



Федеральное государственное бюджетное образовательное учреждение
высшего образования
Московский автомобильно-дорожный государственный технический университет
(МАДИ)
ФГБОУ ВО МАДИ
Кафедра «Автоматизированные системы управления»

«Исследование эффективности систем антивирусной защиты»

Выполнил: Студент группы 2МБД1

Сороковиков Егор Алексеевич

Руководитель: К.Т.Н. Доцент

Остроух А.В.

Цели и задачи работы

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

Для решения поставленной цели в дипломной работе решаются следующие задачи:

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

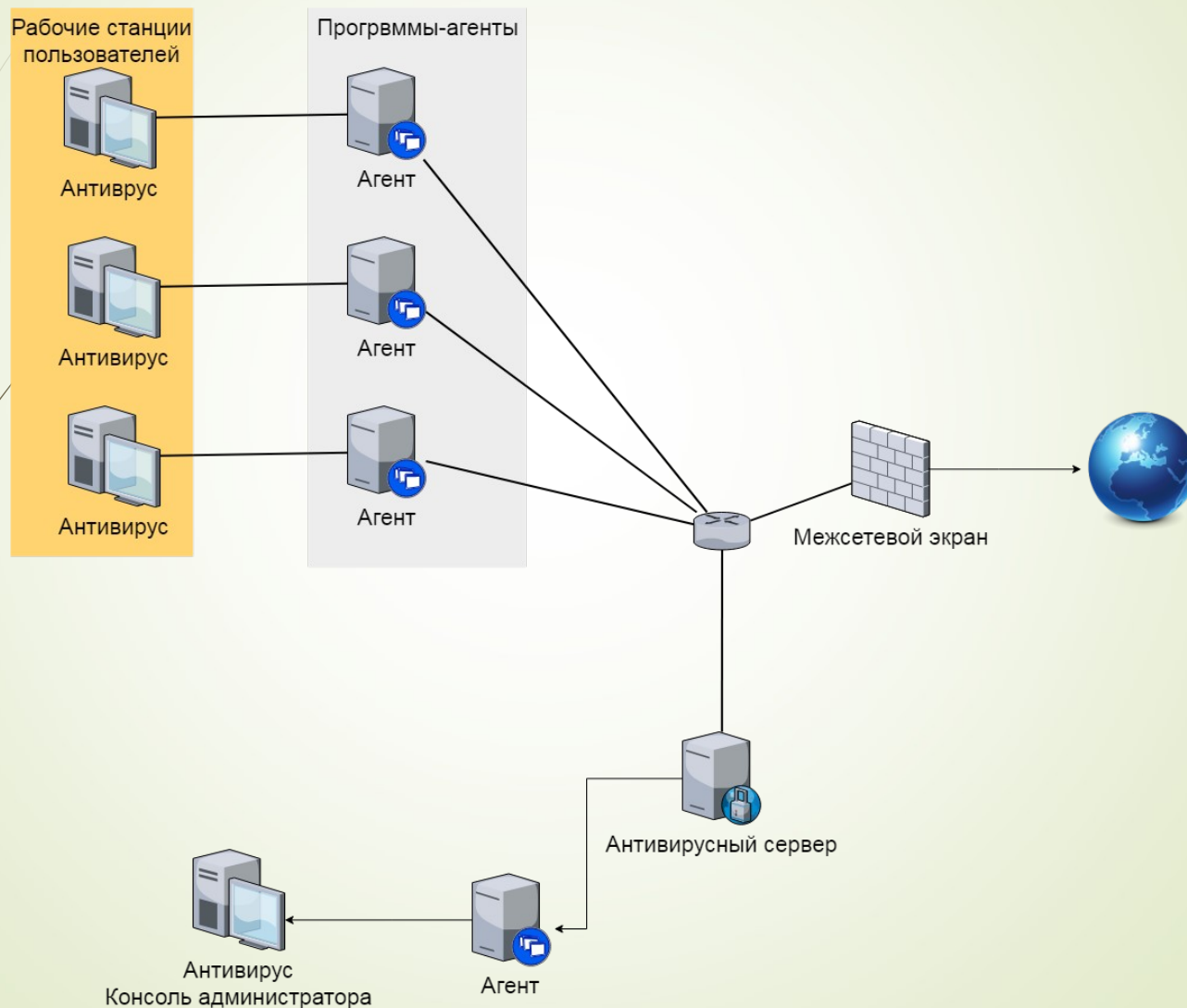
Виды вирусов



Основные требования

- ▶ Обновлять антивирусные базы, по расписанию или по требованию администратора;
- ▶ Настраивать и устанавливать антивирусы централизованно;
- ▶ Автоматическая установка антивирусных программ на новые рабочие станции в сети компании;
- ▶ Сбор статистики о результатах проверки, количестве заблокированных файлах, потенциально опасных и т.д.
- ▶ Отображения процесса работы антивируса на рабочих станциях и на серверах в реальном времени.

