

ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ

п.1. Необходимость защиты информации

Безопасности информации в сетях угрожают:

- возможность раскрытия содержания передаваемых сообщений;
- возможность определения принадлежности отправителя и получателя данных;
- возможность изменения потока сообщений;
- возможность отказа в предоставлении услуг и др.

Причинами потерь информации в сетях являются:

- отказы и сбои аппаратуры и передающих устройств;
- структурные, программные и алгоритмические ошибки;
- аварийные ситуации;
- ошибки человека;
- ошибки разработчиков и т. п.

Нарушитель может:

- выдать себя за другого пользователя;
- утверждать факт отправки информации, которая на самом деле не посылалась;
- отказаться от факта получения информации, которая на самом деле была получена;
- незаконно расширить свои полномочия или изменить полномочия других пользователей по доступу к информации и ее обработке;
- скрыть факт наличия некоторой информации;
- подключиться к линии связи между другими пользователями.

п.2. Направление защиты информации

Идентификация предполагает присвоение какому-либо объекту или субъекту уникального образа имени, или числа.

Цель идентификации — установление подлинности объекта в вычислительной системе, допуск его к информации ограниченного пользования.

Объектами идентификации и установления подлинности в вычислительной системе могут быть:

- человек (оператор, пользователь, должностное лицо);
- технические средства (дисплей, ЭВМ);
- документы (распечатки, листинги программ);
- носители информации (магнитные диски, ленты);
- информация на дисплее, табло.

Установление подлинности объекта может производиться человеком, аппаратным устройством, программой, вычислительной системой и т. д.

В качестве идентификаторов личности для реализации разграничения широко распространено применение кодов, паролей, которые записываются на специальные носители (электронные ключи или карточки).

Защита информации от преднамеренного доступа предполагает:

- ограничение доступа;**
- разграничение доступа;**
- распределение доступа (привилегий);**
- криптографическое преобразование информации;**
- контроль и учет доступа;**
- законодательные меры.**

п.3. Обеспечение безопасности

Актуальность данной проблемы объясняется следующими основными причинами:

- рост числа компьютерных преступлений и атак;
- неудовлетворительное состояние защиты в существующих компьютерных сетях;

Для борьбы с вирусами используются специальные программы — антивирусы. Самыми именитыми антивирусными программами являются: антивирус **Касперского (KAV)**,
□ **Dr.Web**, □ **Norton Antivirus**.

- необходимость минимизации информационных рисков.

п.4. Понятие системы информационной безопасности

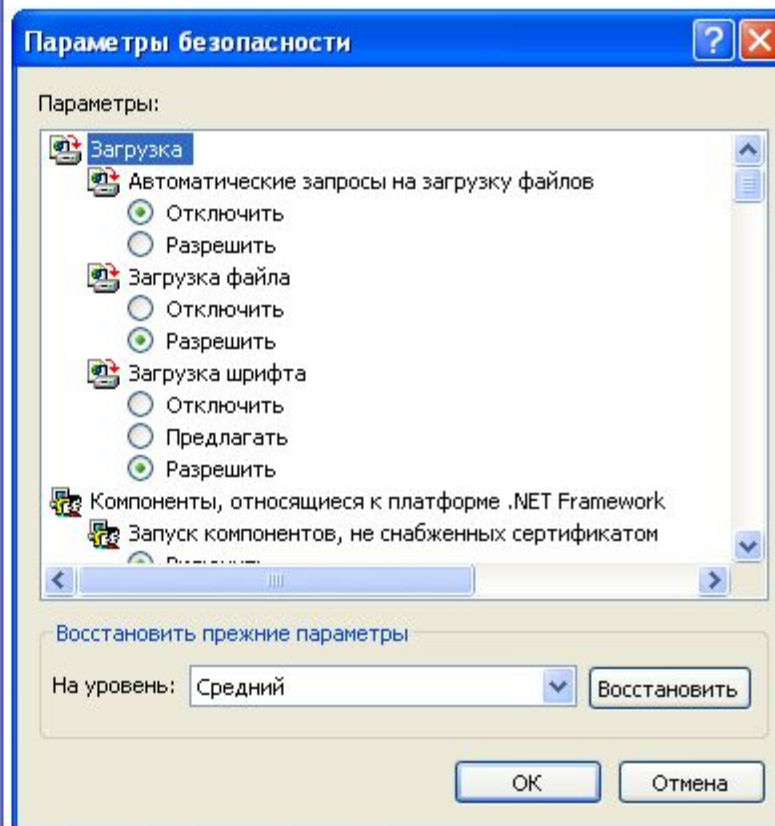
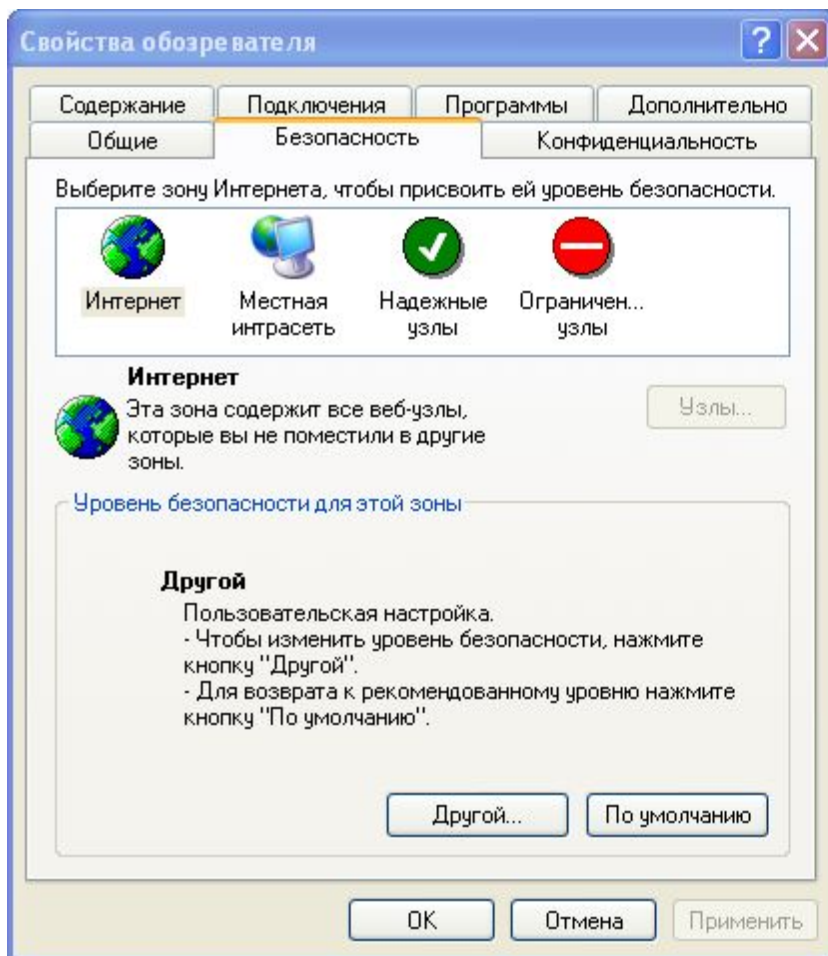
Необходимо собрать систему, для которой можно будет доказать отсутствие **недекларированных** возможностей работы злоумышленника и ошибок.

