ЛЕКЦИЯ

по дисциплине «Автоматизированные системы специального назначения»

(Д-3110-02)

Тема № 4 «Программное обеспечение цифровой телекоммуникационной системы УС МО РФ»

Занятие № 30 «Методы и средства защиты информации от НСД в ОС СН»

Учебные вопросы

.Модели управления доступом

.Методы и средства идентификации и аутентификации субъектов доступа

.Методы и средства обеспечения целостности данных

Литература

1. В.Е Дементьев, М.А. Коцыняк, Ю.И. Стародубцев. Комплексная защита информации в локальных вычислительных сетях. /Под общ. ред. Ю.М. Ровчака. СПб.:ВАС,2010. 436 с.
2. **Назаров И.В., Стефанович А.Б. Защита информации в среде ОС МСВС 3.0. Учебное пособие. – М.: изд. ВНИИ АУНС, 2005. – 222 с.**
3. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. /, Москва: ДМК Пресс, 2012. – 592 с.
4. Саенко И. Б., Авраменко В. С., Гетманцев А. и др. Новые информационные и сетевые технологии в системах управления военного назначения. Часть 2. Новые информационные технологии в системах военного назначения. Учебник / Под ред. И. Б. Саенко. – СПб.: ВАС. 2010. 520 с.

Введение

Основным документом, определяющим систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от НСД является «**Концепция защиты СВТ и АС от НСД к информации**».

В соответствии с Концепцией… методы и средства защиты информации от (НСД) к компьютерным системам реализуют типовой **набор функций защиты**:

- **аутентификации пользователей,**
- **разграничения доступа к информации,**
- **обеспечения целостности,**
- **криптографического преобразования данных при передаче и хранении,**
- **протоколирования и аудита.**

Учебный вопрос №1

Модели управления доступом

Основные функции СРД

- реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;
- реализация ПРД субъектов и их процессов к устройствам создания твердых копий;
- изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;
- управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;
- реализация правил обмена данными между субъектами для АС, построенных по сетевым принципам.

Основные термины и определения

Политика безопасности - совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое (а иногда и достаточное) условие безопасности системы.

Модель политики безопасности - формальное выражение политики безопасности.

Управление доступом к информации - заключается в разделении обрабатываемой информации на части и организации доступа к ним пользователей в соответствии с их функциональными обязанностями и полномочиями.

Модель управление доступом – основа формальной модели политики безопасности.

Варианты разделения доступа субъектов к совместно используемым объектам

1. **Физическое** – субъекты обращаются к физически различным объектам (однотипным устройствам, наборам данных на разных носителях и т.д.).
2. **Временное** – субъекты с различными правами доступа к объекту получают его в различные промежутки времени.
3. **Криптографическое** – все объекты хранятся в зашифрованном виде, права доступа определяются наличием ключа для расшифрования объекта.
4. **Логическое** – субъекты получают доступ к совместно используемому объекту в рамках единой операционной среды, но под контролем средств разграничения доступа, которые моделируют виртуальную операционную среду «один субъект - все объекты»

В основе логического управления доступом - концепция диспетчера доступа.

Модель диспетчера доступа

Диспетчер доступа должен обладать тремя свойствами:

1. полнота – ни один запрос на доступ субъекта к объекту не должен выполняться в обход монитора безопасности пересылок;
2. целостность – работа диспетчера доступа должна быть защищена от постороннего вмешательства;
3. простота – представление диспетчера доступа должно быть достаточно простым для верификации корректности его работы.

Диспетчер доступа – реализует модель управления доступом

Основные формальные модели управления доступом (политик безопасности)

1. Дискреционная

2. Мандатная

3.Ролевая

Дискреционная модель

Дискреционная модель - для каждой пары (субъект - объект) устанавливается перечень прав (разрешений) субъекта по отношению к объекту, права доступа каждого субъекта (пользователя) к каждому объекту (диску, каталогу, файлу) задаются в виде матрицы (таблицы)

S- множество субъектов, O - множество объектов, U – множество пользователей.

