1 сл: Управление доступом к информационным ресурсам является ключевой функцией обеспечения информационной безопасности. Данная задача в том или ином виде решается в каждой информационной системе, а также на уровней всей ИТ-инфраструктуры компании или организации в целом. Управление доступом на современном уровне  предполагает обеспечение процессного подхода с четко детерминированной ролевой моделью.

2 сл:

**Управление доступом предполагает администрирование следующих сущностей:**

* объекты доступа (информационные системы, объекты ИТ-инфраструктуры, информационные сущности в базах данных и пр.);
* субъекты доступа (учетные записи в системах, аккаунты в разнородных источниках, включая облачные идентификаторы);
* матрица доступа (правила разграничения доступа).

3 сл: **Современные системы управления доступом обеспечивают функционирование как минимум следующих процессов жизненного цикла:**

* управление учетными записями (создание / изменение / удаление / блокирование / разблокирование учетных записей, управление паролями, управление учетными данными);
* управление информационными ресурсами (декларирование / изменение / удаление / назначение прав по умолчанию);
* правами и полномочиями (назначение / изменение / отзыв / блокирование / разблокирование / аудит(сверка);
* отчетность (контроль всей совокупности полномочий, расследование исторических операций и пр.).

4 сл: Идентификация заключается в сообщении пользователем системе своего идентификатора.

* Идентификаторы пользователей применяются в системе с теми же целями, что и идентификаторы любых других объектов (файлов, процессов, структур данных), и они не всегда связаны непосредственно с обеспечением безопасности.

Процедура идентификации напрямую связана с аутентификацией (это процедура проверки подленности) : субъект проходит процедуру аутентификации, и если аутентификация успешна, то информационная система на основе факторов аутентификации определяет идентификатор субъекта. При этом достоверность идентификации полностью определяется уровнем достоверности выполненной процедуры аутентификации.

5 сл: **Пароль** ([фр.](https://ru.wikipedia.org/wiki/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%83%D0%B7%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *parole* — [слово](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B2%D0%BE)) — условное слово[[1]](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8C#cite_note-1) или набор знаков, предназначенный для подтверждения личности или полномочий.

Пароли часто используются для защиты [информации](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F) от [несанкционированного доступа](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D1%81%D0%B0%D0%BD%D0%BA%D1%86%D0%B8%D0%BE%D0%BD%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF_%D0%BA_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8). В большинстве [вычислительных систем](https://ru.wikipedia.org/wiki/%D0%92%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) комбинация «[имя пользователя](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%B3%D0%B8%D0%BD_(%D1%83%D1%87%D1%91%D1%82%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D1%8C)) — пароль» используется для [удостоверения](https://ru.wikipedia.org/wiki/AAA_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C)) пользователя.

**Токен** представляет собой учетную единицу, применяемую для интерпретации цифрового баланса в конкретном активе. Токены учитываются в специальной базе данных посредством технологии блокчейн. Доступность токенов для предварительно идентифицированных пользователей становится возможной благодаря онлайн-приложениям, которые базируются на использовании электронной (цифровой) подписи.

**Смарт — карта** — это пластиковая карта, в которой установлена микросхема. Такие кадры предназначены для контроля и записи данных, также часто они способны проводить криптографические вычисления. Смарт — карта может выполнять различные функции по обработке информации, а затем ее сохранять. Само название говорит о возможностях карты, поскольку Smart означает «интеллектуальный», т.е. смарт — карта является умной.

Штриховой код (штрих-код) - это последовательность черных и белых полос, представляющая некоторую информацию в удобном для считывания техническими средствами виде. В настоящее время активно применяются два способа штрих-кодирования информации: • линейный; • двухмерный. Линейными (обычными) называются штрих-коды, читаемые в одном направлении (по горизонтали). Двухмерные символики были разработаны для кодирования большого объема информации. Расшифровка такого кода проводится в двух измерениях (по горизонтали и по вертикали).

# 6 сл:Электронный замок ПАК Соболь - это аппаратно-программное средство защиты компьютера от несанкционированного доступа (аппаратно-программный модуль доверенной загрузки ПАК Соболь).

Электронный замок Соболь может применяться как устройство, обеспечивающее защиту автономного компьютера, а также рабочей станции или сервера, входящих в состав локальной вычислительной сети.

**Возможности электронного замка ПАК Соболь**

* Аутентификация пользователей
* Блокировка загрузки ОС со съемных носителей
* Контроль целостности программной среды
* Контроль целостности системного реестра Windows
* Контроль конфигурации компьютера (PCI-устройств, ACPI, SMBIOS)
* Сторожевой таймер
* Регистрация попыток доступа к ПЭВМ