«МОСКОВСКИЙ АВТОМОБИЛЬНО-ДОРОЖНЫЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ(МАДИ)»

Направление подготовки	**09.04.01 (230100) – «Информатика и вычислительная техника**
Кафедра	**«Автоматизированные системы управления»**
Магистерская программа	**«Базы и банки данных»**

Допустить к защите
Зав. кафедрой «АСУ»

_____Максимычев О.И.
«___» Июня 2018г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ МАГИСТРА

Исследование эффективности систем антивирусной защиты

Выполнил: _____ (Сороковиков Е.А.)

Руководитель: _____ (Остроух А.В.)

Москва – 2018г.

ФГБОУ ВО «МОСКОВСКИЙ АВТОМОБИЛЬНО-ДОРОЖНЫЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ(МАДИ)»

Направление подготовки **09.04.01 (230100) – «Информатика и вычислительная техника**

Кафедра **«Автоматизированные системы управления»**
Магистерская программа **«Базы и банки данных»**

Утверждаю
Зав. кафедрой «АСУ»

_____Максимычев О.И.
«____»_____201___г.

ЗАДАНИЕ
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ МАГИСТРА

Исследование эффективности систем антивирусной защиты

Перечень подлежащих разработке вопросов:

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;

Срок представления ВКР «18» июня 2018

Руководитель: _____ (Сороковиков Е.А.)

Исполнитель: _____ (Остроух А.В.)

Введение.....4
1. ОБЗОР ЗАДАЧ И РАБОТ ПО ТЕМЕ ИССЛЕДОВАНИЯ (BACKGROUNDS).....6
1.1. Вирусы.....6
1.1.1. Макровирусы.....9
1.1.2. Полиморфные вирусы.....9
1.1.3. Программные вирусы.....9
1.1.4. Загрузочные вирусы.....11
1.1.5. Файловые вирусы.....11
1.1.6. Комбинированные вирусы.....12
1.1.7. Стелс вирусы.....12
1.1.8. «Троянские» программы.....12
1.2. Методы распространения вирусов на ПК.....12
1.3. Антивирусные программы.....14
1.3.1. Методы работы антивирусов.....17
1.3.2. Firewall.....20
1.4. Антивирусы для Android.....25
1.4.1. Сравнение имен пакетов.....26
1.4.2. База Данных Пакетов.....29
1.4.3. Доступ к файлам пакетов.....29
1.4.4. Методы Вредоносных Программ Для Android.....30
1.4.5. Вывод Android.....31
2. ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННЫХ МОДЕЛЕЙ И РАЗРАБОТКА АЛГОРИТМОВ (MODELS AND METHODS).....33
2.1. Логическое проектирование.....33
2.2. Управление антивирусными продуктами в корпоративной сети.....38
3. ТЕХНОЛОГИЯ ПРОГРАММНОЙ РЕАЛИЗАЦИИ РАЗРАБОТАННЫХ МОДЕЛЕЙ И АЛГОРИТМОВ (RESULTS).....41
3.1. Классификация антивирусных программ.....41
3.2. Антивирус Касперского.....42
3.3. Trend Micro ServerProtect for Microsoft Windows/Novell NetWare.....43
3.4. Panda Security for File Servers.....44
3.5. ESET NOD32 Smart Security Business Edition.....45
3.6. Программно-аппаратный МЭ.....50
3.7. Выбор программно-аппаратного МЭ.....53
3.7.1. Cisco ASA 5520.....53
3.7.2. D-Link - DFL-2500 [DFL-2500].....54
3.7.3. D-Link - DFL-260 [DFL-260].....55
3.7.4. D-Link - DFL-210 [DFL-210].....58
3.8. РАСЧЁТ ЗАТРАТ НА РАЗРАБОТКУ И ВНЕДРЕНИЕ ИС.....62

3.8.1. Расчет затрат на разработку ИС.....62
3.8.2. Затраты на заработную плату разработчиков.....62
3.8.3. Расчёт затрат на внедрение ИС.....67
3.8.4. Затраты на подготовку персонала.....67
3.8.5. Дополнительные затраты на заработную плату персонала, обслуживающего ИС. 68
3.8.6. Отчисления в Государственные внебюджетные фонды от затрат на заработную плату персонала.....69
3.8.7. Дополнительные затраты на электроэнергию, связанные с выполнением функций ИС.....69
3.8.8. Амортизационные отчисления.....70
3.8.9. Расчет экономии на расходах потребителя.....70
3.9. Расчет экономической эффективности проекта.....71
3.8.10. Финансовый план (расчет эффективности инвестиций в разработку и внедрение системы) расчет ЧДД проекта.....71
4. ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ПОЛУЧЕННЫХ РЕШЕНИЙ (DISCUSSIONS) 74
4.1. Влияние антивирусов на загрузку операционной системы.....74
4.2. Скорость работы антивирусных мониторов в реальном времени.....75
4.3. Среднее время открытия файлов и приложений.....76
4.4. Математическое исследование эффективности предложенных решений.....78
ЗАКЛЮЧЕНИЕ (CONCLUSIONS).....84
СПИСОК ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ (REFERENCES).....85

Введение

В настоящее время для обработки информации, общения и обмена данными повсеместно используются компьютерные сети. Однако благодаря Интернету и большой пропускной способности систем связи распространение вирусов превращается в сетевые эпидемии. Поэтому остро встает вопрос о защите компьютерных сетей и информации, и в связи с развитием электроники появляются все новые и новые угрозы. По статистическим данным, опубликованным на сайте Лаборатории Касперского, 95 % отечественных организаций как минимум один раз подвергались внешней компьютерной атаке. Россия входит в двадцатку стран, подвергшихся наибольшему риску заражения через Интернет, и занимает одиннадцатое место в мире по уровню зараженности компьютеров. С каждым годом положение в IT-сфере ухудшается: появляется большое количество новых вирусов и, как следствие, растут материальные потери. Важной научной задачей в данной ситуации является построение действенной защиты компьютерной сети.

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

Для решения поставленной цели в дипломной работе решаются следующие задачи:

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;

Модели, методы и программные средства, применяемые для решения поставленных задач.

В своей работе для решения поставленных задач я проанализировал несколько программных сред и выбрал некоторые из них:

- В качестве основного антивирусного средства по результатам работы я выбрал Nod32 он, оказался одним из лучших антивирусов по результатам анализа;
- Для контроля над входящей и исходящей информацией межсетевой экран D-Link - DFL-2500;

Что дают предложенные решения

- Снижение угрозы вирусной атаки;
- Улучшение контроля над информацией в сети предприятия;
- Повышение защищенности сети;

На защиту выносятся:

- Проект антивирусной зашиты информационной системы Call-центра
- Исследования эффективности предложенных решений

1. ОБЗОР ЗАДАЧ И РАБОТ ПО ТЕМЕ ИССЛЕДОВАНИЯ (BACKGROUNDS)

1.1.Вирусы

Компьютерный вирус - Программное обеспечение способное внедриться в чужую программу лил в системный код со способностью само-клонирования, а также нанесения вреда информации, хранящейся на компьютере и аппаратной его части.

Главной задачей любого вредоносного ПО является нанесения вреда, хищение информации или наблюдение за компьютером. Возможность распространяться не только на локальной машине, но и по сети в том числе по сети компании позволяет нанести максимальный урон как обычному пользователю, так и материальный вред компании.

Классификация вирусов

Вирусные программы классифицируются по следующим признакам:

1. Особенности алгоритмов: макровирусы, стелс-вирусы, «Троянские» программы.
2. Месту распространения: загрузочные вирусы, файловые вирусы, комбинированные вирусы, сетевые вирусы;
3. Степени влияния на компьютер пользователя: неопасные, опасные и очень опасные;
4. Методу заражения компьютера: нерезидентные и резидентные;
    a. Резидентные - Вирусные программы способные прописываться в системную (оперативную) память и оставлять свои копии внутри ее. Они умеют перехватывать некоторые события, такие как обращение к файлу или диску. Главной их особенностью является возможность инфицирования даже, когда программа распространитель вируса не выполняется. От таких вирусов очень трудно избавиться. Удаления всех копий зараженных файлов и программ и перезагрузка системы не дает гарантии полного лечения компьютера.

b. Нерезидентные - вирусы не способные оставлять свои копии в системной (оперативной) памяти компьютера или использующие данную возможность, но без дальнейшего распространения из нее. Ниже приведен алгоритм работы большинства нерезидентных вирусов.

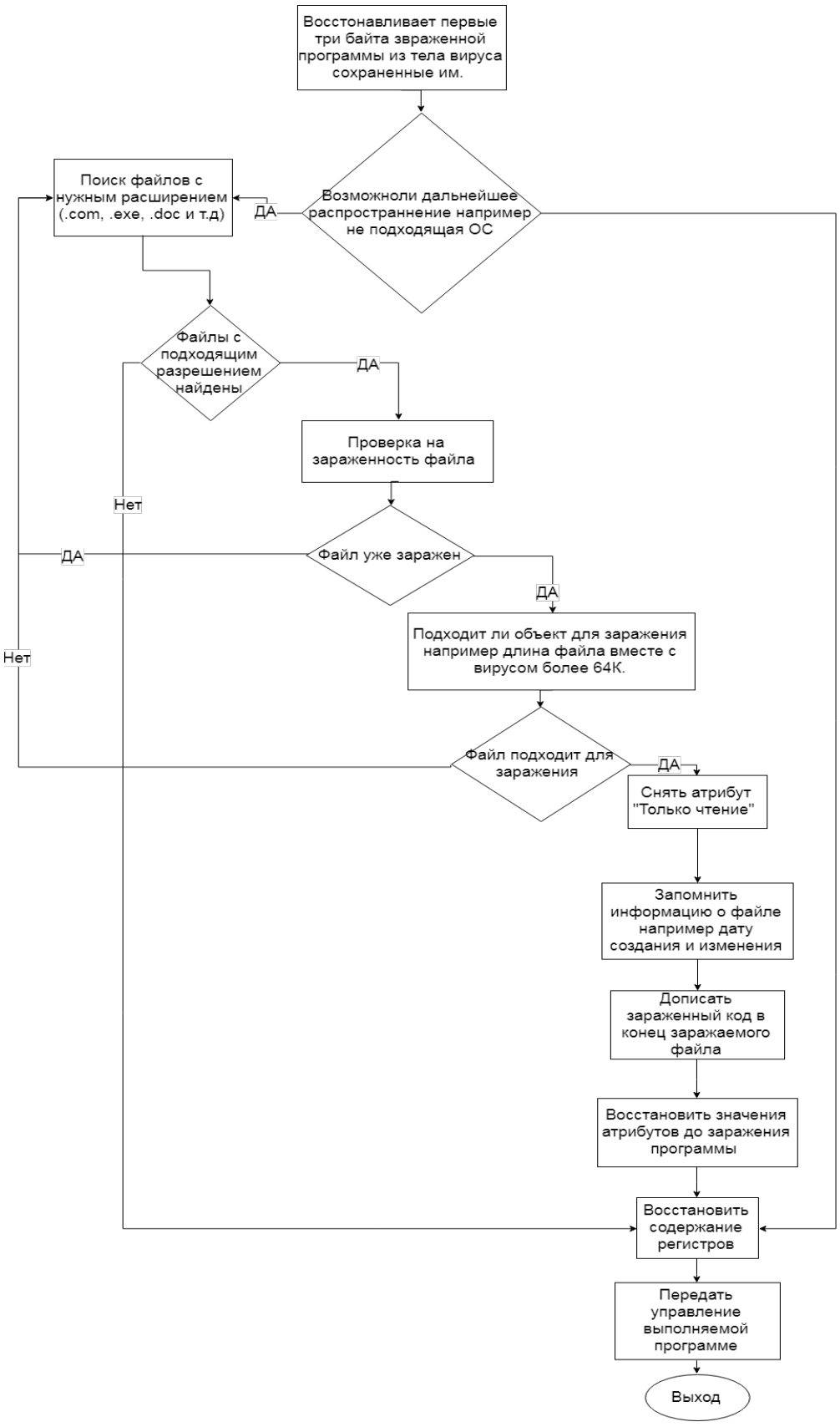

Рисунок 2.1 Алгоритм работы Нерезидентных вирусов.

