

ДЕТИ **НЕШПИОНОВ: КАК ЗАЩИТИТЬ КОМПЬЮТЕРНЫЙ КЛАСС?**

***Баричев Сергей Геннадьевич, к.т.н.
преподаватель информатики
СОШ №593 (г. Москва)***

ПОСТАНОВКА ПРОБЛЕМЫ

КОМПЬЮТЕРНЫЙ КЛАСС:

- **Что защищать?**

Компьютерный класс как ресурс учебного процесса
(работоспособность)

- **От кого защищать?**

От учеников (любопытство, вредность, ошибочные действия)

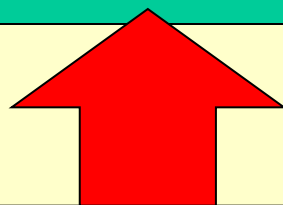
УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Привнесение из дома программ (обычно игровых) и документов, которые могут быть источником вирусов;
- Изменение настроек операционной системы и удаление программ, используемых на занятиях (случайное или преднамеренное);
- Посещение сайтов (порно- и трз), почти гарантированно содержащих вредоносный код*;
- Получение электронной почты с опасными вложениями (опять же вирусы и троянские программы)*;
- Активная загрузка содержимого из Интернета*.

* При наличии Интернет-подключения

ПОСЛЕДСТВИЯ ЭТИХ УГРОЗ

- Финансовые потери (школы, департамента образования);
- Потеря времени преподавателя и администратора;
- Снижение эффективности занятия.



ПРОТИВОДЕЙСТВИЕ:

- Организационные меры;
- Программно-технические средства;

ОРГАНИЗАЦИОННЫЕ МЕРЫ

- 1. Инструктаж;**
- 2. Санкции за нарушение дисциплины;**
- 3. Размещение компьютеров мониторами к преподавателям;**
- 4. Использование ПК без дисководов и USB-портов, отключение Интернета.**

ОРГАНИЗАЦИОННЫЕ МЕРЫ

1. Инструктаж;
2. Санкции за нарушение дисциплины;
3. Размещение компьютеров мониторами к преподавателям;
4. Использование ПК без дисководов и USB-портов, отключение Интернета.

? НЕДОСТАТКИ ?

1. Эффективны для сознательной части обучаемых (1,2).
2. Ограниченно реализуемы и негибки (3,4)

ПРОГРАММНО-ТЕХНИЧЕСКИЕ СРЕДСТВА

1. Подготовка операционной системы:

- Использование **ТОЛЬКО Windows 2000, XP или 2003** (но не Windows 95/98/ME);
- Создание учетных записей («Преподаватель/Администратор», «Ученик»), защищенных **ПАРОЛЕМ**.

ЭТО МИНИМУМ!

ПРОГРАММНО-ТЕХНИЧЕСКИЕ СРЕДСТВА

1. Подготовка операционной системы:

- Использование ТОЛЬКО Windows 2000, XP или 2003 (но не Windows 95/98/ME);
- Создание учетных записей («Преподаватель/Администратор», «Ученик»), защищенных ПАРОЛЕМ.

2. Специальные программы:

- Антивирусные программы;
- Программы ограничения доступа к съемным носителям (дисководам, портам);
- Программы удаленного контроля;
- Межсетевые экраны (файрволлы, брандмауэры).

АНТИВИРУСНЫЕ ПРОГРАММЫ

ПРИМЕР: «Антивирус Касперского», NOD32, Dr. Web

Надо понимать:

- 1. Не всегда помогают в борьбе с троянскими программами;**
- 2. Не помогают от внешних атак;**
- 2. Эффективны только при:**
 - резидентном использовании с периодическим полным сканированием дисков;**
 - регулярном обновлении (не реже 1 раза в неделю)**
 - контроле работоспособности (!)**

ПРОГРАММЫ ОГРАНИЧЕНИЯ ДОСТУПА К СЪЕМНЫМ НОСИТЕЛЯМ

ПРИМЕР: Device Lock (1С:Дистрибуция)

Возможности:

- 1. Запрет или гибкое управление доступом к съемным носителям;**
- 2. «Журналирование»;**
- 3. «Теневое копирование».**

Делает компьютерный класс БЕССМЫСЛЕННОЙ штукой
для:

- 1. Любителей игр (приносимых с собой)**
- 2. Любителей закачек (музыка, кино и т.д.)**

ПРОГРАММЫ УДАЛЕННОГО КОНТРОЛЯ

ПРИМЕР: Remote Administrator (1С:Дистрибуция)

Возможности:

- 1. Наблюдение за компьютерами в сети;**
- 2. Помощь в выполнении заданий;**

(+) Методические возможности:

- 1. Создание полиэкрана из ученических компьютеров (сравнение скорости и качества выполнения заданий);**
- 2. Совместное рисование в графическом редакторе.**

Само наличие (!) программы отбивает «охоту» делать что-либо кроме выданных заданий

МЕЖСЕТЕВЫЕ ЭКРАНЫ

ПРИМЕР: ViPNet Personal Firewall (1С:Дистрибуция)

Возможности:

- 1. Блокировать активность вредоносных программ;**
- 2. Гибко ограничить Интернет-приложения (разрешить Internet Explorer, но запретить электронную почту, ICQ, сетевые игры и т.д.);**
- 3. Защитить от внешних атак (первым испытательным объектом для «юного хакера» на 99% будет родная школа).**

Гарантия защиты компьютера при подключении к Интернету

ВОПРОСЫ

???