$O \to U$ - каждый объект является собственностью соответствующего пользователя

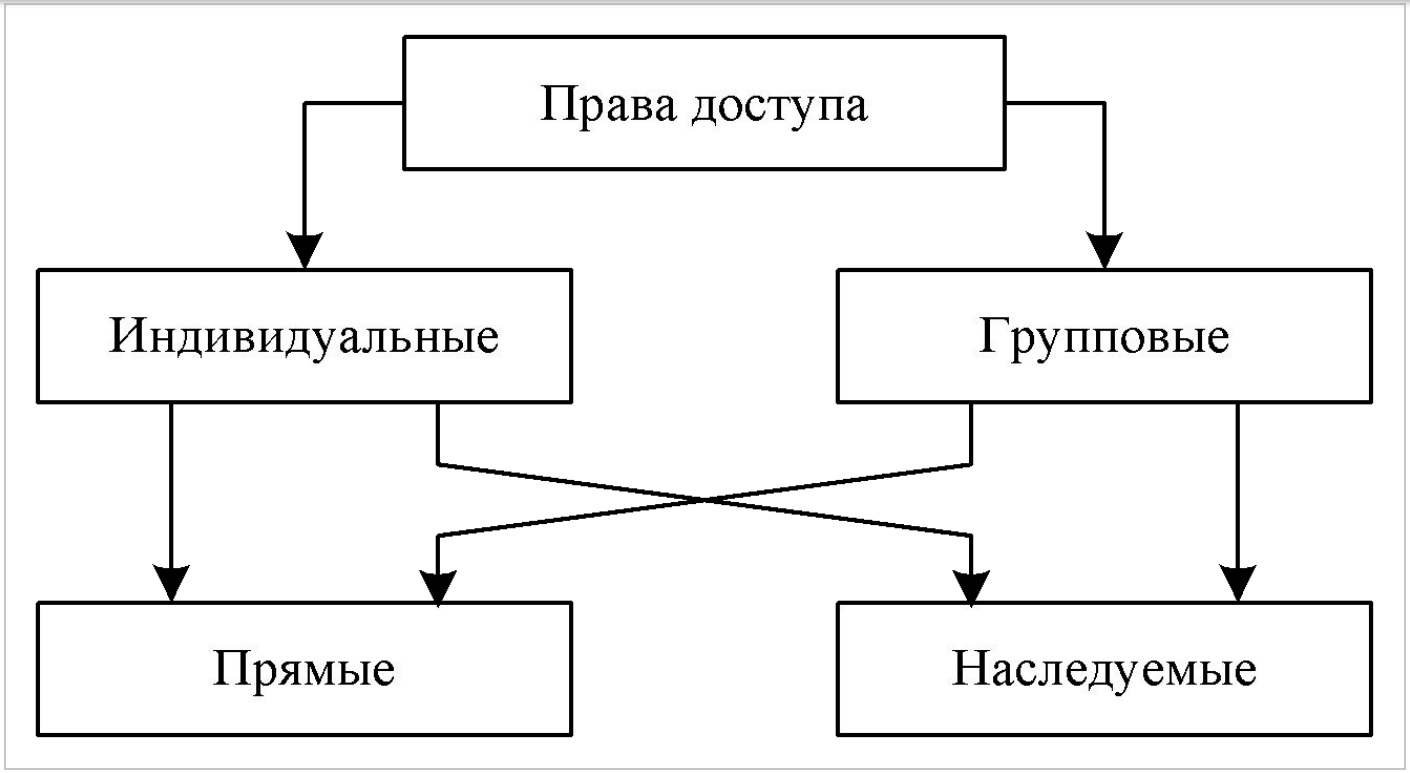
Собственник:

- имеет все права доступа
- может передавать права другим пользователям
- может определять права доступа других субъектов

Пример матрицы доступа

	O_1	O_2	…	Ок	S_1	…	Sn
S_1	Own R	W	…				
. . .							
Sn							

Типы прав доступа



Основные способы реализации дискреционного управления доступом

1."парольная" зашита;
2.**списки прав доступа** (Access Control List – ACL);
3.**биты доступа.**