Здесь описаны наиболее распространенные типы вирусов:

1. Макровирусы;

2. Полиморфные вирусы;
3. Программные вирусы;
4. Загрузочные вирусы;
5. Файловые вирусы;
6. Комбинированные вирусы;
7. «Троянские» программы;
8. Стелс – вирусы.

1.1.1. Макровирусы

Они поражают прикладные программы пользователя, которые имеют возможность исполнения макрокоманд. К таким программа относятся Microsoft Office, Open Office. Заражение происходит при попытке открыть программу с включенной возможностью выполнения макрокоманд.

1.1.2. Полиморфные вирусы

Эта особая разновидность вирусов, которая модифицирует(шифрует) свой код в зараженных программах. Вирусы этого типа помимо шифровки своего кода, также имеют кож генерации шифровщика и расшифровщика, такое свойство вируса говорит о том, что 2 экземпляра одного и того же вируса могут не совпадать ни в одном бите.

Полиморфный тип вирусов с учетом наличия самомодифицирующегося расшифровщика не позволяет проанализировать его ког с помощью дизассемблирования, даже имея зараженный и оригинальный файл. Код его зашифрован и будет представлять собой бессмысленный набор команд. Расшифровка происходит в процессе выполнения либо сразу весь свой код, либо по мере выполнения и шифровать уже отработавшие участки.

1.1.3. Программные вирусы

Программные вирусы - это программный код, специально внедренный в код других программ. При запуске программы, несущей вирус, происходит запуск имплантированного в нее вирусного кода. Работа этого кода вызывает

скрытые от пользователя изменения в файловой системе жестких дисков и/или в содержании других программ. Так, например, вирусный код может воспроизводить себя в теле других программ - этот процесс называется размножением. По прошествии определенного времени, создав достаточное количество копий, программный вирус может перейти к разрушительным действиям - нарушению работы программ и операционной системы, удалению информации, хранящейся на жестком диске. Этот процесс называется вирусной атакой. Самые разрушительные вирусы могут инициировать форматирование жестких дисков. Поскольку форматирование диска - достаточно продолжительный процесс, который не должен пройти незамеченным со стороны пользователя, во многих случаях программные вирусы ограничиваются уничтожением данных только в системных секторах жесткого диска, что эквивалентно потере таблиц файловой структуры. В этом случае данные на жестком диске остаются нетронутыми, но воспользоваться ими без применения специальных средств нельзя, поскольку неизвестно, какие сектора диска каким файлам принадлежит. Теоретически восстановить данные в этом случае можно, но трудоемкость этих работ исключительно высока.

Считается, что никакой вирус не в состоянии вывести из строя аппаратное обеспечение компьютера. Однако бывают случаи, когда аппаратное и программное обеспечение настолько взаимосвязаны, что программные повреждения приходится устранять заменой аппаратных средств. Так, например, в большинстве современных материнских плат базовая система ввода-вывода (BIOS) хранится в перезаписываемых постоянных запоминающих устройствах (так называемая флэш-память). Возможность перезаписи информации в микросхеме флэш-памяти используют некоторые программные вирусы для уничтожения данных BIOS. В этом случае для восстановления работоспособности компьютера требуется либо замена микросхемы, хранящей BIOS, либо ее перепрограммирование на специальных устройствах, называемых программаторами.

Программные вирусы поступают на компьютер при запуске непроверенных программ, полученных на внешнем носителе (гибкий диск, компакт-диск и т. п.) или принятых из Интернета, і Особое внимание следует обратить на слова при запуске. При обычном копировании зараженных файлов заражение компьютера произойти не может. В связи с этим все данные, принятые из Интернета, должны проходить обязательную проверку на безопасность, а если получены незатребованные данные из незнакомого источника, их следует уничтожать, не рассматривая. Обычный прием распространения "троянских" программ - приложение к электронному письму с "рекомендацией" извлечь и запустить якобы полезную программу.

1.1.4. Загрузочные вирусы

Загрузочные вирусы заражают запоминающие устройства (USB-флеш-накопитель или магнитные носители). При попытке загрузки информации с носителя вирус загружается в оперативную память компьютера. После этого они располагаются в загрузочном секторе и компьютер сам становится источником заражения.

1.1.5. Файловые вирусы

При запуске исполняемого файла данный тип вируса получает управление над выполняемой программой и можжет передать управление другому. Заражая исполняемый файл вирус меняет его код, так, что данный тип вирусов легко отследить. Такие вирусы работают следующим образом:
Информация о файлах хранится в каталогах. Каждая запись из каталога включает в себя данные файл например дату и время создания, имя файла, номер первого кластера файла и т.д.. Самой главной для вируса является резервные байты. Они оставлены “про запас” и операционной системой никак не используются. При запуске операционная система считывает первый кластер и так до конца все остальные кластеры. Вирус в свою очередь записывается как кластер в резервные байты как кластер и операционная система сама запускает вирус и передает ему управление.

1.1.6. Комбинированные вирусы

Комбинированные вирусы объединяют в себе возможности файловых и загрузочных вирусов. Они поражают главный загрузочный сектор (MBR) и исполняемые файлы. Главное отрицательное действие таких вирусов это то что они шифруют сектора винчестера при каждом запуске зараженного файла. после шифрования болле половины винчестера вирусы такого типа как правило сообщают об этом пользователю и требуют плаату для разшифровки. Главной проблемой лечения такого вируса в том, что недостаточно удалить вирус из MBR и файлов, надо распознать зашифрованную информацию. Наиболее «смертельное» действие - просто переписать новый здоровый MBR.

1.1.7. Стелс вирусы

Данный тип вирусов имеет свойства, скрывающие наличие вируса на зараженном компьютере. Их практически нельзя обнаружить. Одним из способов является удаление себя из зараженного файла, а затем после его закрытия возвращается назад. Самое действенное мероприятием по удалению такого вируса - полное форматирование диска.

1.1.8. «Троянские» программы

«Троянские» программы в отличие от остальных типов вирусов рассмотренных в данной главе то что ее вилияние может и не быть вредоносным. Она в отличии от остальных вирусов запускается самим пользователем, маскируясь под другие программы (не перезаписывая из код а лишь названием, иконкой и расширением). Не зря ее название происходит от знаменитого “Троянского коня”. Далее она уже подгружает другие программы без согласия пользователя.

1.2.Методы распространения вирусов на ПК

Главными путями распространения вирусов является съемные носители или через сеть.

В основном, вирусы маскируются в исполняемой программе. При запуске сначала управление получает зараженный код, исполняет все свои команды а затем передает управление обратно исполняемой команде. Как правило, после выполнения своих команд вирус может заражать и другие файлы.

заражение компьютера вирусными программами в основном происходит следующими способами:

1. При открытии программы, которая уже инфицирована;
2. При открытии или работе в программе, в которой включена возможность выполнения макрокоманд например Openoffice или Microsoft Office;
3. При установке ОС со съемных носителей, которые уже инфицированы вредоносным кодом;
4. через электронную почту. При просмотре зараженных вложений (документов или программ);
5. Через сеть интернет при открытии или просмотре документов, в которой включена возможность выполнения макрокоманд;

Чаще всего вирусы инфицируются файлы и программы имеющие следующие расширения:

- .doc - Текстовый файлы с разметкой или без (Openoffice, Microsoft Office);
- .exe - исполняемые файлы;
- .bat - файлы использующие команды операционной системы Windows;
- .ppt - Файлы презентаций Microsoft Power Point;
- .dll, .lib, .obj - Библиотеки кода или данных используемые программами;
- .xml, .xls - является языком разметки, который определяет набор правил для кодирования документов в формате, который является удобочитаемым и машиночитаемым;
- .vbs - файлы на языке Microsoft Visual Basic Script, являются

- .sys - файл настроек и системных переменных используется для запуска и установки. В основном используется для драйверов;
- .scr - тип файлов заставки для Windows;
- .dot, .docm - формат шаблонов для текстовых файлов с разметкой или без;

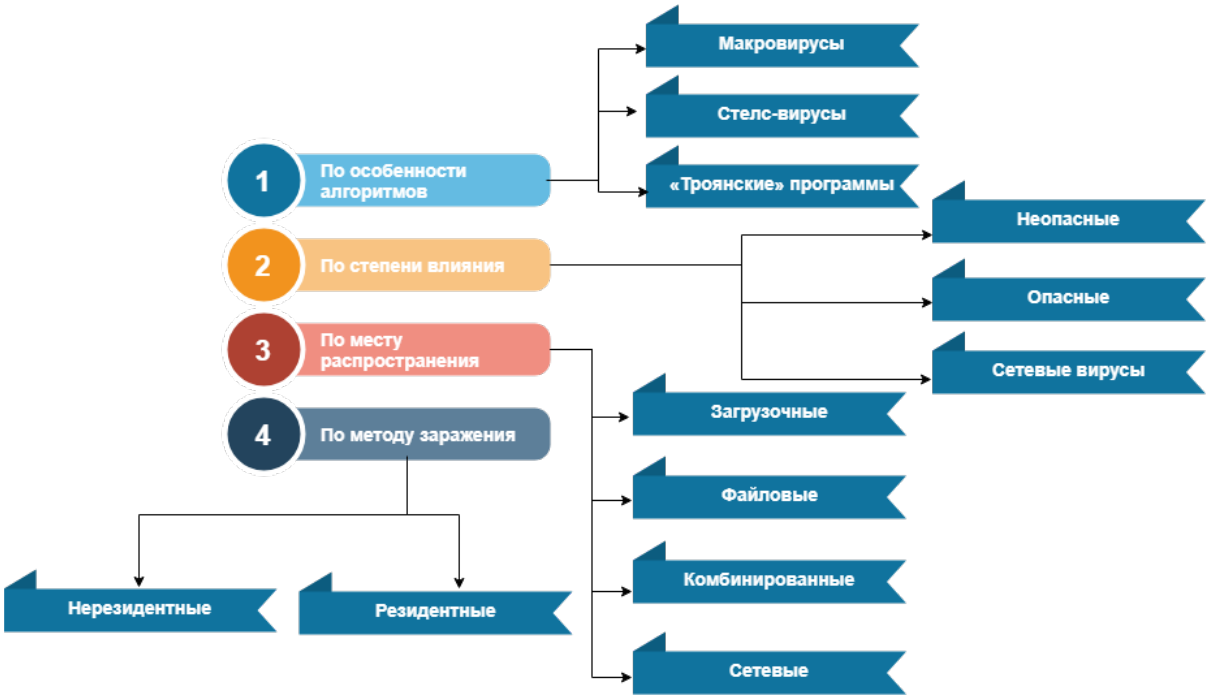

Рисунок 2.2 Виды вирусов

1.3. Антивирусные программы.

