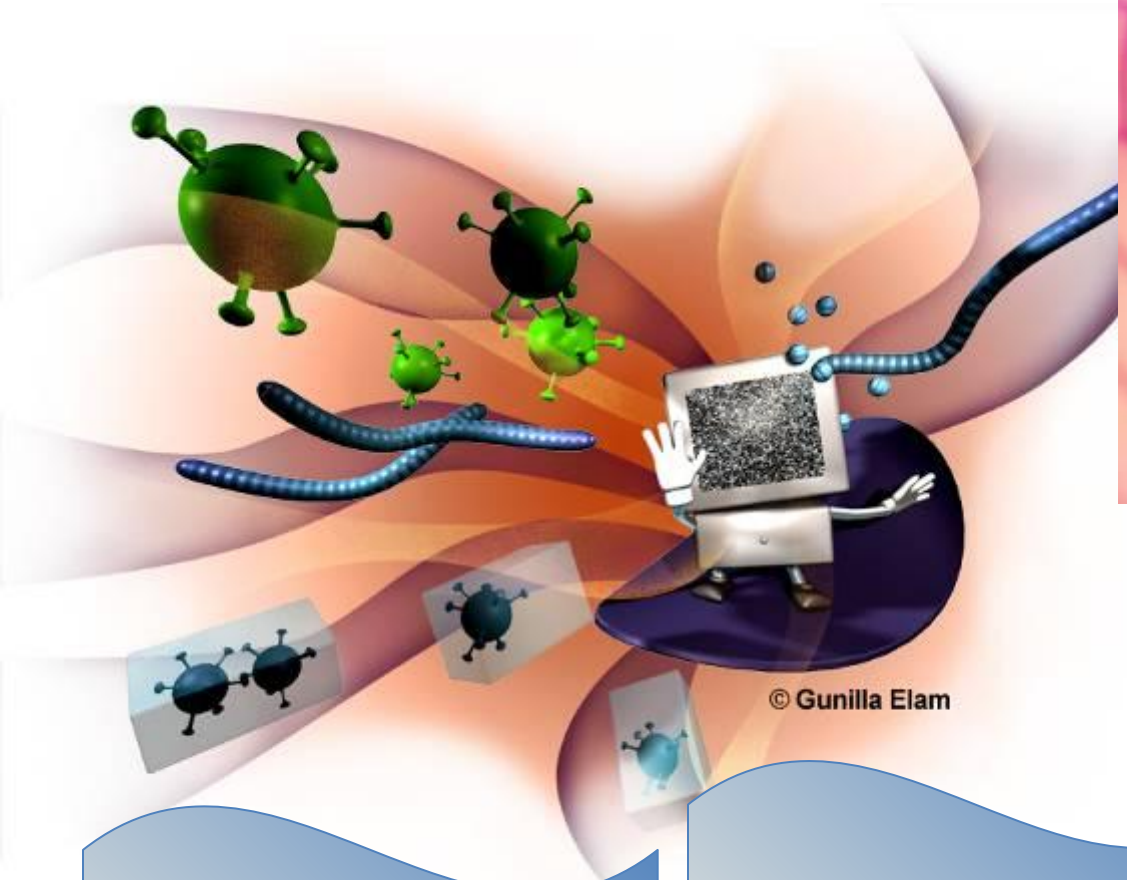
Безопасность в сети Интернет

МАОУ СОШ № 25 г. Челябинска
Учитель информатики и ИКТ :Григорян Д.Г.

Безопасность в интернете

Интернет стал неотъемлемой частью нашей жизни. С его помощью мы получаем информацию, общаемся, обмениваемся данными, оплачиваем товары и услуги, отправляем документы для поступления в вузы и делаем многое другое. Вместе с тем интернет таит в себе опасности — о них необходимо знать, чтобы избегать их.

