
«Защита информации»
www.vuvk.gino-net.ru

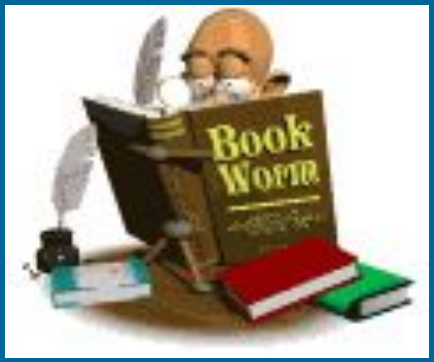
Оглавление

Понятие и определение информации

Информация - (от лат. informatio - ознакомление, разъяснение, представление, понятие) это сведения, знания или сообщения, которые являются объектом хранения, передачи, преобразования и которые могут оказать помощь в решении проблем, возникающих в процессе жизнедеятельности человека.

Сведения, хранящиеся в отдельном компьютере или группе компьютеров сети, имеют потребительскую ценность, так как либо непосредственно сами, либо их использование при организации процедуры работы с данными (получаемой при наблюдении за процессами и вводимой в компьютер информации) позволяет удовлетворить какую-либо потребность.

По мнению американских деловых кругов, утрата 20% информации ведет с вероятностью 60% к разорению фирмы в течение одного месяца.



Факторами, способствующими повышению уязвимости информационных сетей, являются:

1) рост количества информации, накапливаемой, хранимой и обрабатываемой в сети;
2) соединение в единых базах данных информации различного содержания и различной принадлежности;
3) расширение круга пользователей сети, возможностей их непосредственного доступа к ресурсам сети;
4) усложнение режимов работы вычислительных средств, использование многопользовательского режима, режимов реального времени и разделения во времени;
5) автоматизация межмашинного обмена информацией;
6) как ни странно, этому способствует и упрощение использования операционных систем, более дружественный человеко-машинный интерфейс;
7) более высокая подготовка пользователей и более высокая стоимость информации.

Основными умышленными угрозами безопасности сети являются:

1) раскрытие конфиденциальности информации;
2) компрометации информации, снижение доверия к ней;
3) несанкционированное использование ресурсов сети, целью которого является раскрытие или компрометация информации, либо решение своих проблем без ведома владельца сети и за его счет;
4) несанкционированный обмен информацией между пользователями, что может привести к получению одним из них не предназначенных ему сведений;
5) отказ от информации, непризнание получателем или отправителем информации факта ее получения (отправления), что ведет к злоупотреблению при использовании информации и компрометации сети

Виды защиты вычислительной сети информационной системы

В зависимости от угрозы и ценности функционирования сети используются разные компоненты системы защиты, а также организуется совместное использование отдельных видов и средств защиты.

Организационные аспекты защиты информации должны уменьшить как возможность похищения или физического разрушения ее оборудования рациональным размещением, подбором и оборудованием помещения и ее охраной, так и организацией работы с пользователями, персоналом, правильным определением их статуса и его соответствием статусу используемой информации, распределением ресурсов, разработкой мер идентификации пользователей и организацией их работы, ведением соответствующей учетно-планирующей документации.

Аппаратные аспекты защиты информации направлены в первую очередь на применение в ней совместимого оборудования, его грамотное подключение, обеспечивающее циркулирование информации в требуемом объеме и с требуемым качеством, ограничение возможности несанкционированного подключения к сети, повышение сохранности информации и возможности ее восстановления в случае искажения, уменьшение вероятности ее считывания внешними устройствами.

Программные аспекты защиты информации направлены на сохранение информации в ней, например, периодическим перезаписыванием информации, а также недопущение к информации лиц, превышающих свой статус, или пытающихся незаконно проникнуть в сеть. Важным аспектом программной защиты является и борьба с вирусами, и архивирование информации.