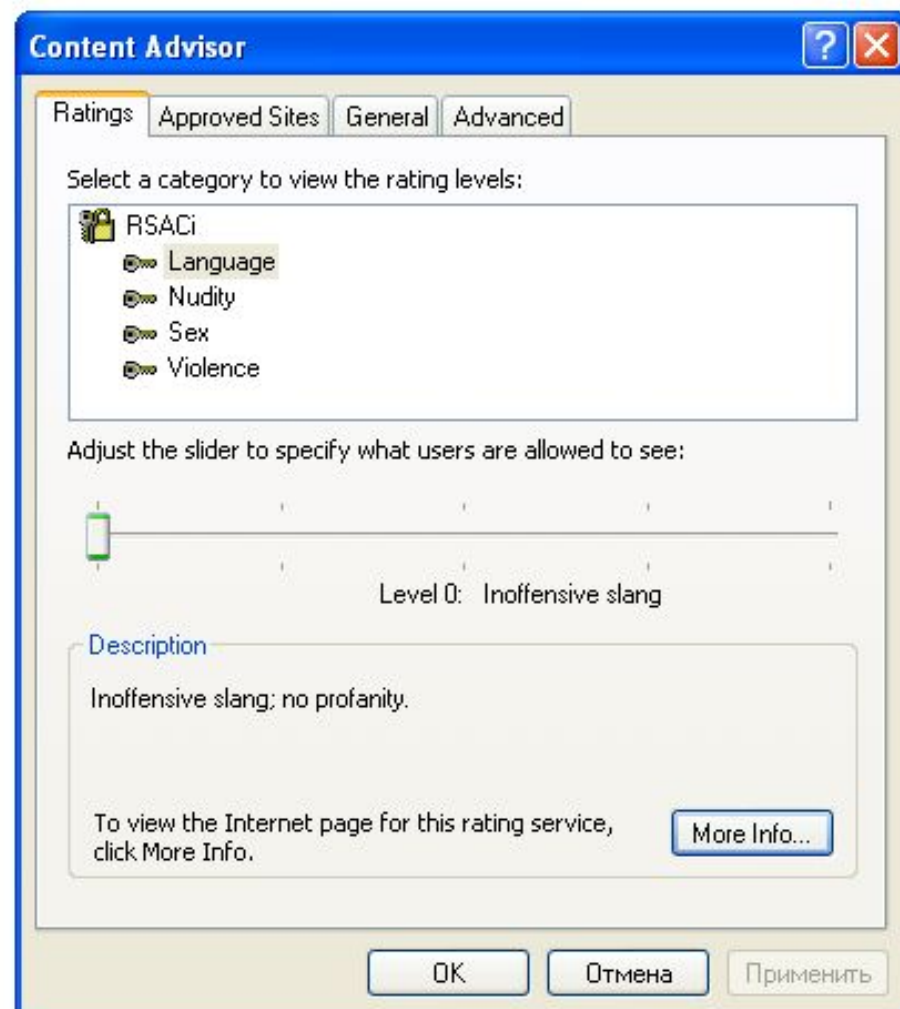
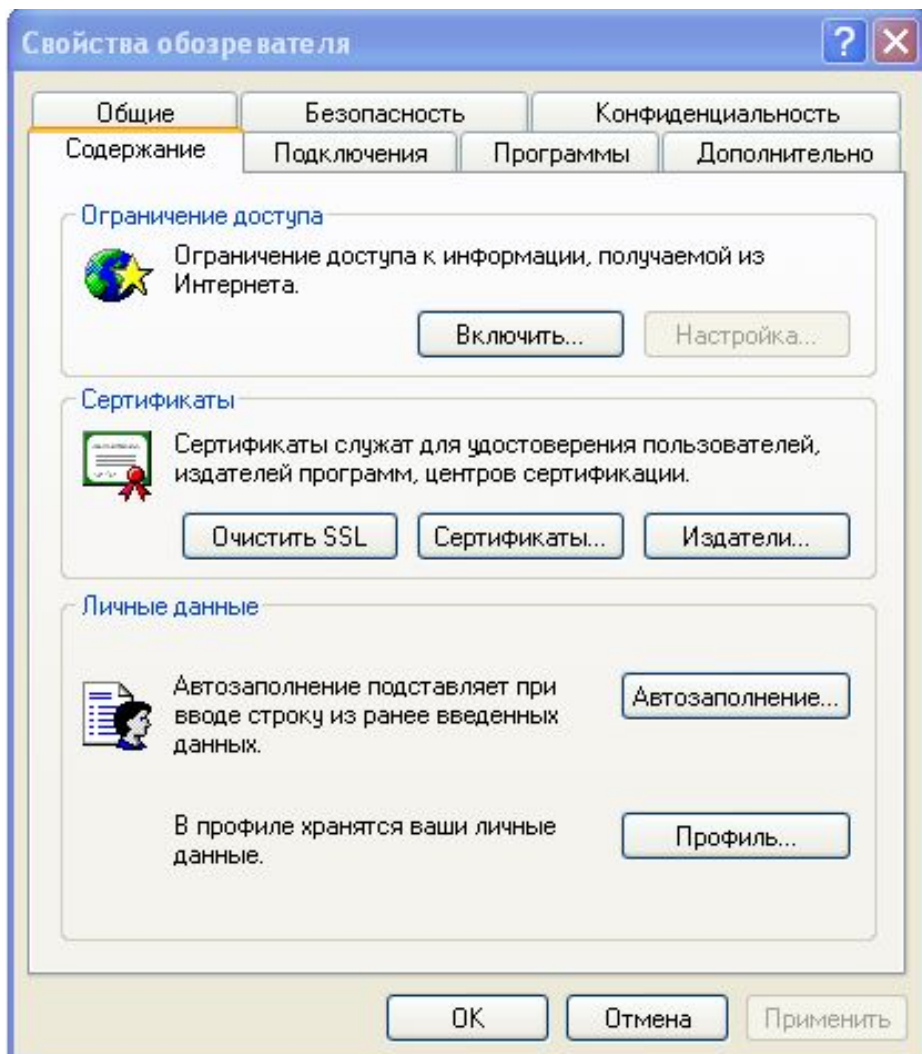
Система должна быть защищена от ошибок и злонамеренных действий ее легальных пользователей и системных администраторов, удобна в эксплуатации и по возможности прозрачна и гибка для конечных пользователей.

