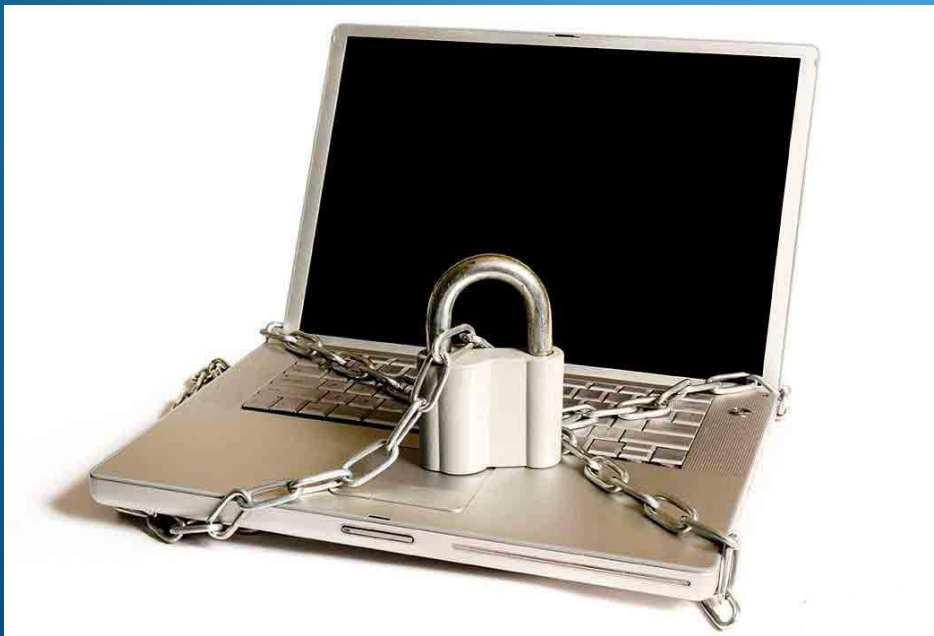


Защита информации

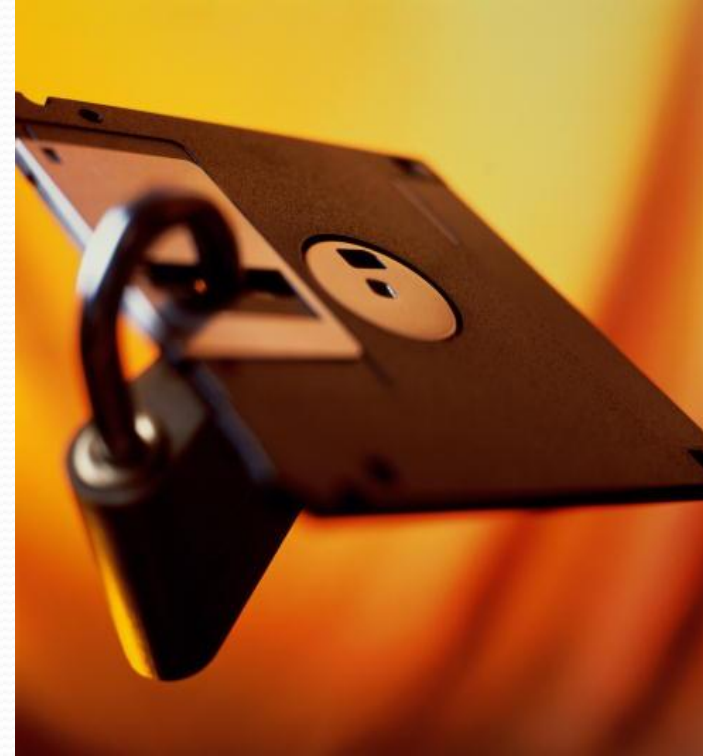




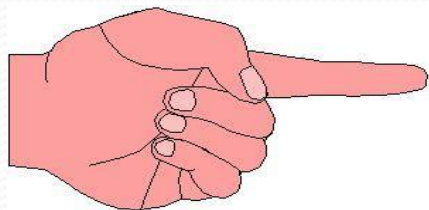
Защита информации

Защита - система мер по обеспечению безопасности с целью сохранения государственных и коммерческих секретов. Защита обеспечивается соблюдением режима секретности, применением охранных систем сигнализации и наблюдения, использованием шифров и паролей.

