ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ КОРПОРАТИВНОЙ СЕТИ В УСЛОВИЯХ ВРЕДОНОСНОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ

Л. М. Груздева (Владимир)

Корпоративные сети (КС) подвергаются серьезным угрозам в связи с многочисленными атаками вредоносных программ (ВП). Успешная реализация атаки влечет за собой как минимум снижение качества функционирования сети. Одним из самых распространенных видов вредоносных программ являются классические компьютерные вирусы [1], для защиты от которых активно применяются антивирусные программы (АП).

Работу антивирусных программ нельзя оценивать однозначно, так как во многом АП похожи на вирусы. Так, антивирусные программы используют больше ресурсов компьютера, чем требуют для своей работы вирусы. Зачастую антивирусы тем или иным образом ограничивают функциональные возможности программного обеспечения, установленного в узлах сети. Для оптимальной работы антивирусов требуется постоянное их обновление, что может создавать значительную нагрузку на КС.

Эффективное управление корпоративными сетями, их модернизация, в том числе и систем защиты, невозможны без оценок качества функционирования, одной из которых является производительность КС. Показателями производительности называют показатели, характеризующие затраты времени на получение системой каких-либо полезных результатов. К их числу относятся, например, средние значения времён ответа КС на разные типы запросов, средние числа задач разного типа, решаемых системой в единицу времени, коэффициенты загрузки устройств КС и другие показатели.

В [2] рассмотрены аналитические модели оценки влияния вредоносных и антивирусных программ на показатели производительности корпоративных сетей, но нарастающее усложнение сетей приводит к пониманию невозможности адекватного описания процессов функционирования только аналитическими методами. Мировая практика научных исследований свидетельствует о том, что методы имитационного моделирования занимают около 70% в общем объеме исследовательского инструментария.

Объект исследования: корпоративная сеть предприятия Гос. НИИЛЦ РФ «Радуга» на 13 производственной площадке. В состав корпоративной сети (рис.1) входят: 4 рабочих станций, 1 сервера, 1 сетевого коммутатора, объединенных сетевыми кабелями. Имеется связь с внешней локальной сетью и сетью Интернет.

Постановка задачи: исследовать влияние вредоносных и антивирусных программ на характеристики КС с помощью системы имитационного моделирования GPSS World.

Работа КС формализуется в виде СМО с ограниченной очередью. Поток заявок распределен по закону Пуассона с интенсивностью λ заявок на ед.вр. (увеличивается при воздействии ВП), а время обработки заявки распределено экспоненциально, интенсивность обработки – μ (увеличивается при воздействии АП).

Характеристики СМО:

– среднее количество пакетов (заявок) в очереди;

– общее число пакетов (заявок) в очереди, то есть запросов, ожидавших момента обслуживания в течение работы системы;

– средняя продолжительность пребывания заявки в системе.

Требуется: провести сравнительный анализ характеристик КС в условиях работы вредоносных и антивирусных программ.

