Минимальные требования безопасности

- Информирование и обучение персонала
- Планирование
- Реагирование на нарушения ИБ
- Физическая защита
- Защита систем и телекоммуникаций
- Сертификация, аккредитация и оценки ИБ
- Кадровая безопасность
- Протоколирование и аудит
- Защита носителей
- Обеспечение целостности
- Аутентификация, авторизация
- Мониторинг регуляторов ИБ
- Управление конфигурацией
- Действия ИБ к сервисам и системам
- Политика ИБ
- Оценка рисков

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 щелкать по ссылке

www.microsoft.com/rus/protect

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.

Содержание

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.

Программные и программно-аппаратные методы защиты

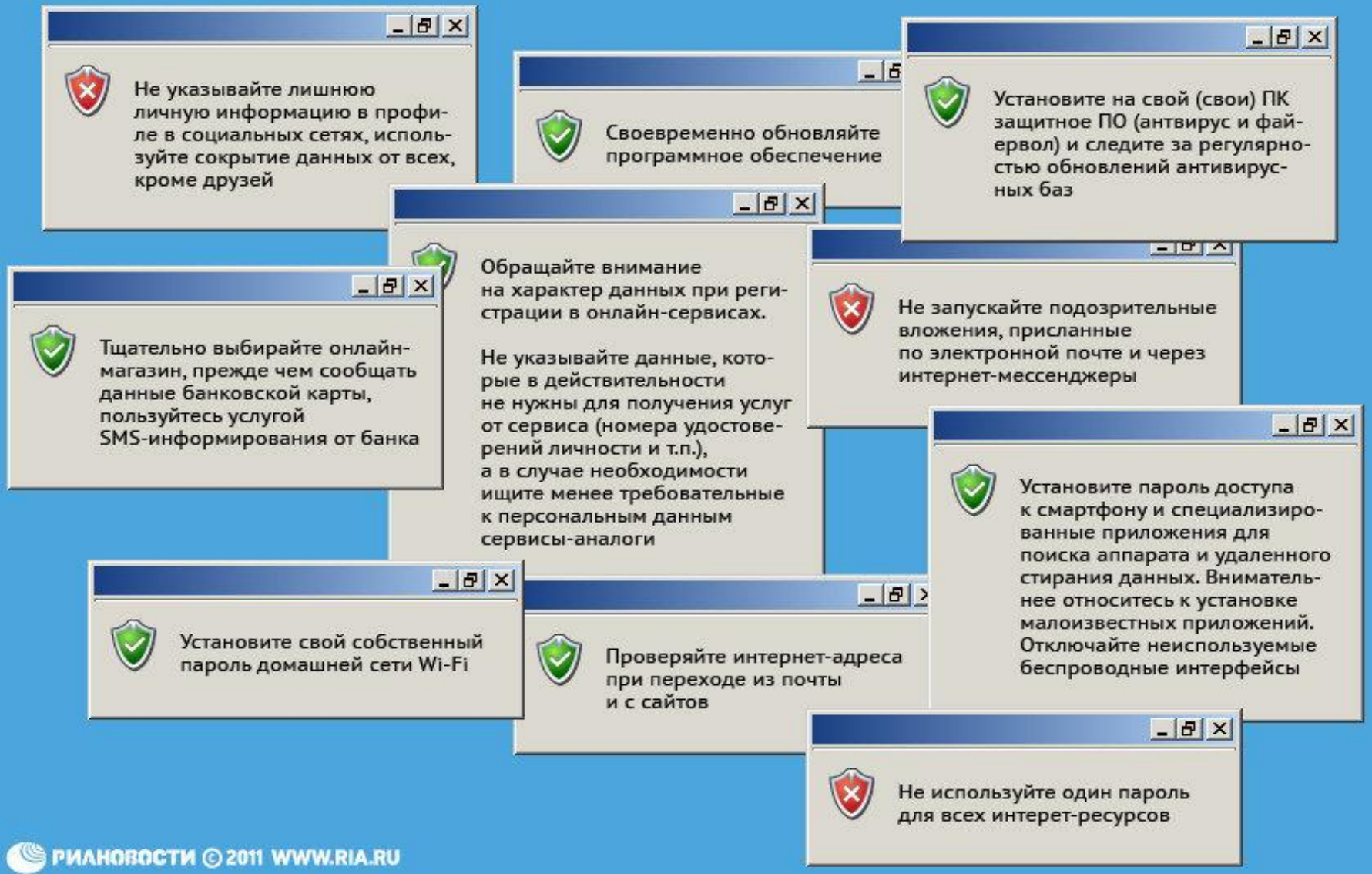
Защита от компьютерных вирусов.

Защита от несанкциони - рованного доступа

Защита информации при удаленном доступе

10 способов защиты личных данных

Как не стать жертвой интернет-мошенников



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 Re-cord**).**
- ***Файлово-загрузочные вирусы*** заражают как файлы, так и загрузочные сектора дисков**.**