Опасности в сети Интернет



Вирусы

Черви

Трояны

СОВЕТЫ ПО БЕЗОПАСНОЙ РАБОТЕ В ИНТЕРНЕТЕ

СЛОЖНЫЙ ПАРОЛЬ

Если ты регистрируешься на сайте, в социальной сети или в электронной почте, придумай сложный пароль, состоящий из цифр, больших и маленьких букв и знаков. Чем сложнее пароль, тем сложнее взломать твой аккаунт. Помни, что твой пароль можешь знать только ты.

СОВЕТ ВЗРОСЛЫХ

Всегда спрашивай взрослых о непонятных вещах, которые ты встречаешь в Интернете: ты не знаешь, какой пункт выбрать, на какую кнопку нажать, как закрыть программу или окно. Они расскажут тебе, как поступить - что можно делать, а что нет.

ЛИЧНАЯ ИНФОРМАЦИЯ

Никогда не рассказывай о себе незнакомым людям в Интернете: где ты живешь и учишься, не сообщай свой номер телефона. Не говори никому о том, где работают твои родители и номера их телефонов. Эта информация может быть использована во вред тебе и твоим родителям.

НЕ ОТПРАВЛЯЙ СМС

Если в Интернете ты решил скачать картинку, игру или мелодию, а тебя просят отправить смс - не делай этого! Смс на короткие номера могут стоить несколько сотен рублей. Ты потеряешь деньги, которые мог бы потратить на что-то другое.

НЕ ЗАБУДЬ ВЫЙТИ

При использовании чужих компьютеров или мобильных устройств, не забывай выходить из своего ящика электронной почты или профилей в социальных сетях. Иначе, следующий пользователь этого устройства сможет просмотреть твою личную информацию.

ОСТОРОЖНО, НЕЗНАКОМЕЦ

Никогда не отвечай на сообщения от незнакомцев в Интернете и не отправляй им смс. Если незнакомый человек предлагает встретиться или пишет тебе оскорбительные сообщения - сразу скажи об этом взрослым! Не все люди являются теми, за кого себя выдают в Интернете!

БЕСПЛАТНЫЙ Wi-Fi

При выходе в Интернет через общественную Wi-Fi сеть, не совершай никаких покупок и оплаты, не проверяй личную электронную почту и не передавай конфиденциальную информацию. Злоумышленники могут похитить ваши пароли и данные.

ЗАЩИТИ КОМПЬЮТЕР

Попроси родителей или сам установи систему фильтрации SkyDNS на сайте www.skydns.ru. Она защитит тебя от потери денег и кражи паролей, а также будет блокировать большую часть рекламы, ускоряя загрузку страниц в Интернете.