Устройство защиты в компании



Сравнительная таблица

Антивирусные программные продукты / Наименование показателя	Kaspersky Antivirus	Trend Micro ServerPr otect	Panda Security	Nod 32
Алгоритм нахождения вируса	Эмуляц. Эврист.	Эврист.	Эврист	Эмуляц. Эврист
Анализ поведения программ	Есть	Есть	Есть	Есть
Проверка макросов	Есть	Нет	Нет	Есть
Firewall	Есть	Нет	Нет	Есть
Структура программной системы	модульная	монолитная	монолитная	модульная
Число поддерживаемых семейств ОС	17	10	11	20
Объем дистрибутива	70МБ	81 МБ	85МБ	46 МБ

Нормализация данных

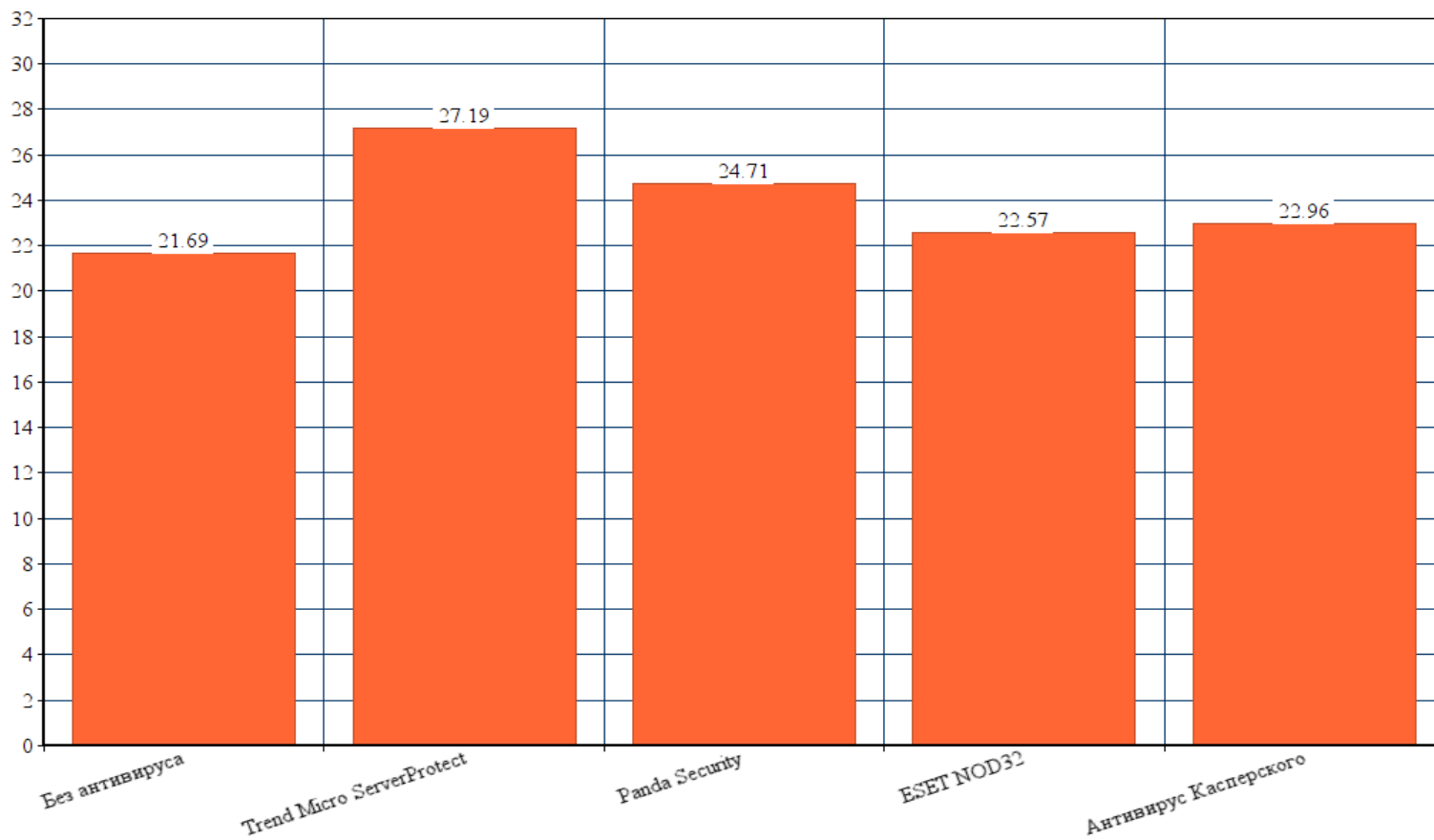
Антивирусные программные продукты / Наименование показателя	Kaspersky Antivirus	Trend Micro ServerP rotect	Panda Security	Nod 32
Алгоритм нахождения вируса	1	0,5	0,5	1
Анализ поведения программ	1	1	1	1
Проверка макросов	1	1	0	1
Firewall	1	0	0	1
Структура программной системы	1	0,5	0,5	1
Число поддерживаемых семейств ОС	0,7	0,33	0,33	1
Объем дистрибутива	0,27	0,16	0,18	0,6