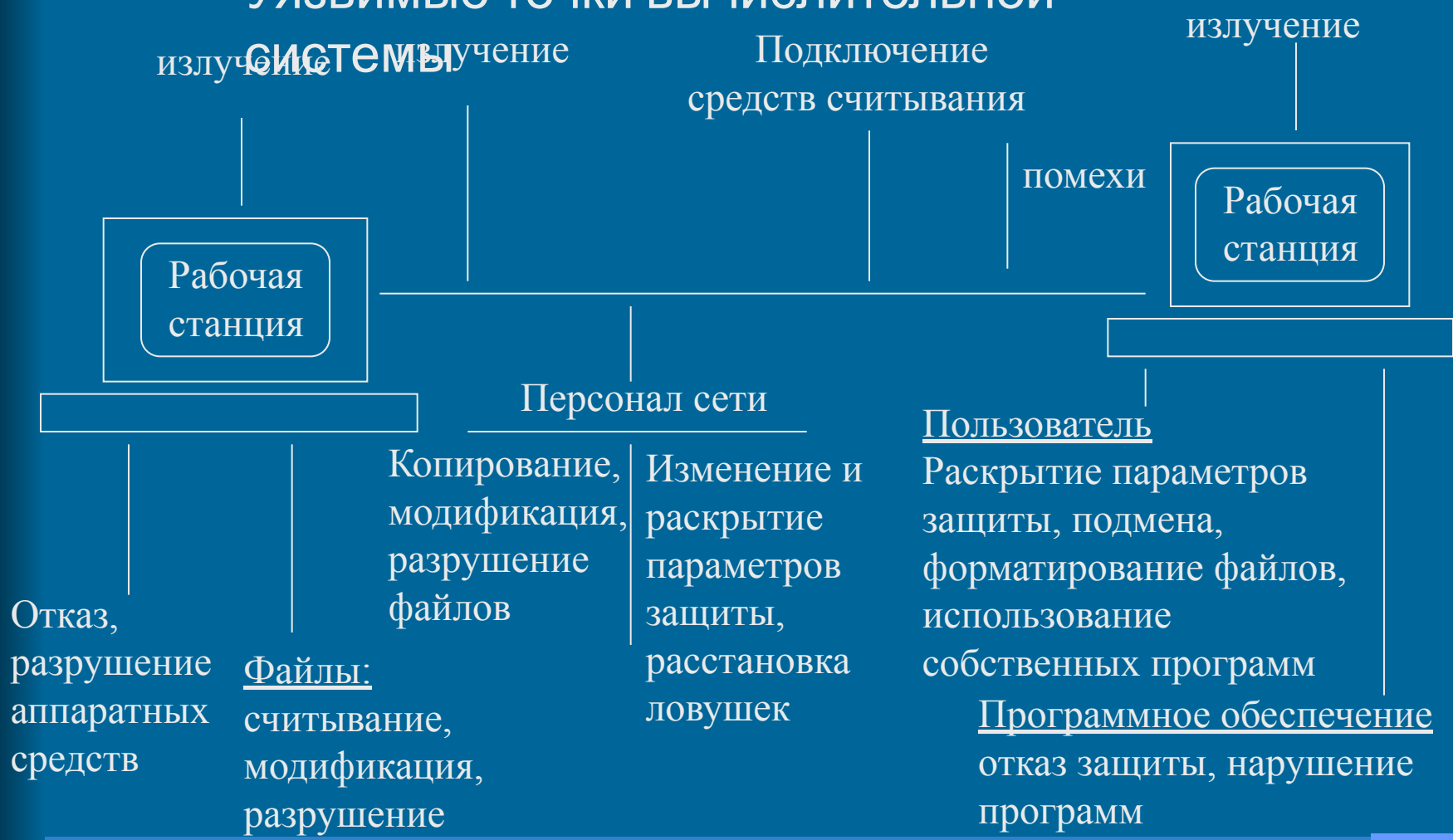
Требования к системе обеспечения безопасности

В области безопасности информации сети необходимо:

