подлинности.

   А) *биометрия* (статическая (может измениться только от механического воздействия) и динамическая (меняется со временем)). К динамическим относится голос. К статическим относится сетчатка, отпечаток пальца, опознавание по лицу.

   Б) программно-аппаратный комплекс (пропуск, БД)

   В) программные (логин и пароль)

   Требования к системе: надежность, цена.

Ошибки 1-го рода предполагают, что не допустили того, кого нужно; 2-го рода – пустили того, кого не должны.

1.2 Система контроля доступа

А) *Мандатная модель* – всем элементам системы, объектам и субъектам присваиваются определенные метки и уровни безопасности, далее организуется метод по принципу чтения потоков разного уровня (высокому уровню доступа доступны файлы более низкого доступа).

Б) *Дискреционная схема* – набор объектов, набор субъектов и матрица прав доступа.

В) *Ролевые политики* – набор ролей, набор прав и матрица, которая настраивает доступ.

1.3 Управление потоками информации

Уровень конфиденциальности получателя (накопителя) должен быть не ниже уровня конфиденциальности информации (отправителя).

2. ***Подсистема криптографии***

2.1 Шифрование

2.2 Сертификация средств защиты

3. ***Подсистема регистрации и учета.***

3.1 Регистрация входа, выхода, доступа, модификации, создания, удаления объектов

3.2 Учет носителя информации

3.3 Очистка оперативной памяти

3.4 Сигнализация попыток нарушения

4. ***Подсистема контроля целостности***

4.1 Обеспечение целостности программных средств и информации за счет расчета и хранения контрольных сумм.

4.2 Тестирование НСД (несанкционированного доступа)

4.3 Резервное копирование и наличие средств восстановления.

Службы и механизмы обеспечения безопасности

Существует документ архитектуры безопасности открытых систем, который предлагает нам схему взаимодействия служб и механизмов защиты.

Механизмы

1 – механизмы шифрования, являются эл практически всех функций безопасности

2 – механизмы цифровой подписи, обеспечивают услуги опознавания и доказательства

3 – механизмы управления доступа, реализуют контроль доступа, обеспечивая набор прав доступа

4 – механизмы контроля целостности, поддерживают услуги целостности и являются элементами механизма доказательства

5 – механизмы обменной аутентификации (услуги для одноранговых объектов)

6 – механизмы защиты трафика, средства обеспечения конфиденциальности и средства предотвращения анализа трафика

7 – механизмы управления маршрутизацией, используются услугами конфиденциальности

8 – механизмы арбитража, используются для подтверждения характеристик данных, передаваемых объектом

Лекция 3

Теоретические основы информационной безопасности

10.09.2024

Все существующие теоретические разработки делят на 2 принципиальных подхода – ***политика безопасности*** и ***криптография***.

Криптография используется для контроля целостности, идентификации и аутентификации, шифрования, цифровой подписи.

Формальные модели **политик безопасности** предлагают разрабатывать систему на основе базовых принципов, положенных в основу архитектуры безопасности и определяют концепцию ее построения.

Криптография в свою очередь предлагает конкретные способы защиты в виде вышеназванных алгоритмов.

Теория кодирования

Классическая теория кодирования делится на три направления:

1 Помехоустойчивое кодирование (избыточное).

Применяется для обнаружения и исправления ошибок при передаче данных по каналам связи.

2 Примитивное кодирование (безызбыточное)

Используется для преобразования одного алфавита или словаря в другой (шифрование).

3 Экономное кодирование

К ним относятся алгоритмы архивации или сжатия данных.

Темы криптографии

Проблемой защиты информации путем ее преобразования занимается наука ***криптология***. Она делится на два направления: ***криптографию*** и ***криптоанализ***.

Криптография занимается поиском и исследованием математических методов преобразования информации, криптоанализ – исследованием возможности расшифровки без знания секретных элементов.

P – открытый текст

C – закрытый текст

K – ключ

КА – крипто-алгоритм

Функция зашифровывания открытого текста (Ек) дает с

Функция расшифрования - преобразовательный процесс, при котором исходный открытый текст пропускается через крипто-алгоритм с помощью ключа или …

Ключ – информация необходимая для беспрепятственного шифрования и дешифрования.

Ключ выбирается среди значений, принадлежащих множеству значений, которое называется ключевым пространством. Размер ключевого пространства определяется как

2^n,

где n – длина ключа в битах.

В зависимости от логики работ с ключами системы могут быть симметричными (один ключ) и ассиметричными.