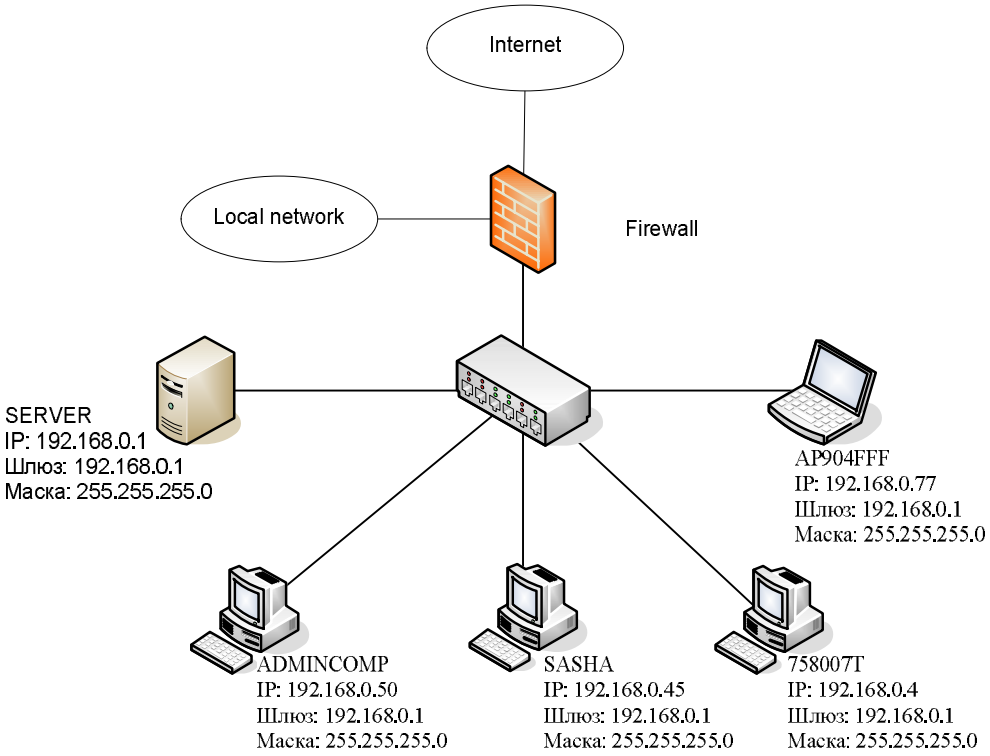

Рис. 1. Структура корпоративной сети

Формализация задачи

Моделируемый процесс: передача пакетов (заявок) от рабочих станций пользователей к серверу КС. При построении модели определены следующие базовые параметры системы:

1) Единица времени в моделируемой системе – 1 секунда. Размер передаваемого пакета в моделируемой системе: 100 Мбайт.

2) Пропускная способность канала связи: 100 Мбит/с. Исходя из этого, задержка на передачу пакета по каналу связи равна 8 секундам.

3) Количество рабочих станций – 4. Станции генерируют пакеты для отправки по каналу связи обрабатывающему серверу (табл. 1). Количество обрабатывающих каналов сервера – 3. Пакеты, поступают в один из свободных каналов на обработку.

Таблица 1

Средние интервалы времени генерации пакетов рабочими станциями

Рабочая станция	Интервал времени, сек.
PC1	23 ± 3
PC2	30 ± 2
PC3	25 ± 4
PC4	40 ± 6

4) Ёмкости накопителя пакетов, поступивших на обработку, – 5. Если все обрабатывающие каналы заняты, то пакеты встают в очередь на обработку. Если очередь заполнена, то пришедший пакет получает отказ в обслуживании.

5) Время обработки пакета в ЦП сервера – 110 секунд. После обработки пакет выходит из системы.

Определены изменения параметров СМО при моделировании воздействия ВП на характеристики КС:

1) Количество генерируемых пакетов увеличивается на 69% (табл. 2) [3].

Таблица 2

Средние интервалы времени генерации пакетов рабочими станциями с повышенной частотой генерации

Рабочая станция	Интервал времени, сек.
PC1	7,13 ± 1
PC2	9,3 ± 0,6
PC3	7,75 ± 1,25
PC4	12,4 ± 1,85

2) Задержка на обработку пакетов сервером увеличивается на 75%. Время обработки пакета в ЦП сервера с учётом данного влияния равна 192,5 секунды.

3) Возможность доступа пакетов к серверу уменьшается на 18%. Ёмкость накопителя пакетов с учётом данного влияния – 4.

При моделировании воздействия АП на характеристики КС рассматривались три продукта: Антивирус Касперского 7.0; Dr.Web 4.44; Avast! 4 Home Edition.

Определены изменения параметров моделируемой системы под воздействием АП (табл. 3) [4]:

1) Ухудшается пропускная способность канала. Задержка на передачу пакета по каналу связи увеличивается.

2) Уменьшается производительность системы. Задержка на обработку пакетов сервером увеличивается.

Таблица 3

Изменение параметров моделируемой системы под воздействием АП

	Задержка на обработку пактов, сек	Ухудшение пропускной способности канала связи, %	Задержка на передачу пакетов, сек.
Антивирус Касперского 7.0	152,75	12,6	9
Dr.Web 4.44	140,5	5,15	8,4
Avast! 4 Home Edition	170	4,4	8,35

Моделирование системы: на рис. 2 представлена графическая схема имитационной модели, которая отображает логику взаимодействия блоков имитационной модели.

Прогон модели с разными входными данными в среде GPSS World позволяет получить статистические результаты, которые выводятся в виде стандартных отчётов и могут быть представлены графически в виде графиков и гистограмм.

