

**ЧЕРНОМОРСКОЕ ВЫСШЕЕ ВОЕННО-МОРСКОЕ УЧИЛИЩЕ
имени П.С. Нахимова**

Кафедра электроники и информационной безопасности

**ДИПЛОМНАЯ РАБОТА
на тему:**

**«Разработка алгоритма защиты операционной системы
Windows от троянских программ»**

Выполнил:

фио

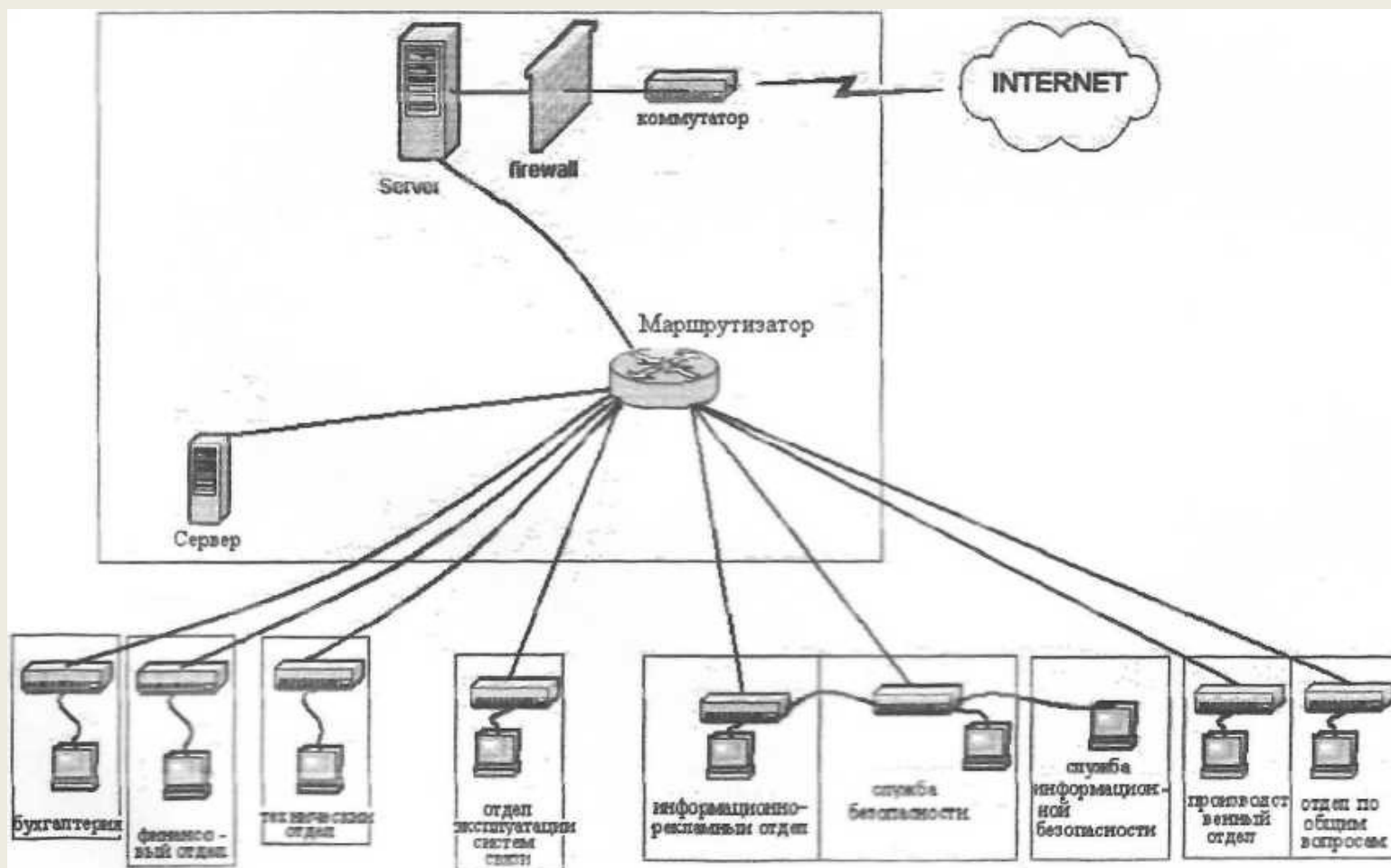
Научный руководитель:

