



Технологии и средства защиты информации от разрушения и несанкционированного доступа включают в себя:

- уровни и меры по защите информации;
- установку паролей на ПК и папки;
- меры безопасности при работе с электронной почтой;
- безопасность работы в локальной сети.



# Другие способы защиты компьютера



**Архивируйте** регулярно Ваши данные

**Читайте** заявления о конфиденциальности на веб-узлах

**Закрывайте** всплывающие окна при помощи красной кнопки «X»

**Думайте**, прежде чем щелкнуть по ссылке

# ЗАЩИТА ИНФОРМАЦИИ

## Защита от несанкционированного копирования

— система мер, направленных на противодействие несанкционированному копированию информации, как правило представленной в электронном виде (данных или программного обеспечения).



## Термины, связанные с защитой от несанкционированного доступа

- **Защита от записи** [write protection] - комплекс программных и аппаратных средств, обеспечивающий защиту данных, записанных на магнитные диски, дискеты и ленты, который позволяет только считывать данные и предотвращает возможность их стирания, изменения или перезаписи.
- **Защита от копирования** [copy protection] - комплекс программных и аппаратных средств, обеспечивающий предотвращение нелегального копирования компьютерных программ и данных. Частными средствами защиты от копирования являются донглы, пароли и др.



# Антивирусные программы

предназначены для предотвращения заражения компьютера вирусом и ликвидации последствий заражения.



# 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.



# Програмные и программно-аппаратные методы защиты

```
graph TD; A[Програмные и программно-аппаратные методы защиты] --> B[Защита от компьютерных вирусов.]; A --> C[Защита от несанкционированного доступа]; A --> D[Защита информации при удаленном доступе]; C --- D;
```

Защита от компьютерных  
вирусов.

Защита от несанкционированного доступа

Защита информации при удаленном  
доступе



# 10 способов защиты личных данных

Как не стать жертвой интернет-мошенников



Не указывайте лишнюю личную информацию в профиле в социальных сетях, используйте сокрытие данных от всех, кроме друзей



Своевременно обновляйте программное обеспечение



Установите на свой (свои) ПК защитное ПО (антивирус и фаервол) и следите за регулярностью обновлений антивирусных баз



Тщательно выбирайте онлайн-магазин, прежде чем сообщать данные банковской карты, пользуйтесь услугой SMS-информирования от банка



Обращайте внимание на характер данных при регистрации в онлайн-сервисах.

Не указывайте данные, которые в действительности не нужны для получения услуг от сервиса (номера удостоверений личности и т.п.), а в случае необходимости ищите менее требовательные к персональным данным сервисы-аналоги



Не запускайте подозрительные вложения, присланные по электронной почте и через интернет-мессенджеры



Установите пароль доступа к смартфону и специализированные приложения для поиска аппарата и удаленного стирания данных. Внимательнее относитесь к установке малоизвестных приложений. Отключайте неиспользуемые беспроводные интерфейсы



Установите свой собственный пароль домашней сети Wi-Fi



Проверяйте интернет-адреса при переходе из почты и с сайтов



Не используйте один пароль для всех интернет-ресурсов

# По среде обитания вирусы подразделяются на:

- **Сетевые вирусы** распространяются по различным компьютерным сетям.
- **Файловые вирусы** внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE.
- **Загрузочные вирусы** внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record).
- **Файлово-загрузочные вирусы** заражают как файлы, так и загрузочные сектора дисков.