SkyDNS

Какие опасности могут поджидать в интернете

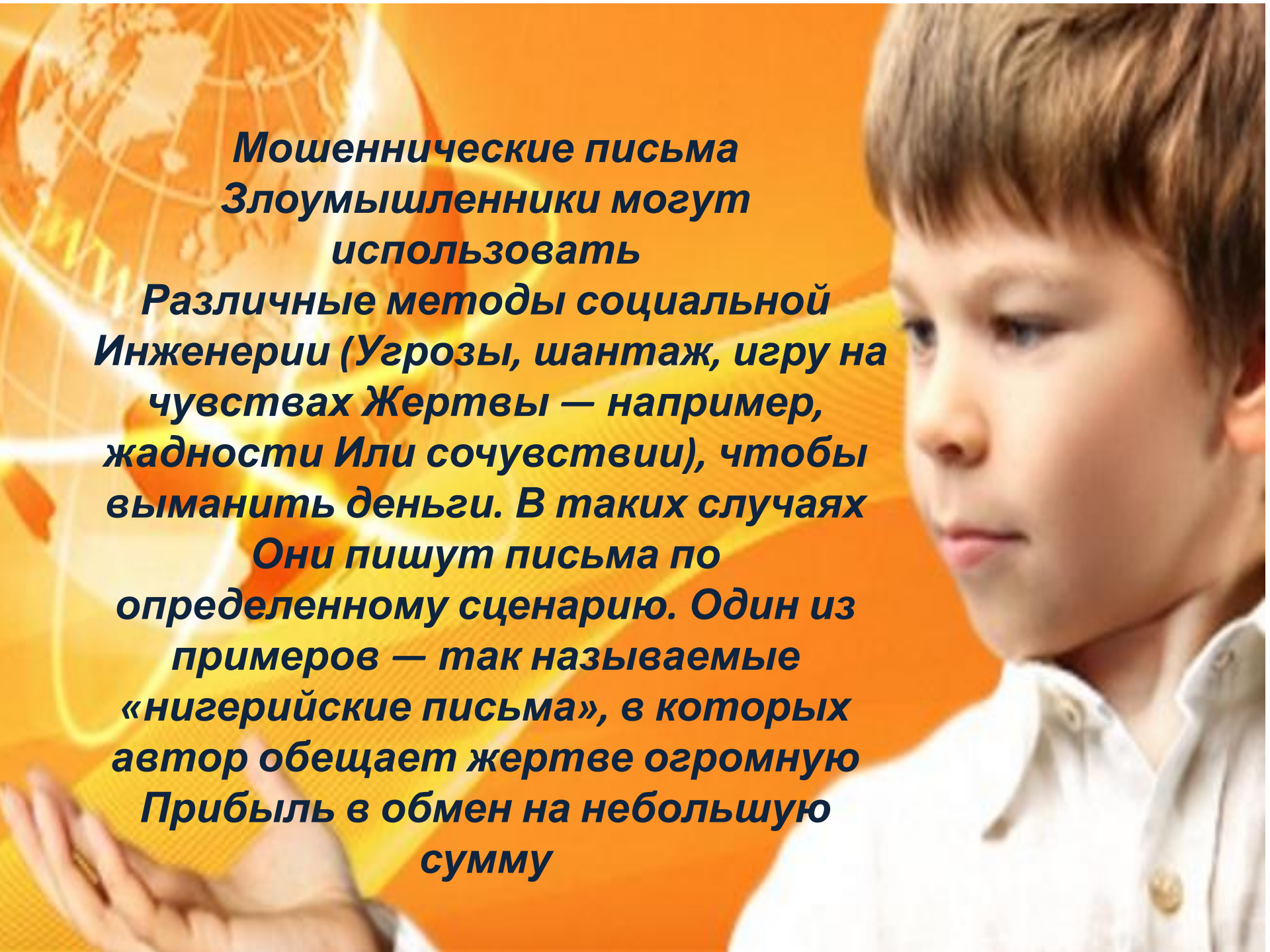
В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Мошенники могут использовать самые разные инструменты и методы — например, вирусное программное обеспечение (или «вирусы»), поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и на почтовых сервисах.

Вирусы

Вирусы могут распространяться с помощью вложенных файлов, ссылок в электронных письмах или в соцсетях, на съемных носителях, через зараженные сайты. Сообщение с вирусом может прислать как посторонний человек, так и знакомый, но уже зараженный участник социальной сети или почтовой переписки. Зараженными могут быть сайты, специально созданные в целях мошенничества, или обычные ресурсы, но имеющие уязвимости информационной безопасности.

Рекомендации

- Используйте антивирусное программное обеспечение с обновленными базами вирусных сигнатур.
- Не открывайте вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства связи, не удостоверившись, что файл или ссылка не содержит вирус.
- Внимательно проверяйте доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).
- Обращайте внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.
- Не подключайте к своему компьютеру непроверенные съемные носители.
- Не поддавайтесь на провокации злоумышленников, например, требование перевести деньги или отправить смс, чтобы снять блокировку компьютера.


