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).

Зашита 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

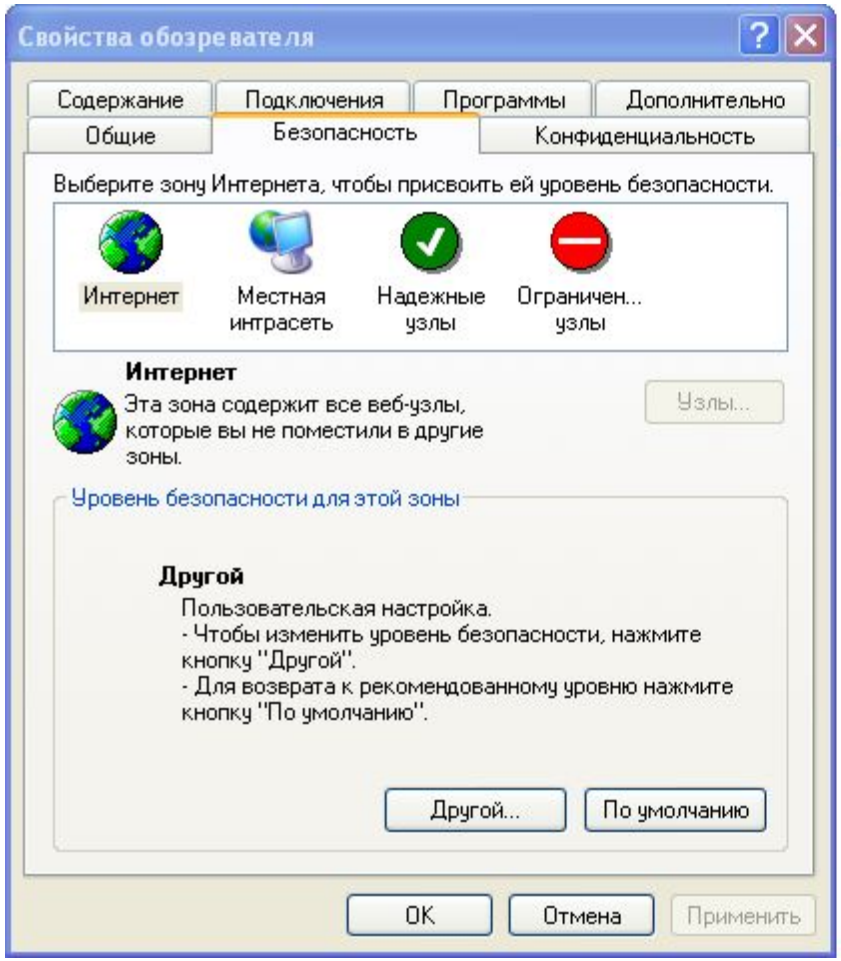
Необходимо собрать систему, для которой можно будет доказать отсутствие недекларированных возможностей работы злоумышленника и ошибок.

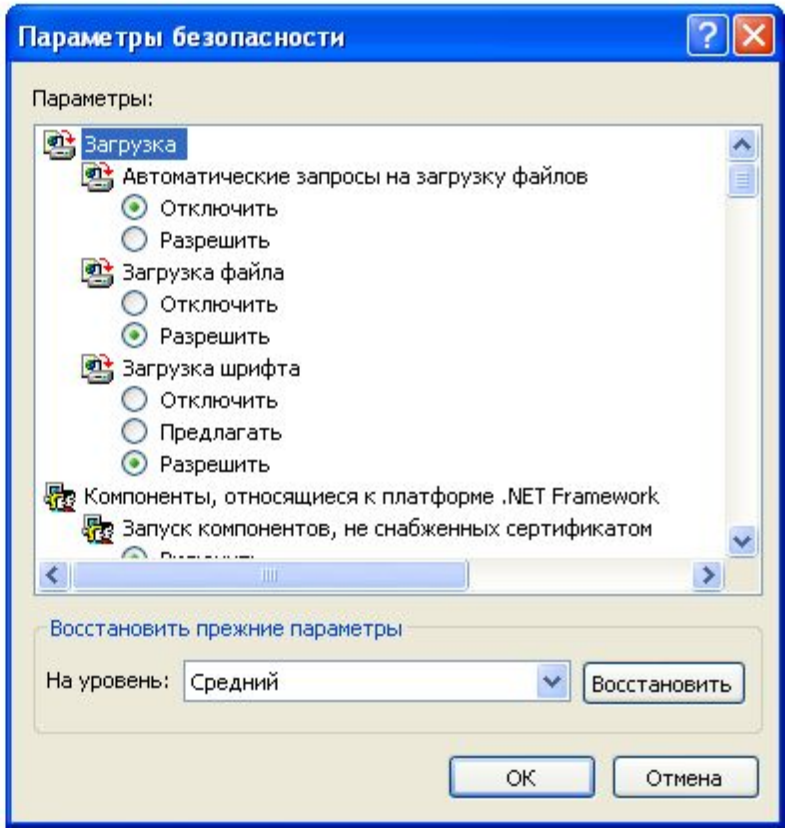
Система должна быть защищена от ошибок и злонамеренных действий ее легальных пользователей и системных администраторов, удобна в эксплуатации и по возможности прозрачна и гибка для конечных пользователей.

