Несмотря на перечисленные недостатки антивирусной программы AVG Internet Security 2012, он является стабильным, надежным и полностью удовлетворяющим современному уровню защиты.

Конечно, антивирусная программа, порой неспособна найти и обезвредить все вирусы, это происходит потому, что с каждым днем, в сеть попадает огромное количество вредоносных программ и их просто невозможно отследить. Поэтому каждый должен решить для себя, какой антивирус лучше и выбрать тот, который надежней обеспечит работу вашего компьютера.

Библиографический список

1. Обзор AVG Internet Security 2012. Оценка SoftwareCrew 4.5/5. [Электронный ресурс]. – Режим доступа: http://www.comss.ru/page.php ?id=659.

2. AVG Free Anti-Virus [Электронный ресурс]. – Режим доступа: http://www.freeavg.com/about.php?lng=ru-ru&cmpid=other.

Д.Ф. Балагутдинов, Д.Ю. Мартюшева, РГППУ
студенты группы КТ-307

А ВЫ ЗАЩИЩЕНЫ ОТ ВИРУСОВ?

Довольно не все, кто владеет компьютером, заботится о безопасности своих данных. На сегодняшний день вирусные атаки приобрели неимоверные масштабы, поэтому вопрос о безопасности своих данных должна быть первейшей при приобретении компьютера. Только какое антивирусное программное обеспечение выбрать? Вот в чем вопрос…

По результатам тестов авторитетных международных исследовательских центров и компьютерных изданий, лидерские позиции занимает Антивирус Касперского. Основным критерием выбора Антивируса Касперского – это популярность.

Лаборатория Касперского - лидер среди разработчиков технологий для антивирусных систем и систем защиты данных. Одной из последних разработок компании является технология под названием «Тройная защита». В ее основе лежит не одна, а несколько технологий, которые формируют целый комплекс. Данная технология внедряется во все выпускаемые продукты компании «Лаборатория Касперского» начиная с версии 7.0.

«Лаборатория Касперского» является ведущим разработчиком антивирусного программного обеспечения. Их продукты признаны одними из самых лучших разрабатываемых программ своего класса.

Рассмотрим три самых распространенных метода.

Фишинг – это особый вид компьютерного мошенничества. Фишинг-атаки организуются следующим образом: киберпреступники создают подложный сайт, который выглядит в точности так же, как сайт банка или сайт, производящий финансовые расчеты через интернет. Затем мошенники пытаются обманным путем добиться, чтобы пользователь посетил фальшивый сайт и ввел на нем свои конфиденциальные данные – например, регистрационное имя, пароль или PIN-код. Используя их, злоумышленники крадут деньги со счетов попавшихся на удочку пользователей [2].

Вторым методом кражи секретных данных является отслеживание всех действий пользователя и их дальнейшее протоколирование. Это стало возможным после появления так называемых «троянов».

Третий метод чем-то схож со вторым, но в этом случае троянская программа не занимается отслеживанием действий пользователя, а сразу начинает поиск на компьютере конфиденциальных данных. В случае обнаружения таких данных, они будут переданы злоумышленнику в скрытом от пользователя виде, то есть пользователь об этом знать не будет.

Вредоносное программное обеспечение, с помощью которого конфиденциальная информация пользователя в нежелательные руки, может попасть на компьютер пользователя различными методами. Самыми распространенными являются: рассылка по средствам ICQ, через прикреп-

ленные файлы в электронных письмах, при загрузке веб-ресурсе на котором расположен заранее написанный для этих целей скрипт.

Программа, которая нашла на вашем компьютере конфиденциальную информацию, шифрует полученные данные в бинарном файле небольшого размера. Чаще всего данный файл отправляется вору как вложение в электронное письмо, но также может быть использована передача по FTP протоколу.

Из всего выше сказанного можно сделать вывод. Защитная технология которая следит за всеми запущенными приложениями является более эффективной нежели технология основанная на простом сканировании трафика на наличие заранее внесенных в программу персональных данных [1].

Любой пользователь может выбрать те или иные антивирусные программы для защиты своего компьютера. Не стоит забывать, что один пакет Лаборатории Касперского не сможет обеспечить полную защиту компьютера, как в комплексе с его различными утилитами, постоянным обновлением антивирусных баз и периодической проверкой данных.

Библиографический список

1. Методы защиты антивируса Касперского. [Электронный ресурс]. – Режим доступа: http://avp-my.ru/publ/24-metody-zashhity-antivirusa-kasperskogo.html.

2. Что такое фишинговая атака? [Электронный ресурс]. – Режим доступа: http://www.kaspersky.ru/phishing.

М.М. Путров, Е.Ю. Болгова, РГППУ
студенты группы КТ-307

АНТИВИРУСНАЯ ЗАЩИТА: ДЕШЕВО, НО СЕРДИТО, ИЛИ ДОРОГО, НО КАЧЕСТВЕННО?

В современной индустрии IT-технологий существует проблема кражи, незаконного использования персональных данных и нарушения целостности рабочего процесса пользователя. Для этого злоумышленниками