

РАЗДЕЛ 3. БАЗОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

3.7 Информационные технологии обеспечения безопасности обработки информации

МОТИВАЦИЯ

Почему важно защищать информацию?

Характерной особенностью электронных данных является возможность легко и незаметно исказить, копировать и уничтожить их. Поэтому необходимо организовать безопасное функционирование данных в любых информационных системах, т.е. защищать информацию

Защита информации или информационная безопасность (ИБ)

- это совокупность методов, средств и мероприятий, направленных на исключение искажений, уничтожения и несанкционированного использования накапливаемых, обрабатываемых и хранимых данных

Задание № 105 РТ

Основные составляющие ИБ

- **целостность** - защищенность от разрушения и несанкционированного изменения.
- **конфиденциальность** - защита от несанкционированного доступа, хищения, изменения или уничтожения
- **доступность для санкционированного доступа** – возможность получить требуемую информацию в срок

Задание № 106 РТ

Основные виды информационных угроз:

Преднамеренные – хищение информации, компьютерные вирусы, физическое воздействие на технические средства

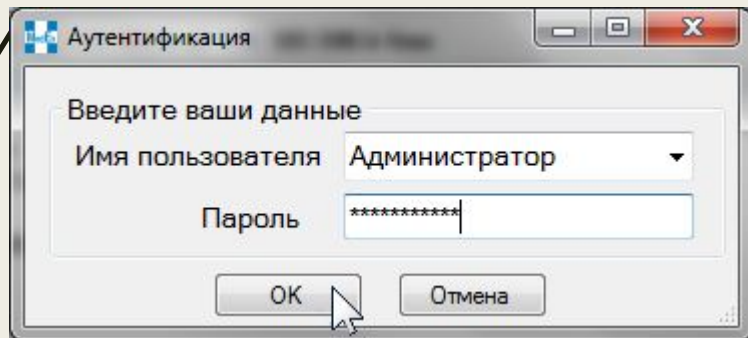
Случайные – ошибки пользователя, отказы и сбои в работе программных и аппаратных средств, природные явления и катастрофы

Задание № 107 РТ

Методы и средства защиты информации

Ограничение доступа к информации

- **Аутентификация** — процесс подтверждения, что этот человек и **он** выдает.



Задание № 108 РТ

Методы ограничения доступа к информации


- **Авторизация** — процесс принятия решения о том, что именно этой аутентифицированной персоне разрешается делать.

Задание № 108 Р

Авторизация
Пожалуйста, авторизуйтесь

Логин

Пароль

Запомнить меня на этом компьютере

[Забыли свой пароль?](#)

Методы ограничения доступа к информации

Задание №108 РТ

- **Идентификация** — процесс определения, что за человек перед нами.



Задание № 108 РТ

Средства защиты информации

Программные средства

- Операционной системой осуществляется проверка подлинности пользователя: идентификация и аутентификация (средство **идентификации** – имя пользователя, а средство **аутентификации** – пароль)

Задание № 109 РТ

- Программы-антивирусы – предназначены для профилактики и лечения от компьютерных вирусов

Абсолютно надежных программ, гарантирующих обнаружение и уничтожение любого вируса, не существует. Важным элементом защиты от компьютерных вирусов является профилактика.

Меры профилактики от вирусов

- 1) применение лицензионного программного обеспечения;
- 2) регулярное использование обновляемых антивирусных программ для проверки носителей информации;
- 3) Проверка на наличие вирусов файлов, полученных по сети;
- 4) периодическое резервное копирование данных и программ.

Задание № 110 РТ

Средства защиты информации

Технические средства защиты – электрические, электромеханические и электронные устройства

- Аппаратные технические устройства – устройства встраиваемые в ЭВМ
- Физические средства - замки на дверях, где размещена аппаратура; сигнализация; видеонаблюдение и пр.

Задание № 111 РТ

Криптографические методы защиты информации

Задание № 112

РТ

Криптография - это тайнопись, система изменения информации с целью ее защиты от несанкционированных воздействий, а также обеспечения достоверности передаваемых данных.

Для кодирования электронных данных используют **электронную цифровую подпись (ЭЦП)**

Задание № 113

РТ

Биометрические методы защиты

Задание № 112

БИ *Биометрия* - это совокупность автоматизированных методов и средств идентификации человека, основанных на его физиологических или поведенческих характеристиках:

- Статические (отпечатки пальцев)

- Динамические (почерк, голос)

Задание № 113

МЕТОДЫ БИОМЕТРИИ

Физиологические методы

Снятие отпечатков пальцев

Сканирование радужной оболочки глаза

Сканирование сетчатки глаза

Геометрия кисти руки

Распознавание черт лица

Поведенческие методы

Анализ подписи

Анализ тембра голоса

Анализ клавиатурного почерка

Задание № 114 РТ

Сетевые методы защиты

Задание № 115

- **фильтры пакетов**, ^{PT}запрещающие установление соединений, пересекающих границы защищаемой сети - **брандмауэр** – ограничивает трафик, пресекает попытки несанкционированного доступа, в т.ч. нежелательную почту и спам);
- **шлюзы прикладных программ**, проверяющие права доступа к программам

Задание N° 115

- **фильтрующие маршрутизаторы** – позволяют запретить/ограничить доступ некоторым пользователям к различным серверам, а также определенному «хосту»

Термин хост отражает роль устройства или программы как центр хранения данных или управления сервисами, услуги которых хост предоставляет клиентам

Задание N° 116 РТ