Если надежность крипто-алгоритма обеспечивается за счет сохранения в тайне самого алгоритма, то такие алгоритмы называются ограниченными.

Правило Кирхгофа

Все современные крипто системы построены по правилу:

Секретность сообщения определяется только секретностью ключевой информации и не зависит от знания алгоритма, поскольку все алгоритмы, как и сам алгоритм, полагается, известен противнику.

В качестве информации, подлежащей шифрованию и дешифрованию, рассмотрим тексты, построенные на некотором алфавите.

Алфавит – конечное множество используемых для преобразования информации знаков.

Текст – упорядоченный набор эл алфавита

Z2 = (0,1);

Z33 – русский алфавит и пробел;

Z256 – раскладка клавиатуры в ASCII и т д.

Под крипто-системой понимается алгоритм шифрования + множество всех возможных ключей + плюс множество открытых и шифрованных текстов.

Термины распределение ключей и управление ключами относятся к процессам обработки, касающихся к распределению ключей между пользователями.

Электронная подпись – построенное на основании хэш-функции и ассиметричного крипто-алгоритма преобразование исходного документа,

используемое для подтверждения авторства отправителя и целостности сообщения, а также функций датирования и недоказуемости.

Криптостойкость – характеристика шифра, определяющая стойкость к дешифрованию без знания ключа, то есть стойкость к крипто-анализу.

Основными показателями криптостойкости являются: размер ключевого пространства, среднее время, необходимое для криптоанализа, мощность.

Эффективность системы шифрования с целью защиты зависит от ***сохранения в тайне ключа*** и ***криптостойкости шифра***.

Требования к криптосистемам

Процесс криптопреобразований может быть реализован программно или аппаратно. Аппаратный подразумевает установку специальных плат, за счет этого она более дорогая, а производительность выше. Программная реализация значительно дешевле, значительно гибче и проще в использовании, но медленнее.

Требования:

1 Знание алгоритма не должно влиять на надежность защиты.

2 Шифрованное должно поддаваться чтению только при знании ключа.

3 Незначительное изменение ключа должно приводить к значительным изменениям в шифрованном сообщении.

4 Не должно быть простых, легко устанавливаемых зависимостей между последовательностями, используемых в алгоритме ключей.

5 Число операций для расшифровывания информации путем прямого перебора должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров даже с учетом использования распределенных вычислений.

6 Дополнительные биты, вводимые при шифровании, должны быть скрыты в шифрованном сообщении.

7 Алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно приводить к качественному ухудшению самого алгоритма.

Лекция 4

17.09.2024

Классификация криптоалгоритмов

Шифр замены – символ открытого текста заменяется на символ закрытого текста.

1. Простая замена (одноалфавитный шифр)

   Каждая буква открытого текста всегда заменяется на один символ шифрованного текста (шифр Цезаря).
2. Омофонная замена

   Для каждой буквы открытого текста в соответствие ставится несколько вариантов закрытого текста, а их выбор зависит от некоторого конкретного условия (дня недели, даты).
3. Блочная замена

   Замена производится блоками.
4. Многоалфавитная замена

   Состоит из нескольких шифров простой замены, но при этом какой именно из вариантов будет использоваться зависит от местоположения буквы в тексте.
5. Кодовые блокноты

   Каждому слову или предложению заранее предусматривается в соответствие другое слово.

Шифры перестановки – изменение порядка букв в тексте.

Гаммирование – наложение на исходный открытый текст в двоичном виде некой гаммы ключа в двоичном виде.

Генератор псевдослучайных чисел

Стандартный генератор выглядит следующим образом:

$$T_{i+1} = (a * T_i + b)\ mod\ m;$$

a, b – постоянные заранее известные числа;

m – разрядность процессора;

b – нечетное.

Преимущества и недостатки:

1. Простота и быстродействие (для n людей необходимо $\frac{n(n-1)}{2}$ ключей. 2
2. Передача ключа по открытому каналу.

Малая теорема Ферма позволяет определить, является ли число простым или составным.

Для любого простого P и любого целого K при K<P справедливо тождество:

$$K^{P-1}\ mod\ P = 1$$

20.09.2024

Системы идентификации

1 часть

Авторизация = аутентификация + идентификация

1. Биометрическая

   А. Статическая

   Б. Динамическая

      a. Голос

      b. Клавиатурный почерк

- Убираем максимальные ошибки на каждом интервале

- Заложить допустимые отклонения (некоторый % от среднего)

2. Программно-аппаратная
3. Программные (логин и пароль)

2 часть

Доступ к блокноту без знания секретного элемента

Лекция 4

17.09.2024

ГОСТ 28147-89

Имитовставка – цифровой ключ и контрольная комбинация.