Понятие "система информационной безопасности" предполагает разделение задачи обеспечения безопасности на ряд взаимно связанных составляющих, каждая из которых имеет свое место в системе и влияет на окончательный облик всей системы.

п.5. Защита от негативной информации. Фильтры

Для начала можно настроить браузер для фильтрации информации и обеспечения личной информационной безопасности:





К дополнительным средствам защиты относятся всевозможные **фильтры**: специальные программы, отфильтровывающие нежелательную информацию.

К числу таких программ относятся **персональные фейрволлы (брандмауэр)**.

В переводе на русский язык это слово значит — «огненная стена».

Обнаружив попытку несанкционированного проникновения в компьютер, программа может просто подать сигнал тревоги, а может сразу заблокировать доступ. Это — основная функция всех программ такого класса.

Самыми популярными являются следующие файрволлы:

- **ZoneAlarm (zone labs);**
- **Norton Internet Security (Symantec).** Главный козырь программы — способность убивать всплывающие рекламные окна и даже вырезать со страниц баннеры. В итоге работа становится не только безопасной, но и быстрой.
- **Mcafee Firewall;**
- **Outpost (Agnitum — российская компания).** Отечественная программа выполняет следующие задачи: блокировка активных элементов e-mail; блокировка атак и сканирования; поддержка «невидимого» режима; уменьшает время соединения с удаленным узлом за счет кэширования DNS и многое другое.