1) обеспечить сохранность и неизменность всей имеющейся в ней информации без разрешения пользователей;
2) обеспечить регулярное сохранение получаемой информации, свести к минимуму риск полной или частичной потери информации,
3) сформированной в результате обработки данных, выполнения вычисли тельного процесса;
4) исключить возможность несанкционированного считывания, модификации или разрушения как хранящейся в сети информации, так и передаваемой по линиям связи между отдельными ее элементами;
5) уменьшить потери информации в случае нарушения работоспособности отдельных элементов сети или отключения питания;
6) предупредить случайное удаление информации из-за ошибки, рассеянности или неопытности персонала и пользователей;
7) исключить проникновение вирусов на сервер сети и его распространение на рабочие станции.

Обзор методов доступа к информации сети и ее модификации

Уязвимые точки вычислительной системы



Необходимость защиты информации

Любой работающий в сети пользователь может совершить практически любые действия с содержащимися в них файлами информации: удалить их, модифицировать находящуюся в них информацию или скопировать файлы. Такое грубое вмешательство в работу сети часто может быть достаточно легко обнаружено и дать основания и возможности для обнаружения злоумышленника. Более того, могут быть приняты меры к созданию препятствий для совершения таких действий в дальнейшем. Поэтому чаще всего такой вид компьютерного преступления совершается более тонко, что затрудняет как его обнаружение, так и обнаружение злоумышленника.

Модификация типа «логическая бомба»

Применение "бомб" может иметь целью нанесение ущерба организации в случае наступления определенных условий, например, увольнения сотрудника или невыполнения некоторых договоренностей, которые фиксируются в компьютере.

При этом заложенная бомба может срабатывать либо от команды выполнения стандартных, предусмотренных программой действий, например, удаление фамилии сотрудника из списка, либо нажатия каких-либо клавиш. Общее, что объединяет механизм действия такой бомбы, - обязательное использование при совпадении определенных условий действий, без которых программа не может обойтись. Если же условия не совпадают, увольнение не состоялось, то механизм действия бомбы не запускается и никак себя не проявляет.

Модификация типа «троянский конь»

Программы, имеющие общее название "троянский конь", обычно маскируются под распространенные программы, используемые сетью, либо маскируются в самих этих программах. Но эти программы имеют закладку, которая может заставить компьютер выполнять с информацией совсем иные, не предусмотренные основной программой, действия.

Это может быть либо разрушение, модификация отдельных файлов, изменение важной информации, либо пересылка информации отдельных файлов по определенному маршруту. Известен "троянский конь", который, внедрившись в систему, переслал пароли доступа к ее информации злоумышленнику, что в дальнейшем позволило ему неоднократно обращаться в эту сеть.

Аппаратные аспекты защиты информации

Работа лютой технической системы подвержена опасности, называемой отказами. Отказ - это сбой в работе какой-либо системы, ее нежелание выполнять возложенную на нее функцию или ее выполнение в неполном объеме или неправильно.

Предвидя возможность отказов системы, можно принять адекватные меры по уменьшению последствий отказа.

Для снижения последствий отказа в системах работы с информацией есть один надежный реальный выход - резервное копирование массивов информации, создание копий блоков или данных. Одновременно это часто помогает и определить сам отказ, его вид или причину сравнением дублирующих блоков.

Обеспечение сохранения данных на уровне пользователя

В 1991 году деловой мир США потерял около четырех миллиардов долларов по причине происшествий, связанных с компьютерами. В среднем каждая компания переживает девять таких происшествий в год, каждый раз тратит не менее четырех часов на их устранение. В подавляющем большинстве случаев сбоев в работе с информацией повинны пользователи.

Более 30% пользователей деловых приложений персональных компьютеров теряют данные, по крайней мере, один раз в год и тратят около недели на их восстановление. США теряют ежегодно 24 млрд. рабочих дней на восстановление данных, что обходится примерно в 4 млрд. долларов. Но не все пользователи искренни в своих ответах в этом виде своей деятельности, не все хотят признаваться в своих потерях.