Категории пользователей ОС МСВС

- ***владелец – u*** (процессы, имевшие идентификатор пользователя, совпадающий с идентификатором владельца файла);
- ***группа – g*** (процессы, имеющие идентификатор группы, совпадающий с идентификатором группы, которой принадлежит файл);
- ***остальные пользователи – o*** (процессы, не попавшие в первые две категории);

Существует возможность обратиться к трем категориям сразу при помощи ключа – ***a.***

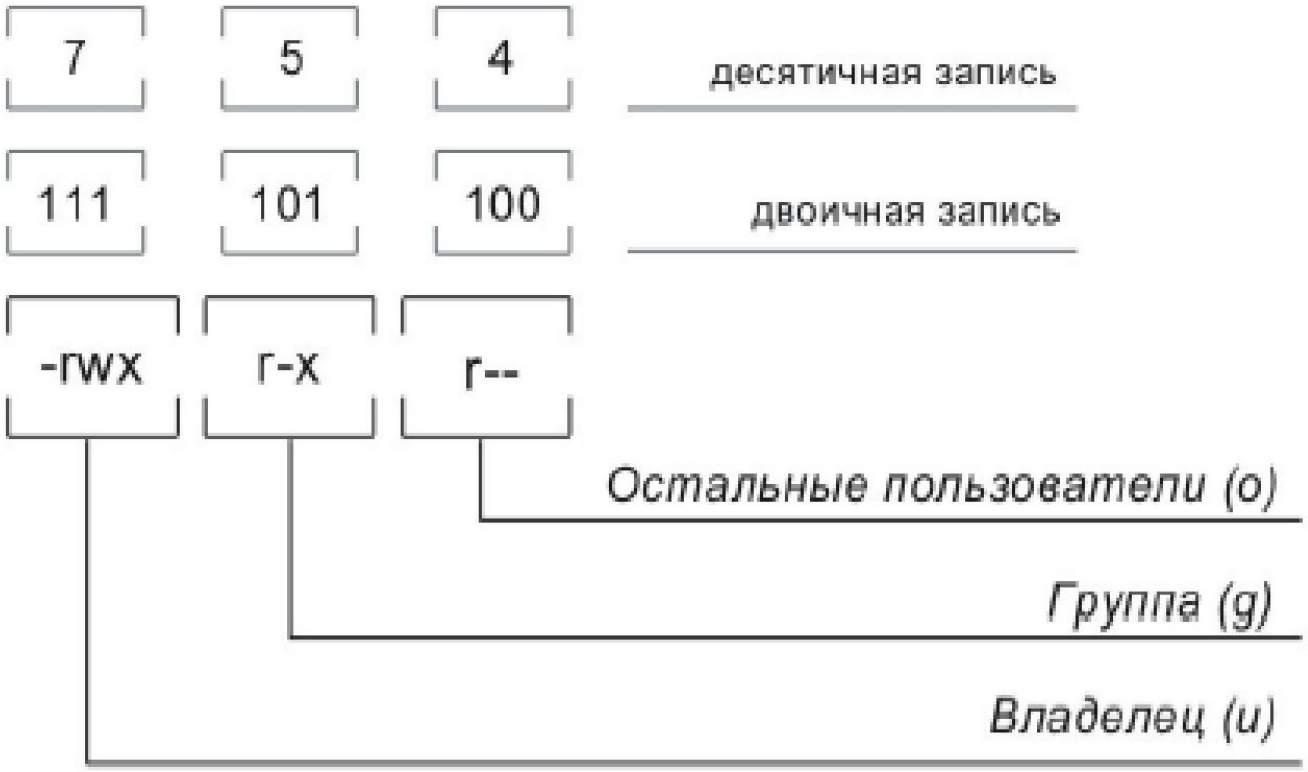
Команды для изменения прав доступа к объекту

Каждый файл содержит **код защиты**, который присваивается файлу при его создании. Код защиты располагается в индексном дескрипторе файла и содержит десять символов, причем **первый символ** определяет тип файла, а последующие девять - право на доступ к нему.

