

2 курс

ПЛАН – КОНСПЕКТ
проведения вводного занятия по дисциплине
«Информатика»

Раздел 4. «Сетевые информационные технологии.»

Тема № 4.2: «Обработка, хранение, размещение, поиск, передача и защита информации. Антивирусные средства защиты информации».

Подготовил: преподаватель
В.Н. Борисов

**Вводное занятие
по Теме № 4.2 «Обработка, хранение, размещение, поиск, передача и
защита информации. Антивирусные средства защиты информации».**

Цель занятия: изучить со студентами основные сведения об обработке, хранении, размещении, поиске, передаче, защите информации, антивирусной защите средств вычислительной техники, программном обеспечении антивирусной защиты, работе с данными программными средствами.

Основные вопросы:

1. Передача и хранение информации. Средства хранения и передачи данных. Телекоммуникации.
2. Информационная безопасность. Защита информации от несанкционированного доступа.
3. Требования к выбору пароля.
4. Электронная подпись.
5. Основные положения Доктрины информационной безопасности Российской Федерации.
6. Компьютерные вирусы: методы распространения, профилактика заражения.
7. Защита информации от компьютерных вирусов.

Литература:

1. учебник: Гаврилов, М. В. Информатика. Базовый уровень. 10—11 классы : учебник для среднего общего образования / М. В. Гаврилов, В. А. Климов. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 352 с. — (Общеобразовательный цикл). — ISBN 978-5-534-16226-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/530644>, главы 11-12.
2. [2 учебник раздела «Основной учебной литературы» рабочей программы изучения дисциплины]: М. В. Гаврилов, В. А. Климов. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 355 с. — (Профессиональное образование). — ISBN 978-5-534-15930-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/viewer/informatika-i-informacionnye-tehnologii-536598#page/2>, главы 11-12, с.271-325.

Примерный расчет времени:

1. Вступительная часть – 20 мин.
2. Основная часть – 60 мин.
3. Заключительная часть – 10 мин.

Вступительная часть:

Занятие начать с объявления темы занятия, основных рассматриваемых вопросов, времени изучения темы (нового материала), закрепления на практике полученных знаний, перечисления литературы.

Основная часть (теоретическая):

Первый вопрос: Передача и хранение информации. Средства хранения и передачи данных. Телекоммуникации.

Передача, обработка и хранение информации происходит в форме сигналов или знаков.

Сигналы: можно разделить на несколько типов:

- по физической природе (электромагнитный, световой, тепловой, звуковой, биохимический);
- по способу восприятия (зрительный, слуховой, осязательный, вкусовой, болевой, физиологический).

Знаками можно считать алфавит любого языка, знаки языка жестов, любые коды и шифры, ноты и т.д.

Рассмотрим по отдельности передачу и хранение информации.

Передача информации.

Информация представляется и передается в форме последовательности сигналов, символов. От источника к приёмнику сообщение передается через некоторую материальную среду. Если в процессе передачи используются технические средства связи, то их называют каналами передачи информации (информационными каналами). К ним относятся телефон, радио, ТВ. Органы чувств человека исполняют роль биологических информационных каналов.

Передача информации — физический процесс, посредством которого осуществляется перемещение знаков (сведений, способных предоставлять информацию) в пространстве или осуществляется физический доступ субъектов к знакам. Передача информации — заблаговременно организованное техническое мероприятие, результатом которого становится воспроизведение информации, имеющейся в одном месте так называемый источник информации) или в другом месте (приёмник информации).

Передача информации – это целенаправленный процесс, в результате которого информация передается от одного объекта к другому.



Схема передачи информации

Любой процесс передачи информации упрощённо можно представить следующей схемой:



Передача информации



Как можно передать информацию?



Передача информации

Схема передачи информации



- Кодирующее устройство необходимо для преобразования информации в форму, удобную для передачи.
- Декодирующее устройство преобразует информацию в форму, понятную получателю.

Способы передачи информации

- ▶ Лекция (монолог, рассказ)
- ▶ Беседа (развернутые ответы на вопросы, рассуждения, пресс-конференции и т.п.).
- ▶ Работа с документом (индивидуальное чтение, анализ или групповой обсуждение, постановка вопросов и поиск ответов, выделение главного, формулирование выводов и т.п.).
- ▶ Обмен опытом (социальным и другим, в том числе и через проведение исследования).
- ▶ Интернет коммуникация (электронная почта, поисковые сайты, скайп).



Основные принципы передачи данных в компьютерных сетях.

Передача данных – в широком смысле – процесс передачи данных по каналу связи от источника к приемнику. Передача данных (обмен данными, цифровая передача, цифровая связь) – физический перенос данных (цифрового битового потока) в виде сигналов от точки к точке или от точки к нескольким точкам по каналу передачи данных.

Передача данных в компьютерных сетях – это процесс перемещения информации из одного места в другое с использованием сетевых устройств, таких как компьютеры, маршрутизаторы, коммутаторы и другие сетевые устройства. Передача данных может происходить через проводные или беспроводные сети, а также с использованием различных протоколов передачи данных.

Среды передачи данных в локальных вычислительных сетях.

Среда передачи – физическая субстанция, по которой происходит передача электрических, электромеханических, оптических, радиосигналов, использующихся для переноса той или иной информации.

Информация переносится с помощью сигналов. Сигналы могут иметь различную природу:

- электрическую (электроны по меди, заряженные ионы);
- механическую (звуковые волны по воздуху, сейсмические волны в грунте);
- электромеханическую;
- электромагнитную (радиоволны по воздуху, в безвоздушном пространстве или в грунте);
- оптическую (свет лазера по оптоволокну).

Среда передачи может быть естественной или искусственной.

Естественные среды:

- Космическое (безвоздушное) пространство;

Сигналы:

- электромагнитное излучение;
- свет;
- рентгеновское излучение;
- и другие виды излучения;

- Газообразные среды;

Сигналы:

- радиоволны;

- Жидкие (киселеобразные) среды;

Сигналы:

- звуковые волны;

- Твёрдые среды (грунт, камень, дерево ;

Сигналы:

- звуковые волны;
- сейсмические волны.

Звуковые и сейсмические волны хорошо проводятся твёрдыми материалами естественного происхождения (камень, дерево), что используется при создании электромеханических устройств приёма-передачи информации.

Искусственные среды для передачи сигналов по большей части представлены проводами и кабелями.

Среда передачи данных является составной частью канала связи.

Канал связи – система технических средств и среда распространения сигналов передачи данных (информации) от отправителя (источника) к получателю (приёмнику).

Выделяют следующие среды передачи:

- воздушная;
- проводная.

В качестве среды передачи сигналов между рабочими станциями в компьютерных сетях зачастую используется проводная среда.

Наиболее распространённые:

- коаксиальный кабель;
- оптоволоконный кабель;
- витая пара.