Защита информации
представляет собой
деятельность по
предотвращению утечки
защищаемой информации,
несанкционированных и
непреднамеренных
воздействий на
защищаемую информацию,
то есть процесс,
направленный на
достижение этого
состояния.



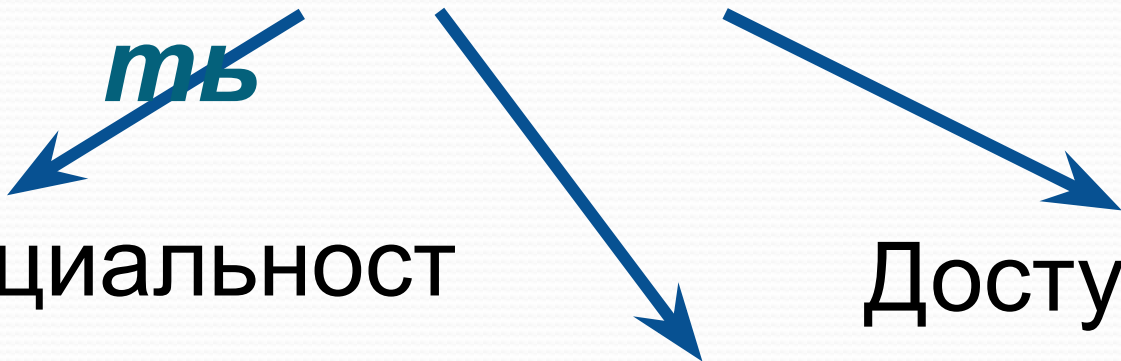
Безопасность



Конфиденциальность

Целостность

Доступность



Информационная безопасность — это состояние защищённости информационной среды

В вычислительной технике понятие безопасности подразумевает

- **надёжность работы компьютера,**
- **сохранность ценных данных,**
- **защиту информации от внесения в нее изменений неуполномоченными лицами,**
- **сохранение тайны переписки в электронной СВЯЗИ.**



Несанкционированный доступ

Несанкционированный доступ - действия, нарушающие установленный порядок доступа или правила разграничения, доступ к программам и данным, которые получают абоненты, которые не прошли регистрацию и не имеют права на ознакомление или работу с этими ресурсами.

Для предотвращения несанкционированного доступа осуществляется контроль доступа.



Защита с использованием паролей



Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются *пароли*.

Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль.

Каждому конкретному пользователю может быть разрешен доступ только к определенным информационным ресурсам.

При этом может производиться регистрация всех попыток несанкционированного доступа.

Защита с использованием пароля используется при загрузке операционной системы

Вход по паролю может быть установлен в программе BIOS Setup, компьютер не начнет загрузку операционной системы, если не введен правильный пароль. Преодолеть такую защиту нелегко.

От несанкционированного доступа может быть защищены

- **каждый диск,**
- **каждая папка,**
- **каждый файл локального компьютера.**

Для них могут быть установлены определенные права доступа

- **полный доступ,**
- **возможность внесения изменений,**
- **только чтение,**
- **запись и др.**

Права могут быть различными для различных

Биометрические системы защиты

В настоящее время для защиты от несанкционированного доступа к информации все более часто используются **биометрические системы идентификации**.

Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными.

К биометрическим системам защиты информации относятся системы идентификации:

- по отпечаткам пальцев;
- по характеристикам речи;
- по радужной оболочке глаза;
- по изображению лица;
- по геометрии ладони руки.