Имитозащита – защита от искажения.

Помимо нескольких тесно связанных между собой процедур шифрования, в документе описан один построенный на общих принципах с ними алгоритм выработки имитовставки. Последняя является не чем иным, как криптографической контрольной комбинацией, то есть кодом, вырабатываемым из исходных данных с использованием секретного ключа с целью имитозащиты, или защиты данных от внесения в них несанкционированных изменений.

ГОСТ 28147-89 предусматривает три следующих режима шифрования данных:

- простая замена,
- гаммирование,
- гаммирование с обратной связью,

и один дополнительный режим выработки имитовставки.

08.10.2024

Криптографические преобразования в целях аутентификации и контроля целостности

Базовыми средствами контроля целостности при цифровой передаче данных являются:

- Контрольные суммы;
- Циклические избыточные коды (CRC);
- Хеш-функции;
- Цифровая подпись.

Общий контроль целостности осуществляется путем вычисления некоторых характеристик и сравнения их с эталонными значениями. При этом контрольные характеристики вычисляются при каждом изменении файла по определенному алгоритму.

1. Контрольные суммы

Самый простой и ненадежный метод. Под контрольной суммой понимается значение, рассчитанное путем сложения всех чисел из входных данных. Если сумма входных чисел превышает максимально допустимое значение, заранее заданное для этой величины, то величина контрольной суммы равна остатку от деления итоговой суммы на максимально возможное значение контрольной суммы, увеличенное на единицу.

$$CS = T \ mod \ (Max + 1),$$

где T – итоговая сумма, полученная по входным данным

Max – максимальное значение контрольной суммы, заданное заранее

Пусть документ, в целостности которого надо удостовериться, представляет собой последовательность величин длиной 10 байт, имеет следующий вид:

36 211 163 4 109 192 58 247 47 92 : = T = 1159

Max = 2^8 = 256

CS = 1159 mod 256 = 135.

2. Циклические избыточные коды

Исходная двоичная последовательность представляется в виде полинома $\mathrm{F}(x)(n-1)$, где *n* – число бит в последовательности.

Для выбранного порождающего полинома *F(x)* можно выбрать

$$\mathrm{F}(x) * x^m = G(x) * P(x) \oplus R(x)$$

где *m* – степень порождающего полинома,

G(x) – частное,

R(x) – остаток от деления $\mathrm{F}(x) * x^m$ на $P(x)$

Тогда $\mathrm{F}(x) * x^m \oplus R(x) = G(x) * P(x)$

При контроле целостности информации контролируемая последовательность, сдвинутая на m разрядов, делится на выбранной порождающий полином и запоминается полученный остаток, который называется синдром. Синдром хранится как эталон.

При контроле целостности к полиному контролируемой последовательности добавляется синдром и осуществляется деление на порождающий полином. Если остаток от деления равен 0, то считается, что целостность не нарушена. Обнаруживающая способность метода зависит от степени порождающего полинома и не зависит от длины контролируемой последовательности. Чем выше степень полинома, тем выше вероятность определения изменений, который рассчитывается как $\mathrm{d} = \frac{1}{2^m}$.

Пусть требуется проконтролировать последовательность вида A = 1010010.

$$P(x) = x^3 + x - 1$$

1. Получение контрольной характеристики (представляем А в виде полинома)

$$G_A(x) = x^6 + x^4 + x$$

$$G_A(x) * x^3 = x^9 + x^7 + x^4$$

При вычислении синдрома операция деления заменяется операцией сложения по модулю.

2. **Хеш-функция** – процесс получения контрольной характеристики двоичной последовательности, основанный на двоичном суммировании и … Хеш-функция, примененная к исходным данным, дает в качестве результата из небольшого фиксированного числа бит, которое называется дайджестом.

ГОСТ Р 34.11-94

Свойства:

1. Односторонность (без соблюдения этого они не могут использоваться в криптоалгоритмах). Принцип разбитой вазы: разбить вазу из целой легко, а получить целую из разбитой – никак.

Основные требования к функциям хеширования

1. Сжатие

Функция отображает входное сообщение *X* любой произвольной конечной длины в хеш-значение *Y* небольшой фиксированной длины. *X* называется прообразом.

2. Простота вычислений

Для заданной функции h и сообщения X h от X должно вычисляться не больше, чем с полиномиальной сложностью.

3. Стойкость к нахождению прообраза

Невозможность нахождения неизвестного прообраза для любых предварительно заданных хеш-значений.