Обзор современных технологий передачи данных в локальных вычислительных сетях.

Для высокоскоростной передачи данных предпочтительно создавать и использовать специальные каналы и сети передачи данных. В сетях передачи данных используют специальные программно-технические средства, обеспечивающие соединение сетей между собой и с абонентами, а также высокоскоростную, надёжную и, как правило, защищённую передачу различной информации.

1. Технология Wi-Fi.

Wi-Fi (Wireless Fidelity) – технология радиосвязи, которая появилась еще в 1999 году. Она эволюционировала, но не изменила свое название.

2. Технология WiMAX.

Технология WiMAX это стандарт беспроводной связи.

3. Технология LTE.

Основной целью технологии LTE является предоставление более быстрой и стабильной связи для пользователей.

4. Технология Bluetooth.

Bluetooth – это стандарт беспроводной связи, обеспечивающий обмен данными между устройствами на основе ультракоротких радиоволн. От других стандартов беспроводной связи он отличается используемыми частотами, правилами передачи и способом шифрования данных.

5. Технология VLAN (локальных вычислительных сетей).

Телекоммуникации.

Телекоммуникация (греч. *tele* – вдаль, далеко и лат. *communicatio* – общение) – передача данных на большие расстояния.

Средства телекоммуникации – совокупность технических, программных и организационных средств для передачи данных на большие расстояния.

Телекоммуникационная сеть – множество средств телекоммуникации, связанных между собой и образующих сеть определённой топологии (конфигурации). Телекоммуникационными сетями являются (рис.2.1):

- телефонные сети для передачи телефонных данных (голоса);
- радиосети для передачи аудиоданных;
- телевизионные сети для передачи видеоданных;
- цифровые (компьютерные) сети или сети передачи данных (СПД) для передачи цифровых (компьютерных) данных.



Данные в цифровых телекоммуникационных сетях формируются в виде *сообщений*, имеющих определенную структуру и рассматриваемых как единое целое.

Данные (сообщения) могут быть:

- *непрерывными*;
- *дискретными*.

Непрерывные данные могут быть представлены в виде непрерывной функции времени, например, речь, звук, видео. Дискретные данные состоят из знаков (символов).

Передача данных в телекоммуникационной сети осуществляется с помощью их физического представления – *сигналов*.

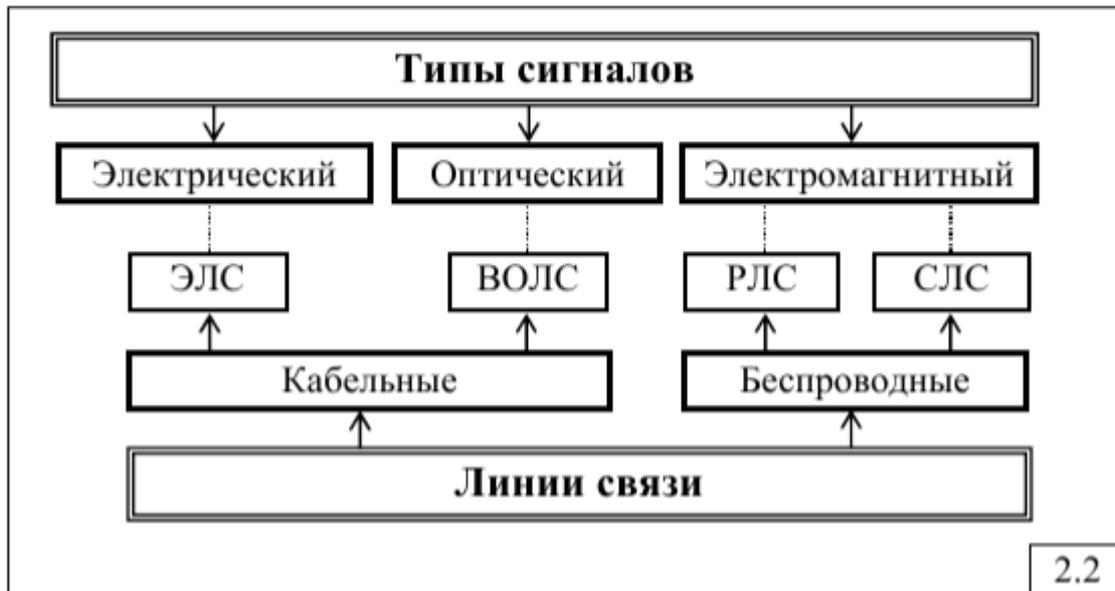
В компьютерных сетях для передачи данных используются следующие **типы сигналов** (рис.2.2):

- электрический (электрический ток);
- оптический (свет);
- электромагнитный (электромагнитное поле излучения – радиоволны).

Для передачи электрических и оптических сигналов применяются кабельные линии связи соответственно (рис.2.2):

- электрические (ЭЛС);
- волоконно-оптические (ВОЛС).

Передача электромагнитных сигналов осуществляется через радиолинии (РЛС) и спутниковые линии связи (СЛС).



Сигналы, как и данные, могут быть:

- непрерывными;
- дискретными.

При этом, непрерывные и дискретные *данные* могут передаваться в телекоммуникационной сети либо в виде непрерывных, либо в виде дискретных *сигналов*.

Процесс преобразования (способ представления) данных в вид, требуемый для передачи по линии связи и позволяющий, в некоторых случаях, обнаруживать и исправлять ошибки, возникающие из-за помех при их передаче, называется *кодированием*. Примером кодирования является представление данных в виде двоичных символов. В зависимости от параметров среды передачи и требований к качеству передачи данных могут использоваться различные методы кодирования.

Линия связи – физическая среда, по которой передаются информационные сигналы, формируемые специальными техническими средствами, относящимися к линейному оборудованию (передатчики, приемники, усилители и т.п.). Линию связи часто рассматривают как совокупность физических цепей и технических средств, имеющих общие линейные сооружения, устройства их обслуживания и одну и ту же среду распространения. Сигнал, передаваемый в линии связи, называется *линейным* (от слова линия).

Линии связи можно разбить на 2 класса (см. рис.2.2):

- кабельные (электрические и волоконно-оптические линии связи);
- беспроводные (радиолинии).

На основе линий связи строятся каналы связи.

Канал связи представляет собой совокупность одной или нескольких линий связи и каналообразующего оборудования, обеспечивающих передачу данных между взаимодействующими абонентами в виде физических сигналов, соответствующих типу линии связи.

На сегодняшний день основными отраслями телекоммуникаций являются:

- 1 Интернет, на который приходится около 30 %.
- 2 Мобильная связь, на которую приходится порядка 20 %.
- 3 Сети передачи данных, на которые приходится 15 %.
- 4 Спутниковые системы связи, на которых приходится около 10 %.
- 5 Аналоговое и цифровое телевидение, на которые приходится около 10 %.
- 6 Телефонная связь, на которую приходится около 10 %.
- 7 Электронных банкинг, на который приходится 5 %.