Защита



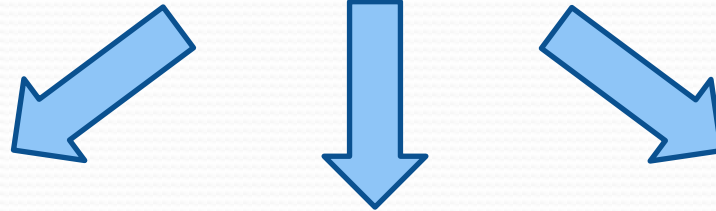
от вредоносных программ

Вредоносная программа (буквальный перевод англоязычного термина **Malware**, *malicious* — злонамеренный и *software* — программное обеспечение, жаргонное название — «малварь», «маловарь», «мыловарь» и даже «мыловарня») — злонамеренная программа, **то есть программа, созданная со злым злом и/или злыми намерениями.**



Вредоносные программы

**Вирусы,
черви,
троянские и
хакерские
программы**



**Потенциально
опасное
программное
обеспечение**

**Шпионское,
рекламное
программное
обеспечение**

Антивирусные программы



Современные антивирусные программы обеспечивают **комплексную защиту программ и данных** на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер.

- Интернет,
- локальная сеть,
- электронная почта,
- съемные носители информации.



Для защиты от вредоносных программ каждого типа в антивирусе предусмотрены отдельные компоненты.

Принцип работы антивирусных программ основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вредоносных программ.

Компьютерные вирусы и защита от них

Компьютерные вирусы являются вредоносными программами, которые могут «размножаться» (самокопироваться) и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

Название «**вирус**» по отношению к компьютерным программам пришло из биологии именно по способности к саморазмножению.

По «**среде обитания**» вирусы можно разделить на загрузочные, файловые и макровирусы.



Рекламные программы

Рекламные программы (англ. *Adware: Advertisement* — реклама и *Software* — программное обеспечение) встраивают рекламу в основную полезную программу и могут выполнять функцию троянских программ. Рекламные программы могут скрытно собирать различную информацию о пользователе компьютера и затем отправлять ее злоумышленнику.

Хакерские утилиты и защита от них. Сетевые атаки

Сетевые атаки на удаленные серверы реализуются с помощью специальных программ, которые посылают на них многочисленные запросы. Это приводит к отказу в обслуживании (зависанию сервера), если ресурсы атакуемого сервера недостаточны для обработки всех поступающих запросов.

Утилиты взлома удалённых компьютеров

Утилиты взлома удаленных компьютеров

предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими или для внедрения во взломанную систему других вредоносных программ.

Профилактическая защита от таких хакерских утилит состоит в своевременной загрузке из Интернета обновлений системы безопасности операционной системы и приложений.



Заключение



Создающаяся в стране система защиты информации и формирование комплекса мер по ее реализации не приведет к необратимым последствиям на пути зарождающегося в России информационно - интеллектуального объединения со всем миром.



Литература

- Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008. — 176 с.
- Угринович Н.Д. Информатика и ИКТ. Учебник для 11 класса. М.: БИНОМ. Лаборатория знаний, 2010. - 188 с.
- Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009. — 352 с.
- Википедия <http://ru.wikipedia.org/>
- <http://igk.ucoz.ru>
- <http://www.bio-profile.ru/images/Test-Anviz.jpg>
- <http://www.ixbt.com/short/images/FR4.0.jpg>
- http://tele4n.ru/uploads/posts/2009-04/1239903545_ec84da84d98daf506704f42676f785a6.jpg
- <http://www.interflex.ru/SiteCollectionImages/Sicherheitsl%C3%B6sungen/Ingersoll-Rand%20HandKey%20ID3D-R.gif>
- <http://clip2net.com/clip/m55674/1284807698-clip-67kb.jpg>
- <http://j.foto.radikal.ru/0611/6c9d7cd648b7.gif>
- http://konovalov.ucoz.ru/_tbkp/antivirus.jpg
- <http://images.yandex.ru/>
- <http://www.securitylab.ru/upload/iblock/9c4/9c428c9ff81bbc7cb7dc636b0366ccba.gif>