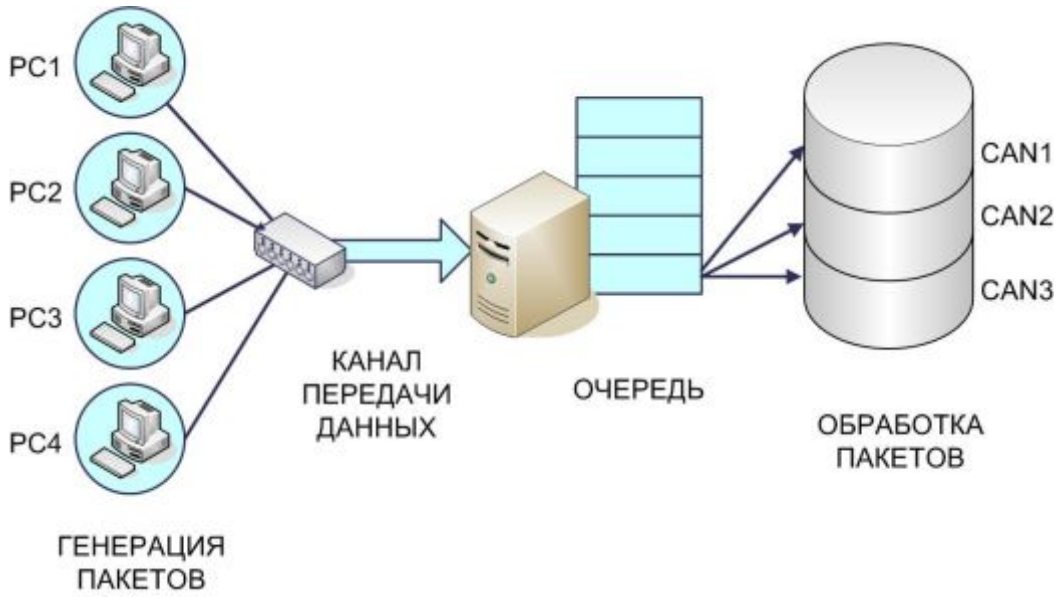

Рис. 2. Схема функционирования имитационной модели

Для решения поставленной задачи были выполнено следующие:

1) Моделирование системы в условиях отсутствия вредоносных и антивирусных программ.

2) Моделирование системы при воздействии вредоносных программ.

3) Моделирование системы при воздействии антивирусных программ.

Средние значения характеристик КС по проведенным экспериментам представлены в табл. 4.

Таблица 4

Средние значения характеристик КС

Эксперимент	Среднее количество пакетов в очереди	Средняя продолжительность пребывания пакета в КС, ед.вр.	Общее число пакетов, ожидавших момента обслуживания
Без влияния	105,8	1716,617	257,664
Влияние ВП	746,975	3571,554	1549,5
Влияние АП	165,674	2001,583	383,710

Выводы

Наиболее негативно на параметры производительности сети оказывают вредоносные программы (увеличивают частоту генерации пакетов, что перегружает очередь). Однако и действие антивирусных средств также значительно ухудшает основные характеристики сети (АП увеличивают задержку пакетов в системе, что замедляет обработку потока пакетов по времени).

Исследование доказывает, что при развертывании систем защиты на предприятиях необходимо учитывать, что системы призваны обеспечить не только максимальную защищенность информационных ресурсов, но и не ухудшить производительность корпоративных сетей.

Литература

1. Viruslist.com. Классические вирусы [Электронный ресурс]. Режим доступа: http://www.viruslist.com/ru/viruses/encyclopedia?chapter=156769 328.
2. **Груздева Л. М.** Исследование влияния вредоносных и антивирусных программ на характеристики замкнутой компьютерной сети предприятия / Комплексная защита объектов информатизации. Труды НТС / Комитет по информатизации, связи и телекоммуникациям Администрации Владимирской области. 2008. // http://ksi.avo.ru/seminar/11.pdf
3. **Биячуев Т. А.** Безопасность корпоративных сетей. Учебное пособие. М.: СПб.: СПбГУ ИТМО. 2004. 161 с.
4. Computerra.ru. Влияние антивирусов на производительность компьютера [Электронный учебник]. Режим доступа: http://www.computerra.ru/gid/342272/