Подключение к Интернет.

С каждым днём всё больше разнообразных устройств получают возможность подключаться к сети Интернет. Это персональные и мобильные компьютеры, серверы и локальные сети, телефоны, игровые приставки и музыкальные центры. Их доступ к Сети и обслуживание обеспечивают Интернет-провайдеры – организации, предоставляющие услуги Интернет. Подключение к сети Интернет может осуществляться различными способами. Наиболее распространёнными являются:

1. Коммутируемый доступ по телефонной линии Dial-Up.
2. Доступ по цифровой абонентской линии ADSL.
3. Доступ по выделенному каналу связи.
4. Беспроводная цифровая связь.
5. Беспроводное подключение по мобильному телефону.



Преобразование информации из цифровой формы в электрические сигналы для передачи их по линиям связи и наоборот осуществляется с помощью модема (сокращение от слов «модулятор-демодулятор»).

Выбор типа модема определяется способом подключения к сети: аналоговый – для обычного подключения по телефону, цифровой – для ADSL подключения, радио-модем – для беспроводного подключения.

Для персональных компьютеров чаще всего используют внутренний модем, который с помощью стандартного разъёма подключается к слоту на материнской плате. Большинство современных ноутбуков имеют встроенный модем.

Важной характеристикой любой компьютерной сети является скорость передачи информации, т.е. количество информации, которое передаётся в единицу времени. За единицу скорости передачи принят 1 бит/с.

Скорость передачи информации в современных компьютерных сетях достигает сотен миллионов битов в секунду. Поэтому используют производные единицы: килобиты в секунду или мегабиты в секунду.

При коммутируемом доступе по телефонной линии модем по команде компьютера набирает номер телефона провайдера и, если телефонная линия не занята, устанавливает соединение с модемом провайдера. Поэтому такой способ подключения называется Dial-Up(по звонку). Затем проверяется имя пользователя и пароль. Если авторизация прошла успешно, осуществляется подключение к Интернету. На время сеанса компьютеру присваивается временный адрес. Во время сеанса работы в Интернете никто не может дозвониться до абонента – телефонная линия занята.

Скорость приёма передачи данных для аналоговых модемов достигает 56 кбит/с. Реальная скорость при коммутируемом доступе зависит от многих факторов: пропускной способности внешнего канала связи, количества одновременно подключенных пользователей, состояния телефонной линии.

Чем больше пользователей подключается, тем больше должна быть пропускная способность внешнего канала. Поэтому провайдер должен иметь многоканальный телефон и скоростной внешний канал связи, например со скоростью 30-60 Мбит/с и выше.

Более перспективной является технология ADSL (Asymmetric Digital Subscriber Line – асимметричная цифровая абонентская линия), которая позволяет передавать данные по телефонным сетям со скоростью до 8 Мбит/с к абоненту и до 1,5 Мбит/с от абонента (отсюда и название асимметричная). Реальная скорость передачи зависит от протяженности и качества линии. Обмен данными не мешает телефонному разговору благодаря разделению диапазонов частот сигналов в телефонной линии. Для подключения к ADSL требуется цифровой модем и устройство разделения сигналов. Доступ по выделенному каналу осуществляется путём постоянного подключения компьютера пользователя к серверу провайдера. Провайдер проводит к компьютеру абонента выделенную линию и выдаёт постоянный адрес. Пользователь получает постоянную связь с Интернетом, высокое качество соединения и передачи данных, высокую скорость (до 100 Мбит/с). Из оборудования необходима только сетевая карта.

Стоимость прокладки выделенной линии зависит от расстояния до точки подключения провайдера. Для индивидуальных пользователей этот способ доступа оправдан лишь тогда, когда на прокладку самой линии не требуется значительных затрат. Оптимальным вариантом является подключение к домашним или городским локальным сетям, в которых организован общий доступ к высокоскоростным интернет-соединениям. Подключаться к подобным сетям можно различными способами – фактически это обычные локальные сети. В последнее время получило широкое распространение подключение к Интернету по сетям кабельного телевидения. Возможны два варианта. При индивидуальном варианте кабельный модем устанавливается отдельно у каждого компьютера. При коллективном варианте в доме на несколько пользователей устанавливается один модем. Затем проводится локальная сеть и устанавливается необходимое оборудование. Достоинства: хорошая скорость, возможность просматривать цифровые каналы кабельного телевидения.

Беспроводная цифровая связь WiFi позволяет получить доступ к Интернету с помощью специального адаптера. В большинство современных ноутбуков он встроен. Существует несколько стандартов WiFi. Они различаются скоростью передачи данных, которая может достигать 50 Мбит/с. Реальная скорость передачи данных значительно ниже, но и этого достаточно для удобной работы в Интернете. Использование WiFi возможно, если Вы находитесь в зоне действия приёмных устройств. Достоинства: мобильность, неплохая скорость, минимум оборудования. Недостатки: небольшой радиус зоны покрытия одной точки доступа, проблема прямой видимости, ограничение количества пользователей в зоне действия WiFi.

Беспроводное подключение к Интернету по мобильному телефону осуществляется с помощью специальных протоколов мобильной связи. Один из сервисов наиболее распространённых в настоящее время сетей связи – GPRS. Максимальная скорость передачи данных по стандарту GPRS достигает 170 кбит/с. Реальная скорость не превышает 30-40 кбит/с и зависит от загруженности и возможностей сети сотового оператора, расстояния до антенны, характеристик конкретного мобильного телефона. Иногда GPRS-сети называют сетями второго поколения. Начинают развиваться и сети третьего поколения. Например, к ним относятся стандарты мобильного подключения CDMA и EDGE.

Способы подключения к интернету.

В середине девяностых единственным способом **подключиться к сети Интернет** был **телефонный модем**. Пользователь должен был установить модем на своем компьютере, подключиться к телефонной сети, ввести номер модемного пула, логин и пароль в специальной программе и дозваниваться до провайдера. Дозвон мог длиться от нескольких минут до нескольких часов,

телефонная линия была занята, да и скорость передачи данных оставляла желать лучшего. Через некоторое время появилась возможность **подключаться к сети Интернет с помощью технологии ADSL**. Пользователь приобретал специальный модем, который с помощью сплиттера подключался к телефонной сети, пользователь получал доступ в интернет и свободный телефон. Скорость и бесперебойность работы по ADSL-каналу определялась пропускной способностью АТС и телефонных сетей, основным преимуществом подобного соединения была возможность подключения по безлимитному тарифу. С течением времени появились новые технологии передачи данных, а простые пользователи интернета узнали новое слово – «**выделенка**». В квартиру пользователя монтажник прокладывал провод, в компьютер устанавливалась сетевая плата, и пользователь получал возможность пользоваться сетью интернет и локальными ресурсами местной сети. Первоначально провайдеры тарифицировали каждый скаченный мегабайт информации, ежемесячный счет за интернет мог составлять 100 долларов, но скорость работы, отсутствие сбоев и свободный домашний телефон делал такой способ подключения к сети очень удобным. Кроме того, провайдеры предоставляли бесплатный доступ к сетевым ресурсам, где можно было найти фильмы, музыку и полезные программы. Количество провайдеров постоянно росло, стоимость прокладки «последней мили» становилась все ниже, и провайдеры перешли на безлимитные тарифы, которые предоставляют возможность пользования интернетом без учета входящего трафика.

