

Слайд 1

Уважаемые председатель и члены Государственной аттестационной комиссии! Вашему вниманию предлагается работа на тему «Исследование эффективности систем антивирусной защиты».

Слайд 2

Актуальность исследования эффективности систем антивирусной защиты, обусловлена, прежде всего, проблемной ситуацией новых информационных технологий, порожденной высокой пропускной способностью Интернета и количеством кибер-атак.

Целью исследования является – организация и исследование эффективности систем антивирусной защиты корпоративной компьютерной сети предприятия «Навиком».

Для решения поставленной цели необходимо решение следующих задач:

1. Обзор и системный анализ задач по теме исследования;
2. Анализ предметной области;
3. Рассмотрение вопросов безопасности сети;
4. Расчет затрат на приобретение программных и аппаратных средств защиты для сети предприятия
5. Исследование эффективности предложенных решений методом математического анализа.

Слайд 3

В первой части исследования были рассмотрены теоретические основы вредоносных технологий, в частности, были выделены и классифицированы различные виды вирусов. Полученные результаты теоретического исследования позволили спроектировать информационную модель и разработать алгоритм (models and methods) создан для информационной системы Call центр Ip телефонии.

Слайд 4

Следует заметить, что эффективность работы антивирусов может быть нарушена, если выполнять все работы, описанные ранее не вовремя. Для того чтобы не допускать таких случаев я предлагаю использовать функции контроля и управления, представленные на слайде.

Слайд 5

Эти функции реализовывают центры управления, которые будут находится на машине у администратора и позволят управлять все защитой сети. Если компьютер подключен к сети предприятия через медленную сеть, то для него создается локальный дистрибутивный каталог для ускорения процесса установки и обновления. Антивирусный сервер выполняет управляющие и координирующие действия. Помимо агентов, на каждой рабочей станции и сервере корпоративной сети устанавливается антивирус, выполняющий сканирование файлов и проверку файлов при их открытии (функции сканера и антивирусного монитора).

Слайд 6

Для нахождения оптимального защитного средства был проведен сравнительный анализ популярных защитных средств современно информационного рынка.

Слайд 7

Для решения задачи оптимизации сравнительная таблица была преобразована в числовую форму с одновременной нормализацией данных.

Слайд 8

Таким образом, анализ показал, что наиболее оптимальным антивирусным средством является NOD 32. Следующим по значимости идет Антивирус Касперского, чуть хуже - Trend Micro ServerProtect, следом Panda Security.

Слайд 9

Длительность запуска операционной системы является хорошим показателем влияния на время работы компьютера. Так, были проведены тесты, для определения скорости загрузки, чтобы выявить этот показатель. Сначала узнав время работы эталонной системы, а затем установив по очереди каждый антивирус на нее, было определено, как они влияют на время загрузки ОС. Для каждой антивирусной продукции проведены тесты 10 раз для чистоты эксперимента.

Слайд 10

Важный элемент антивирусной программ для обеспечения безопасности компьютера — это монитор осуществляющий работу в реальном времени. Он производит проверку файлов в системе над которыми производятся какие-либо действия. Для проверки этого механизма был проведен следующий тест: я измерил время копирования тестовой папки с USB накопителя на жесткий диск компьютера. Папка состояла из не зараженных файлов различного типа (дистрибутивы программ, документы, медиа файлы, системные файлы и прочие) их общий объем составил 6.06 Гб.

Наихудшим образом себя проявил Trend Micro ServerProtect антивирус, время копирования папки с установленным антивирусом и включенным монитором защиты в реальном времени по сравнению с эталонной системой составило 8 минут 38 сек., что на 238% больше, чем без антивируса. ESET NOD32 антивирус практически не повлиял на скорость копирования файлов.

Слайд 11

Антивирусное ПО может повлиять на время открытия приложений и файлов. Для этого были проведены измерения времени запуска приложений с помощью утилиты AppTimer. Для чистоты эксперимента все измерения времени всех файлов производилось сразу после загрузки ОС без повторного открытия. Результаты представлены на слайде.

Слайд 12

В данной работе приведено исследование нештатной ситуации работы сети (активное развитие эпидемии компьютерного вируса) в течение 24 часов. Рассматриваемый период был разбит на 50 равных отрезков времени.

Слайд 13

В таблицах представлены вводимые экспериментальные данные.

Слайд 14

На рисунке показаны траектории динамики функций, характеризующие количество компьютеров разных типов, и функции управления. На приведенном графике можно заметить, что при большой скорости распространения вредоносного кода за рассматриваемый период удастся погасить эпидемию. При этом выполнено требование, что в конечный момент времени рассматриваемого периода количество невосприимчивых компьютеров $R(t)$ составляет более 80 % (а именно 89,9 %).

Данная программа может быть полезна системным администраторам при формировании структуры компьютерных сетей, максимально защищенных от вирусных атак. При этом работа администратора максимально упрощена: программа высчитывает оптимальное значение частоты обновления антивирусных баз, позволяет моделировать различные ситуации.

Слайд 15

Таким образом, разработанные решения соответствуют требованиям, поставленным компанией: повысить эффективность компании за счет внедрения системы антивирусной защиты, уменьшение затрат времени на работу инженера безопасности за счет автоматизации процессов управления системой антивирусной защиты для повышения качества работы компании «Навиком».

Таким образом, цель работы достигнута.

Спасибо за внимание! Доклад окончен!