Символ	Тип файла
-	Обычный или исполняемый файл
d	Каталог
l	Символьная ссылка
s	Сокет
b	Блочное устройство
c	Символьное устройство
p	Именованный канал

Права и категории разграничения доступа в ОС МСВС

- ***право на чтение – r (Read);***
- ***право на запись – w (Write);***
- ***право на исполнение – x (eXecute).***



Права разграничения доступа

Файл:

- **Чтение – возможность читать содержимое файла;**
- **Запись – возможность модифицировать содержимое файла (в том числе полное удаление содержимого);**
- **Исполнение – возможность выполнить загрузочный модуль или командный файл.**

Каталог:

- **Чтение – возможность получения листинга каталога;**
- **Запись – возможность создания и удаления файлов в каталоге (нет права на модификацию файла);**
- **Исполнение – возможность обращения к файлам в каталоге, использование каталога как части путевого имени.**

Мандатная модель

основана на использовании так называемых меток (мандатов) секретности (конфиденциальности) - чисел, отражающих уровень (класс) доступа субъекта к информации c(S) и, соответственно, уровень ценности (секретности) информации, принадлежащей объекту c(O).

Субъект может получить доступ к объекту только в том случае, если его мандат (метка) не ниже, чем у объекта.

Мандатный контроль для системы с двумя видами доступов (чтение и запись):

Чтение (r) разрешено, если $c(S) \geq c(O)$

Запись (w) разрешена, если $c(S) \leq c(O)$

Уровни и категории безопасности ОС МСВС

Метки безопасности ОС МСВС состоят из двух частей — **уровня секретности** (до 8) и **списка категорий** (до 64).

Для разных систем набор уровней секретности может различаться. Категории образуют неупорядоченный набор. Их назначение - описать предметную область, к которой относятся данные.

Горизонтальные метки

категории

Вертикальные метки (уровни)

0 - несекретно
1 - секретно
2 - СС
3 - ОВ
4-7 - резерв

Ролевая модель

В основу модели положена идея принадлежности всех данных системы некоторой организации, а не пользователю.

Особенности:

- Разрешения на использование конкретных данных выдается пользователю администратором в соответствии с ролью, которая ему предписывается при выполнении конкретной функции.
- Управление доступом к данным самим пользователем (в том числе и с помощью передачи привилегий) не предусмотрено.