4. Стойкость к нахождению второго прообраза

Невозможность нахождения любого другого прообраза, который давал бы такое же хеш-значение, как и заданный. Т. е. для заданной функции h и прообраза X вычислительно невозможно найти прообраз $X' \neq X$, который давал бы одинаковое соответствие их хеш-значений $h(X) = h(X')$.

5. Стойкость к коллизиям

Невозможность нахождение двух прообразов, для которых вырабатывалось бы одинаковое хеш-значение (то, что не нашли коллизию на текущий момент не гарантирует, что её не найдут потом. 5-е условие это идеальное условие). Пятое условие более жесткое по сравнению с четвертым

Если обладает всем 4 свойствам – ***однонаправленная криптографическая хеш-функция***, если 5 – ***бесколлизионная***.

Все хеш-функции можно разделить на два класса:

1. Бесключевые (зависят только от нашего прообраза)
2. Хеш-функции с секретным ключом (КАС функции или функции идентификации сообщений). Зависят и от сообщения, и от секретного элемента (ключа).

Все атаки на хеш-функции подразделяются на два вида:

- Атаки, базирующиеся на уязвимости самого алгоритма (аналитические, ищут недостатки функции);
- Атаки, независящие от алгоритма (атаки грубого перебора).

К таким атакам уязвимы все хеш-функции. От грубого перебора – увеличиваем размерность.

Минимальное требование по стойкости соответствует сложности атаки 2^{138}.

15.10.2024

Политика безопасности

а – точно спрашивает на защите (с ее слов)

Под политикой безопасности понимают совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивают защиту от определенного множества угроз и составляет необходимое, а иногда и достаточное условие безопасности системы.

Модель безопасности позволяет обосновать жизнеспособность системы, определяет базовые принципы ее архитектуры и используемые при ее построении технологические решения.

Основная цель разработки политики безопасности и ее описание в виде формальной модели – это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и приведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений.

Пользователи эталонов:

- Разработчики используют эталоны (формальные модели) для разработки спецификации систем при выборе архитектуры и реализации сред защиты, а также для подтверждения свойств новой разработанной системы;
- Потребители систем безопасности или заказчики;
- Эксперты по квалификации – те, кто оценивают вновь появившиеся на рынке системы по отношению к эталону.

Принципы, на которых основаны модели безопасности (базовые минимальные структурные элементы)

1. Система является совокупностью взаимодействующих субъектов и объектов. В любой системе должен быть организован порядок доступа субъектов к объектам. Считается, что **система безопасна**, если субъекты не имеют возможности нарушить правила политики безопасности.
2. Все отношения в системе моделируются как взаимодействия между субъектами и объектами. Множество типов отношений определяется набором операций, которые разрешены субъекту над объектом (изменить, переместить, удалить …).
3. Все операции контролируются монитором взаимодействия и разрешаются/запрещаются в соответствии с правилами политики (**аудит безопасности**).
4. Совокупность множеств субъектов, объектов и их отношений определяют состояние системы. Каждое состояние считается безопасным или небезопасным в соответствии с действующим в системе критерием безопасности.
5. Основной элемент модели безопасности – это доказательство утверждения или теоремы о том, что система, находясь в безопасном состоянии, не может перейти в небезопасное при соблюдении всех правил и ограничений.

Выделяют две исторически классических модели политики:

1. Дискреционные (произвольные, избирательные)
2. Мандатные (нормативные, полномочные)

Дискреционная модель Харрисона-Руззо-Ульмана

Система обработки информации представляется в виде множества активных субъектов $s \subset S$, множества пассивных объектов $o \subset O$ и набором прав доступа $R = \{r_1, r_2, \dots, r_n)$.

Поведение системы моделируется с помощью понятия состояния, при этом пространства состояний образуются как декартово произведение O x S x R (декартово состояние множества). Текущее состояние системы есть текущее состояние соответствующих множеств Q = (S, O, M), где M – прямоугольная матрица прав доступа.

Поведение системы во времени моделируется переходами между состояниями. Переход осуществляется внесением изменения в матрицу с помощью специализированных команд.

Команда – набор операций, которые запускаются при выполнении определенного условия.

1. Добавление нового права субъекту S права R к o
2. Удаление прав R у s к o
3. Создание нового субъекта/объекта s/o
4. Удаление субъекта/объекта s/o

Применение любой операции переводит систему из одного состояния в другое. Операции, в которых происходит добавление – называются монотонными, там где удаление – немонотонные.