Применение операции копирования

Существует много разных программ сохранения данных, причем иногда и в них могут оказаться сбойные участки, которые могут быть длительное время быть незамеченными. При этом операции копирования внешне могут проходить так, что сбои копирования не будут ничем проявляться и даже не будут замечены администратором операционной системы. Проявляются такие ошибки при попытке прочесть записанную информацию в виде отказа чтения файла. В лучшем случае информация такого копирования может быть восстановлена лишь частично.

Резервному копированию стоит подвергать только файлы с ценной информацией. Создание резервных копий связано с затратой некоторого времени, для резервных копий требуется другой носитель информации. Поэтому необходимо определить разумный компромисс между частотой создания резервных копий и ценностью той информации, которую требуется резервировать.

Защита информации при нестабильном питании

Назначение источников электропитания состоит в поставке электрической энергии требуемых параметров отдельным блокам компьютера в течение всего времени его работы. Наиболее распространенный способ питания - это питание от сети переменного тока, когда напряжение сети в специальных блоках преобразуется до нужной величины и вида.

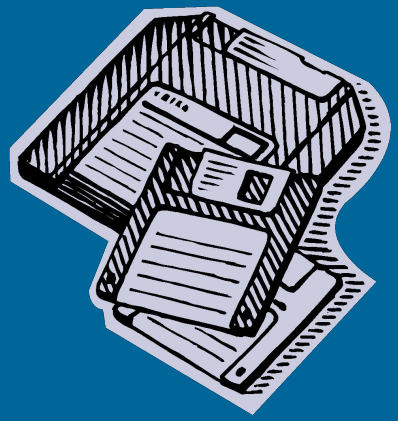
Защитить компьютерную систему от изменения уровня напряжения в сети способны регуляторы и стабилизаторы напряжения, защиту от помех и определенную защиту от считывания информации по сети способны обеспечить сетевые фильтры.

По сети питания в компьютер может поступить помеха - посторонний сигнал, способный вызвать сбои в его работе. Сеть может оказаться и той средой, по которой может быть считана информация о выполняемой в компьютере программе и результатах ее выполнения.

Архивирование информации

Программа архивации предоставляет следующие возможности

- ✔ Архивация выбранных файлов и папок на жестком диске;
- ✔ Восстановление архивированных файлов и папок на локальный жесткий диск или любой другой доступный диск;
- ✔ Создание диска аварийного восстановления, помогающего восстанавливать системные файлы, если они повреждены или случайно удалены;
- ✔ Создание копии данных из любого внешнего хранилища или данных, хранящихся на присоединенных дисках;
- ✔ Создание копии данных состояния системы локального компьютера, включающих реестр, загрузочные файлы и системные файлы;
- ✔ Планирование периодического выполнения архивации для получения текущих версий архивов.



Административные методы защиты информации

Административная служба сети - это самая высшая ее служба. Администратор имеет не только самый высокий уровень доступа, самый высокий статус, но и сам определяет уровни доступа отдельных пользователей к ресурсам сети.

Уровень доступа - это место пользователя сети в иерархии пользователей, который определяет его возможности в работе с информацией и аппаратурой сети. Согласно этому уровню, пользователи могут работать со всей, или только частью информации, имеют разные возможности по ее использованию, Например, только читать или еще и копировать, и модифицировать информацию, вносить изменения во все файлы или только в часть их, устанавливать связи с пользователями, посылать или получать сообщения и т.д.

Администратор имеет все права работы с информацией в сети и подключенной к ней аппаратурой.

Защита информации в Интернете

При работе в Интернете следует иметь в виду, что насколько ресурсы Всемирной сети открыты каждому индивидуальному пользователю, настолько же и ресурсы его компьютера открыты всей Всемирной сети, то есть тоже каждому пользователю. Это понятно, если учесть, что при работе в Сети мы отправляем запросы и получаем ответы, то есть, объявляем всем серверам, с которыми общаемся (а также и промежуточным), свой текущий IP-адрес (иначе ответы к нам бы не поступали).

