Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования

Финансовый университет при правительстве Российской Федерации

Кафедра «Информатики и программирования»

РЕФЕРАТ

на тему: «Проблемы обеспечения безопасности информации в сети интернет»

Выполнила:

студентка группы ФК 1-2

Балова Марьяна

Научный руководитель:

Голубева Н.Н.

МОСКВА

2010 г.

ОГЛАВЛЕНИЕ

1. Интернет сегодня. Его значение и роль 3

2. Способы защиты информации 4

3. Недостатки способов защиты информации 6

Заключение 8

Список использованной литературы 9

1. ИНТЕРНЕТ СЕГОДНЯ. ЕГО ЗНАЧЕНИЕ И РОЛЬ

Интернет. Сегодня он стал неотъемлемой частью жизни каждого из нас. Вряд ли найдется человек, не знающий про его существование. Трудно представить себе нашу современность без глобальной сети, которая затронула практически все сферы жизни современного человека.

Что же такое интернет? Какова его роль в современном обществе?

С одной стороны, интернет может быть очень полезен. Он может стать источником полезной информации, которая необходима при обучении. Он помогает общаться на больших расстояниях, что я считаю так же немаловажным. Но с другой стороны, всемирная паутина может быть не только помощником, но и порой может приносить огромный вред. Сегодня практически все в той или иной степени зависимы от него. Интернет может быть источником не только нудной, но и вредной информации. Всё зависит от того с какими целями и как его использовать.

Интернет—это компьютерная сеть, где вся информация хранится в виде файлов. Сами файлы расположены на серверах[[1]](#footnote-1), постоянно подключенных к линиям связи, через которые происходит доступ к ним. Все файлы в совокупности – это ресурсы Интернета.

Ресурсы могут быть нескольких типов:

1. Текстовые;

2. Гипертекстовые;

3. Электронные письма;

4. Звуковые;

5. Другие.

2. СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

Как известно, работая в интернете, постоянно сталкиваешься с вирусами и спамами. Вирусы могут привести к сбою всей системы компьютера, уничтожить информацию, хранящуюся в нем. Постоянно существует огромная вероятность «подхватить» тот или иной вирус.

По опросу, проведенному в 1997 году, большая угроза для информации могла прийти из интернета. То есть большее число опрошенных видело угрозу для хранения информации в компьютерах. По мере улучшения и развития техники и способов безопасности, этот процент уменьшался.



Диаграмма 1

Иными словами, работа во Всемирной паутине не всегда может быть безопасной. Для защиты компьютера и различных файлов, хранящихся в нем, нужно использовать некоторую профилактику. Она может снизить вероятность проникновения вируса в компьютер.

Начнем с окна настройки параметров браузера, точнее, к вкладке Безопасность Internet Explorer (в Netscape Navigator – окно Preferences, категория Advanced). В разделе Активное содержание нужно снять все флажки (Загрузка активного содержимого, Элементы ActiveX и модули plug-ins, Сценарии ActiveX, Программы Java). Далее, щелкнув на кнопке Уровень безопасности, установить уровень безопасности в положение Высокая. Средний уровень безопасности, наиболее подходящий для просмотра мультимедийных Web-страниц можно устанавливать только для просмотра сайтов, которым можно доверять!

Другим, довольно действенным способом защиты от нежеланных гостей является так называемый прокси-сервер (proxy server). Этот термин можно встретить в договоре с провайдером и в меню настроек браузера.

Главной функцией прокси-сервера является защита внутренних компьютеров локальной сети от чужого вторжения, в том числе и защита от вирусов. Например, в любой локальной сети выход в Интернет проходит через прокси-сервер, контролирующий все потоки информации между соединенными сетями, запрещая опасные или сомнительные процедуры.

Когда компьютер не подключен к локальной сети, пользователь может установить в настройках браузера адрес прокси-сервера провайдера. В этом случае прокси-сервер будет выполнять функцию кэша[[2]](#footnote-2)1, расположенного на сервере провайдера. Это позволит ускорить получение файлов из Интернета.

Помимо перечисленных мер безопасности, которые являются пассивными, при работе в Интернете требуется использование активных методов борьбы с различными компьютерными вирусами. Существует огромное количество антивирусных программ[[3]](#footnote-3). Они сразу сообщают «заражение» компьютера тем или иным вирусом. Антивирусы принимают специальные меры для «излечения» «зараженных файлов». В противном случае они эти файлы удаляют.

Ошибочно считать, что компьютер можно «заразить» только через электронную почту или браузеры. IRC-каналы часто служат каналами для отправки тайных программ (вирусов) от недоброжелателей. Очень часто в тех или иных чатах собеседник может отправить пользователю такую программу. Следует помнить, что нельзя сразу открывать полученный файл!!! Лучше всего проверять полученные файлы доступными методами, не надеясь на антивирусные программы. Как минимум посмотреть хотя бы разрешение файла.