Формальное описание системы записывается как $\sum(Q, R, C)$, где

1. R – конечный набор прав доступа $R = \{r_1, r2, \dots, r3\}$
2. $s \subset S, o \subset O, S \subset O$
3. Исходная матрица доступа M0 M_0
4. Конечный набор команд C = $\{x_i\}$

Критерий безопасности: Для заданной системы с начальным состоянием Q0 = (S0, O0, M0) является безопасным относительно права r_i, если не

существует применимой к Q0 последовательности команд, в результате которой право R появится в матрице M, если оно отсутствовало в M0. Т.е. для безопасной конфигурации системы субъект никогда не получит право доступа, если его там не было изначально.

Основной минус модели: размер матрицы + доказательство критерия безопасности очень относительно.

Мандатная Модель Белла-ЛаПадулы

Модель основана на принципах секретного документооборота, пришедшим из гос/оборон структур. Всем участникам процесса, и пользователям, и документации, присваиваются специальные метки.

1. Все субъекты и объекты должны быть однозначно идентифицированы.
2. Каждому объекту присваивается метка критичности, определяющая целостность информации.
3. Каждому субъекту присваивается уровень прозрачности, определяющий макс значение метки критичности, к которой субъект имеет доступ.
4. Т.о. чем важнее субъект или объект, тем выше его метка критичности.

Контроль доступа осуществляется в зависимости от уровня взаимодействующих сторон на основании двух правил (очень любит правила спрашивать):

1. Субъект может читать только те объекты (документы), уровень безопасности которых не выше его собственного (защита от несанкционированного доступа).
2. Субъект имеет право заносить информацию только в те объекты (документы), уровень безопасности которых не ниже его собственного (защита от утечки «сверху»).

Проблемы:

1. Контролируется не операция, а поток информации.
2. Нет разграничения потока для одноранговых объектов.
3. Есть только два правила доступа – чтение и запись.

В основе лежит **решетка уровня безопасности**.

В мандатных моделях функция уровня безопасности F вместе с решеткой уровней определяют все допустимые отношения доступа между сущностями системы.

Модель системы записывается как $\sum(V_0, R, T)$, где

V0 – начальное состояние,

R – множество запросов,

T – функция перехода, которая есть декартово произведение T: (VxR)->V, переводящая систему в новое состояние

Состояние (F, M) называется безопасным по чтению тогда и только тогда, когда для каждого субъекта, осуществляющего в этом состоянии доступ чтения к объекту уровень безопасности субъекта доминирует над уровнем безопасности объекта, т. е. $\vee s \in S, o \in O, read \in M[s, o] \rightarrow F(s) \geq F(o)$

Состояние (F, M) называется безопасным по записи, если $\vee s \in S, o \in O, write \in M[s, o] \rightarrow F(o) \geq F(S)$. Для каждого субъекта, осуществляющего доступ к записи объекта, уровень безопасности объекта доминирует над уровнем субъекта.

Состояние (F, M) называется безопасным, если оно безопасно и для чтения, и для записи.

(Критерий безопасности (V0, R, T))Система безопасна тогда, когда ее начальное состояние V_0 безопасно, и все состояния достижимы из V_0 путем применения конкретной конечной последовательности запросов из R тоже безопасны.

Ролевая политика (схема)

1. Субъект заменяется двумя понятиями – пользователь и роль.
2. Пользователь – конкретно человек, работающий с системой (U).
3. Роль – некоторая абстрактная сущность (R), с которой заведомо с в системе связан набор полномочий и ограничений (P). (S – сеанс)
4. У одного пользователя может быть несколько ролей, как и у одной роли может быть несколько пользователей.

При ролевой политике управление доступом осуществляется в два этапа:

1. Для каждой роли указывается набор полномочий, который представляет собой набор прав доступа к конкретному объекту.
2. Пользователем назначается список доступных ролей. Полномочия назначаются ролям в соответствии с принципом наименьших привилегий (меньше знаешь – крепче спишь).

1. Взаимоисключающие роли

Все роли в системе разбиваются на подмножества, которые не могут назначаться одному пользователю и считаются несовместимыми, т. е. конфликт ролей разрешается на стадии выдачи ролей, это называется статическое разделение обязанностей.

2. Ограничение на одновременное использование ролей в рамках одной сессии

Множества ролей разбивается на подмножества несовместимых ролей, но назначит пользователю мы можем любую комбинацию ролей, при этом одновременно пользователь может активировать не более одной роли из каждого подмножества. (динамическое разделение обязанностей).

3. Политика с количественным ограничением