Учебный вопрос №2

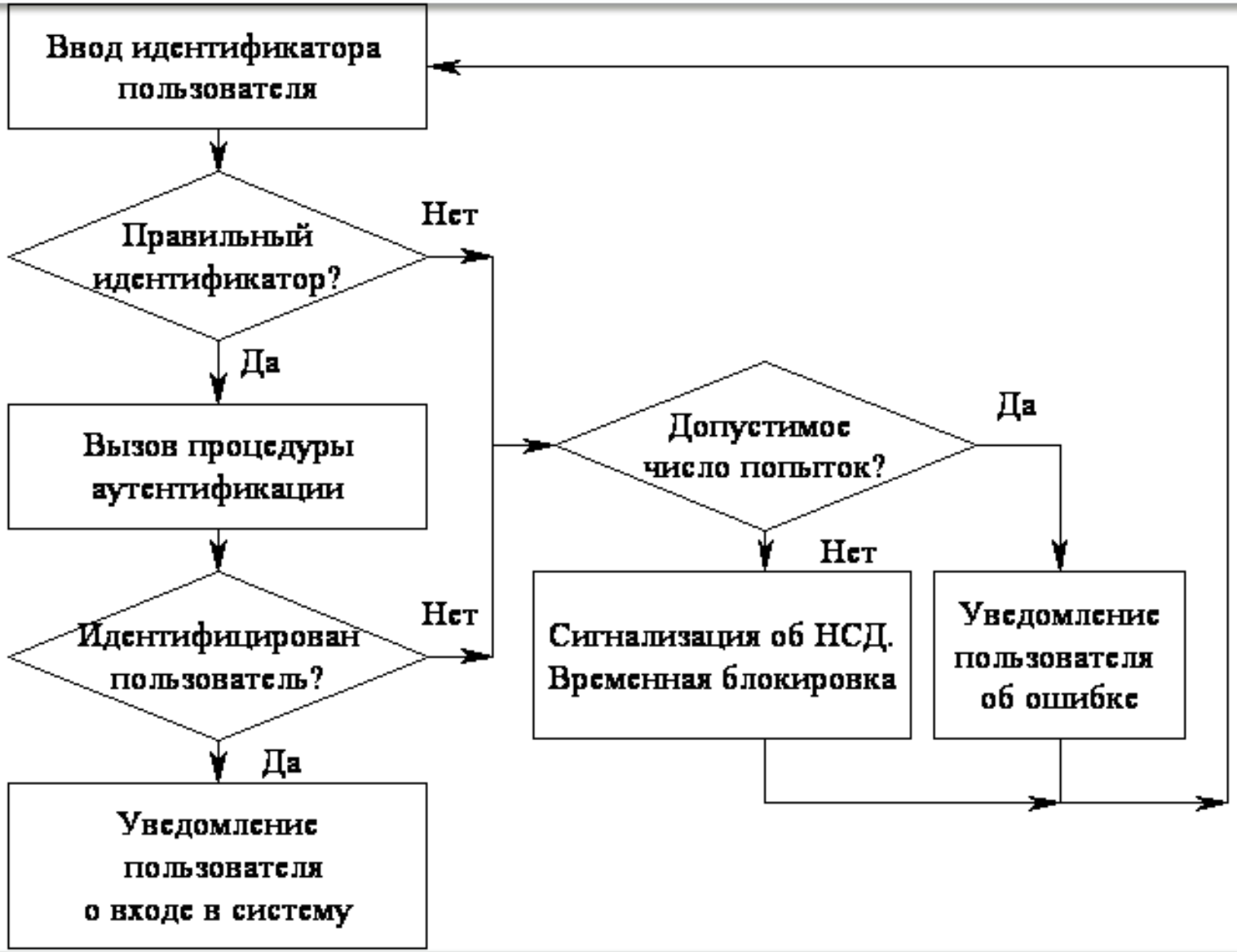
Методы и средства идентификации и аутентификации субъектов доступа

Основные термины и определения

Идентификация - присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов *(ФСТЭК, Термины и определения,1998)*

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности *(ФСТЭК, Термины и определения,1998)*

Классическая процедура идентификации и аутентификации



Способы аутентификации

1. Аутентификация по паролю;
2. Аутентификация по биометрическим характеристикам;
3. Аутентификация с применением специализированных устройств;
4. Комплексная аутентификация.