Расчет критерия для выбора антивируса

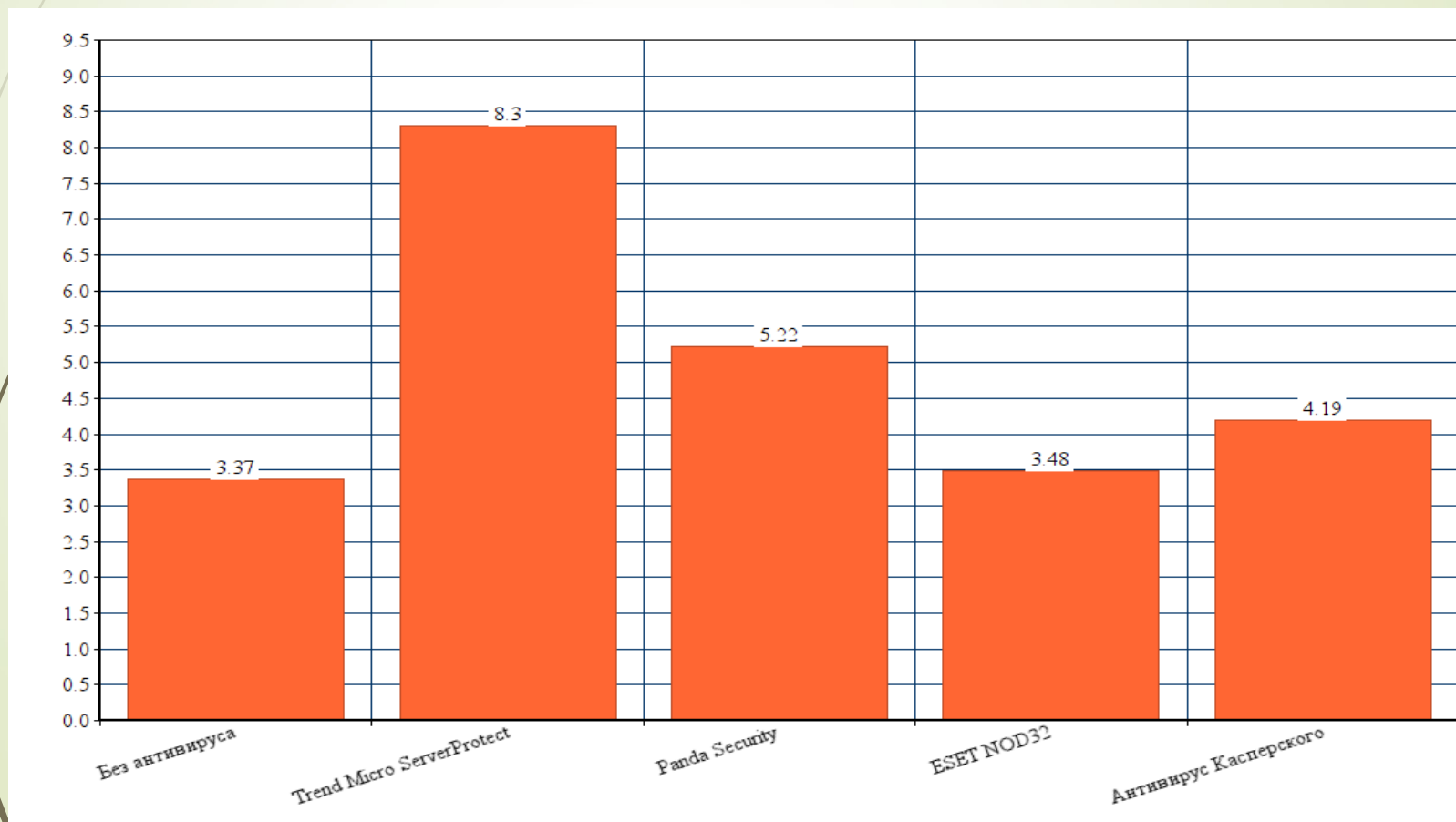
$$J = \sum_{i=1}^7 a_i p_i$$

Антивирусные программные продукты / Наименование показателя	Ai	Kaspersky Antivirus	Trend Micro Server Protec t	Panda Security	Nod 32
Алгоритм нахождения вируса	0,25	0,5	0,5	1	1
Анализ поведения программ	0,2	1	1	1	1
Проверка макросов	0,17	1	1	0	0
Firewall	0,13	1	1	1	1
Структура программной системы	0,08	1	0,5	0,5	1
Число поддерживаемых семейств ОС	0,12	0,7	0,33	0,33	1
Объем дистрибутива (Мб)	0,05	0,27	0,16	0,18	0,6
Критерий J	1	0,7581	0,7126	0,6686	0,81