Выбор провайдера.

При выборе провайдера стоит обратить внимание на два основных параметра. Многие **интернет-провайдеры** предоставляют пользователям несимметричный канал, то есть скорость получения данных в несколько раз выше, чем скорость передачи. Если вы не закачиваете на удаленные сервера свои файлы, например, фотографии и видеоматериалы, а используете интернет только для просмотра страниц, то вы не заметите никакой разницы. Часто провайдеры заявляют о высокой скорости передачи данных, в настоящее время большинство пользователей предпочитают 10 мегабитные каналы, но довольно часто реальная скорость не соответствует заявленной. Часто оборудование для передачи данных устаревает, та и кабели, которые были проложены лет десять назад, изнашиваются, что приводит к значительной потере скорости передачи данных. Со временем пользователи смогли не только пользоваться интернетом, но и **подключаться к IP-телевидению**, которое транслировалось по этому же каналу связи. Для подключения данной услуги необходимо было приобрести специальный декодер и свитч. Кабель для передачи данных подключался к свитчу, от которого один кабель шел к компьютеру, а другой - к телевизионному декодеру, который подсоединялся к телевизору. В настоящее время многие провайдеры предлагают услугу доступа в интернет совместно с возможностью просмотра телевизионных программ. Такой пакет услуг очень выгоден футбольным болельщикам, так как большинство провайдеров имеют возможность предлагать пакеты «НТВ+».

WI-FI и другие современные способы подключения к интернету

Со временем технологии менялись, и передача данных в сеть интернет стала возможна с помощью **радиоканала WI-FI**. Во многих современных новостройках не прокладываются кабели, а устанавливается мощный **WI-FI передатчик**, который подключен к кабельной линии. Для доступа в интернет пользователь должен установить специальное устройство в свой компьютер, получить логин и пароль, и после этого он может начать пользоваться интернетом. Многие современные ноутбуки оснащены **WI-FI картой**, что делает доступ в интернет еще более доступным. **WI-FI роутер** можно установить в квартире или на лестничной площадке, но доступ в интернет желательно защитить паролем.

Доступ в интернет можно получить и **от провайдера цифрового телевидения**. Поток информации передается по коаксиальному (антенному) кабелю, на который устанавливается сплиттер. Далее один провод идет к декодеру видеозображения, который подключается к телевизору, а другой – к роутеру, который передает поток информации на компьютер пользователя. Если использовать WI-FI роутер, то не будет необходимости прокладывать дополнительные провода, но, к сожалению, вы получите асимметричный канал с невысокой скоростью передачи данных. Как правило, декодер и роутер берутся в аренду, но при покупке роутера, стоимость которого около 4000 рублей вы сможете получить бесплатный доступ в интернет. Для тех, кому важен **мобильный доступ в интернет**, можно посоветовать воспользоваться подключением к сети с помощью мобильного телефона. Подсоединив его к компьютеру, вы сможете по **каналам GSM- связи** передавать и получать информацию из сети. Данный способ информации очень дорог, да и скорость передачи невысока. В настоящее время можно приобрести USB – модемы, в которые работают по такой же технологии. **USB – модем** продается вместе с SIM-картой для доступа в Интернет. Несмотря на обилие тарифов, этот способ доступа к интернету является одним из самых дорогих, так как не существует единой технологии передачи данных. Одним из недорогих и надежных мобильных способов **подключения к сети интернет** является подключение по **технологии 4 G**. Данную технологию активно продвигает на российский рынок компания Yota. Для подключения к сети вам нужно приобрести специальный модем и подключить его к компьютеру. Вы сможете получить доступ в сеть интернет практически в любом месте в крупных российских городах за 900 рублей в месяц. В настоящее время многие современные устройства оснащаются модемами, предназначенными для работы с **сетью 4 G**, в этом случае вам понадобится только **настроить ваш компьютер** или мобильный телефон, стоимость услуг составит 500 рублей в месяц. Данный способ связи удобен в качестве дополнительного канала связи или для жителей мегаполисов, которым необходим **выход в сеть интернет** в любой точке города. Интернет позволяет рационально использовать нам своё время - теперь мы можем оплатить услуги и товары, не выходя из дома, имея электронный кошелек и электронные деньги, или расплачиваться с помощью банковских карточек, или передавать/получать нужную информацию практически мгновенно. Именно поэтому нам так важно выбрать наиболее удобное подключение к системе интернет.

Хранение информации.

Под хранением обычно понимают запись данных на некоторые накопители данных (запоминающие устройства) с целью их (данных) дальнейшего использования.

Хранение информации осуществляется записью на носителях и накопителях информации. Носителем данных может являться любой материальный предмет, используемый человеком для записи, хранения, чтения и передачи информации (например, книги, диски, фотографии, flash-карты, облачные хранилища и так далее). Накопителями считаются приспособления позволяющие хранить и дополнять информацию.

Хранение является одной из основных операций, осуществляемых над информацией, с целью обеспечения её доступности в течение некоторого промежутка времени.

Основные параметры устройств хранения информации.

Классификация по типу устройства хранения информации		
Внутренние	Внешние	Мобильные
1. Оперативная память - хранения обрабатываемой информации (данных) и программ, управляющих процессом обработки информации;	1. Жесткий магнитный диск - постоянная память, предназначена для долговременного хранения всей имеющейся в компьютере информации;	1. Мини или микро CD (для мобильных телефонов);
2. Кэш-память - Наличие такой памяти позволяло микропроцессору всегда хранить данные "под рукой";	2. CD,DVD;	2. Онлайн-хранилище – это способ дистанционного хранения данных в электронном виде, в том числе и больших объемов.
3. CMOS-память для длительного хранения данных о конфигурации и настройке компьютера (дата, время, пароль), в том числе и когда питание компьютера выключено.	3. Стримеры - по принципу действия очень похож на кассетный магнитофон;	
	4. Flesh-карта - устройства, выполненные на одной микросхеме (кристалле) и не имеющие подвижных частей	