Основным способом борьбы с вирусами являются антивирусные программы. Они позволяют обнаруживать и предотвращать заражение вирусами компьютеров пользователей. Для начала хотелось бы дать описание Антивирусной программы.

Антивирус (антивирусная программа) – специализированная программа, созданная для поиска и последующего удаления вредоносного кода (вирусов), зараженных файлов спама (спам-рассылок). С возможностью предотвращения проникновения нежелательного ПО на компьютер, телефон и других электронных устройств, а также лечить зараженные файлы без их удаления.

Основным способом выявления вируса Антивирусным ПО является следующий алгоритм.

Проверка компьютера на предмет нахождения в нем сигнатур вирусов.
Возможны следующие варианты работы антивируса после проверки
Файл содержит похожий на вирус код, но он не найден в базе при таком варианте антивирус помещает файл в карантин, не давая ему выполнять процессы и при каждом обновлении базы данных проверяет его, до появлении информации об этой сигнатуре (Эвристический метод описанный далее).
Проверенный файл содержится в вирусных базах данных, в таком случае антивирус, также помещает его в карантин и предлагает пользователю выбор попытаться его вылечить или же удалить файл.
И третий вариант, самый благоприятный для пользователя, файл не заражен в таком случае можно спокойно работать с файлом

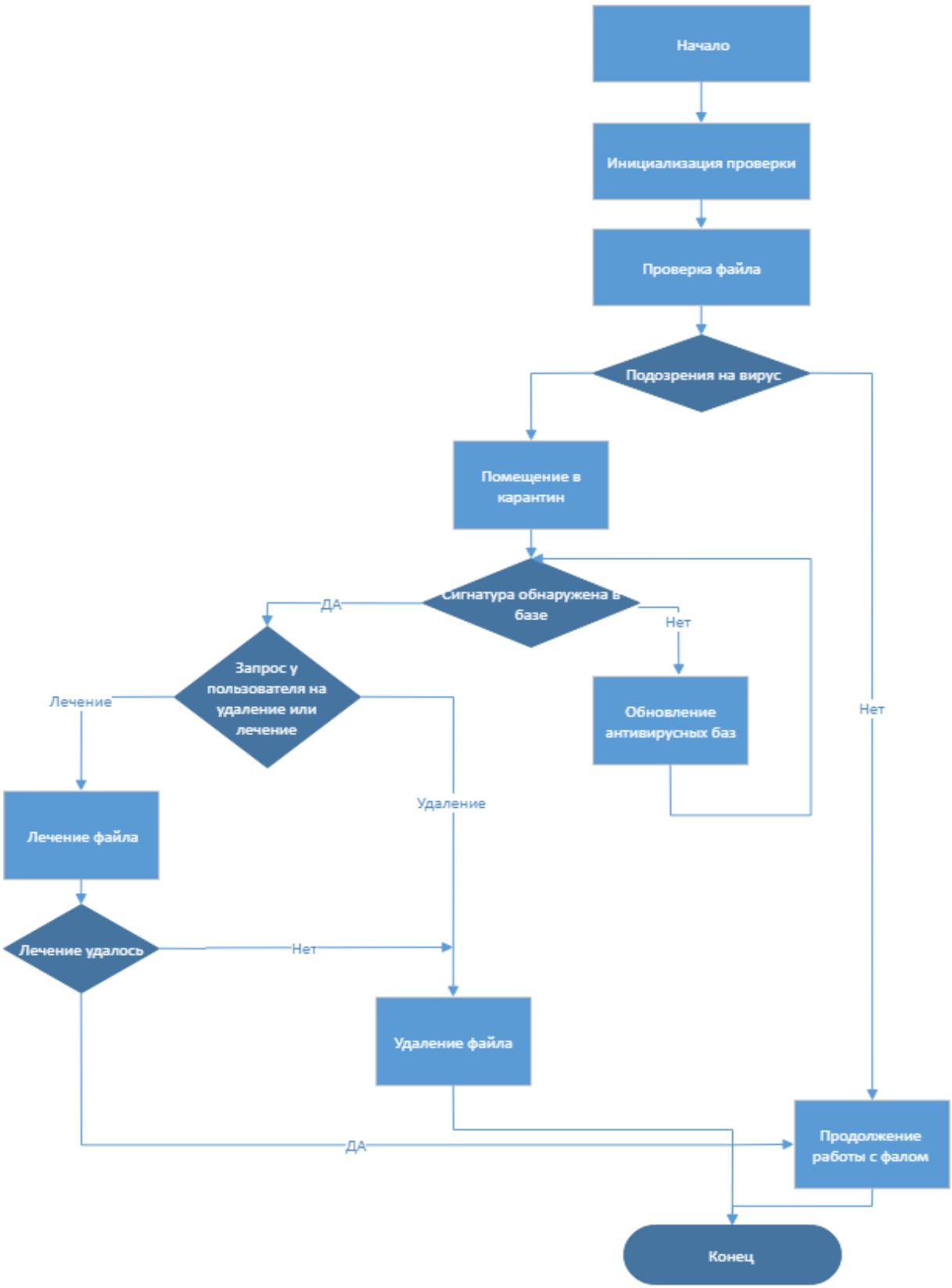

Рисунок 2.3 алгоритм проверки вирусов

1.3.1. Методы работы антивирусов.

У защитных программных продуктов в настоящий момент есть несколько способов защиты компьютера.

2.3.1.1. Сканирование (Проверка сигнатур)

Работа антивирусов сильно зависит от их антивирусных баз. В них находится информация о всех известных данному антивирусу вредоносных программах. И при прохождении первого этапа работы описанным в предыдущем разделе он проверяет файлы на предмет совпадения в базе данных. Соответственно компаниям разработчикам антивирусов необходим постоянный мониторинг на наличие новый сигнатур вирусов, для дальнейшего выявления алгоритмов работы вирусов, и последующей разработки метода борьбы с данной вредоносной программой, а также добавления их в антивирусную базу.

Метод поиска вирусов основанный на проверки их сигнатур с базой данных называется сигнатурным методом. Но у некоторых производителей 90 тыс. сигнатур, а у других 120 тыс. значит ли это что у первой компании антивирусное программное обеспечение лучше, чем у второй? А вот и нет! У разных производителей существуют свои алгоритмы сравнения сигнатур и у некоторых компаний одна сигнатура может обозначать целую кучу вирусов.

Однако у этого метода есть большой недостаток – его не динамичность. Разработчика антивирусов необходимо несколько дней для внесения обновлений в базу, а создать новый вирус нужно всего несколько часов.

2.3.1.2. «Эвристический» метод проверки.

Существует еще один метод «Эвристический» он появился дабы устранить недостатки предыдущего из-за его медленного обновления баз и усложнения алгоритмов вирусов. Он представляет собой поиск ошибок в методах обнаружения, возможные варианты будущих алгоритмов поведения

вирусов и устанавливая при этом необходимые закономерности проводит обнаружение вредоносного кода. На данный момент — это единственный метод, который помогает защититься от вирусов, не занесенных в базу данных. Он различается на 2 метода.

1. статический эвристический метод, пытаются определить, является ли подозрительная программа вредоносной, изучая структуру и содержимое программы в неактивном (статическом) состоянии и пытаясь найти (например) фрагменты кода, которые обычно использовались для вредоносных целей в прошлом. Этот тип техники особенно зависит от наличия подробных знаний не только о содержимом прошлых вредоносных программ, но и особенностях вредоносных программ, чтобы избежать предупреждения о наличии кода, который, хотя и широко используется вредоносными программами, также распространен в законном программном обеспечении одной из сильных сторон статической эвристики является то, что, в отличие от динамической эвристики, она способна исследовать несколько возможных путей выполнения программы из-за того, что она смотрит на все содержимое программы, а не только на код, который будет выполняться во время одного конкретного вызова программы. К сожалению, авторы вредоносных программ разработали ряд методов, чтобы запутать свой код таким образом, чтобы осложнить выполнения эвристического метода.
2. Динамический эвристический метод определяет, является ли подозрительная программа вредоносной, запустив программу в моделируемой среде и пытаясь обнаружить активное (динамическое) вредоносное поведение. Есть несколько способов достичь этого, будь то эмуляция программы до тех пор, пока она не покажет ранее известную версию себя, или запуск ее в какой-то

песочнице, чтобы каталогизировать более широкий диапазон ее поведения, ища признаки злого умысла. Одна из сильных сторон динамической эвристики заключается в возможности обойти многие из методов запутывания, которые используют авторы вредоносных программ, чтобы блокировать статический эвристический анализ, поскольку выполнение традиционно должно быть отложено во время выполнения для работы вредоносных программ. К сожалению, авторами вредоносных программ были разработан ряд трюков, чтобы попытаться бороться с этими методами, и они, как правило, используют более естественную и общую слабость, включающую в себя тот факт, что для любой нетривиальной программы есть несколько путей, которые выполнение программы может привести, но любой из вызовов программы будет следовать только одним из этих путей. Выполнение программы может принимать различные пути (и, таким образом, показывать различное поведение) в зависимости от любого количества различных условий, присутствующих во время выполнения, поэтому вредоносное поведение динамического эвристического метода может не отображаться (случайно или по проекту) во время анализа.

2.3.1.3. Антивирусные мониторы

При проверки таким методом защиты антивирус постоянно находиться в оперативной памяти компьютера и проверяет все действия файлов. Таким образом он пытается выявить подозрительные действия программ или при открытии файлов.

Проверка осуществляется не только при открытии, но и при загрузке через интернет или копирования файлов с внешних носителей (съемных дисков, usb устройств и т.д.).

2.3.1.4. Отслеживание изменений

Как было сказанно ранее многиу вирусы пытаются препесать код программы, либо заразить другие файлы. Данный метод проверки как раз основывается на этой особенности вирусов. Он пытается обнаружить действия вируса по изменению программы или файла путем запоминания данных а затем периодически проверяет их сравнивая с данными, которые он запомнил до этого. Таким образом он может обнаружить зараженные файлы.

1.3.2. Firewall

Для защиты вашего компьютера важны не только антивирусные программы но также и использование брандмауэра (firewall).