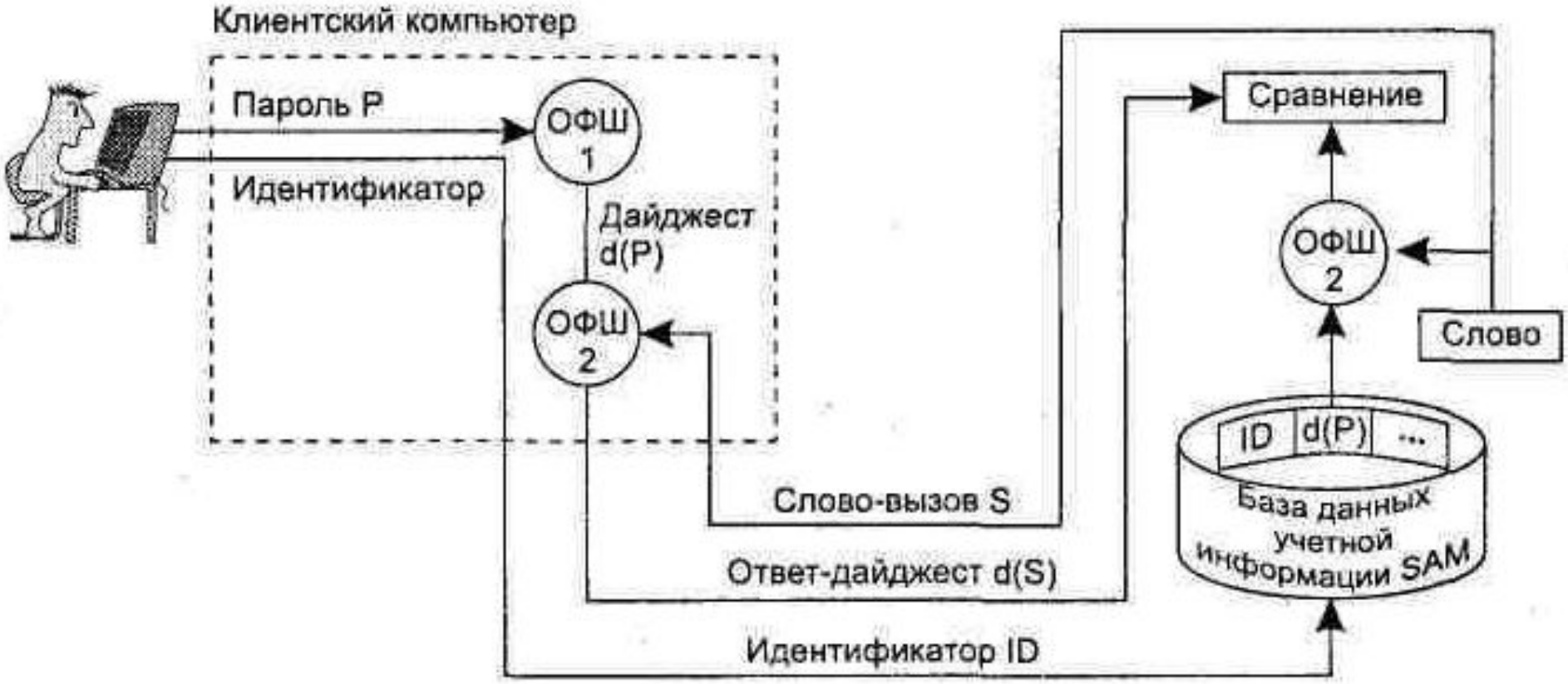
Парольные методы

1. методы, использующие постоянные (многократно используемые) пароли,
2. методы, использующие одноразовые (динамично изменяющиеся) пароли.

Меры, направленные на повышение надежности многоразовых паролей защиты:

1. наложение ограничений (длина, алфавит)
2. управление сроком действия паролей, их периодическая смена;
3. ограничение доступа к файлу паролей;
4. ограничение числа неудачных попыток входа в систему,
5. обучение и воспитание пользователей;
6. использование программных генераторов паролей

Схема сетевой аутентификации на основе многоразового пароля



Пароль в сети не передается!!!

Токены

Токен - это предмет или устройство, владение которым подтверждает подлинность пользователя.

Типы токенов:

- пассивные (токены с памятью, только хранят, но не обрабатывают информацию);
- активные (интеллектуальные карточки).

Биометрические методы

Физиологические методы	Поведенческие методы
1. Снятие отпечатков пальцев 2. Сканирование радужной оболочки глаза 3. Сканирование сетчатки глаза 4. Геометрия кисти руки 5. Распознавание черт лица	1. Анализ подписи 2. Анализ тембра голоса 3. Анализ клавиатурного почерк

Устройства с биометрической аутентификацией

Учебный вопрос №3

Методы и средства обеспечения целостности данных

Основной метод обеспечения целостности

Резервное копирование - дублирование данных (файла, каталога, тома) путем копирования на устройства хранения информации (дискету, магнитную ленту, жесткий диск), является основным методом обеспечения целостности данных.