🔒 Где купить

Интерфейс	Пропускная способность (Мбит/с.)	Макс. длина кабеля, м	Кабель питания	Кол-во накопителей на канал	Число проводников в кабеле	Особенности
ATA 100 (PATA)	800	0.46	3.5" Да 2.5" Нет	2	40	Controller+2Slave, горячая замена невозможна
ATA 133	1064	0.46	3.5" Да 2.5" Нет	2	40/80	Controller+2Slave, горячая замена невозможна
SATA(150)	1200	1	Да	1	7	Host/Slave, возможна горячая замена на некоторых контроллерах
SATAII(300)	3000	1	Да	1	7	Host/Slave, возможна горячая замена на некоторых контроллерах
SATAIII(600)	6144	нет данных	Да		7	
eSATA	3000	2	Да	1 (с множителем портов до 15)	4	Host/Slave, горячая замена возможна
Ultra-320 SCSI	2560	12	Да	16	50/68	устройства равноправны, горячая замена возможна
SAS	3000	8	Да	Свыше 16384		горячая замена; возможно подключение SATA-устройств в SAS-контроллеры
FireWire/400	400	4.5 (при послед-ном соединении до 72 м)	Да/Нет (зависит от типа интерфейса и накопителя)	63	4/6	устройства равноправны, горячая замена возможна
FireWire/800	800	4.5 (при послед-ном соединении до 72 м)	Нет	63	4/6	устройства равноправны, горячая замена возможна
USB 2.0	480	5 (при послед-ном соединении, через хабы, до 72 м)	Да/Нет (зависит от типа накопителя)	127	4	Host/Slave, горячая замена возможна
USB 3.0	4800	нет данных	Да/Нет (зависит от типа накопителя)	127	9	Двухнаправленный, совместим с USB 2.0

Также сведения по данному вопросу представлены в файлах Приложение № 1 - Накопители информации.pdf, Приложение № 2 - Носители информации.pdf.

Второй вопрос: Информационная безопасность. Защита информации от несанкционированного доступа.

Информационная безопасность.

Если компания хранит бухгалтерскую информацию, клиентскую базу, анкеты сотрудников или корпоративные тайны, то важно, чтобы эти данные не попали не в те руки, то есть были защищены. Защитой данных занимается информационная безопасность.

Информационная безопасность — это различные меры по защите информации от посторонних лиц. В доцифровую эпоху для защиты информации люди запирали важные документы в сейфы, нанимали охранников и шифровали свои сообщения на бумаге.

Сейчас чаще защищают не бумажную, а цифровую информацию, но меры, по сути, остались теми же: специалисты по информационной безопасности создают защищенные пространства (виртуальные «сейфы»), устанавливают защитное

ПО вроде антивирусов («нанимают охранников») и используют криптографические методы для шифрования цифровой информации.

Однако цифровую информацию тоже нужно защищать не только виртуально, но и физически. Антивирус не поможет, если посторонний похитит сам сервер с важными данными. Поэтому их ставят в охраняемые помещения.

За что отвечает информационная безопасность?

Она отвечает за три вещи: конфиденциальность, целостность и доступность информации. В концепции информационной безопасности их называют принципами информационной безопасности.

Конфиденциальность означает, что доступ к информации есть только у того, кто имеет на это право. Например, ваш пароль от электронной почты знаете только вы, и только вы можете читать свои письма. Если кто-то узнает пароль или другим способом получит доступ в почтовый ящик, конфиденциальность будет нарушена.

Целостность означает, что информация сохраняется в полном объеме и не изменяется без ведома владельца. Например, на вашей электронной почте хранятся письма. Если злоумышленник удалит некоторые или изменит текст отдельных писем, то это нарушит целостность.

Доступность означает, что тот, кто имеет право на доступ к информации, может ее получить. Например, вы в любой момент можете войти в свою электронную почту. Если хакеры атакуют серверы, почта будет недоступна, это нарушит доступность.

Какая бывает информация и как ее защищают.

Информация бывает общедоступная и конфиденциальная. К общедоступной имеет доступ любой человек, к конфиденциальной — только отдельные лица.

Может показаться, что защищать общедоступную информацию не надо. Но на общедоступную информацию не распространяется только принцип конфиденциальности — она должна оставаться целостной и доступной. Поэтому информационная безопасность занимается и общедоступной информацией.

Например, возьмем интернет-магазин. Карточки товаров, статьи в блоге, контакты продавца — все это общедоступная информация, ее может просматривать любой. Но интернет-магазин все равно нужно защищать, чтобы никто не нарушил его работу, например, не изменил важную информацию в карточках товаров или не «уронил» его сайт.

Главная задача информационной безопасности в IT и не только — защита конфиденциальной информации. Если доступ к ней получит посторонний, это приведет к неприятным последствиям: краже денег, потере прибыли компании, нарушению конституционных прав человека и другим неприятностям.

Информация бывает общедоступная и конфиденциальная. К общедоступной имеет доступ любой человек, к конфиденциальной — только отдельные лица.

Основные виды конфиденциальной информации.

Персональные данные. Информация о конкретном человеке: ФИО, паспортные данные, номер телефона, физиологические особенности, семейное положение и другие данные. В России действует 152-ФЗ — закон, который обязывает охранять эту информацию. Мы подробно рассказывали об этом в статье «Как выполнить 152-ФЗ о защите персональных данных и что с вами будет, если его не соблюдать».

Тот, кто работает с персональными данными, обязан защищать их и не передавать третьим лицам. Информация о клиентах и сотрудниках относится как раз к персональным данным.

Коммерческая тайна. Внутренняя информация о работе компании: технологиях, методах управления, клиентской базе. Если эти данные станут известны посторонним, компания может потерять прибыль.

Компания сама решает, что считать коммерческой тайной, а что выставлять на всеобщее обозрение. При этом не вся информация может быть коммерческой тайной — например, нельзя скрывать имена учредителей юрлица, условия труда или факты нарушения законов. Подробнее о коммерческой тайне рассказывает закон 98-ФЗ.

Профессиональная тайна. Сюда относятся врачебная, нотариальная, адвокатская и другие виды тайны, относящиеся к профессиональной деятельности. С ней связано сразу несколько законов.

Служебная тайна. Информация, которая известна отдельным службам, например, налоговой или ЗАГСу. Эти данные обычно хранят государственные органы, они отвечают за их защиту и предоставляют только по запросу.

Государственная тайна. Сюда относят военные сведения, данные разведки, информацию о состоянии экономики, науки и техники государства, его внешней политики. Эти данные самые конфиденциальные — к безопасности информационных систем, в которых хранится такая информация, предъявляют самые строгие требования.

Если ваша компания хранит персональные данные, коммерческую или профессиональную тайну, то эти данные нужно защищать особым образом. Для этого необходимо ограничить доступ к ней посторонним лицам — установить уровни доступа и пароли, поставить защитное ПО, настроить шифрование.

Кратко об информационной безопасности и защите информации.

1. Информационная безопасность отвечает за защиту данных и обеспечивает их конфиденциальность, целостность и доступность.
2. Конфиденциальность означает, что доступ к данным есть только у тех, кто имеет на это право.