Брандмауэр - это программное обеспечение или микропрограмма, которая применяет набор правил о том, какие пакеты данных будут разрешены для входа или выхода из сети. Межсетевые экраны включены в широкий спектр сетевых устройств для фильтрации трафика и снижения риска того, что вредоносные пакеты, пройдут к вам через публичный интернет, и смогут повлиять на безопасность компьютера или внутренней сети.

3.3.2.1. Типы брандмауэра

Брандмауэры делаться на следующие типы с фильтрацией пакетов, с отслеживанием состояния, прокси-брандмауэры и брандмауэры следующего поколения (NGFWs).

- Брандмауэр фильтрации пакетов проверяет пакеты изолированно и не знает контекста пакета.
- Брандмауэр проверки состояния проверяет сетевой трафик, чтобы определить, связан ли один пакет с другим пакетом.

- Прокси-брандмауэр проверяет пакеты на прикладном уровне эталонной модели Open Systems Interconnection (OSI).
- NGFW использует многоуровневый подход для интеграции возможностей брандмауэра предприятия с системой предотвращения вторжений (IPS) и контроля приложений.

Когда организации начали переходить от мэйнфреймов к клиент-серверной модели, возможность управления доступом к серверу стала приоритетной. До появления первых брандмауэров, основанных на работе, проделанной в конце 1980-х годов, единственной реальная форма сетевой безопасности была применение, через списки управления доступом (ACL), расположенные на маршрутизаторах. Списки ACL указывают, каким адресам протокола Интернета (IP) был предоставлен или запрещен доступ к сети.

Экспоненциальный рост интернета и, как следствие, увеличение подключенных сетей, означало, что фильтрации сетевого трафика только по IP-адресу больше не было достаточно. Статические брандмауэры с фильтрацией пакетов, которые изучают заголовки пакетов и используют правила для принятия решений о том, какой трафик пропускать, возможно, стали самой важной частью каждой сетевой безопасности к концу прошлого века.

3.3.2.2. Как работают брандмауэры фильтрации пакетов

Когда пакет проходит через брандмауэр фильтрации пакетов, проверяется его адрес источника и назначения, протокол и номер порта назначения. Пакет отбрасывается, если он не соответствует набору правил брандмауэра. Например, если межсетевой экран настроен с правилом для блокирования доступа Telnet, то межсетевой экран отбросит пакеты, предназначенные для номера порта 23 протокола управления передачей (TCP), порта, где Приложение сервера Telnet будет прослушивать.

Брандмауэры фильтрации пакетов работают в основном на сетевом уровне модели OSI, хотя транспортный уровень используется для получения

номеров портов источника и назначения. Они рассматривают каждый пакет независимо и не знают, является ли какой-либо данный пакет частью существующего трафика. Брандмауэры с фильтрацией пакетов эффективны, но поскольку они обрабатывают каждый пакет изолированно, они могут быть уязвимы перед подделкой IP-адресса и в значительной степени заменены брандмауэрами с проверкой состояния.

3.3.2.3. Как работают брандмауэры с отслеживанием состояния

Брандмауэры с отслеживанием состояния, также известные как брандмауэры с динамической фильтрацией пакетов, поддерживают таблицу, которая отслеживает все открытые соединения. При поступлении новых пакетов брандмауэр сравнивает информацию в заголовке пакета с таблицей состояний и определяет, является ли она частью установленного соединения. Если это часть существующего соединения, то пакет пропускается без дальнейшего анализа. Если пакет не соответствует существующему соединению, он оценивается в соответствии с набором правил для новых соединений.

Брандмауэры с отслеживанием состояния отслеживают пакеты связи в течение определенного периода времени и проверяют входящие и исходящие пакеты. Отслеживаемые исходящие пакеты пропускаются только на запросы для конкретных типов входящих пакетов. Несмотря на то, что брандмауэры проверки состояния достаточно эффективны, они могут быть уязвимы для атак типа DoS.

3.3.2.4. Как работают брандмауэры уровня приложений и прокси-сервера

Поскольку атаки на веб-серверы стали более распространенными, стало очевидно, что существует необходимость в брандмауэрах для защиты сетей от атак на уровне приложений. Брандмауэры фильтрации пакетов и проверки состояния не могут различать допустимые запросы протокола уровня приложения, данные и вредоносный трафик, инкапсулированные в явно допустимый трафик протокола.

Брандмауэры, обеспечивающие фильтрацию на уровне приложений, могут проверять опасные данные пакета и различать допустимые запросы, данные и вредоносный код, замаскированный под обычный запрос или данные. Поскольку этот тип брандмауэра принимает решение на основе содержимого пакета, он предоставляет инженерам безопасности более детальный контроль над сетевым трафиком и устанавливает правила, разрешающие или запрещающие определенные запросы или команды приложений. Например, он может разрешить или запретить определенную входящую команду Telnet от определенного пользователя, тогда как другие брандмауэры могут управлять только общими входящими запросами от определенного хоста.

Установка брандмауэра на прокси-сервер затруднит злоумышленнику доступ к сети сети и создаст еще один уровень безопасности.

При наличии брандмауэра прокси-сервера клиент и сервер вынуждены проводить сеанс через посредника - прокси-сервер, на котором размещен брандмауэр уровня приложений. Теперь каждый раз, когда внешний клиент запрашивает соединение с внутренним сервером (или наоборот), клиент вместо этого открывает соединение с прокси. Если соединение соответствует критериям в базе правил брандмауэра, прокси-сервер откроет соединение с запрашиваемым сервером. Поскольку брандмауэр расположен в середине логического соединения, он может отслеживать трафик на уровне приложений для любых признаков вредоносной активности.

Ключевым преимуществом фильтрации на уровне приложений является возможность блокировать определенный контент, например известные вредоносные программы или определенные веб-сайты, и распознавать случаи неправильного использования определенных приложений и протоколов, таких как протокол передачи гипертекста (HTTP), протокол передачи файлов (FTP)

и система доменных имен (DNS). Правила брандмауэра уровня приложений также могут использоваться для управления выполнением файлов или обработкой данных определенных приложений.

3.3.2.5. Будущее брандмауэра

Большая часть трафика в центре обработки данных поступает от клиента к серверу и от сервера к клиенту. Однако за последние несколько лет виртуализация и такие тенденции, как конвергентная инфраструктура, создали больше трафика в центре обработки данных перемещается от сервера к серверу. Чтобы справиться с этим изменением, некоторые корпоративные организации перешли от традиционных трехуровневых архитектур центров обработки данных к различным формам архитектур конечных элементов. Это изменение в архитектуре заставило некоторых экспертов по безопасности предупредить, что, в то время как межсетевые экраны все еще играют важную роль в поддержании безопасности сети, современные примеры сети имеют так много точек входа и различные типы пользователей, что требуется более сильный контроль доступа и безопасность на хосте. Потребность в еще большем многослойном подходе привела к появлению того, что производители называют брандмауэрами следующего поколения.

NGFWs объединяет три ключевые особенности: традиционный функции брандмауэра, распространение использования приложений и IPS. Как и введение проверки состояния брандмауэров первого поколения, NGFWs привносит дополнительный контекст в процесс принятия решений брандмауэром.

NGFWs сочетают возможности традиционных корпоративных брандмауэров , включая преобразование сетевых адресов(NAT), блокировку URL-адресов и виртуальные частные сети (VPN), с функциональностью и функциями качества обслуживания (QoS), которые традиционно не используются в продуктах брандмауэра. Эти продукты поддерживают сеть на основе трех базовых принцепов, включая проверку Secure Sockets Layer (SSL)

и Secure Shell (SSH), глубокую проверку пакетов (DPI) и обнаружение вредоносных программ на основе репутации, а также использование приложений.

1.4. Антивирусы для Android

В связи с ростом количества мобильных телефонов остро встает вопрос и о защите данных хранящихся на этих устройствах от вирусов. Поэтому я решил рассмотреть проблемы связанный с антивирусным программным обеспечением на базе Android.

На платформе Android антивирусное программное обеспечение имеет ряд недостатков. Из-за ограничений платформы, оно не может получить полный доступ или отслеживать всю файловую систему, а только некоторые ее части. Современное антивирусное программное обеспечение полагается в основном та проверку имен файлов. Нельзя отследить поведение программы соответственно и вируса при выполнении приложения.

Существуют только 2 метода обнаружения вируса в Android системе. Сравнение имен пакетов, т. е. антивирусное программное обеспечение сканирует устройства Android и ищет соответствие с известными ему вирусами в своей базе данных.

При таком подходе, часто бывает достаточно изменить имя пакета вредоносных программ для обхода антивирусного ПО. Если вредоносные программа не распространена широко, то производители антивирусных программ вероятно, не скоро добавят его в свою базу данных, что оставит ваш телефон или планшет уязвимы на длительный срок.

Второй подход это проверка файлов пакета. Однако, как было сказано ранее, большинство частей файловой системы Android, включая рабочие каталоги приложения, не доступны с помощью антивирусного программного обеспечения.

Второй подход можно легко обойти, не включая какие-либо вредоносные действия, при первоначальной установке файла приложения, а только в компоненты, которые загружаются и выполняются во время выполнения. Использование этих двух подходов, в тестах антивирусного программного обеспечения, может сообщать о высокой скорости обнаружения для большинства продуктов в теории, но на практике они не обеспечивают высокий уровень защиты.

Недостатки антивирусных решений на андроиде и отсутствие каких-либо эффективных методов обнаружения для динамического поведения, таких как. эвристический или отслеживание изменений в приложениях на произвольные объекты файловой системы, в результате ограничивают возможности платформы.

Как и любые другие приложения установленные на базе Android антивирусное программное обеспечение устанавливается в песочницу (sandbox). Из-за этого оно не может получить доступ к каталогам любого другого приложения, и, таким образом, сканировать другие приложения файлы для выявления вредоносных шаблонов или поведения. Любое приложение, которое не входит в базы данных антивирусных программ не будет обнаружено при загрузке вредоносных файлов.

1.4.1. Сравнение имен пакетов.

В компьютерных операционных системах процессы запущенные одним пользователем наследуют его единственный идентификатор пользователя (UID - user Id). Таким образом основой управления доступом в компьютерных операционных системах основано на том что процесс может получить доступ ко всем файлам другого процесса.

Чтобы ввести дополнительную конфиденциальность данных, а также запретить доступ к объектам файловой системы другими приложениями. Операционная система Android меняет традиционные методы работы системы,

вместо назначения одного UID для каждого процесса, каждому приложению присваивается свой уникальный UID во время установки по умолчанию. Владение рабочим каталогом, каждого приложения (где находятся данные включая имя пакета) и всеми файлами, содержащимися в этом рабочем каталоге, устанавливается на UID соответствующего приложения.