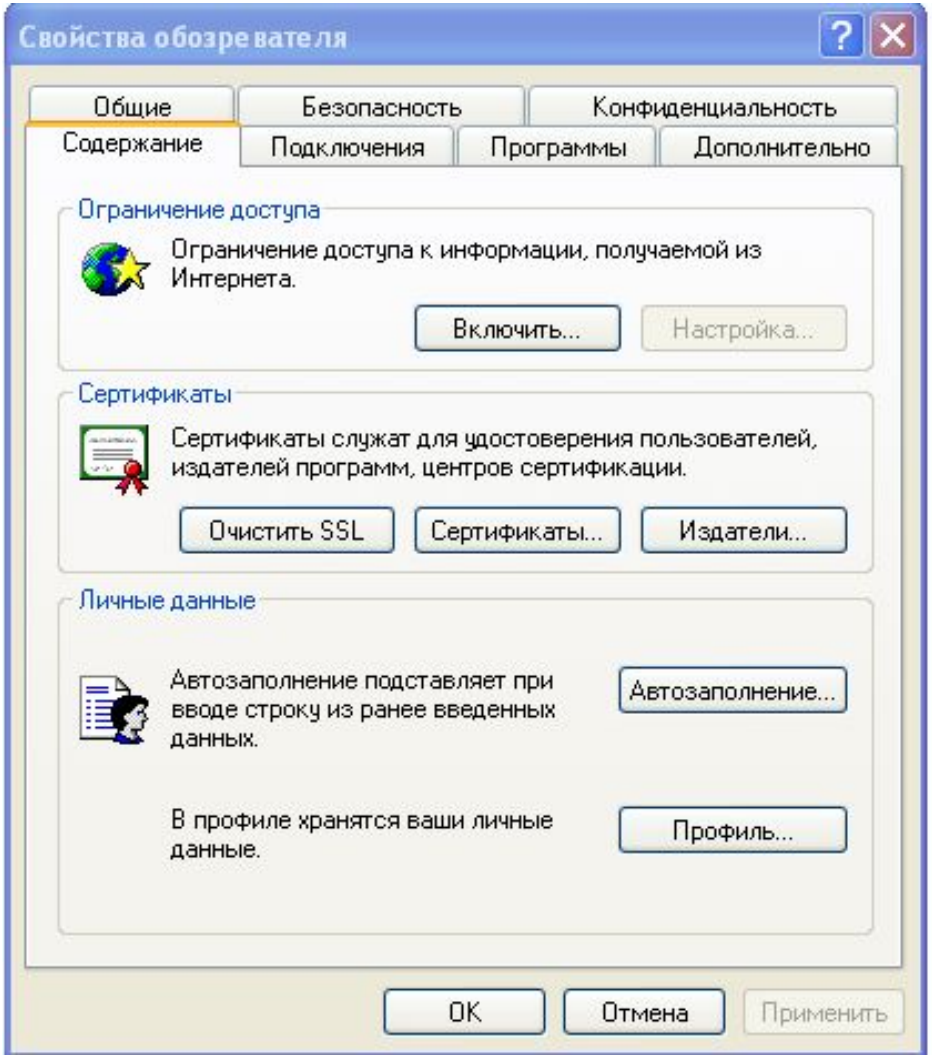
Понятие "система информационной безопасности" предполагает разделение задачи обеспечения безопасности на ряд взаимно связанных составляющих, каждая из которых имеет свое место в системе и влияет на окончательный облик всей системы.