3. Целостность означает, что данные хранятся в неизменном виде и остаются достоверными.
4. Доступность означает, что человек, у которого есть право на доступ к информации, может ее получить.
5. Информационная безопасность защищает и конфиденциальные, и общедоступные данные. Общедоступным она обеспечивает целостность и доступность, конфиденциальным — еще и нужный уровень секретности.
6. К конфиденциальной информации относятся персональные данные, коммерческая, профессиональная, служебная и государственная тайны.

Основные определения по информационной безопасности.

Объекты защиты.

Основными объектами защиты при обеспечении информационной безопасности являются:

- все виды информационных ресурсов. Информационные ресурсы (документированная информация);
- информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать;
- права граждан, юридических лиц и государства на получение, распространение и использование информации;
- система формирования, распространения и использования информации (информационные системы и технологии, библиотеки, архивы, персонал,
- нормативные документы и т.д.);
- система формирования общественного сознания (СМИ, социальные институты и т.д.).

ФЗ "Об информации, информационных технологиях и о защите информации".

В Российском законодательстве базовым законом в области защиты информации является ФЗ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ. Поэтому основные понятия и решения, закрепленные в законе, требуют пристального рассмотрения.

Закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;

• обеспечении защиты информации. Закон дает основные определения в области защиты информации.

Приведем некоторые из них:

- информация – сведения (сообщения, данные) независимо от формы их представления;
- информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
- конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

В вышеназванном ФЗ дается следующее определение защите информации - представляет собой принятие правовых, организационных и технических мер, направленных на:

1. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2. соблюдение конфиденциальности информации ограниченного доступа;
3. реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1. предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
2. своевременное обнаружение фактов несанкционированного доступа к информации;
3. предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
4. недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
5. возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
6. постоянный контроль за обеспечением уровня защищенности информации.

Защита информации от несанкционированного доступа.

Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа к информации.

Защита информации от несанкционированного доступа в государственных и коммерческих структурах организована на основе системы законодательных и нормативно-правовых документов. Комплекс руководящих документов, регламентирующих вопросы защиты информации от НСД разработан Гостехкомиссией РФ, которая является основной организацией курирующей это направление защиты информации.

Комплекс руководящих документов по защите от НСД включает:

- 1) Концепцию защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.)
- 2) Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники
- 3) Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации
- 4) Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации
- 5) Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации
- 6) Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей.

Защита от несанкционированного доступа. Термины и определения.

Известны такие направления исследования проблемы безопасности информации, как радиотехническое, побочные электромагнитные излучения и наводки, акустическое, НСД и другие.

Несанкционированный доступ (НСД) определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС.

Под **штатными средствами** понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

Определение НСД в руководящих документах Гостехкомиссии РФ отличается по содержанию от определения НСД по ГОСТ Р 50922-96 «Защита информации. Основные термины и определения», в котором акцент на использование штатных средств при осуществлении НСД не делается.

Защита СВТ и АС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от НСД к информации.

Защита СВТ обеспечивается комплексом программно-технических средств. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

В качестве **нарушителя** рассматривается субъект, имеющий доступ к работе со штатными средствами АС и СВТ как части АС. Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей. Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС - запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

В своем уровне нарушитель является специалистом высшей квалификации, знает все об АС и, в частности, о системе и средствах ее защиты.

К основным способам НСД относятся:

1) непосредственное обращение к объектам доступа. Появление этого способа НСД возможно при выборе неправильной политики информационной безопасности, когда остаются возможности непосредственного обращения субъектов к объектам доступа без посредничества механизмов защиты. Например, если в таблице разграничения доступа не ограничены права пользователя по доступу к файлам и каталогам;

2) создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты. Этот способ НСД появляется, если используемые программные и технические средства не проверены на отсутствие недеklarированных возможностей или в АС имеются инструментальные средства для создания программ. В этом случае имеющиеся или специально созданные пользователем средства могут иметь возможность обращаться к объектам защиты в обход механизмов защиты, используя низкоуровневые команды;

3) модификация средств защиты, позволяющая осуществить НСД. Модификация средств защиты возможна при наличии в них конструктивных дефектов, например, «люков» в программных средствах, не удаленных после отладки программы;

4) внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

Внедрение программных или программно-аппаратных закладок, как правило, производится на этапе разработки и создания средств СВТ. Чаще всего, в

программные средства включают программные закладки типа «троянского коня», которые способны на несанкционированные действия, например, перехват пароля пользователя и передачу его по сети создателю закладки.

Обеспечение защиты СВТ и АС осуществляется:

- 1) системой разграничения доступа (СРД) субъектов к объектам доступа;
- 2) обеспечивающими средствами для СРД.

Методы защиты от несанкционированного доступа.

Методы защиты компьютеров от несанкционированного доступа делятся на программно-аппаратные и технические. Первые отсекают неавторизованных пользователей, вторые предназначены для исключения физического проникновения посторонних людей в помещения компании.

Создавая систему защиты информации (СЗИ) в организации, следует учитывать, насколько велика ценность внутренних данных в глазах злоумышленников.

Для грамотной защиты от несанкционированного доступа важно сделать следующее:

- отсортировать и разбить информацию на классы, определить уровни допуска к данным для пользователей;
- оценить возможности передачи информации между пользователями (установить связь сотрудников друг с другом).

В результате этих мероприятий появляется определенная иерархия информации в компании. Это дает возможность разграничения доступа к сведениям для сотрудников в зависимости от рода их деятельности.

Аудит доступа к данным должен входить в функционал средств информационной безопасности. Помимо этого, программы, которые компания решила использовать, должны включать следующие опции:

- аутентификация и идентификация при входе в систему;
- контроль допуска к информации для пользователей разных уровней;
- обнаружение и регистрация попыток НСД;
- контроль работоспособности используемых систем защиты информации;
- обеспечение безопасности во время профилактических или ремонтных работ.

Идентификация и аутентификация пользователей.

Для выполнения этих процедур необходимы технические средства, с помощью которых производится двухступенчатое определение личности и подлинности полномочий пользователя. Необходимо учитывать, что в ходе идентификации

необязательно устанавливается личность. Возможно принятие любого другого идентификатора, установленного службой безопасности.

После этого следует аутентификация – пользователь вводит пароль или подтверждает доступ к системе с помощью биометрических показателей (сетчатка глаза, отпечаток пальца, форма кисти и т. п.). Кроме этого, используют аутентификацию с помощью USB-токенов или смарт-карт. Этот вариант слабее, так как нет полной гарантии сохранности или подлинности таких элементов.

Защита данных на ПК.

Для защиты информации, хранящейся на жестких дисках компьютеров, используются многоступенчатые средства шифрования и авторизации. При загрузке операционной системы используется сложный пароль, который невозможно подобрать обычными методами. Возможность входа в систему пользователя со стороны исключается путем шифрования данных в BIOS и использования паролей для входа в разделы диска.