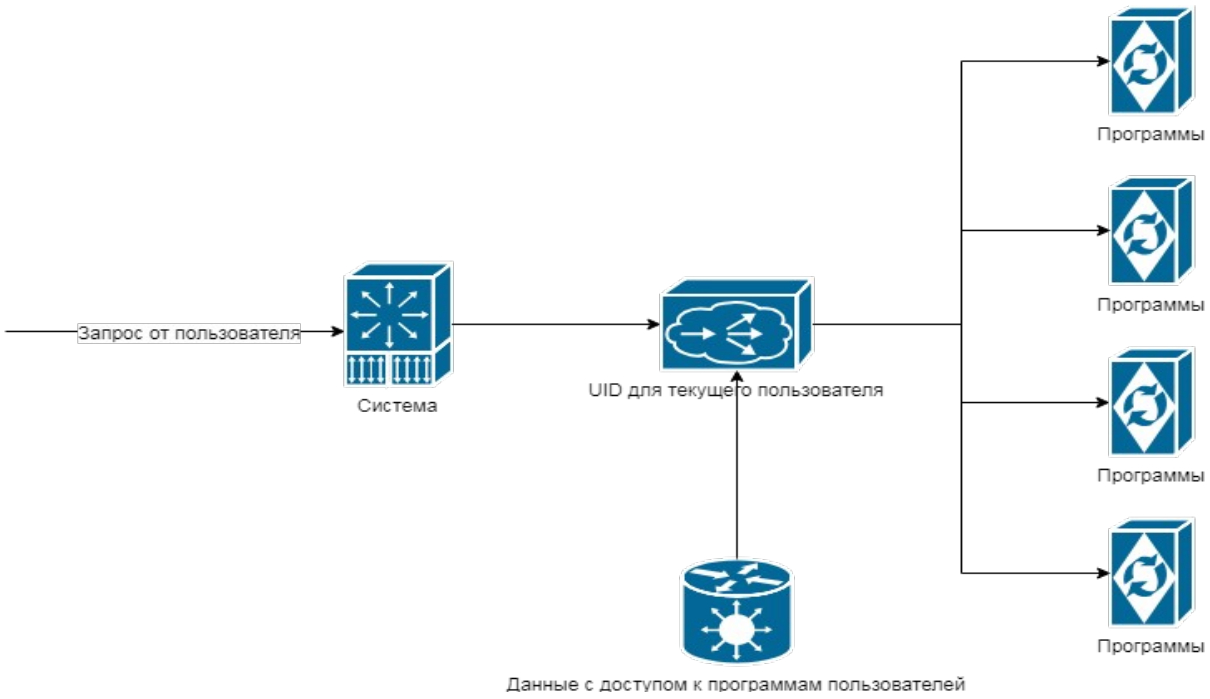

Рисунок 2.4 UID для WIndows

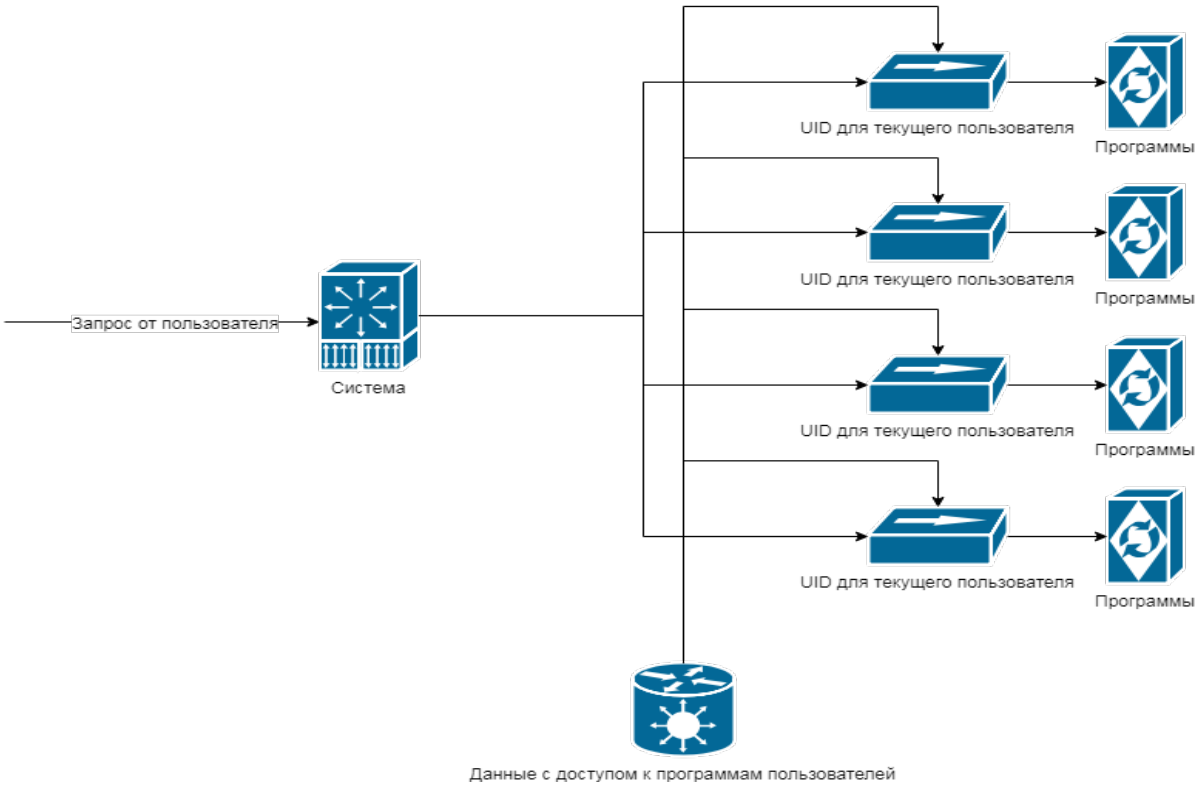

Рисунок 2.5 UID для Android

Большинство файлов, системные объекты вне рабочих каталогов приложений и имеют выданные системной UID и, таким образом, не могут быть доступны. В конечном счете, эта схема назначения UID и разрешения доступа к подключенной файловой системе устанавливают безопасную среду файловой системы для приложений. Они ограничены в своем собственном каталоге, отделяя каждое приложение от всех остальных, и от файлов и папок операционной системы.

Антивирусное программное обеспечение Android, которое также является обычным приложением, резко ограничено из-за такой схемы работы файловой системы на основе песочницы. Как следствие, антивирусные приложения не могут нормально сканировать файловые системы по требованию или отслеживать изменения файловой системы. Самое главное при этом антивирус не может просканировать рабочей директории других приложений и не проверяет любые файлы, которые другие приложения могут загрузить во время выполнения. Приложения могут сделать это добавив

функционал после установки в виде нативного кода, который не показывается в установочных файлах пакета.

Вышесказанное не относится к внешним устройствам хранения данных, таких как карты памяти. Такая память обычно имеет архитектуру файловой системой, которая не поддерживает производные механизмы ядра Linux, такие как контроль доступа, и читается любым приложением. Однако, методы опознавания ограничиваемые применением к внешней памяти мало эффективны и полезны,так как вредоносный код обычно заражает системную память, ведь именно там расположены основные каталоги, а не на внешней памяти.

1.4.2. База Данных Пакетов

Операционная система Android отслеживает установленные приложения в базе данных пакетов (находится в каталоге / data/system / packages.xml). В этом файле хранится набор данных для каждого приложения. Он включает в себя путь к директории приложения, где хранится исполняемый файл приложения, имя пакета приложения, его UID и другие записи. В отличие от многих других ресурсов операционной системы Android, база данных пакетов является общедоступной.Так как антивирусные программы не могут сканировать файловую систему для выявления вредоносных файлов они прибегают к сравнению имен пакетов всех перечисленных приложений в базе данных пакетов с антивирусной базой известных вредоносных программ.

1.4.3. Доступ к файлам пакетов

В то время как каталог файла пакета (/data / app) не доступен для любых приложений, и таким образом просмотр файлов приложения в нем запрещен, база данных пакета доступна для всех. Кроме того, файлы пакета в то время как они не могут быть доступны через доступ к файловой системе,они доступны для чтения любыми приложениями. Это в комбинации дает чтение

файлов пакетов: антивирусному программному обеспечению возможность извлечь пути к пакету файла из базы данных пакетов, а затем открытию файлов пакетов напрямую, а не через операционную систему. Таким образом, антивирусные методы обнаружения можно по крайней мере применить к статическому файлу пакета приложения.

1.4.4. Методы Вредоносных Программ Для Android

Методы распространения вирусов в ОС Android посравнению с компьютерными операционными системами различается.

Следует отдельно рассмотреть способы распространения вирусов в телефонах для лучшего понимания их работы и как следствие выявления методов борьбы с ними:

1. Код вредоносной программы может включать в себя метод для расширения прав доступа - root. Фактически это учетная запись администратора (суперюзера) которая предоставляет полный доступ к файлам системы, возможность запускать исполняемые программы (без ведома пользователя), менять и удалять системные файлы, изменять настройки системы и некоторые другие возможности.
2. Загружать вредоносный код во время установки файла. Такие методы распространения в большинстве случаев останавливает антивирусная защита в Android Market (”Google Play"). Однако, если пользователь скачал .apk файл из интернета то вирус может обнаружить только антивирус установленный на телефоне или планшете, но у большинства пользователей нет антивирусной защиты на Android устройстве.
3. Самым эффективным способом распространения - не выполнять не проявлять себя как вредоносная программа до установки на телефон, а после установки подгрузить дополнительные файлы которые уже несут в себе вирусы. Код во время установки приложения выглядит абсолютно

нормальным, не содержащим вируса. Поэтому не удается определить что программа заражена. Такой способ заражения имеют RootSmart / BSmart. Также, этот метод демонстрирует недостатки антивирусного программного обеспечения для Android.

Если происходит получение вредоносного кода из интернета. Такой недавно добавленный код не может быть замечен антивирусным программным обеспечением. Особенно, когда вредоносная программа не очень широко распространена, маловероятно, что базы антивирусов будет быстро обновлена. В худшем случае будет атака, останется незамеченной на очень долгое время. Кроме того, когда корень эксплойты используются вредоносными программами, обнаружение с задержкой в несколько дней.

1.4.5. Вывод Android

Основной причиной неэффективности антивирусного программного обеспечения Android является невозможность получить прямой доступ к файловой системе и ее содержанию. Это большое преимущество для всех других случаев, так как это обеспечивает безопасность данных и конфиденциальность установленных приложений, особенно против доступа другими приложениями. Однако это является основным препятствием для антивирусного программного обеспечения.

Антивирусы на Android не могут развертывать методы распознавания на основе эвристики (эвристический) или проверку подписи к произвольным объектам файловой системы. Таким образом, динамически скачиваемый код найден не будет. Этот динамически загружаемый код также может быть единственным компонентом, который демонстрирует вредоносное поведение, сохраняя приложение, которое скачало вредоносный код после установки не вызовет, каких-либо подозрений. Кроме того, приложения, которые не демонстрировать вирусного поведения, с большим количеством пользователей, или даже хуже, только с некоторыми потребители или одним потребителем в случае точечных нападений, никогда или только когда будет

поздно могут быть включены в антивирусные базы андроид.При запоздалом распознавании вируса, даже после удаления вредоносной программы может не помочь. Потому что вредоносные программы могли взять на себя полный контроль над устройством с помощью эксплойтов повышения привилегий (root- прав). Подобные вредоносные программы должны быть обнаружены до, во время, или вскоре после установки.