Мошеннические письма
Злоумышленники могут
использовать
Различные методы социальной
Инженерии (Угрозы, шантаж, игру на
чувствах Жертвы — например,
жадности Или сочувствии), чтобы
выманить деньги. В таких случаях
Они пишут письма по
определенному сценарию. Один из
примеров — так называемые
«нигерийские письма», в которых
автор обещает жертве огромную
Прибыль в обмен на небольшую
сумму

Получение доступа к аккаунтам в социальных сетях и на других сервисах

Злоумышленники часто стремятся получить доступ к аккаунтам жертвы, например, в социальных сетях, на почтовых и других сервисах. Украденные аккаунты они используют, в частности, для распространения спама и вирусов.

Мошенники могут получить доступ к учетной записи жертвы следующими способами:

- Заставить жертву ввести свои данные на поддельном сайте.
- Подобрать пароль жертвы, если он не сложный.
- Восстановить пароль жертвы с помощью «секретного вопроса» или указанной при регистрации электронной почты.
- Перехватить пароль жертвы при передаче по незащищенным каналам связи.

Похищение данных при использовании бесплатных сетей Wi-Fi

Сейчас мы много общаемся через компьютер или смартфон и часто делаем это в общественных местах — **подключившись к Wi-Fi-сети, которая не защищена паролем**. Когда никто из окружающих не заглядывает в экран, создаётся ощущение приватности. На самом деле, передача данных через открытую Wi-Fi-точку – это в каком-то смысле разговор в полный голос в людном месте. Злоумышленники создают сети с распространёнными названиями и просматривают всё, что подключившиеся к ней пользователи делают в интернете: читают и пишут личные сообщения в соцсетях, вводят пароли или данные банковских карт.

Бесплатное скачивание файлов

Часто пользователям, которые хотят бесплатно скачать файл или посмотреть видео в хорошем качестве без рекламы, предлагают ввести на сайте мобильный номер. Если так и сделать, может включиться платная смс-подписка и с указанного номера будут списываться деньги.

Рекомендации

- Не указывайте свой мобильный номер на незнакомых сайтах.
- Если подписка уже оформлена, позвоните в службу поддержки оператора мобильной связи и попросите отключить её.