В целях обеспечения оперативного восстановления данных в АС реализуется **система резервного копирования.**

Классификация способов резервного копирования

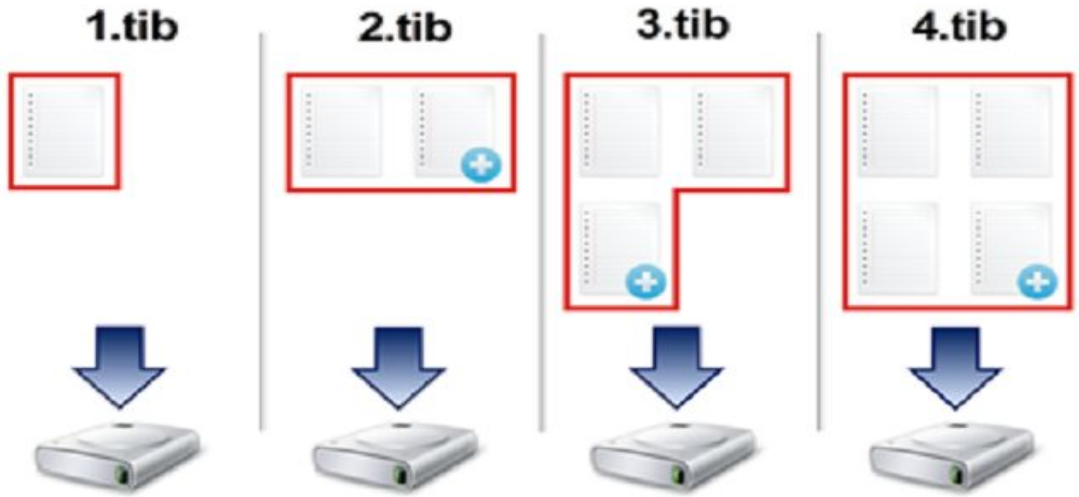
1. По способу резервного копирования:
- дисковая резервная копия;
- файловая резервная копия;

2. По количеству копируемых данных:
- полное (full);
- инкрементальное (incremental);
- дифференциальное (differential);
- путем прямого копирования (copy backup)

3. По способу передачи копируемых данных:
- локальное (local)
- сетевое (LAN)
- внесерверное (serverless)
- внесетевое (LAN-free) (SAN)

Полное резервное копирование

В файл бэкапа записываются все данные, которые были выбраны для резервного копирования.

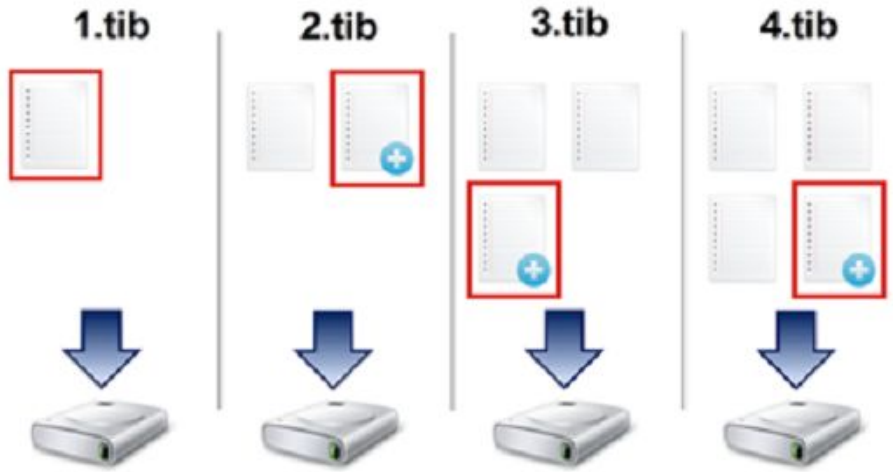


На рисунке: все бэкапы — полные.

Этот метод самый надежный, но занимает много времени и ведет к большому расходу свободного места носителя. Восстановление информации при полном копировании осуществляется наиболее быстро, так как для этого достаточно только одного записанного образа.

Инкрементное резервное копирование (добавочное)

В файл бэкапа записываются только изменения, которые произошли с момента последнего резервного копирования.