Типичные тесты антивирусных продуктов исключительно на основе скорости обнаружения, такие как обычно проводятся с настольными антивирусными продуктами не показывают картину целиком для антивирусов на Android. Из-за природы этих тестов, в которых взятый набор вирусы и затем используемый в качестве тестового сценария, известен поставщику антивирусов. Для многих образцов вирусов эти тесты действительны только несколько недель или месяцев после их первоначального обнаружения. Я не считаю такие тесты как действительные показатели реального уровня защиты, предлагаемые в реальном времени, при появлении новых угроз. На самом деле, большое значение имеет как быстро были обновлены базы данных,это определяет, как долго у пользователей могут быть установлены вредоносные программы без предупреждения пользователей антивирусным приложением. Тесты не берут в расчет, что ни одно антивирусное приложение не будет способно обнаруживать вредоносную активность внутри рабочего каталога неизвестных вирусов, независимо от того, насколько высока теоретическая скорость обнаружения. Также игнорируется изменение имен пакетов, которое приведет к вредоносным программам идентичным обычным, за исключением измененного имени пакета. Они обнаруживаться, только если применяется сравнение имен пакетов.

2. ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННЫХ МОДЕЛЕЙ И РАЗРАБОТКА АЛГОРИТМОВ (MODELS AND METHODS)

2.1.Логическое проектирование

В моей бакалаврской работе я создал информационную систему Call центра для Ip телефонии. В текущей работе мне бы хотелось рассмотреть создание антивирусной защиты для этого предприятия.

«Навиком» - Российская компания занимается продажей видеорегистраторов и их комплектующих.

Компания была основана в марте 2015 года, тогда же был открыт и первый магазин «Навиком» в Москве. Магазин расположен в пятиминутной шаговой доступности от метро. Площадь магазина составляет 450 кв.м., из них 150 занимают склады 300 отводиться под площадь самого магазина.

За год доход компании составил 2 млн 300 т рублей. По расчетным темпам развития, которые позволит увеличить моя информационная система и

Call-Центр доход «Навиком» составит около 3,5 млн. рублей в год.

В перспективе компания собирается открыть еще один офис на севере Москвы.

Главным приоритетом компании остается покупатель, поэтому ее политика основана на сохранении ее постоянных клиентов и привлечении новых.

Основной бизнес процесс компании строиться на продаже оборудования клиентом его схема представлена ниже:

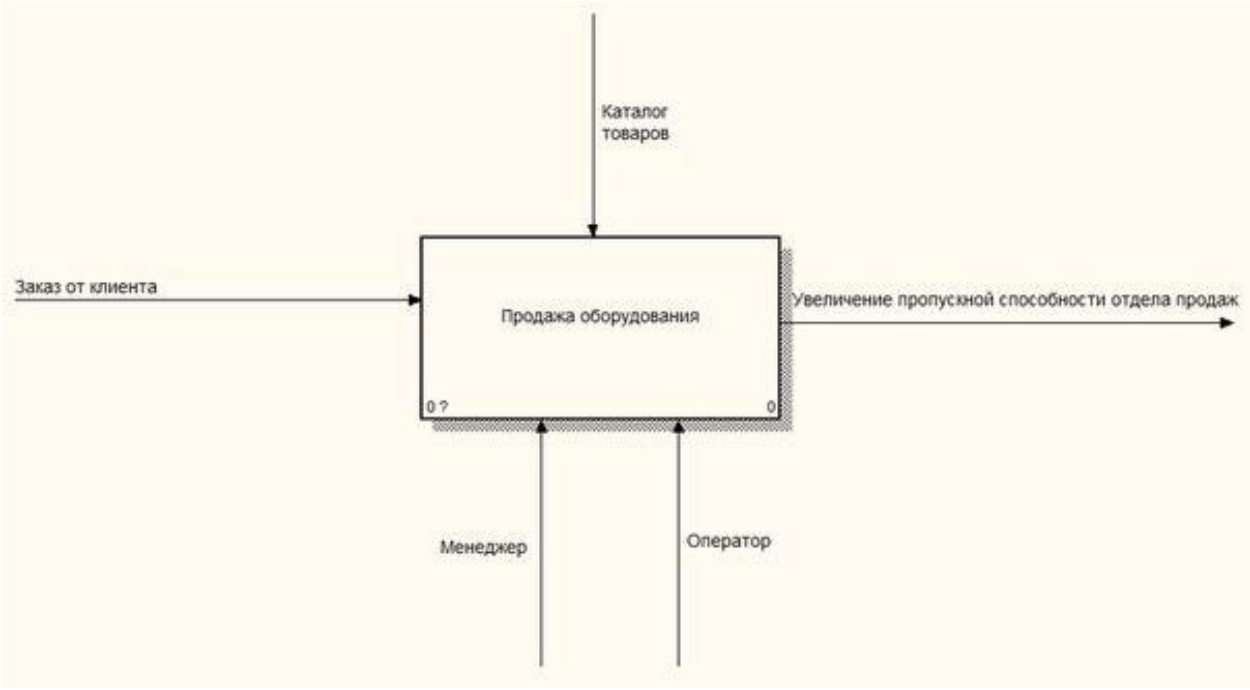

Рисунок 3.1 Модель продажи оборудования IDEF0

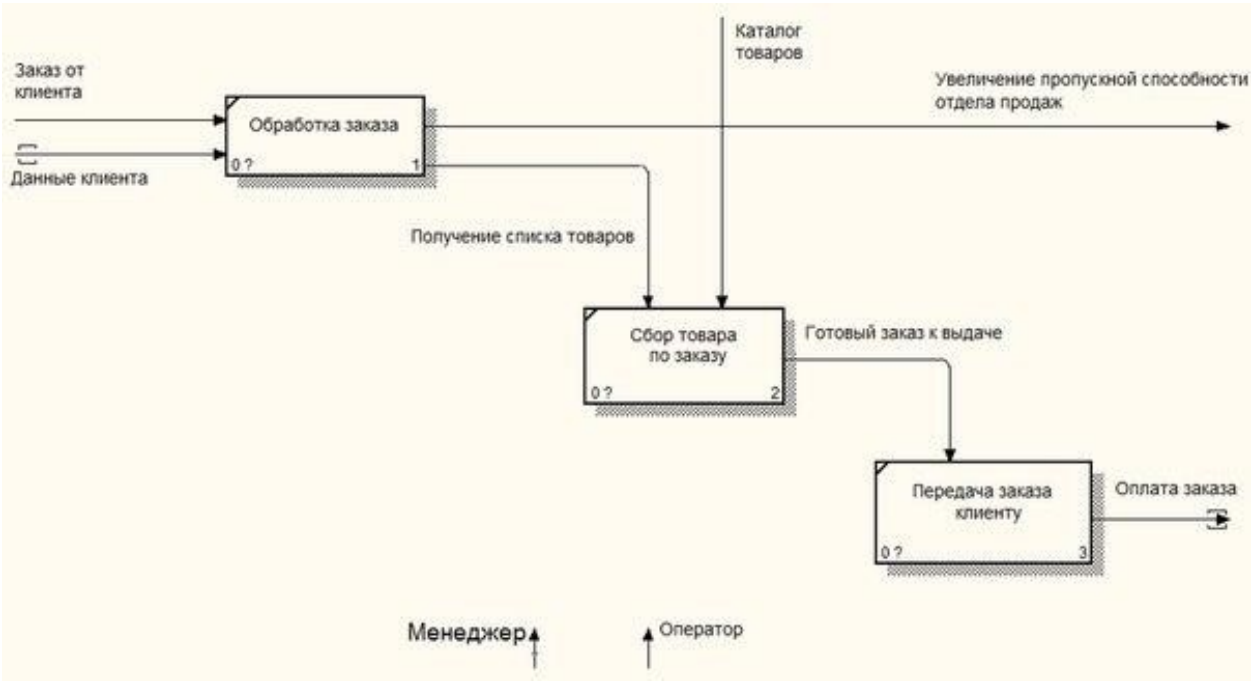

Рисунок 3.2 Схема алгоритма продажи товаров IDEF0

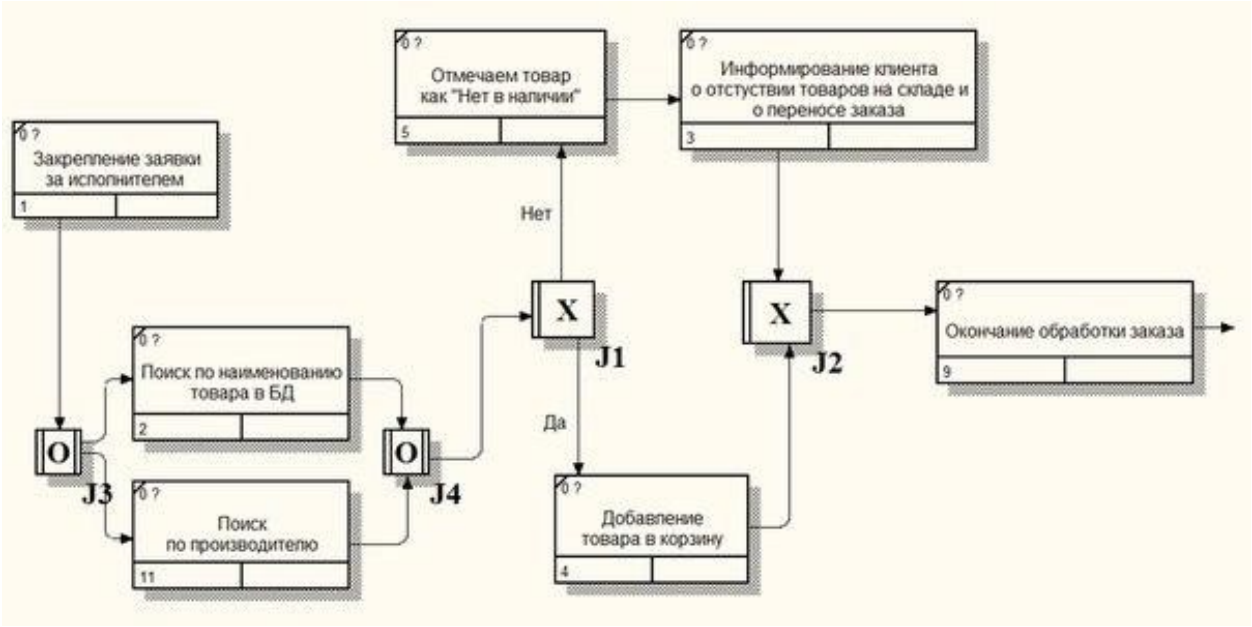

Рисунок 3.3 Схема алгоритма обработки заказа IDEF3



Рисунок 3.4 Блок схема алгоритма приема и выполнение заказа.

Для хорошей защиты сети компании и данных компании необходимо использовать не только стандартные системы антивирусной защиты на рабочих станциях, но также и специально сетевое антивирусное программное обеспечение.