фио

Организационная структура предприятия

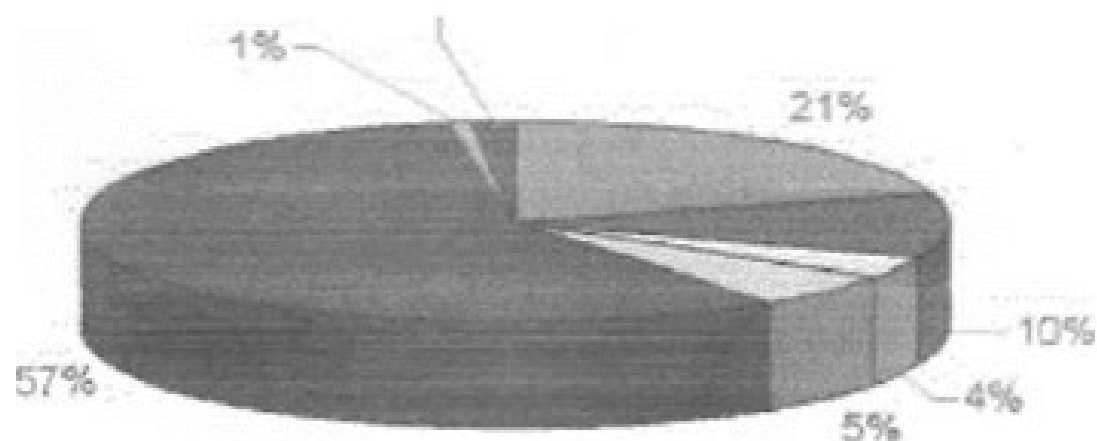


Сеть предприятия



Основные каналы НСД, через которые нарушитель может получить доступ к компонентам АС и осуществить хищение, модификацию или разрушение информации:

- штатные каналы доступа к информации (терминалы пользователей, оператора, администратора системы; средства отображения и документирования информации; каналы связи);
- технологические пульта управления;
- линии связи между аппаратными средствами АС;
- побочные электромагнитные излучения от аппаратуры, линий связи, сетей электропитания и заземления и др.



■ AdWare	■ Dialer	■ Trojan	■ Прочие
■ Backdoor	■ Worm	■ Virus	

Классы мероприятий по защите

1. Организационные мероприятия;
2. Технические мероприятия;
3. Программный комплекс мероприятий.