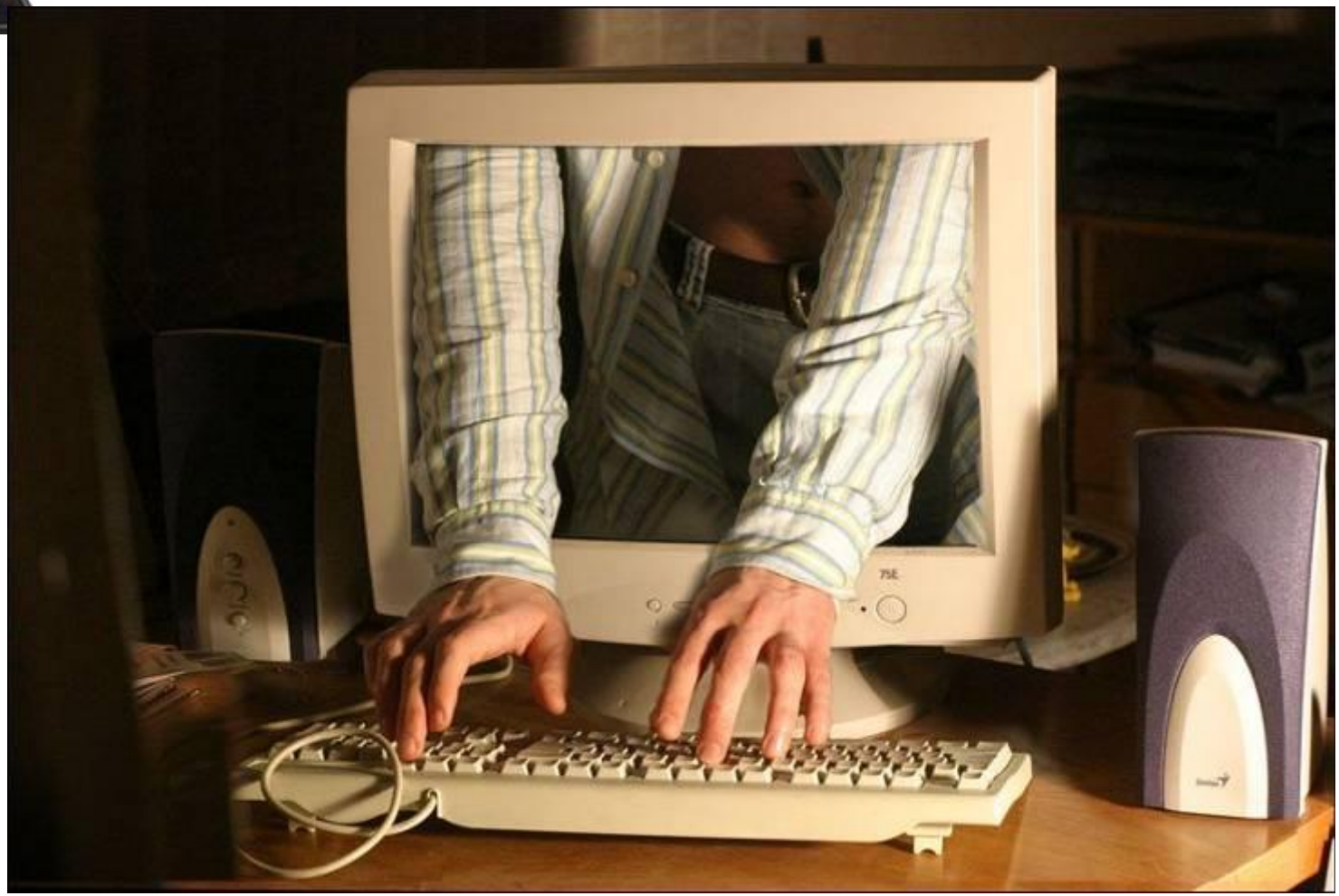
Поведение в сети Интернет

Пользователям запрещается:

- *1. Передавать по сети информацию, оскорбляющую честь и достоинство других абонентов сети, содержащую призывы к насилию, свержению существующего строя, разжиганию межнациональной розни а также передавать информацию, которая по закону не подлежит разглашению.*
- *2. Разрабатывать и распространять любые типы вирусов.*
- *3. Вести деятельность, противоречащую национальным интересам России.*
- *4. Производить действия, запрещенные положением статей УК РФ в части преступлений в сфере компьютерной информации, запрещения распространения порнографии, национальной дискриминации и призывов к насилию.*
- *5. Наносить ущерб работоспособности Сети, создавать помехи работе других Пользователей.*
- *6. Искажать или уничтожать информацию, на компьютерах других пользователей.*
- *7. Заниматься хакерством.*
- *8. Заниматься в Сети или посредством Сети любой деятельностью, запрещенной законодательством РФ.*

1. *Не запускайте у себя на компьютере программы из ненадежных источников и не открывайте приложения к письмам.*
2. *Не надо верить всем сообщениям о новых страшных вирусах, появившихся в Интернет, особенно если в сообщении сказано, что надо распространить эту информацию всем Вашим знакомым. (адрес технической службы: admin@ptl.ru.)*
3. *Если Вы получили письмо от незнакомого человека или организации, то знайте, что скорее всего это спам.*
4. *Обязательно установите на ВСЕ компьютеры антивирусную программу для защиты от троянских коней и вирусов в режиме резидентного монитора.*
5. *Ограничьте доступ к Вашему компьютеру с помощью программ управления доступом (сайт www.listsoft.ru) и введите запрос пароля BIOSом при включении компьютера).*
6. *Делайте резервные копии системных файлов и важных данных и храните их в безопасном месте.*
7. *Для повышения безопасности следует установить на компьютере персональный пакетный фильтр - программу. (www.sphere.agnitum.com, www.tinysoftware.com, www.grc.com)*
8. *Если ваш компьютер используется только для доступа в Интернет с помощью модема, оставить только протокол TCP/IP. Также стоит отключить*

Опасности в сети Интернет



Хакеры