Антивирусное программное обеспечение должно соответствовать сертификации средств защиты информации ФСТЭК. Это позволит обеспечить надежную защиту для корпоративной сети. В настоящий момент большинство компьютеров пользователей используют систему Windows 7 и Windows 10. На стороне серверной части находиться Windows Server 2008. Антивирус должен обеспечивать антивирусную защиту при работе в локальной сети и в Интернет с Web-страницами, электронной почтой, локальными жесткими дисками и съемными носителями, а также с сетевыми ресурсами. Должна обеспечиваться защита входящей и исходящей электронной корреспонденции, от вредоносных программ. Должно обеспечиваться обнаружение и удаление вирусов всех типов, как из тела сообщения, так и, если это возможно, из вложенных файлов. Для компании важно чтобы использовался одно антивирусное программное обеспечение. Это позволит управлять всеми установленными антивирусам с одного рабочего компьютера.

Должно регулярно производиться обновление сигнатур баз данных всевозможных вредоносных программ для надежной работы системы

В Системе должна быть реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов. Компоненты Системы должны устойчиво функционировать на серверах и компьютерах пользователей в условиях их минимальной и максимальной загрузки без существенного снижения производительности. Web-сайт производителя Системы должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке, пополняемую базу знаний, а

также форум пользователей программных продуктов производителя для возможности.

2.2. Управление антивирусными продуктами в корпоративной сети

Управление антивирусными продуктами в сети предприятия довольно сложная вещь при “ручном” режиме работы. Сеть предприятия может состоять из нескольких сотен компьютеров или рабочие станции территориально могу располагать на большом расстоянии. Поэтому обновление загрузочных баз, выполнение проверки антивирусов, контроль выполнения проверки компьютеров пользователей и т.д. сильно осложняется.

Эффективность работы антивирусов может быть нарушена, если выполнять все работы, описанные ранее не вовремя. Безопасность компьютера может быть нарушена, например, вовремя необходимое при обновлении антивирусных баз или автоматической проверки, компьютер был выключен.

Для того чтобы не допускать таких случаев я предлагаю использовать функции контроля и управления, которые позволяют:

- Обновлять антивирусные базы, для немедленного или отложенного выполнения;
- 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.
- В реальном времени отображения процесса работы на рабочих станциях и на серверах.

Эти функции реализовывают центры управления, который будет находится на машине у администратора и позволяет 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, который устанавливается на один из серверов сети компании является основой сетевого центра управления.

В клиент-серверной архитектуре устройства антивирусной системе защиты сети компании участвуют: Программы-агенты, установленные на компьютерах пользователей вместе с антивирусным программным обеспечение. Через антивирусный сервер они соединяются с управляющей консолью (интерфейсом) администратора схема приведена на рис. 3.5

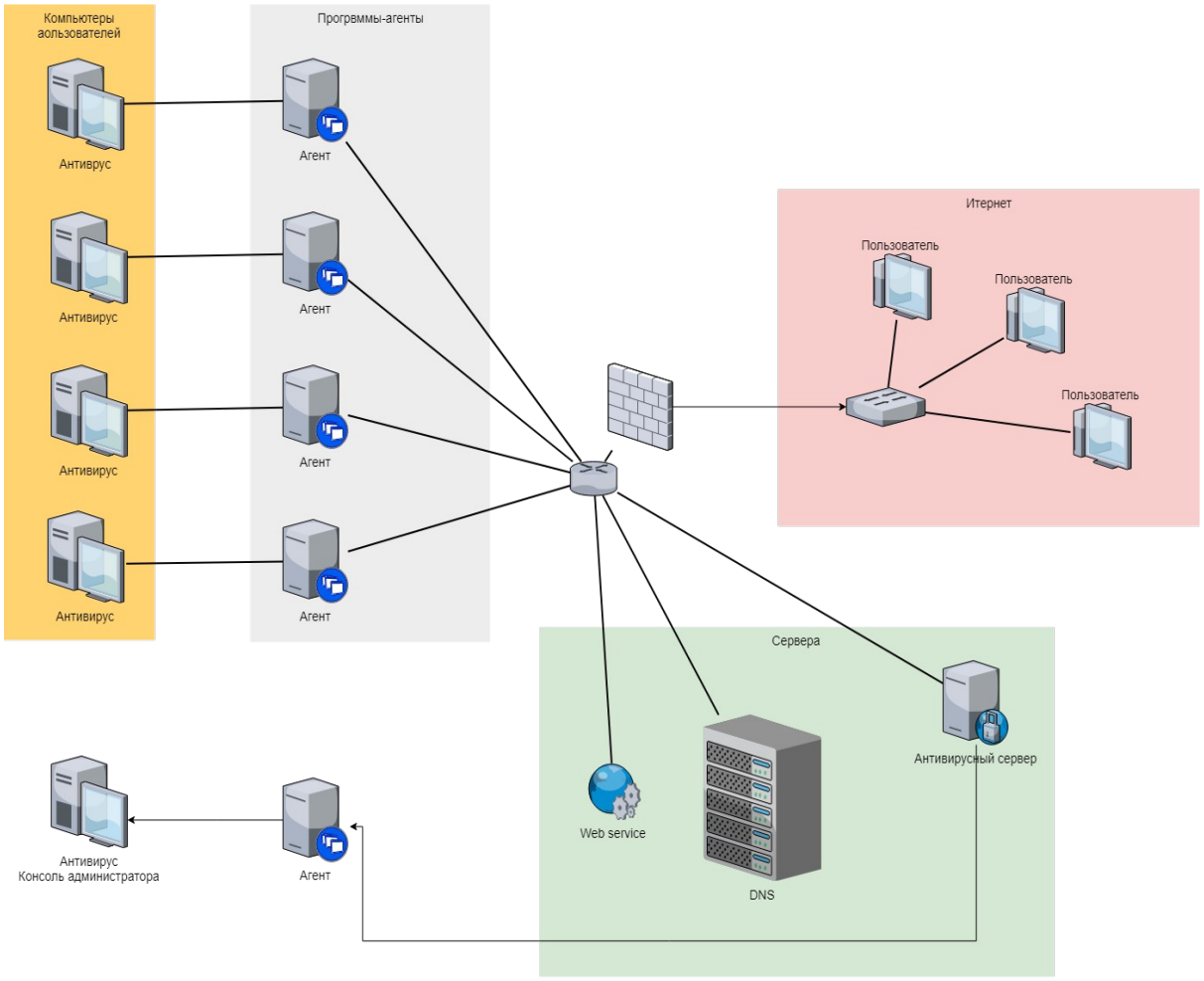

Рисунок 3.5 Устройство защиты в компании

Антивирусный сервер выполняет управляющие и координирующие действия. Он хранит общий журнал событий, имеющих отношение к антивирусной защите и возникающих на всех компьютерах сети, список и расписание выполнения заданий. Антивирусный сервер отвечает за прием от

агентов и передачу администратору антивирусной защиты сообщений о возникновении тех или иных событий в сети, выполняет периодическую проверку конфигурации сети с целью обнаружения новых рабочих станций или рабочих станций с изменившейся конфигурацией антивирусных средств и т.д.

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). Результаты работы антивируса передаются через агентов антивирусному серверу, которых их анализирует и протоколирует в журнале событий.

Пользовательский интерфейс управляющей консоли позволяет просматривать древовидную структуру корпоративной сети, получая при необходимости доступ к отдельным компьютерам тех или иных групп пользователей или доменов.

3. ТЕХНОЛОГИЯ ПРОГРАММНОЙ РЕАЛИЗАЦИИ РАЗРАБОТАННЫХ МОДЕЛЕЙ И АЛГОРИТМОВ (RESULTS)

3.1.Классификация антивирусных программ

Антивирусные программы делятся на основные антивирусы и двойного назначения.

Чистые антивирусы или основные антивирусы имеют в наличие антивирусное ядро, исполняющее функцию сканирования по сигнатурам. Главным отличием в этом случае является то, что лечение возможно, если известен вирус.

Основные антивирусы, классифицируются, по типу доступа к файлам, подразделяются на два вида:

1. Осуществляющие контроль по доступу (on access). On access-продукты называют мониторами
2. По требованию пользователя (on demand). On demand-продукты - сканерами

On demand-продукт осуществляется проверка по запросу пользователя. On access-продукт - это резидентная программа, которая выполняет проверку, когда осуществляется доступ к файлу пользователем или программой в соответствии с рисунком 4.1

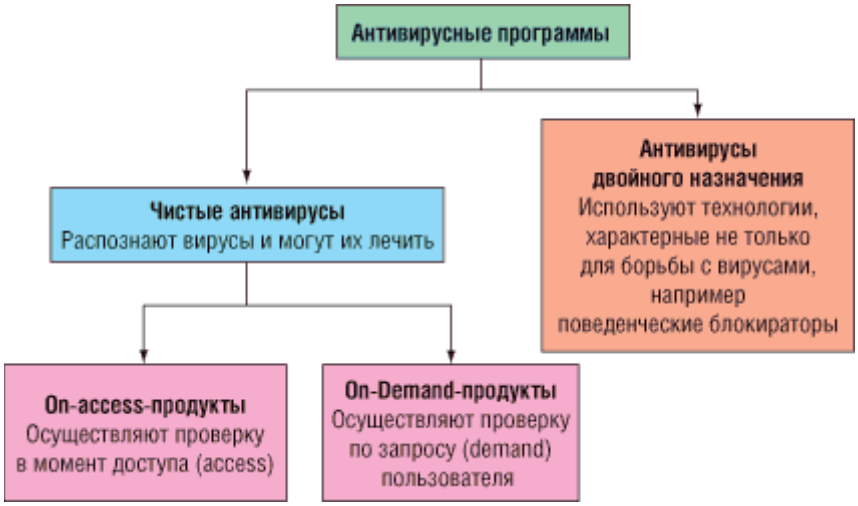

Рисунок 4.1 - Схема классификации антивирусных программ

Помимо разновидностей упомянутых ранее, антивирусные программы можно подразделить в зависимости от операционной системы, для которой данный антивирус создан. Опираясь на аналитические исследования крупных компаний таких, как Samsung можно сказать, что вместе с основными операционными системами Windows или Linux, часто используются и Microsoft Exchange Server, Microsoft Office, Lotus Notes.

3.2. Антивирус Касперского

Антивирус Касперского 6.0 для Windows Servers Enterprise Edition защищает данные на серверах под управлением Microsoft Windows (включая версии x86-64) от вредоносных программ. Продукт разработан специально для высокопроизводительных корпоративных серверов. Эффективная защита от вредоносных программ. Постоянная антивирусная защита. Приложение проверяет все запускаемые, открываемые и модифицируемые файлы, проводит лечение или удаление зараженных объектов, а также изолирует подозрительные объекты в карантине для дальнейшего анализа.

