Московский государственный университет геодезии и картографии (МИИГАиК)

Кафедра информационно-измерительных систем

Тема : Технические и программные средства защиты информации, используемые в СЭД

Выполнил:
Студент ИБ III-1б
Кочетков Д.О.

Проверил:
Доцент
Дубов С.С.

Москва 2020

Защита предприятия

1. **аппаратным элементам системы**. Это компьютеры, серверы, элементы компьютерной сети и сетевое оборудование;
2. **защита необходима файлам системы**. Это файлы программного обеспечения и базы данных. В случае их незащищенности появляется возможность воздействия злоумышленника на файлы СЭД.
3. **необходимо защищать документы и информацию**, находящиеся внутри системы.

Можно выделить несколько, основных, групп источников угроз:

- легальные пользователи системы,
- административный ИТ-персонал,
- внешние злоумышленники.

Основные функции

- обеспечение сохранности документов;
- обеспечение безопасного доступа;
- обеспечение конфиденциальности;
- обеспечение подлинности документов;
- Сертификация;
- DLP система;
- протоколирование действий пользователей.

Обеспечение сохранности документов

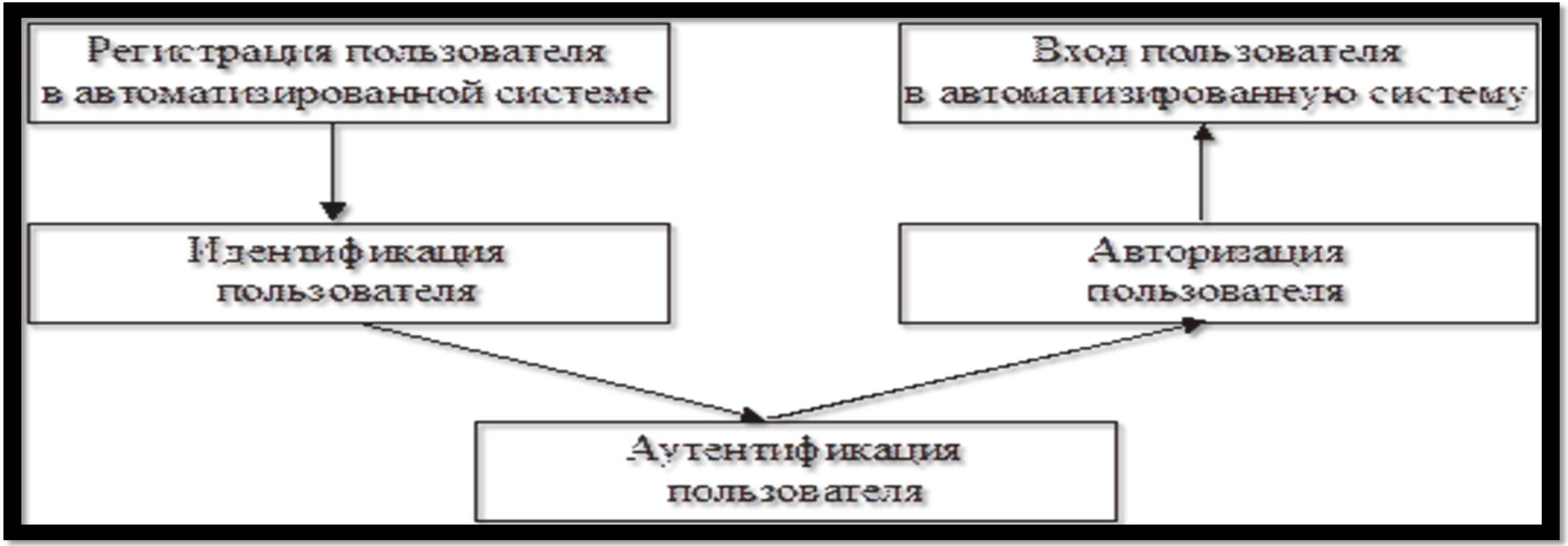
- Например, для СЭД, использующих базы данник Microsoft SQL Server или Oracle, предпочитают применять средства резервного копирования от разработчика СУБД.
- Иные системы имеют собственные подсистемы резервного копирования, разработанные непосредственно производителем СЭД.

Обеспечение безопасного доступа

- применение многоразовых паролей;
- Специальным носителем информации: USB-ключи, смарт-карты, магнитные карты, дискеты и компакт-диски;
- Надежным для проведения идентификации и последующей аутентификации является биометрический метод;
- Процесс аутентификации может быть однофакторным, двухфакторным и т. д. Возможно также комбинирование различных методов: парольного, имущественного и биометрического.

Обеспечение безопасного доступа

Разграничение прав пользователей



Обеспечение безопасного доступа

Разграничение прав пользователей (принципы):

- задание пользователей и групп;
- мандатный доступ по группам;
- разграничение доступа к различным частям документов.