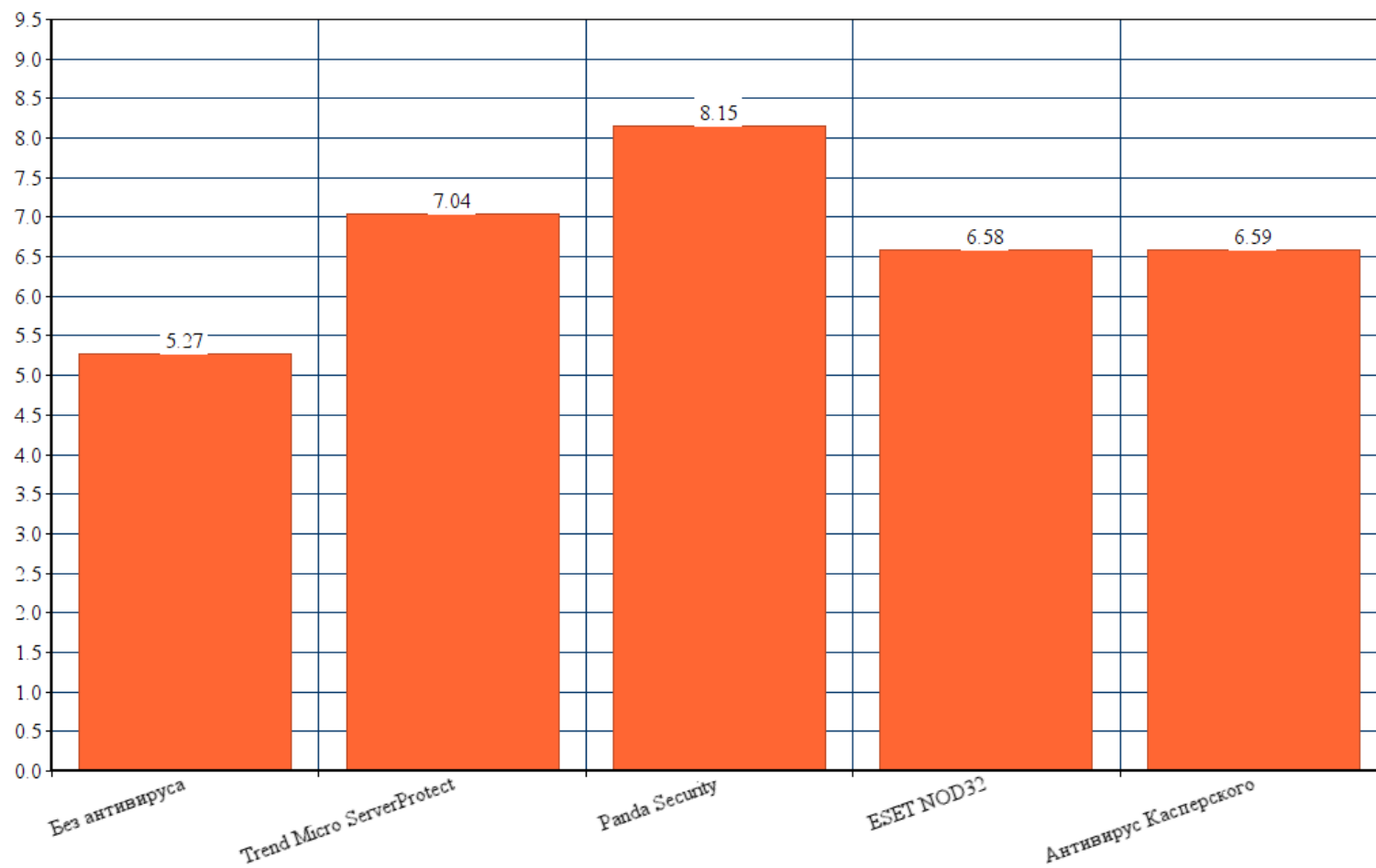
Влияние антивирусов на загрузку системы



Скорость работы антивирусных мониторов в реальном времени



Среднее время открытия файлов и приложений



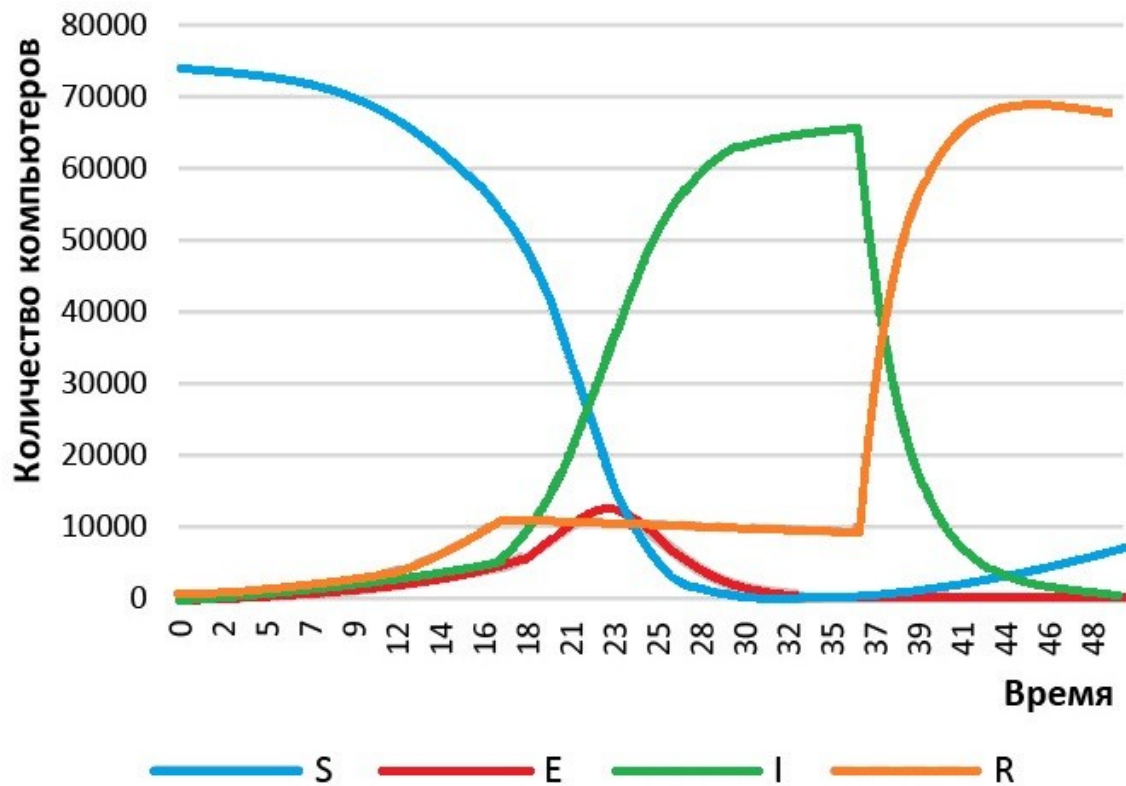
Типы компьютеров сети

Состояние компьютеров	Количество
Всего	75 000
Вновь вводимые в эксплуатацию	0
Подвержены вирусу	74 000
Латентные	300
Зараженные	100
С антивирусом	500

Параметры ПО

Параметр ПО	Значение
Коэффициент периода действия антивирусных баз	0,01
Коэффициент распространения вируса	0,06
Коэффициент отключения компьютеров	0,00001
Коэффициент подключения новых компьютеров	0,00001
Коэффициент обновления антивирусных баз (начальное значение)	0,01
Коэффициент обновления антивирусных баз (максимальное значение)	0,4

Траектория динамики функций, компьютеров разных типов



- S - число уязвимых компьютеров
- E- число зараженных компьютеров (до того как компьютер повредил зараженный узел)
- I - количество инфицированных узлов
- R - число компьютеров не подверженных заражению



Благодарю за внимание.