Работая во Всемирной сети, следует помнить о том, что абсолютно все действия фиксируются и протоколируются специальными программными средствами и информация, как о законных, так и о незаконных действиях обязательно где-то накапливается. Таким образом, к обмену информацией в Интернете следует подходить как к обычной переписке с использованием почтовых открыток. Информация свободно циркулирует в обе стороны, но она доступна всем участникам информационного процесса. Это касается всех служб Интернета, открытых для массового использования.

Понятие о нессиметричном шифровании информации

Компания для работы с клиентами создаёт два ключа: один *открытый(public- публичный)* ключ, а другой – *закрытый(private – личный)* ключ. На самом деле это как бы две “ половинки” одного целого ключа, связанные друг с другом.

Ключи устроены так, что сообщение, зашифрованное одной половинкой, можно расшифровать только другой половинкой (не той, которой оно было зашифровано). Создав пару ключей, торговая компания широко распространяет *публичный ключ* (открытую половинку). Она может опубликовать его на своём сервере, где каждый желающий может его получить.

Понятие об электронных сертификатах

Системой несимметричного шифрования обеспечивается делопроизводство в Интернете. Благодаря ей каждый из участников обмена может быть уверен, что полученное сообщение отправлено именно тем, кем оно подписано. Однако есть ещё одна небольшая проблема, которую тоже надо устранить – это проблема регистрации даты отправки сообщения. Эта проблема может возникать во всех случаях, когда через Интернет стороны заключают договоры.

Отправитель документа легко может изменить текущую дату, если перенастроит системный календарь своего компьютера. Поэтому дата и время отправки электронного документа не имеют никакой юридической силы. В тех случаях, когда они не важны, на это можно не обращать внимание. Но в случаях, когда от них что – то зависит, эту проблему надо решать.

Сертификация даты

Решается проблема утверждение даты очень просто. Для этого между двумя сторонами (например, между клиентом и банком) достаточно поставить третью сторону. Ею, например, может быть сервер независимой организации, авторитет которой признают две стороны. Назовем её *сертификационным центром*. В этом случае поручение отправляется не сразу в банк, а на сертификационный сервер. Там оно получает “приписку» с указанием точной даты и времени, после чего переправляется в банк на исполнение. Вся работа автоматизирована, поэтому происходит очень быстро и не требует участия людей.

Сертификация издателей

При получении программного обеспечения из Интернете надо помнить, что в него могут быть встроены “бомбы замедленного действия”, с которыми не справятся никакие антивирусные программы, потому что “бомбы” и “троянские кони”, в отличие от компьютерных вирусов, не нуждаются в фазе размножения – они рассчитаны на одно разрушительное срабатывание.

Поэтому в особо ответственных случаях клиент должен быть уверен, что получает заказное программное обеспечение от компании, которая несёт за него юридическую ответственность. В этом случае тоже может потребоваться наличие сертификата, выданного независимой организацией. Это называется *сертификацией издателей*.

Программные средства защиты информации в компьютерных сетях

Я рассказала о принципах и методах защиты информации при осуществлении электронных платежей и использовании коммерческих ресурсов Интернета. Знание этих принципов необходимо не только для работы с вычислительной техникой, но и вообще для жизни в XXI веке.

В то же время я не сказала о том, какими программными средствами такая защита выполняется. Это не случайно. Дело в том, что на территории России запрещается эксплуатация средств шифрования, если они не сертифицированы государственными органами.

Это означает, что, становясь клиентом электронного банка или другой системы электронных платежей, всё необходимое программное обеспечение следует получить от них, и его надёжность должна быть удостоверена государством. Вместе с программным обеспечением клиент получает и необходимые указания о порядке работы с ним.

Спасибо за внимание!!!