Очень часто файлы в WWW с расширением .doc и .xls содержат макровирусы. Их следует всегда предварительно проверять. Считается небезопасным открывать их в программах Word или Exel без проверки. Лучше это делать при помощи специальных программ, которые можно найти на сайте: http://www/microsoft.com/msoffice/.

3. НЕДОСТАТКИ СПОСОБОВ ЗАЩИТЫ ИНФОРМАЦИИ

Как было сказано выше, существует много способов для защиты компьютера. Но, к сожалению, ни один из них нельзя назвать идеальным. Каждый имеет свои изъяны, которые хотелось бы рассмотреть более подробно.

Браузеры: В четвертых и более поздних версиях необходимо устанавливать для зоны Интернет высокий уровень безопасности (по умолчанию стоит Средний), который не дает загружать активные компоненты (ActiveX, Java и т.д.). Такой вариант наиболее безопасен для начинающего пользователя, но может не подойти для просмотра некоторых страниц и интерактивной работы с ними. Оптимальным для просмотра мультимедийных Web-страниц средний уровень безопасности можно устанавливать только для просмотра сайтов, которым можно доверять!

Прокси-сервер: это довольно действенное от вирусов средство имеет свой минус. С помощью прокси-сервера не очень надежного провайдера можно получить «зараженный» или искаженный хакерами файл. Значит надо пользоваться услугами провайдера, который вас защищает, или не пользоваться услугами прокси-сервера. В браузерах прокси-сервер по умолчанию отключен, так что выбор способа работы остается за пользователем.

Антивирусные программы: они установлены практически на всех компьютерах мира. Но нужно отметить, что постоянно появляются новые виды вирусов. Они изменчивы, и временами антивирус не в состоянии и обнаружить. Такие вирусы достаточно быстро распространяются по всей сети, фактически за несколько дней, и то и часы. Наиболее популярным примером этого является «червь Морриса». Иногда антивирусы не в состоянии сразу распознать вирус. Например, антивирусные программы научились определять вирус Trojan.PSW.Stealth (по классификации Касперского) только через 2 месяца после появления в Интернете. Поэтому «прошлогодние» антивирусные программы абсолютно неэффективны. Следовательно, нужно как можно чаще обновлять антивирусные программы.

ЗАКЛЮЧЕНИЕ

Итак, мы можем привести некоторый итог. Существует несколько средств защиты информации. Каждый из них имеет свои плюсы и минусы.

Таблица 1

|  |  |  |  |
| --- | --- | --- | --- |
| № | ВИД ЗАЩИТЫ | ПЛЮСЫ | МИНУСЫ |
| 1. | Браузеры | Дает очень высокий уровень безопасности и является довольно надежным способом защиты | Когда в настройках стоит высокий уровень безопасности, некоторые Web-страницы могут не открываться |
| 2. | Прокси-сервер | Контролирует весь поток информации, благодаря чему является надежным средством защиты. Увеличивает скорость работы интернета. | Очень многое зависит от провайдера. Если он не очень надежный можно получить «зараженный» файл |
| 3. | Антивирусные программы | Очень просты в обращении. Могут находить, «лечить» и удалять «зараженные» файлы. | Не всегда надежны, могут не распознавать новые штампы вирусов. Требуют постоянного обновления. |

Сегодня в эпоху развития всего человечества, во время усиленного технического прогресса проблемы информационной безопасности становятся всё более актуальными. Каждый деловой человек без своего ПК, словно без рук. Там вся нужная информация, которая порой очень важна.

В эру, когда интернет занимает все большее место в нашем мире необходимо улучшать способы безопасности. Это требуется не только программисту, но и обычным людям, что и делает эту тему популярной.

Существует много способов защитить свой ПК. Каждый пользователь имеет право выбора, который из них применять. Так или иначе, любой из видов защиты нужен и необходим особенно сейчас.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Соломенчук А.В. , «Интернет». ПИТЕР, 2000г.
2. Берлинер Э.М., Глазырин Б.Э., Глазырина И.Б. «Офис от Microsoft», Москва, ABF, 1997г.
3. Журин А.А. «Интернет», Москва, 1999г.
4. Полярков Н.И. «Компьютерные технологии», Ростов-на-Дону, «Феникс», 2002г.

1. СЕРВЕР – удаленный компьютер, на котором работает серверная программа, выполняющая обработку запросов пользователей: идентификацию пользователей, проверку их полномочий, прием данных от пользователей и передачу им данных. Также можно говорить и обо всем компьютере в целом: сервер, файл-сервер, почтовый сервер и т. д. [↑](#footnote-ref-1)
2. 1 КЭШ – это специальная область на винчестере или в оперативной памяти, которая служит для хранения файлов, полученных из Интернета (временные файлы). [↑](#footnote-ref-2)
3. Фирма «Лаборатория Касперского» разработала и поддерживает антивирусный пакет AntiViral Toolkit Pro (AVP). Один из адресов фирмы в Интернете – http://www.avp.ru. [↑](#footnote-ref-3)