Тема:

Информационная защита и компьютерные вирусы

Выполнил:К.А.Носов

Руководитель: В.Б. Гончаров

Цель:

Обобщить и проанализировать сведения о существующих в настоящее время проблемах в области информационной безопасности, связанных с компьютерными вирусами. Составить рекомендации по защите рабочего места учителя и ученика от компьютерных вирусов.

Актуальность:

В настоящее время в школах появилось большое количество современных компьютеров, объединенных в единую сеть, с возможностью выхода в Интернет. Одновременно с этим растет число компьютерных вирусов, которые несут в себе угрозу информационной безопасности.

Поэтому, направление работы по защите информации от компьютерных вирусов в образовательных учреждениях становится наиболее актуальной.

Статистика

- Благодаря сумасшедшей популярности соц. сетей, количество, качество и изощренность вирусов значительно увеличилась за последний год. И все это ради персональной информации пользователей. Многие крупные фирмы, занимающиеся безопасностью, отслеживают информацию по вредоносам с разных источников, дабы владеть общей картиной. Вот и G Data Software тоже занимается подобной работой. По их данным количество новых вирусов в 1 половине 2010 года была около 1 017 208, а это в 2 раза больше по сравнению с 2009 того же периода.
- Среди этих вирусов больше всего троянов, осуществляющих шпионаж на заражённом компьютере (Trojan-Spy, увеличение за год — 135%). От них немного отстают вирусы, ворующие всевозможные логины и пароли (Trojan-PSW, рост 94%) и пытающиеся перехватить ключи от банковских систем (Trojan-Banker, рост 22%)

- Возможные пути заражения
- Профилактика вирусного заражения
- Действия после заражения вирусом
- Организация защиты рабочего места учителя и ученика

Возможные пути заражения

1.Глобальные сети - электронная почта

2.Электронные конференции, файл-серверы

3.Локальные сети

4.Пиратское программное обеспечение

5.Персональные компьютеры “общего пользования”

6.“Случайные” пользователи компьютера

Профилактика вирусного заражения

1.Организационная

Организационные меры защиты ВТ включают в себя совокупность организационных мероприятий: по подбору, проверке и инструктажу персонала; разработке плана восстановления информационных объектов после входа их из строя; организации программно-технического обслуживания ВТ; возложению дисциплинарной ответственности на лиц по обеспечению безопасности конкретных ВТ;

2. Программная
   - средства архивации данных;
   - антивирусные программы;
   - криптографические средства.

3. Техническая

Аппаратная защита носителя от записи

Действия после заражения вирусом

1. Отключить компьютер от сети(локальной, интернет)

2. Провести полное сканирование компьютера

3. Удалить все найденные вирусы

3. Использовать диск для восстановления системы

4. Принять все возможные меры защиты от вирусов

Организация защиты рабочего места учителя и ученика

1.Установка защитного ПО(Фильтры, *Firewall,антивирусные программы*)

2.Установка пароля

3.Ограничение в доступе к некоторым функциям

4.После работы сохранить все данные на съемные носители

Название антивирусного программного обеспечения	Показатель надежности антивируса (первое полугодие 2010)	Место с учетом AMTSO
Dr.Web Security Space	0.921	1 местов в ТОП10
Eset Smart Security	0.923	2 местов в ТОП10
Avast Antivirus Professional	0.914	3 местов в ТОП10
Kaspersky Internet Security 2010	0.941	4 местов в ТОП10
McAfee Internet Security Suite	0.937	5 местов в ТОП10
Norton Internet Security 2009	0.919	6 местов в ТОП10
Avira Premium Security Suite	0.889	7 местов в ТОП10
Microsoft Security Essentials	0.919	8 местов в ТОП10
AVG Internet Security	0.903	9 местов в ТОП10
Panda Internet Security 2010	0.872	10 местов в ТОП10

Вывод

Проанализировав сведения о существующих в настоящее время проблемах в области информационной безопасности, связанных с компьютерными вирусами я открыл для себя новые пути защиты данных и борьбы с вредоносными программами. Основываясь на этом я составил рекомендации по защите рабочего места учителя и ученика от компьютерных вирусов.В дальнейшем планирую самостоятельно провести тестирования некоторого количества антивирусных программ.

Примерная должностная инструкция инженера (системного администратора) школы

- **1. Общие положения**
- 1.1. Инженер назначается и освобождается от должности директором школы.
- 1.2. На должность инженера принимаются лица с высшим образованием и стажем работы по специальности не менее года.
- **2. Функции**
- Основными направлениями деятельности инженера являются:
- 2.1. Обеспечение процессов создания и развития внутришкольной сети, охватывающей все подразделения школы.
- 2.2. Настройка базового программного и аппаратного обеспечения.
- 2.3. Определение и осуществление сетевой политики школы.
- 2.4. Организация бесперебойной работы всех звеньев информационной системы школы.
- 2.5. Выполнение функции мастера обучения пользователей сети.