Для особо важных устройств следует использовать модуль доверенной загрузки. Это аппаратный контроллер, который устанавливается на материнскую плату компьютера. Он работает только с доверенными пользователями и блокирует устройство при попытках включения в отсутствие владельца.

Также применяются криптографические методы шифрования данных, превращающие текст «вне системы» в ничего не значащий набор символов.

Эти мероприятия обеспечивают защиту сведений и позволяют сохранить их в неприкосновенности.

Определение уровней защиты.

С методической точки зрения процесс защиты информации можно разделить на четыре этапа:

- предотвращение – профилактические меры, ограничение доступа посторонних лиц;
- обнаружение – комплекс действий, предпринимаемых для выявления злоупотреблений;
- ограничение – механизм снижения потерь, если предыдущие меры злоумышленникам удалось обойти;
- восстановление – реконструкция информационных массивов, которая производится по одобренной и проверенной методике.

Каждый этап требует использования собственных средств защиты информации, проведения специальных мероприятий. Необходимо учитывать, что приведенное разделение условно. Одни и те же действия могут быть отнесены к разным уровням.

Стандартность архитектурных принципов построения, оборудования и программного обеспечения персональных компьютеров, мобильность

программного обеспечения определяют сравнительно легкий доступ к информации, находящейся в персональном компьютере.

Несанкционированный доступ к информации персонального компьютера - незапланированное ознакомление, обработка, копирование, применение различных вирусов, модификация или уничтожение информации в нарушение правил доступа.

Под защитой информации понимают создание организованной совокупности средств, методов и мероприятий, предназначенных для предупреждения искажения, уничтожения или несанкционированного использования защищаемой информации. К ним относятся аппаратные и программные средства, криптографическое закрытие информации, физические меры, организационные мероприятия и законодательные меры. Один из методов защиты - парольная идентификация, ограничивающая доступ несанкционированного пользователя.

Включение защиты в программу связано с разработкой программ с запросом информации, т.е. требующих для своей работы ввода дополнительной информации, такой как пароли или номера ключей. Однако такая проверка доступа к программам или системам не должна существенно сказываться на быстродействии программы или требовать от пользователя сложных дополнительных действий.

Третий вопрос: Требования к выбору пароля.

Каждый пользователь компьютера или мобильных устройств сталкивался с необходимостью создания пароля для защиты своих учетных данных (учетная запись устройства, аккаунты электронной почты, интернет банкинга или социальной сети). Однако немногие относятся к созданию надежных паролей с должной аккуратностью.

Прежде всего надежный пароль — это пароль, обладающий следующими качествами:

Сложность. К созданию пароля необходимо подойти ответственно вне зависимости от вида и важности ресурса, где он будет использоваться. При создании сложного пароля стоит придерживаться следующих правил:

- Длина пароля. Пароль должен содержать не менее 8 символов, а лучше – 10 и более.
- Наличие цифр и букв верхнего и нижнего регистров, идущих не подряд – AAaaBBbb.
- Наличие специальных знаков – «@», «\$», «&» и т.д. (если допустимо их присутствие).

Несмотря на то что многие ресурсы при регистрации принудительно заставляют, придумать сложный пароль (требуя определенную длину пароля, наличие цифр и букв, а также специальных символов), пользователи зачастую просто стараются выполнить эти требования, не задумываясь о надежности такого пароля. В результате получается что-то похожее на – p@ssword1234.

Использование паролей типа «qwerty1234», «abcd12345», «p@ssword1234» не гарантирует надежную защиту данных, поскольку программы подбора паролей, которыми пользуются злоумышленники, в первую очередь проверяют именно такие пароли.

Надежный пароль не должен содержать имена, клички животных или названия городов, а также цифры даты рождения или номера телефонов. Пароль типа «M@sha1990» будет угадан программами по подбору паролей, т.к. содержит достаточно распространенную комбинацию букв.

Уникальность. Для каждого ресурса необходимо иметь свой пароль. Это обусловлено необходимостью защиты всех остальных пользовательских ресурсов при компрометации пароля одного ресурса.

Пароль должен быть известен только пользователю, иначе никакой надежной защиты уже быть не может. Нежелательно записывать пароли на бумаге и тем более держать эти записи рядом с компьютером в открытом доступе для всех. Кроме того, не рекомендуется вводить свои пароли на сайтах по проверке надежности паролей, так как они могут оказаться ловушками для паролей.

Как выбирать (создавать) надежные пароли:

1. Генерация пароля с помощью специализированных программ.

Тем пользователям, кому сложно придумать надежный пароль самостоятельно, можно порекомендовать воспользоваться сервисами по генерации надежных паролей. При необходимости программа сгенерирует пароль необходимой длины, с наличием специальных символов и букв разных регистров, например – \$y@85u!K1n3x.

Важным требованием является то, чтобы это была именно программа, установленная на устройстве, а не онлайн сервис. В противном случае, сгенерируемый пароль может быть известен не только пользователю, но и попасть в базы злоумышленников. К оффлайн сервисам можно отнести: ViPNet Password Generator, Random password generator, Drowssap.

2. Самостоятельное создание пароля с помощью своей методики.

Требования к обычному паролю	Требования к парольной фразе
<ul style="list-style-type: none"> • Имеет минимум 8 символов; • Включает в себя заглавные и строчные буквы; • Включает в себя один или более символов (@, #, \$ и т.д.); • Запрещает слова из словаря; • Запрещает личную информацию пользователя 	<ul style="list-style-type: none"> • Нужно хотя бы 16 символов; • Включает в себя заглавную букву или цифру

Требования к надежному паролю:

1. Пароль должен быть секретным
2. Пароль должен быть длинным
3. Пароль должен быть трудно угадываемым
4. Пароль не должен представлять собой распространенные слова, имена, названия
5. Пароль должен быть сложным
6. Пароль должен регулярно меняться

Парольная идентификация.

Пароль - это код, используемый для получения доступа к системам или файлам, оснащенным парольной защитой.

Пароли обеспечивают сохранение целостности программного обеспечения в составе вычислительной системы, но для поддержания паролей требуется высокая дисциплинированность. При первой регистрации пользователя администратор определяет круг полномочий для получения и изменения информации или выполнения определенных управляющих действий в системе, руководствуясь его профессиональными обязанностями и должностными инструкциями. Затем пользователю предлагается ввести свой пароль согласно правилам, принятым в данной системе. Метод паролей требует, чтобы вводимый пользователем пароль (строка символов) сравнивался с тем, который хранится в вычислительной системе для данного пользователя. Если пароль верен, система должна вывести на экран терминала дату и время последнего входа в систему этого пользователя. Затем пользователю предоставляется возможность пользоваться всей информацией, доступ к которой ему разрешен

(пароли можно также использовать независимо от пользователя для защиты файлов, записей, полей данных внутри записей и т.д.).