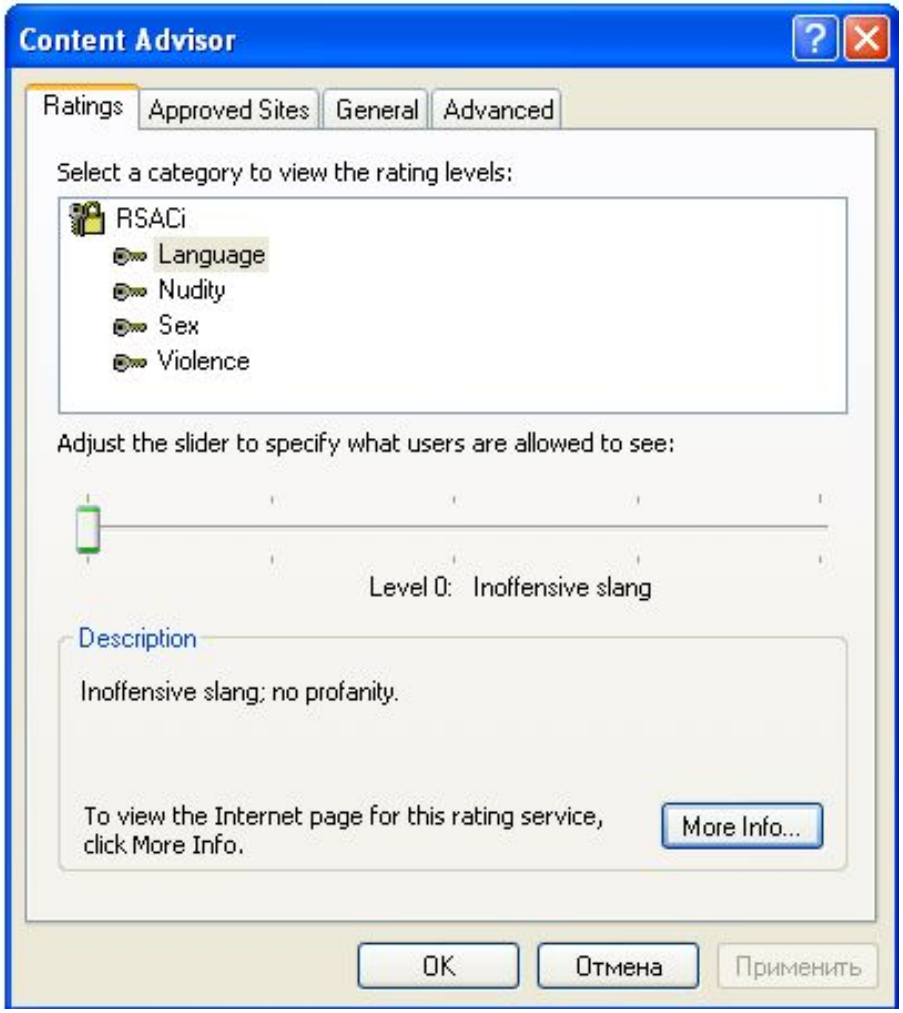
п.5. Защита от негативной информации. Фильтры

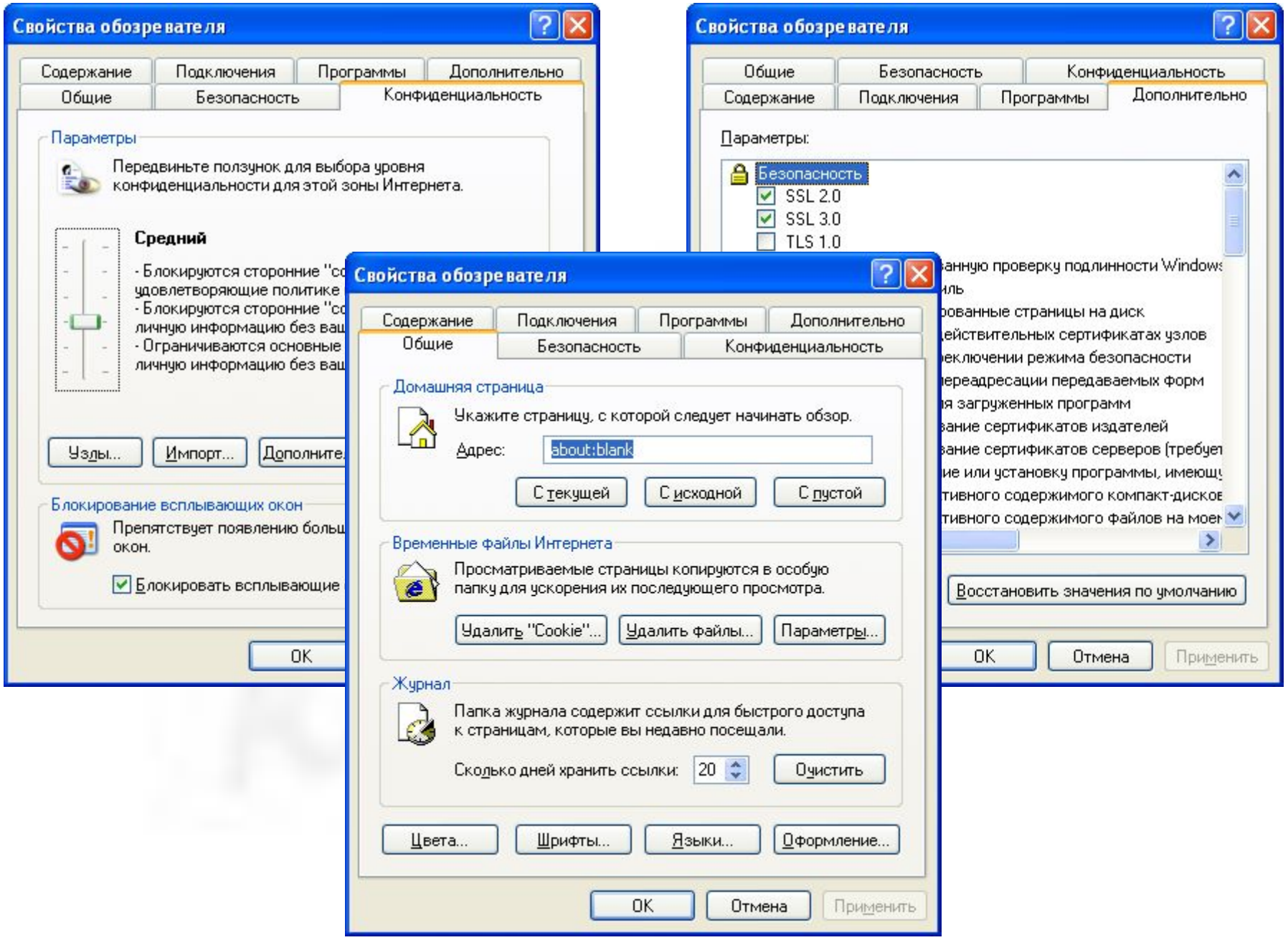
Для начала можно настроить браузер для фильтрации информации и обеспечения личной информационной безопасности:






Свойства обозревателя
Общие
Безопасность
Конфиденциальность
Содержание
Подключения
Программы
Дополнительно
Ограничение доступа
Ограничение доступа к информации, получаемой из Интернета.
Включить...
Настройка...
Сертификаты
Сертификаты служат для удостоверения пользователей, издателей программ, центров сертификации.
Очистить SSL
Сертификаты...
Издатели...
Личные данные
Автозаполнение подставляет при вводе строку из ранее введенных данных.
Автозаполнение...
В профиле хранятся ваши личные данные.
Профиль...
OK
Отмена
Применить


Content Advisor
Ratings
Approved Sites
General
Advanced
Select a category to view the rating levels:
RSACi
Language
Nudity
Sex
Violence
Adjust the slider to specify what users are allowed to see:
Level 0: Inoffensive slang
Description
Inoffensive slang; no profanity.
To view the Internet page for this rating service, click More Info.
More Info...
OK
Отмена
Применить


Свойства обозревателя
Содержание
Подключения
Программы
Дополнительно
Общие
Безопасность
Конфиденциальность
Параметры
Передвиньте ползунок для выбора уровня конфиденциальности для этой зоны Интернета.
Средний
- Блокируются сторонние "со
удовлетворяющие политике
- Блокируются сторонние "со
личную информацию без ваш
- Ограничиваются основные
личную информацию без ваш
Узлы...
Импорт...
Дополните...
Блокирование всплывающих окон
Препятствует появлению больш
окон.
Блокировать всплывающие
OK
Свойства обозревателя
Содержание
Подключения
Программы
Дополнительно
Общие
Безопасность
Конфиденциальность
Домашняя страница
Укажите страницу, с которой следует начинать обзор.
Адрес:
about:blank
С текущей
С исходной
С пустой
Временные файлы Интернета
Просматриваемые страницы копируются в особую папку для ускорения их последующего просмотра.
Удалить "Cookie"...
Удалить файлы...
Параметры...
Журнал
Папка журнала содержит ссылки для быстрого доступа к страницам, которые вы недавно посещали.
Сколько дней хранить ссылки:
20
Очистить
Цвета...
Шрифты...
Языки...
Оформление...
OK
Отмена
Применить
Свойства обозревателя
Общие
Безопасность
Конфиденциальность
Содержание
Подключения
Программы
Дополнительно
Параметры:
Безопасность
SSL 2.0
SSL 3.0
TLS 1.0
Восстановить значения по умолчанию
OK
Отмена
Применить

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 фейрволлы:

- **ZoneAlarm (zone labs);**
- **Norton Internet Security (Symantec). Главный козырь программы — способность убивать всплывающие рекламные окна и даже вырезать со страниц баннеры. В итоге работа становиться 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.**