Статистика тестирования антивирусов в 2011 году

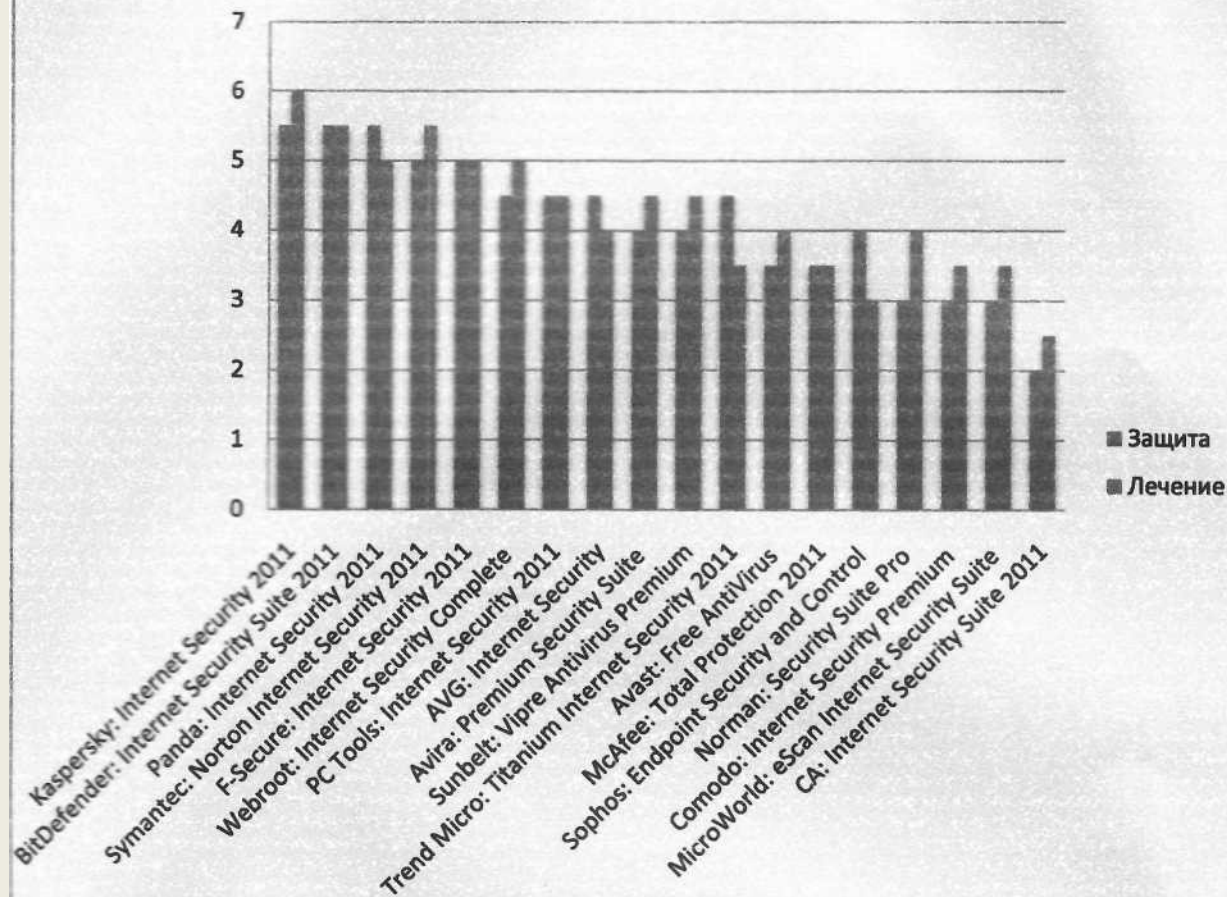
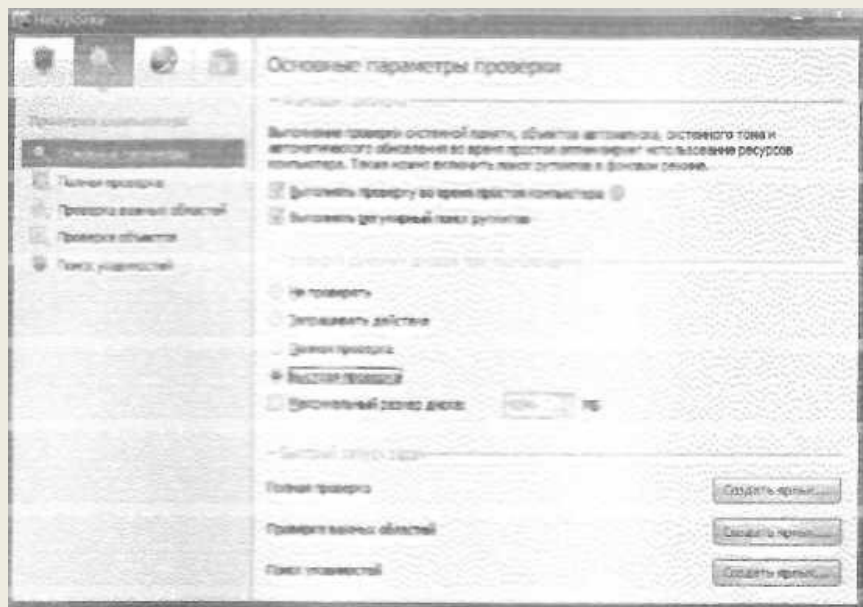
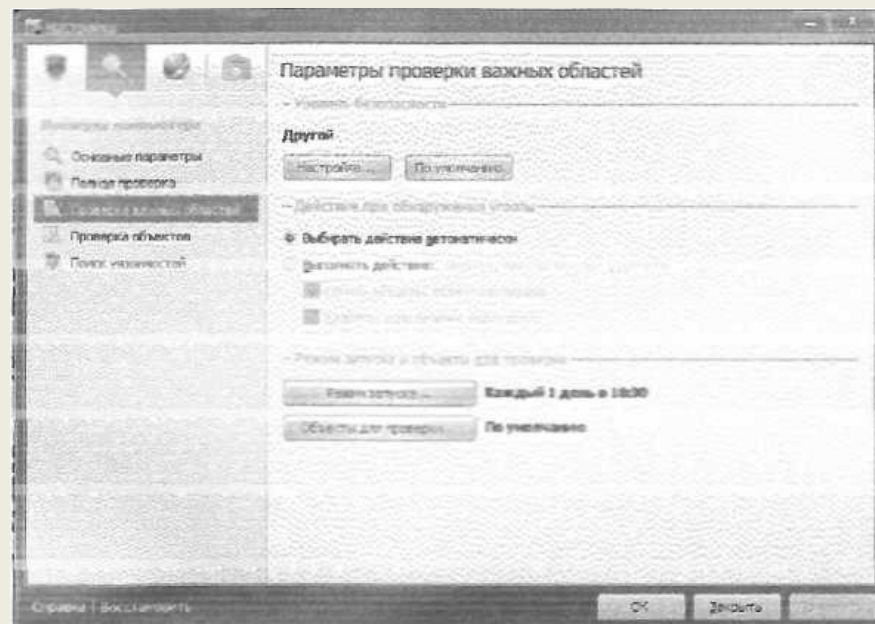


