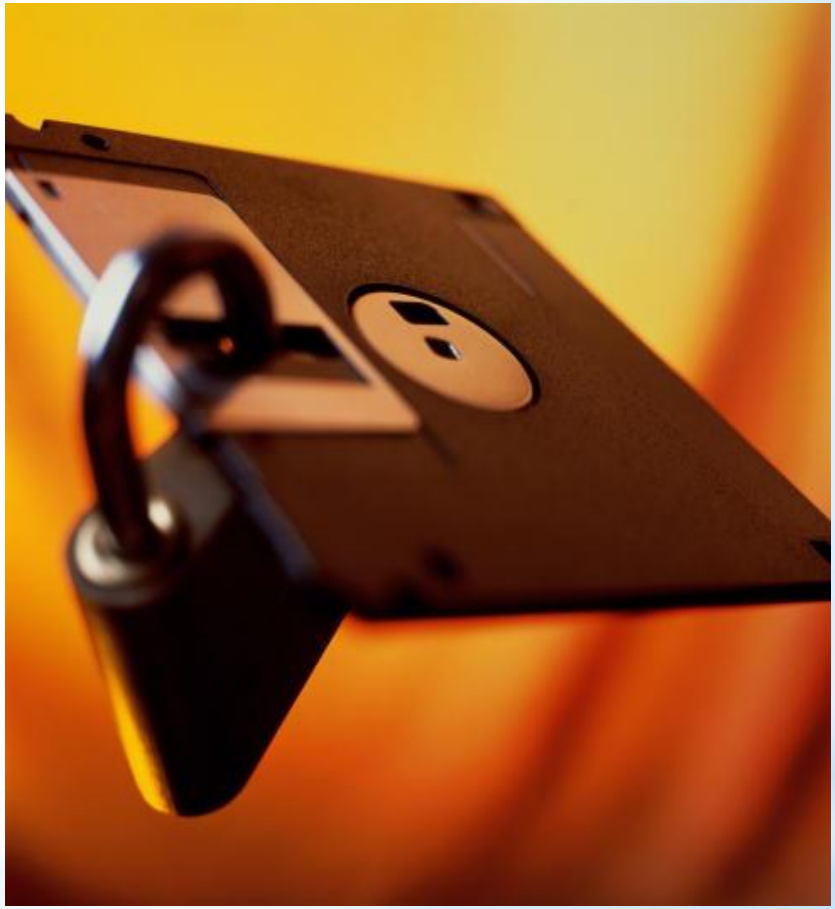
Защита информации

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

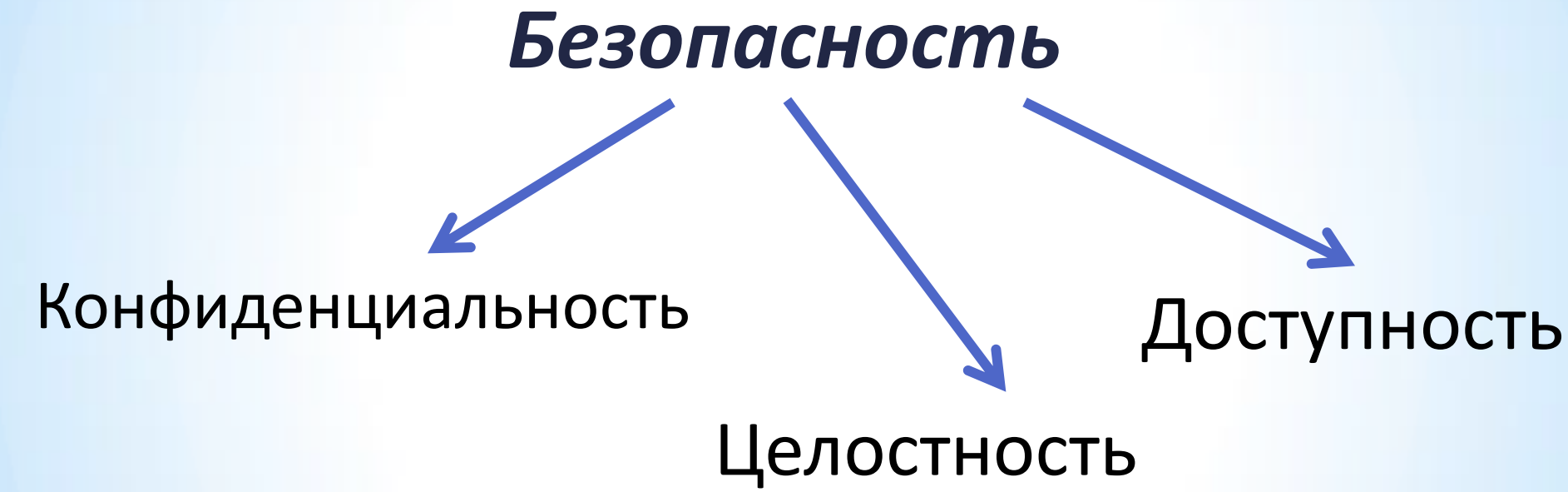
представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.



Информационная безопасность — это состояние защищённости информационной среды.

