Департамент внутренней и кадровой политики Белгородской области Областное государственное автономное профессиональное образовательное учреждение «Валуйский колледж»

Специальность 09.02.07 Информационные системы и программирование

Тема работы: Информационная безопасность

Подготовил: студент 13 группы Королев Даниил Геннадьевич Научный руководитель: Васильченко Елена Сергеевна

Содержание:

- 1. Актуальность
- 2. Проблема и цель работы
- з. Гипотеза
- 4. Задачи
- 5. Методы исследования
- 6. Теоретическая и практическая значимость
- 7. Основная часть работы
- 8. Заключение

Актуальность

В наш век компьютерных технологий появляется все больше компьютерных вирусов и мошенников. С развитием угроз должна развиваться безопасность, средства, ликвидирующие данные угрозы. Я считаю, что данная тема будет очень актуальна для людей, которые хотят познакомиться, лучше изучить данную проблему и не сталкиваться с представленными угрозами

Проблема

Как обезопасить свой компьютер от внешних угроз?

Цель работы

Изучить внешние угрозы и способы их предупреждения

Гипотеза

Если на компьютере установлен антивирус, то он поможет защитить компьютер от вирусов и иных угроз

Задачи

- 1. Выявить, какие существуют угрозы для Персонального компьютера (ПК)
- 2. Изучить какие существуют антивирусы, каково должно быть их количество на ПК и как они работаю.
- 3. Проанализировать полученные сведения и сделать вывод.

Методы исследования

- **1.** Анализ
- 2. Сравнение
- 3. Обобщение

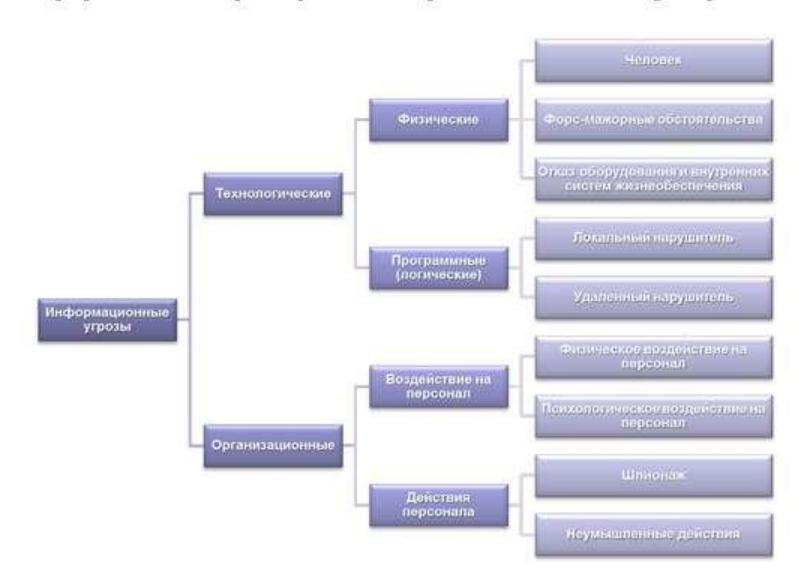
Теоретическая и практическая значимость

Данное исследование восполняет пробел, образовавшийся в результате быстрого скачка технологий в результате чего многие пользователи не осознают всей серьезности данной ситуации.

С помощью данного исследования люди, изучившие данную статью смогут обезопасить себя от большинства угроз



Виды информационных угроз





Политика безопасности - это комплекс мер и активных действий по управлению и совершенствованию систем и технологий безопасности, включая информационную безопасность.





Программные средства защиты информации

Средства защиты от несанкционированного доступа (НСД):
 Средства авторизации;
 Мандатное управление доступом;
 Избирательное управление доступом;
 Управление доступом на основе ролей;
 Журналирование (так же называется Аудит).
Системы анализа и моделирования информационных потоков (CASE-системы).
Системы мониторинга сетей:
 Системы обнаружения и предотвращения вторжений (IDS/IPS).
 Системы предотвращения утечек конфиденциальной информации (DLP-системы).

- Анализаторы протоколов.
- Антивирусные средства.

ВИДЫ АНТИВИРУСНЫХ ПРОГРАММ

- Детекторы позволяют обнаруживать файлы, заражённые одним из нескольких известных вирусов. Некоторые программы-детекторы также выполняют эвристический анализ файлов и системных областей дисков, что часто (но отнюдь не всегда) позволяет обнаруживать новые, не известные программе-детектору, вирусы.
- Фильтры это резидентные программы, которые оповещают пользователя о всех попытках какой-либо программы записаться на диск, а уж тем более отформатировать его, а также о других подозрительных действиях.
- Программы-доктора или фаги не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программывируса, возвращая файлы в исходное состояние.
- Ревизоры запоминают сведения о состоянии файлов и системных областей дисков, а при последующих запусках – сравнивают их состояние исходным. При выявлении несоответствий об этом сообщается пользователю.
- Сторожа или фильтры располагаются резидентно в оперативной памяти компьютера и проверяют на наличие вирусов запускаемые файлы и вставляемые USB-накопители.
- Программы-вакцины или иммунизаторы модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже заражёнными.



Программные средства защиты информации

M	Іеж	ce	гевые	экра	ны.
				AND DESCRIPTION OF THE PERSON	

- Криптографические средства:
 - Шифрование;
 - Цифровая подпись.
- Системы резервного копирования.
- Системы аутентификации:
 - Пароль;
 - Ключ доступа (физический или электронный);
 - Сертификат;
 - Биометрия.
- Инструментальные средства анализа систем защиты:
 - Мониторинговый программный продукт.

Заключение

Проанализировав данный материал я пришел к выводу, что одной антивирусной программы для хорошей безопасности мало, ведь каждая программа нацелена на определенный вид и род вирусной программы

CNACNOO 3A BHNMAHME