Рис.4

Параметры проверки антивируса

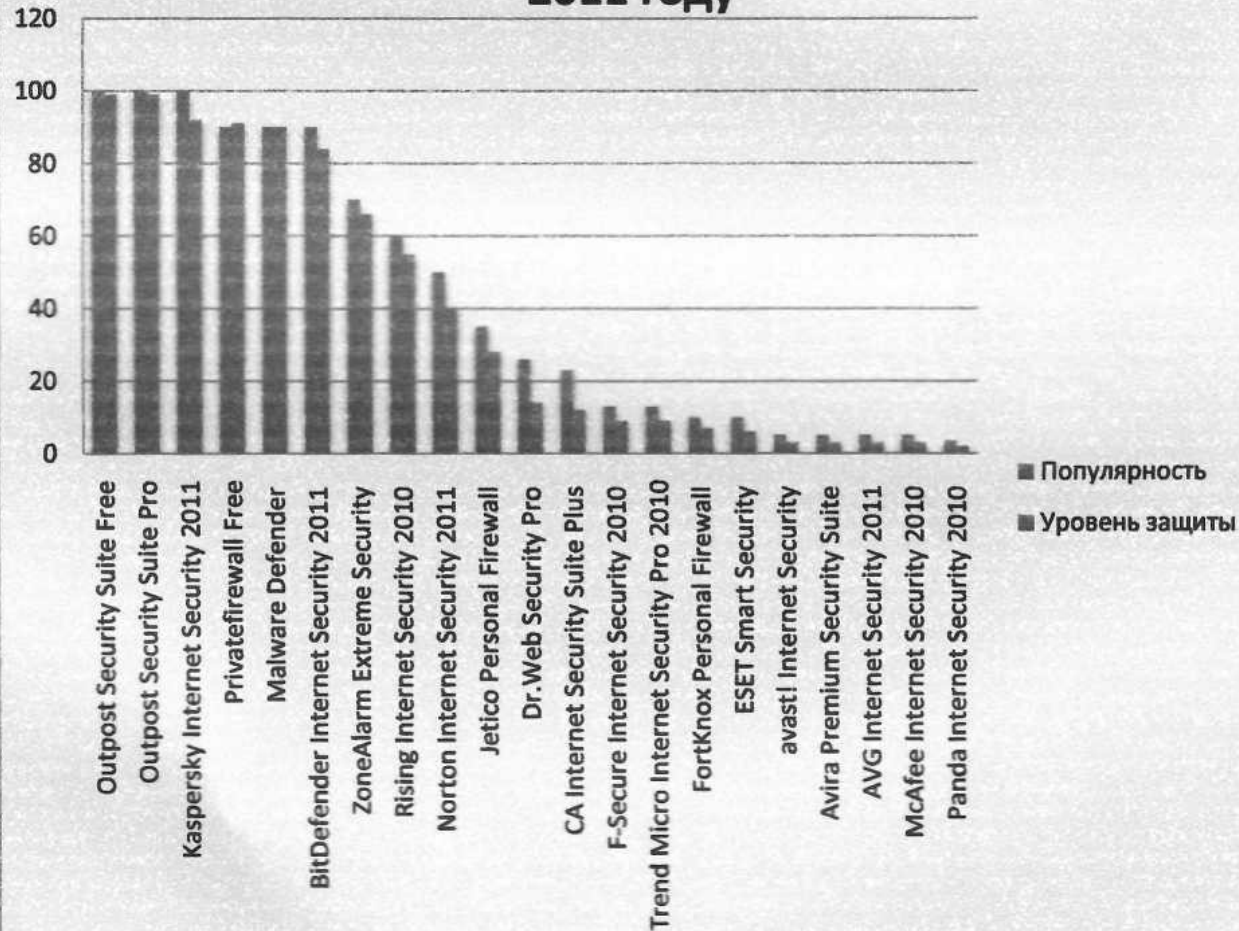


Основные параметры проверки

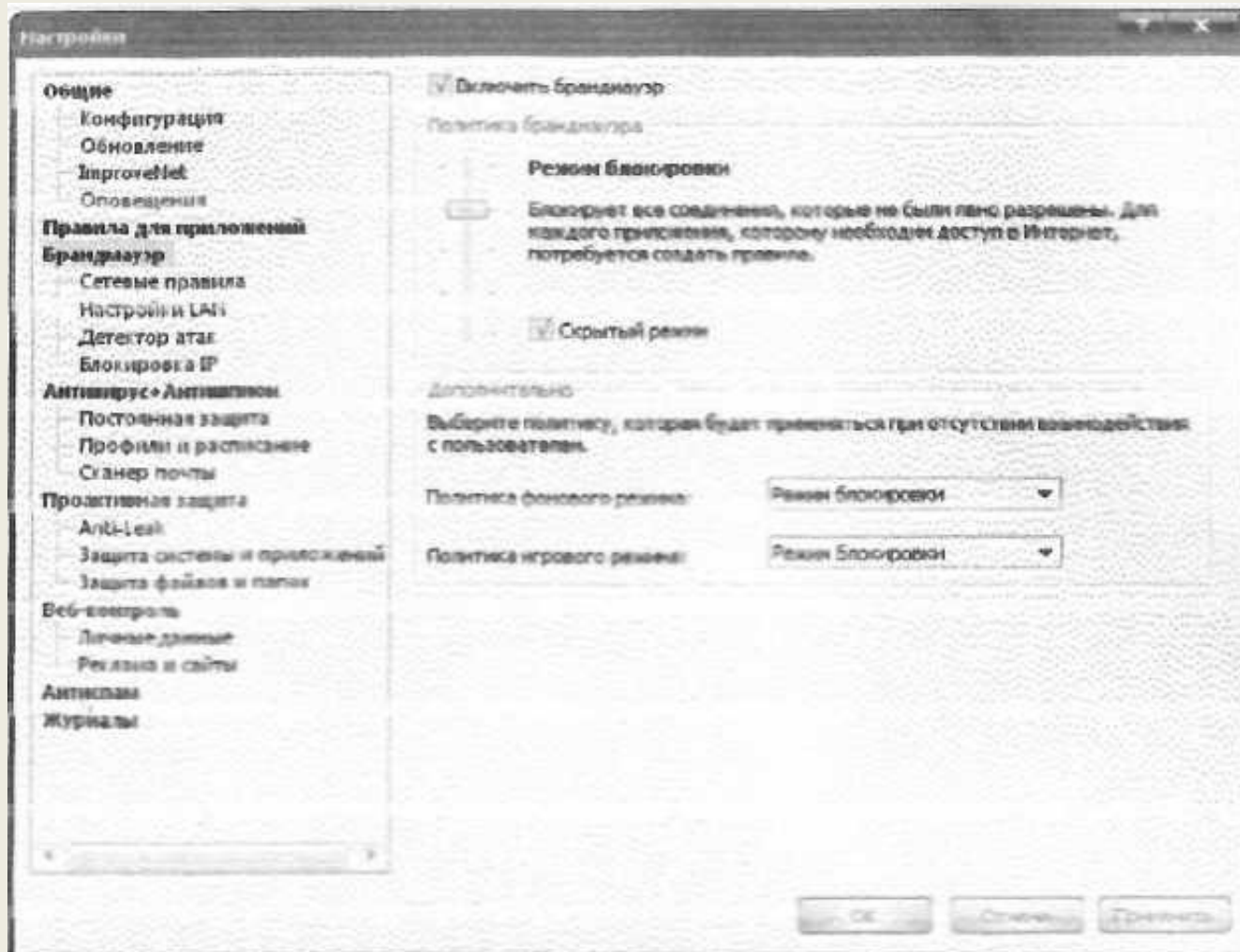


Проверка важных областей

Статистика тестирования брандмауэров в 2011 году



Детальная настройка брандмауэра



Для того, чтобы обеспечить функционирование троянской программы, ее создатели помещают в раздел «Автозагрузка» и в реестр Windows:

1)Раздел «Автозагрузка».

2)Раздел реестра Windows.

Для того, чтобы просмотреть реестр Windows необходимо воспользоваться меню: Пуск->Панель управления -> Редактор реестра.

«Разработка алгоритма защиты операционной системы Windows от троянских программ»

СПАСИБО ЗА ВНИМАНИЕ!