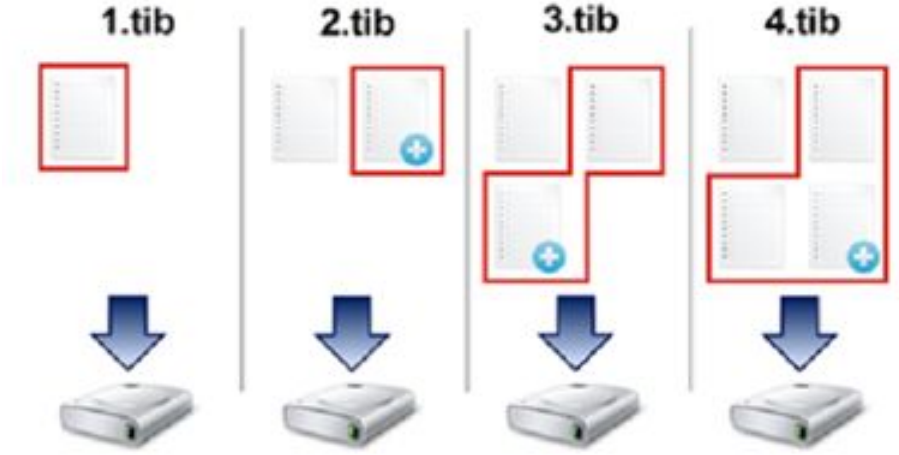


На рисунке : 1.tib — полный бэкап (первый бэкап всегда полный), 2.tib, 3.tib, 4.tib — инкрементные бэкапы.

При использования этого способа первая запись на носитель является полной копией. При второй записи на носитель помещаются только файлы, которые были изменены со времени первой записи. На третьем этапе копируются файлы, модифицируемые со времени второго этапа, и.т.д

Дифференциальное (разностное) резервное копирование

В файл бэкапа записываются только изменения, которые произошли с момента последнего полного резервного копирования.



На рисунке : 1.tib — полный бэкап (первый бэкап всегда полный), 2.tib, 3.tib, 4.tib — дифференциальные бэкапы .

Первая запись на носитель также является полной копией. На последующих этапах копируются только файлы, которые изменились со времени проведения полного копирования. По времени РК этот метод занимает больше времени, чем при инкрементальном копировании. Однако для восстановления данных достаточно всего двух копий — последней полной и последней дифференциальной копии.

Цепочки и схемы резервного копирования

Три метода резервного копирования дают массу всевозможных вариантов так называемых цепочек бэкапов.

Цепочка – это один полный бэкап и все зависящие от него инкрементные и/или дифференциальные бэкапы.

Схема состоит из одной или нескольких цепочек, а также содержит правила удаления старых бэкапов.

Схемы на основе полных бэкапов
Схемы на основе инкрементных бэкапов.
Схемы на основе дифференциальных бэкапов.

Встроенные средства резервного копирования ОС

В ОС Windows: (удобный графический режим)

- архивация заданных папок по расписанию и восстановление их из резервной копии
  (функция «История файлов» в Windows 8)
- создание полного (дискового) образа системы
- создание загрузочного диска или точек восстановления Windows
- теневое копирование тома

В ОС МСВС: архивация дисков и файлов (командная строка)
Системная утилита **tar**
Команды **Dump** и **Restore** (только для файловых систем ext2 и ext3)
dd – для создания и восстановления MBR, создание и восстановление зеркальных копий различных носителей, создание образов и клонов дисков

Заключение

Регистрация и учет (протоколирование) - сбор и накопление информации о событиях, происходящих в автоматизированной системе.

Аудит - это анализ накопленной информации, проводимый оперативно, почти в реальном времени, или периодически.

Цели протоколирования и аудита:

- обеспечение подотчетности пользователей и администраторов;
- обнаружение (прогнозирование) фактов и попыток нарушений информационной безопасности;
- обеспечение возможности реконструкции последовательности событий (расследование попыток и фактов НСД, программных атак);
- предоставление информации для выявления и анализа проблем защиты информации.

Заключение

Создаваемая система защиты информации от НСД по выполняемым функциям условно делится на четыре подсистемы:

- управления доступом;
- регистрации и учета;
- обеспечения целостности;
- криптографическая.

Современные защищенные ОС имеют в своем составе встроенные механизмы, реализующие функции данных подсистем.