Под поиском информации понимают:

а) получение информации по электронной почте;

б) передачу информации на большие расстояния с помощью компьютерных систем;

в) получение нужной информации посредством наблюдения за реальной действительностью, использование каталогов, архивов, справочных систем, компьютерных сетей, баз данных и баз знаний и т.д.;

г) чтение художественной литературы;

д) сортировку информации.

Канал обратной связи в замкнутой информационной системе предназначен:

а) для осуществления объектом управления управляющих воздействий;

б) для кодирования информации, поступающей в аппаратно-программную часть;

в) для получения информации об окружающей среде;

г) для передачи в аппаратно-программную часть реакции потребителя на полученную им информацию;

д) для организации взаимодействия потребителя информации с окружающей средой.

В журнале успеваемости учащихся со сведениями о годовых оценках требуется осуществить поиск всех отличников по информатике. Что в этой ситуации является набором данных, что- ключом поиска, что- критерием поиска?

Набор данных- годовые оценки по информатике , ключ поиска- оценка по информатике, критерий поиска- пятёрка

- Какие методы поиска вы знаете?
- Что относится к атрибутам поиска?
- В журнале успеваемости учащихся со сведениями о годовых оценках требуется осуществить поиск всех отличников по информатике. Что в этой ситуации является набором данных, что- ключом поиска, что- критерием поиска?

14.01.2012

Защита информации

В 1997 году Госстандартом России разработан ГОСТ основных терминов и определений в области защиты информации. В этом документе дано следующее понятие защищаемой информации.

Какая информация называется защищаемой?

Защищаемая информация- информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Какая информация цифровой?

Цифровая информация- информация, хранение, передача и обработка которой осуществляются средствами ИКТ.

Какие основные виды угроз существует для цифровой информации?

1) кража или утечка информации;
2) разрушение, уничтожение информации

Какое определение защиты информации даётся в ГОСТе?

Защита информации- деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Какое воздействие называется несанкционированным?

Несанкционированное воздействие - это преднамеренная порча или уничтожение информации, а также информационного оборудования со стороны лиц, не имеющих на это права (санкции).

Какое воздействие называется непреднамеренным?

Непреднамеренное воздействие происходит вследствие ошибок пользователя, а также из-за сбоев в работе оборудования или программного обеспечения.

Что надо делать, чтобы быть спокойным за информацию в своём личном ПК?

- периодически осуществлять **резервное копирование:** файлы с наиболее важными данными дублировать и сохранять на внешних носителях;
- регулярно осуществлять **антивирусную проверку** компьютера;
- использовать **блок бесперебойного питания.**

Какие меры компьютерной безопасности следует использовать в школьном компьютерном классе?

Разграничение доступа для разных пользователей ПК.

Какие меры компьютерной безопасности следует использовать для защиты компьютеров, подключенных к сети?

- **брандмауэрами-** защитные программы. Критерии подозрительности может определять сам брандмауэр или задавать пользователь. Например, пользователь может запретить прием посланий по электронной почте с определенных адресов или определенного содержания. Брандмауэры могут предотвращать атаки, фильтровать ненужные рекламные рассылки и прочее. Брандмауэры, защищающие сети, подключенные к другим сетям, называются **межсетевыми экранами.**

Какие меры компьютерной безопасности следует использовать для защиты компьютеров, подключенных к сети?

- **системы шифрования**. Утечка информации может происходить путем перехвата в процессе передачи по каналам связи. Если от этого не удается защититься техническими средствами, то применяют. Методами шифрования занимается **криптография.**

Криптография и защита информации

- Самые ранние упоминания об использовании криптографии (в переводе- тайнописи) относятся ко временам Древнего Египта (1900 г. дон. э.), Месопотамии (1500 г. до н. э.).
- В V веке до н. э. в форме тайнописи распространялась Библия. Древнеримский император Юлий Цезарь придумал шифр, носящий название **шифра Цезаря.**
- Во время гражданской войны в США тайнопись использовалась для передачи секретных донесений как северянами, так и южанами.

Криптография и защита информации

- Во время Второй мировой войны польские и британские дешифровальщики раскрыли секрет немецкой шифровальной машины Энигма. В результате было уничтожено множество немецких подводных лодок, потоплен линкор «Бисмарк», и вооруженные силы Германии понесли тяжелые потери в ряде операций.
- С развитием компьютерных коммуникаций, «старая» криптография снова стала актуальной. Существующие методы шифрования делятся на методы с закрытым ключом и методы с открытым ключом. Ключ определяет алгоритм дешифровки.

Чем отличается шифрование с закрытым ключом от шифрования с открытым ключом?

- **Закрытый ключ-** это ключ, которым заранее обмениваются два абонента, ведущие секретную переписку. Это единый ключ, с помощью которого происходит как шифрование, так и дешифрование. Основная задача секретной переписки- сохранить ключ в тайне от третьих лиц.
- Алгоритмы с **открытым ключом,** или **асимметричные алгоритмы,** базируются на использовании отдельных шифровального (открытого) и дешифровального (закрытого) ключей. В алгоритмах с открытым ключом требуется, чтобы закрытый ключ было невозможно вычислить по открытому ключу.

Попробуйте догадаться, в чем секрет одного из вариантов ключа Цезаря, с помощью которого зашифровано слово «КРИПТОГРАФИЯ» в следующем шифрованном сообщении:

ЛСКРНПДСБФКА

Какая подпись называется цифровой?

Цифровая подпись- это индивидуальный секретный шифр, ключ которого известен только владельцу. В методах цифровой подписи часто используются алгоритмы шифрования с открытым ключом, но несколько иначе, чем обычно, а именно: закрытый ключ применяется для шифрования, а открытый- для дешифрования.

Что такое цифровой сертификат?

Цифровой сертификат- это сообщение, подписанное полномочным органом сертификации, который подтверждает, что открытый ключ действительно относится к владельцу подписи и может быть использован для дешифрования.

В левой части таблицы приведены возможные естественные или случайные некомпьютерные угрозы сохранности информации. Установите соответствие между этими угрозами и их «виновниками». К каждой позиции, данной в первом столбце, подберите соответствующую позицию из второго столбца

Факторы, угрожающие сохранности информации	Виновники
1. Ошибки в процессе сбора информации 2. Пожары и последствия их тушения 3. Ошибки подготовки данных 4. Водопроводные протечки 5. Плесень 6. Небрежность при хранении и учет 7. Аппаратные сбои в процессе обработки 8. Ошибки в программах пользователя 9. Ошибки ввода данных 10. Ошибки программного обеспечения 11. Неграмотное обращение с вычислительной техникой и (или) программным обеспечением 12. Ошибки операторов	А.Стихийные бедствия или случайные факторы Б.Человеческий фактор В.Случайные компьютерные ошибки Г.Угрозы со стороны некомпетентных пользователей ЭВМ

БАГААБВГГВГГ

- Учебник. §11. № 9, 10 письменно

ПРАКТИЧЕСКАЯ РАБОТА «АРХИВИРОВАНИЕ ФАЙЛОВ»

Ход выполнения

1. Открытие архивов

Меню KDE → **Служебные →Архиватор (Ark).**

Извлечение из архива

Действие → **Распаковать...** или щёлкнуть правой кнопкой мыши на файле.

Создание архивов и добавление файлов

- **Действие → Добавить файл...** Удерживая нажатой клавишу Ctrl вы можете выбирать несколько файлов или **Действие → Добавить папку...**.
- Другой способ добавления файлов в архив состоит в **переносе файлов мышью из Konqueror в главное окно Ark**