Обеспечение безопасного доступа

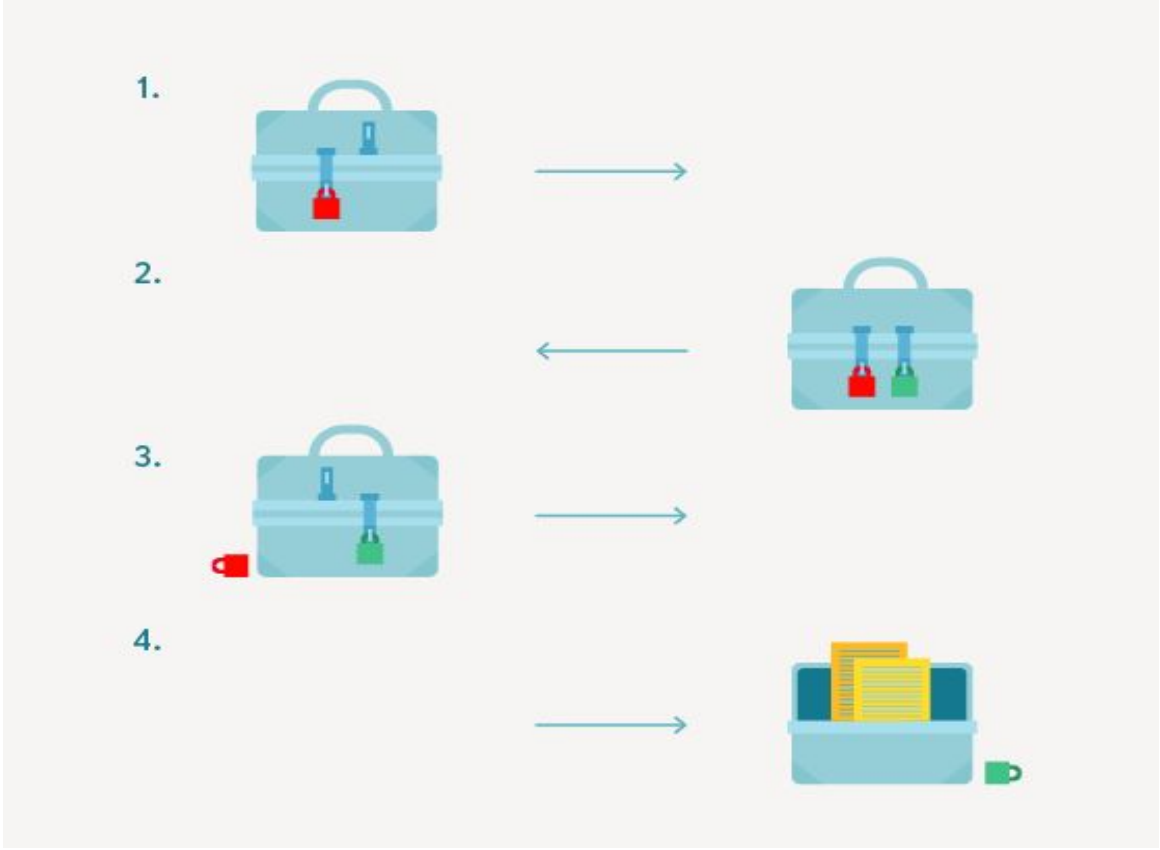
методы разграничения доступа :

- **задание доступа на уровне серверной базы данных;**
- **ограничение доступа на интерфейсном уровне,** когда ряд действий не может быть выполнен через пользовательский интерфейс, но доступен в случае написания отдельной программы.

Обеспечение безопасного доступа

Передача сведений только по защищенным протоколам HTTPS:

- Ваш компьютер и сервер выбирают общий секретный ключ
- Обмениваются информацией, шифруя её с помощью этого ключа