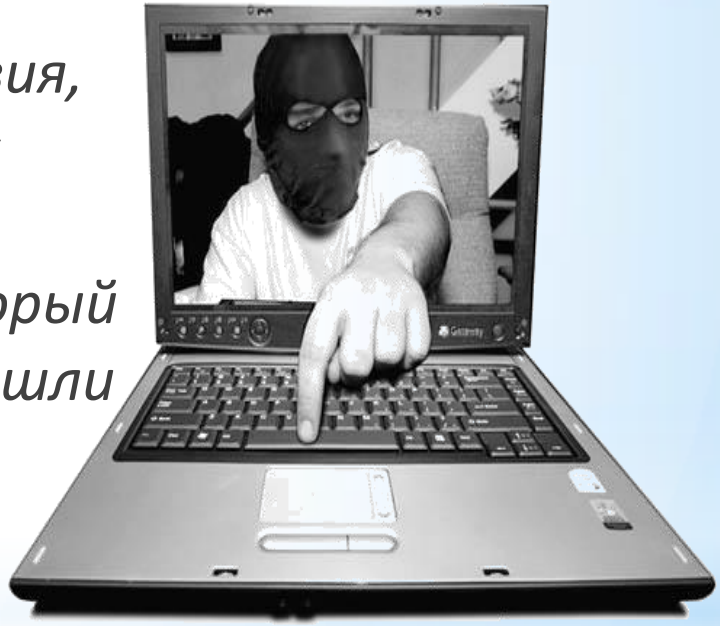
В вычислительной технике понятие безопасности подразумевает

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


Безопасность
Конфиденциальность
Целостность
Доступность

Несанкционированный доступ

Несанкционированный доступ *- действия, нарушающие установленный порядок доступа или правила разграничения, доступ к программам и данным, который 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 пользователей.

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.*

Идентификация по отпечаткам пальцев

Оптические сканеры считывания отпечатков пальцев устанавливаются на ноутбуки, мыши, клавиатуры, флэш-диски, а также применяются в виде отдельных внешних устройств и терминалов (например, в аэропортах и банках).

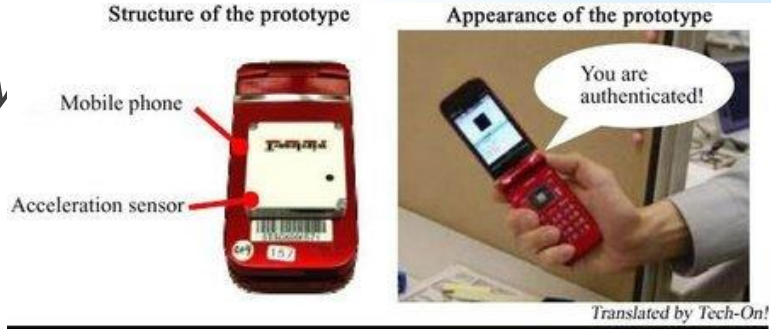
Если узор отпечатка пальца не совпадает с узором допущенного к информации пользователя, то доступ к информации невозможен.

. Оптический сканер отпечатка пальца, вмонтированный в ноутбук

Идентификация по характеристикам речи

Идентификация человека по голосу — один из традиционных способов распознавания, интерес к этому методу связан и с прогнозами внедрения голосовых интерфейсов в операционные системы.

Голосовая идентификация бесконтактна и существуют системы ограничения доступа к информации на основании частотного анализа речи.



Идентификация по изображению лица

Для идентификации личности часто используются технологии распознавания по лицу. Распознавание человека происходит на расстоянии.

Идентификационные признаки учитывают форму лица, его цвет, а также цвет волос. К важным признакам можно отнести также координаты точек лица в местах, соответствующих смене контраста (брови, глаза, нос, уши, рот и овал).

В настоящее время производится выдача загранпаспортов, в микросхеме которых хранится цифровая фотография владельца.

Идентификация по ладони руки

В биометрике в целях идентификации используется простая геометрия руки — размеры и форма, а также некоторые информационные знаки на тыльной стороне руки (образы на сгибах между фалангами пальцев, узоры расположения кровеносных сосудов).

Сканеры идентификации по ладони руки установлены в некоторых аэропортах, банках и на атомных электростанциях .

Токен (также *аппаратный токен*, *USB-ключ*, *криптографический токен*) — компактное устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации его владельца, безопасного удалённого доступа к информационным ресурсам и т. д.

Токены предназначены для электронного Удостоверения личности (например, клиента, получающего доступ к банковскому счёту), при этом они могут использоваться как вместо пароля, так и вместе с ним. В некотором смысле токен — это электронный ключ для доступа к чему-либо.

Некоторые предназначены для хранения криптографических ключей, как электронная подпись или биометрические данные.

Криптогра́фия (от др.-греч. κρυπτός «скрытый» + γράφω «пишу») — наука о методах обеспечения ***конфиденциальности*** (невозможности прочтения информации посторонним), ***целостности данных*** (невозможности незаметного изменения информации), **аутентификации** (проверки подлинности авторства или иных свойств объекта), ***шифрования*** (кодировка данных).

Криптография образует разделы

1) **симметричных криптосистем**, в которых зашифровывание и расшифровывание проводится с использованием одного и того же секретного ключа.
Пример:Шифр АТБАШ, в котором ключом является перевёрнутый алфавит того языка, на котором шифруется текст;

2) **асимметричные криптосистемы** включают системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Защита от вредоносных программ

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

Вредоносные программы

Действия при наличии признаков заражения компьютера

Прежде чем предпринимать какие-либо действия, необходимо сохранить результаты работы на внешнем носителе (дискете, CD- или DVD-диске, флэш-карте и пр.).

Далее необходимо:

* *отключить компьютер от локальной сети и Интернета, если он к ним был подключен;*
* *если симптом заражения состоит в том, что невозможно загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробовать загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows;*
* *запустить антивирусную программу.*