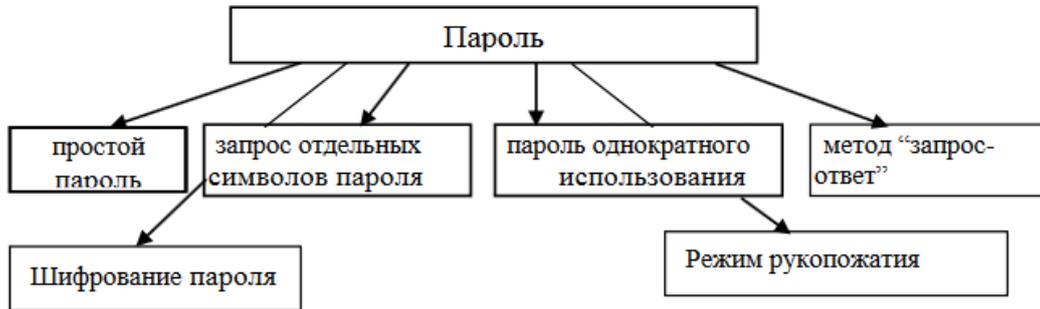


Рисунок 7.2 - Виды паролей

Простой пароль

Простой пароль - вводимая пользователем с клавиатуры строка символов. В схеме с простым паролем пользователю разрешается самому выбирать пароль таким образом, чтобы его было легко запомнить. Иногда в ряду символов пароля и в конце его оставляют пробелы. Отличие действительного пароля от кажущегося (без пробелов) повышает защищенность системы.

Подбор пароля путем простого перебора комбинаций предполагает перебор всех возможных сочетаний символов в пароле. Время, необходимое для разгадывания пароля методом простого перебора, является геометрической прогрессией от длины пароля, но есть различные кривые, зависящие от размера алфавита, на основе которого был создан пароль и от размера набора символов, по отношению к которым рассматриваются различные пароли.

Пароли однократного использования могут применяться также для установления подлинности подтверждения об отключении ЭВМ от обслуживания пользователя и подтверждения подлинности требования пользователя об отключении от ЭВМ. Всякий раз, когда получено требование пользователя об окончании работы, ЭВМ немедленно передает ему свой пароль однократного использования и прерывает связь. Если пользователь отключается и не получает истинного пароля от ЭВМ, ему следует принять меры предосторожности.

Четвертый вопрос: Электронная подпись.

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию⁵.

ЭП представляет собой комбинацию символов, которая формируется в результате математического преобразования исходного документа при помощи специального программного обеспечения. ЭП добавляется к исходному документу при пересылке, и любое изменение исходного документа делает эту ЭП недействительной. Таким образом, ЭП безошибочно указывает на подлинность и авторство, не переносится с одного документа на другой документ, защищает подписанный документ от подделки, а также от изменения или искажения информации.

ЭП основана на асимметричном криптографическом алгоритме. Особенностью такого алгоритма является то, что используются два разных ключа: один ключ для зашифрования информации, а второй, который специальным образом получен из первого и отличается от него, – для ее расшифрования.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Первый ключ является секретным – закрытым (личным) ключом, о котором известно только лицу, подписывающему документ. Вторым ключом является открытый ключ, он может быть известен любому получателю электронного документа.

Открытый ключ публикуется на сайте удостоверяющего центра, услугами которого пользуется владелец ключа, а закрытый ключ он хранит со всеми возможными мерами предосторожности.

УЦ является системой управления ключами в рамках криптографической системы на основе инфраструктуры открытых ключей (закрытый ключ известен только его владельцу).

УЦ создает сертификат открытого ключа и таким образом удостоверяет этот ключ.

УЦ подтверждает или опровергает принадлежность открытого ключа лицу, которое владеет соответствующим закрытым ключом. Удостоверяющий центр – это организация, которая выпускает сертификаты ключей проверки ЭП и отвечает за управление криптографическими ключами пользователей. Открытые ключи и другая информация о пользователях хранится удостоверяющими центрами в виде цифровых сертификатов.

Сертификат – это электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи⁶.

Выдавая сертификат, УЦ удостоверяет подлинность связи между открытым ключом пользователя УЦ и информацией, его идентифицирующей. И ключ, и сертификат хранятся в файлах. Для того, чтобы никто, кроме владельца подписи, не мог воспользоваться закрытым ключом, его обычно записывают на съемный носитель ключа (например, «Рутокен»). Для дополнительной защиты его снабжают PIN-кодом. Для создания электронной подписи необходимо ввести правильное значение PIN-кода. Сертификат содержит всю необходимую информацию для проверки электронной подписи. Данные сертификата открыты и публичны. Поэтому обычно

сертификаты хранятся в хранилище сертификатов операционной системы. И, конечно, все сертификаты всегда хранятся в УЦ⁷.

Схема цифровой подписи – набор алгоритмов и протоколов, позволяющих построить информационное взаимодействие между двумя и более участниками

таким образом, чтобы факт авторства переданного массива данных, «подписанного одним из участников», мог быть надежно подтвержден или опровергнут третьей стороной.

Любая схема цифровой подписи предполагает добавление к подписываемому массиву данных дополнительного кода - цифровой подписи, выработать которую может только автор сообщения, обладающий секретным ключом подписи, а все остальные могут лишь проверить соответствие этой подписи подписанным данным.

Процедура ЭЦП на базе асимметричного криптографического алгоритма включает в себя процедуры выработки и проверки подписи под данным сообщением. Цифровая подпись, состоящая из двух целых чисел, вычисляется с помощью определенного набора правил.

ЭЦП обеспечивает:

Защиту от изменений документа. При любом случайном или преднамеренном изменении документа (или подписи) подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему.

Невозможность отказа от авторства. Так как создать корректную подпись можно лишь, зная закрытый ключ, а он известен только владельцу, то владелец не может отказаться от своей подписи под документом.

Пятый вопрос: Основные положения Доктрины информационной безопасности Российской Федерации.

Основные положения Доктрины информационной безопасности Российской Федерации представлены в приложении № 3 к данному план-конспекту.

Шестой вопрос: Компьютерные вирусы: методы распространения, профилактика заражения.

Седьмой вопрос: Защита информации от компьютерных вирусов.

Сведения о видах компьютерных вирусов, антивирусных средствах защиты, антивирусных программах, представлены в приложениях № с 4-1 по 4-3 к данному план-конспекту.

Заключительная часть.

1. Закончить изложение материала.
2. Ответить на возникшие вопросы.
3. Подвести итоги занятия.
4. Дать задание на самоподготовку (домашнее задание).

Задание на самоподготовку (домашнее задание):

1. Детально проработать, законспектировать материал занятия, размещенный в данном план–конспекте, в учебниках, указанных на с.2 текущего документа, приложениях к данному план-конспекту (теоретическим сведениям по Теме 4.2).
2. Подготовиться к опросу по пройденному материалу.