Сертификация

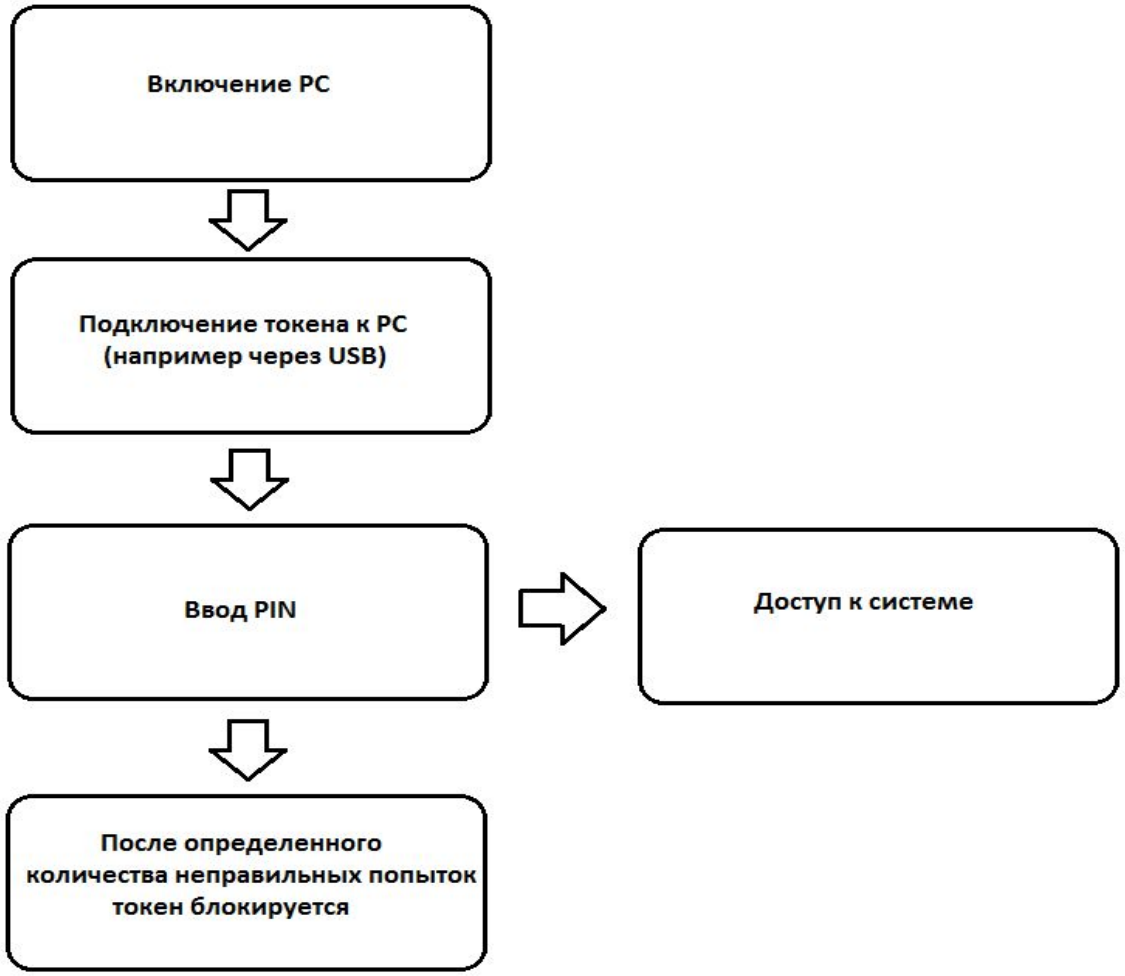
Виды сертификатов

- Самоподписной сертификат.
- Сертификаты, подтверждающие только доменное имя (Domain Validation — DV).
- Сертификаты с валидацией организации (Organization Validation – OV).
- Сертификаты с расширенной проверкой (Extendet Validation – EV).

Обеспечение безопасного доступа

Типы паролей:

- Токен со статическим паро.
- Токен с синхронно динамическим паролем.
- Токен с асинхронным паро.
- Токен вызов-ответ.



Пример схемы использования токена

Обеспечение безопасного доступа

Типы токенов:

- Токены без подключения
  - Беспроводные токены
  - Bluetooth-токены
- Токены с подключением
  - Смарт-карты
  - USB
- Мобильные устройства в качестве токена

Обеспечение конфиденциальности

Обеспечение конфиденциальности информации осуществляется с помощью криптографических методов защиты данных:

- Авторизация данных, обеспечение криптозащиты их юридической значимости в процессе передачи, хранения.
- Криптографическая защита личной или секретной информации, контроль над ее целостностью
- Криптографическая защита прикладного, системного программного обеспечения.
- Управление основными элементами системы согласно установленному регламенту.
- Аутентификация сторон, которые обмениваются данными.
- Криптографическая защита передачи информации с применением протокола TLS.

Обеспечение подлинности документов

Эту задачу можно решить:

- используя систему электронной цифровой подписи;
- инфраструктуру управления открытыми ключами PKI.

Обеспечение подлинности документов

Система электронной цифровой подписи(виды):

- простая электронно-цифровая подпись;
- усиленная неквалифицированная электронно-цифровая подпись;
- усиленная квалифицированная электронно-цифровая подпись.

DLP система

DLP расшифровывается как Data Leak Prevention, то есть, предотвращение утечек данных.

Задачи:

- контроль использования рабочего времени и рабочих ресурсов сотрудниками;
- мониторинг общения сотрудников с целью выявления «подковерной» борьбы, которая может навредить организации;
- контроль правомерности действий сотрудников (предотвращение печати поддельных документов и пр.);
- выявление сотрудников, рассылающих резюме, для оперативного поиска специалистов на освободившуюся должность.

Протоколирование действий пользователей

Платформа:

- Сама СУБД
- Возможности ОС

Позволяет:

- Протоколирование пользовательских сессий позволяет фиксировать факты входа (авторизации) и выхода (закрытие сессии) пользователей.
- Протоколирование вызовов процедур, отчетов, методов OLE-объекта позволяет фиксировать вызов пользователем того или иного метода системы.
- Протоколирование изменений данных заключается в фиксации фактов выполнения пользователями каждого изменения значений полей для объектов определенных классов.