Проверка по требованию. Приложение проводит антивирусную проверку в заданных областях по запросу администратора или по расписанию. Проверка критических областей системы. Отдельная задача позволяет проверять области ОС, наиболее подверженные заражению. Например, проверка объектов автозапуска помогает предотвратить запуск вируса при старте системы, обнаружить скрытые процессы. В числе областей, наиболее подверженных заражению, находятся объекты автозапуска и оперативной памяти. Предотвращение вирусных эпидемий. Приложение фиксирует возникновение вирусных атак, что позволяет администратору системы оперативно предпринимать ответные меры: запускать сканирование, обновлять базы или включать повышенный уровень защиты системы.

Изоляция зараженных компьютеров. Если какая-то из рабочих станций в сети заражена, то приложение запрещает пользователю обращаться к ресурсам сервера в течение определенного времени. За этот период администратор

может выявить источник заражения и провести лечение. Защита терминальных серверов. Поддержка кластеров. Приложение готово к работе на терминальных серверах Citrix и Microsoft Terminal. Оно обеспечивает полноценную нотификацию терминальных пользователей при обнаружении зараженных объектов. Кроме этого, Антивирус Касперского может быть использован для защиты кластера серверов. Масштабируемость. При использовании многопроцессорных серверов администратор задает количество рабочих процессов антивируса для ускорения обработки запросов к серверу.

Оптимизация проверки. Технологии iSwift и iChecker позволяют существенно увеличить скорость работы приложения: программа проверяет все объекты только при первой проверке по требованию, а при последующих – только новые и измененные файлы.

Недостатки: не совместим с Windows 2008 R2 terminal servers.

3.3. Trend Micro ServerProtect for Microsoft Windows/Novell NetWare

Защита от распространения вирусов по вашей сети за счет блокирования угроз до того, как они попадут к конечному пользователю. Trend Micro ServerProtect для Microsoft Windows и Novell NetWare сканирует, находит и удаляет вирусы из обычных и сжатых файлов в реальном времени. ServerProtect предоставляет поддержку и защиту в режиме 24x7 благодаря тому, что его база вирусов постоянно пополняется и автоматически обновляется. Централизованное управление серверами через веб-консоль облегчает защиту сети.

Основные возможности: защита от вирусов в режиме реального времени, проверка файловой системы по запросу или по расписанию, многопоточный сканирующий механизм, сертификат совместимости с Microsoft Windows Server 2003/2000 Datacenter, управление защитой на основе

задач позволяет осуществлять гибкое распределение ресурсов в зависимости от режима работы серверов.

Обеспечивается сбор истории вирусной активности по всем серверам в единый протокол, данные из которого затем можно экспортировать в какое-либо внешнее приложение для подробного анализа. Централизованное управление всеми серверами, расположенными на одной площадке

Используется механизм фрагментарного обновления (incremental update), позволяющий загружать только сигнатуры новых вирусов, добавленные за время, прошедшее с момента последнего обновления базы данных. Автоматическое или ручное обновление вирусных сигнатур и сканирующего модуля.

Примечание: корпорация Trend Micro в большинстве случаев рекомендует использовать для защиты файловых серверов Windows продукт Office Scan Client-server edition. Однако, в случае необходимости использования управления на основе задач, а также для защиты высоконагруженных серверов сохраняется поддержка Server Protect.

3.4. Panda Security for File Servers

Panda Security File Servers разработан для компаний, которым необходима защита их файловых серверов. Продукт гарантирует всестороннюю защиту всей хранимой и открытой сотрудниками для совместного использования информации в корпоративной сети. Продукт представляет собой идеальное высокопроизводительное решение для защиты файловых серверов Windows с минимальным использованием системных ресурсов, предоставляя сканирование как постоянное, так и по запросу.

Продукт содержит технологии TruPrevent (HIPS), которые предлагают проактивную, превентивную защиту от всех типов вредоносных программ.

Продукт предотвращает распространение массивных вирусных атак, шпионов, рекламное ПО, червей, троянцев, когда компьютеры получают доступ к открытым сетевым ресурсам.

Проверяет обновления сигнатурного файла и новые образцы поведений вредоносных программ каждый час. Отслеживает каналы распространения инфекций и гарантирует соблюдение правил доступа к системным ресурсам.

Полноценный антивирусный движок обнаруживает подозрительные файлы даже в тех случаях, когда они открыты в эксклюзивном режиме. Сканирует сжатые файлы на серверах. Централизованное и удаленное администрирование сетей с различными отчетами для облегчения административных задач.

Сканирование процессов в памяти позволяет обнаруживать скрытые процессы и сканировать файлы и следы этих процессов. Если эти файлы или следы содержат вредоносный код, они будут вылечены.

Контролирует поведение пользователя, через которого инфекции могли бы проникнуть в сеть.

3.5. ESET NOD32 Smart Security Business Edition

ESET NOD32 Smart Security Business Edition - комплексная защита серверов и рабочих станций для всех типов организаций, включающая в себя антивирус, антишпион, антиспам, персональный файервол, а также приложение ESET Remote Administrator, которое обеспечивает обновление и централизованное администрирование в корпоративных сетевых средах или глобальных сетях, в соответствии с рисунком 4.2.

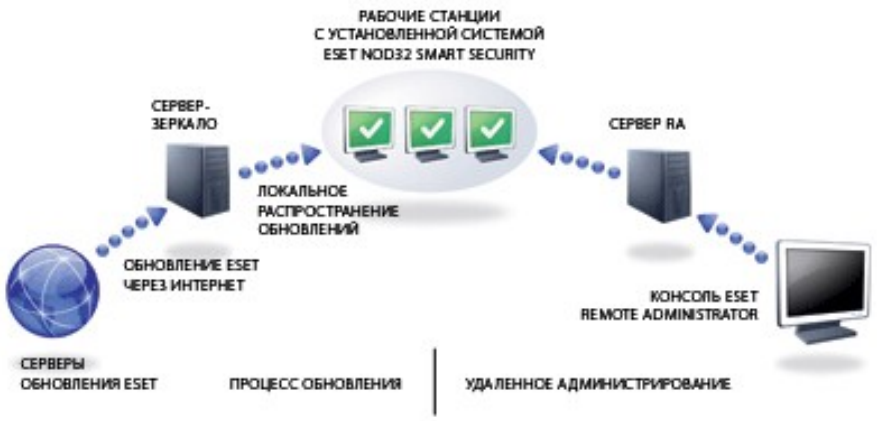

Рисунок 4.2 - Централизованное управление

Масштабируемое решение ориентировано на предприятия от 5 до 100 000 ПК в рамках одной структуры устанавливается как на сервер, так и на рабочие станции. Современные технологии, проактивная защита от неизвестных угроз применение интеллектуальных технологий, сочетающих эвристический и сигнатурный методы детектирования, обновляемое эвристическое ядро ThreatSensetм, регулярное автоматическое обновление сигнатурных баз.

Фильтрация почтового и веб-контента; антиспам полное сканирование всей входящей корреспонденции через протокол POP3 и POP3s, сканирование входящей и исходящей электронной почты, подробный отчет по обнаруженным вредоносным программам и спам-фильтрации,антиспам надежно защищает пользователя от нежелательных сообщений.

Полная интеграция в популярные почтовые клиенты: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail и Mozilla Thunderbird, The Bat!.

Персональный файервол, защита от внешних вторжений, низкоуровневое сканирование трафика обеспечивает высокий уровень защиты от сетевых атак, пять режимов работы: автоматический режим,

автоматический режим с исключениями, интерактивный режим, режим на основе политик и режим обучения.

Централизованное управление. С помощью решения ESET Remote Administrator можно удаленно осуществлять инсталляцию и деинсталляцию программных продуктов ESET, контролировать работу антивирусного ПО, создавать внутри сети серверы для локального обновления продуктов ESET («зеркала»), позволяющие существенно сокращать внешний интернет-трафик.

Удобные отчеты. ESET NOD32 Business Edition автоматически формирует отчет по обнаруженным инфицированным объектам, отправленным в карантин, по динамике угроз, событиям, проверкам, задачам, можно сформировать различные комбинированные отчеты и т.д. Возможна отправка предупреждений и сообщений через протокол SMTP или посредством менеджера сообщений.

Поддержка файловых серверов: Windows, Novell Netware и Linux/FreeBSD. Операционные системы:
Microsoft Windows 7/Vista/XP/ 2000 (32-bit е 64-bit версии)
Microsoft Windows Server 2000 / 2003 / 2008 (32-bit и 64-bit версии)
Linux (RedHat, Mandrake, SuSE, Debian и др., FreeBSD 4.X, 5.X и 6.X, NetBSD 4)
Novell Netware 4.x, 5.x и 6.x, Solaris 10.

Таким образом, сравнительная таблица 1, для решения задач оптимального выбора будет иметь следующий вид:

Таблица 1 - Сравнительная таблица

№	**Наименование показателя**	**Антивирусные программные продукты**			
		Kaspersky Antivirus	**Trend Micro ServerProtect**	**Panda Security**	**Nod 32**
1	Алгоритм нахождения	Эмуляц.	Эврист.	Эврист	Эмуляц.

№	Наименование показателя	Антивирусные программные продукты			
		Kaspersky Antivirus	Trend Micro ServerProtect	Panda Security	Nod 32
	вируса	Эврист.			Эврист
2	Анализ поведения программ	Есть	Есть	Есть	Есть
3	Проверка макросов	Есть	Нет	Нет	Есть
4	Firewall	Есть	Нет	Нет	Есть
5	Структура программной системы	модульная	монолитная	монолитная	модульная
6	Число поддерживаемых семейств ОС	17	10	11	20
7	Объем дистрибутива (Мб)	70МБ	81 МБ	85МБ	46 МВ

Для решения задачи оптимизации преобразуем эту таблицу в числовую форму с одновременной нормализацией данных, таблица 2.

Таблица 2 - Нормализация данных

№	Наименование показателя	Антивирусные программные продукты			
		Kaspersky Antivirus	Trend Micro ServerProtect	Panda Security	Nod 32
1	Алгоритм нахождения вируса	1	0,5	0,5	1
2	Анализ поведения программ	1	1	1	1
3	Проверка макросов	1	1	0	1
4	Firewall	1	0	0	1
5	Структура программной системы	1	0,5	0,5	1

№	Наименование показателя	Антивирусные программные продукты			
		Kaspersky Antivirus	Trend Micro ServerProtect	Panda Security	Nod 32
6	Число поддерживаемых семейств ОС	0,7	0,33	0,33	1
7	Объем дистрибутива (Мб)	0,27	0,16	0,18	0,6

Задачи оптимизации будем решать, как поиск такого средства, для которого взвешенная сумма из 7 основных характеристик будет максимальной:

$$J = \sum_{i=1}^{7} a_i p_i \qquad [4.1]$$

Где a_i–весовой коэффициент, причем $\sum_{i=1}^{7} a_i = 1$, p_i–числовое значение параметра. Вычисления приведены в таблице 3.

Таблица 3 - Критерий J

№	Наименование показателя	Ai	Антивирусные программные продукты			
			Kaspersky Antivirus	Trend Micro ServerProtect	Panda Security	Nod 32
1	Алгоритм нахождения вируса	0,25	0,5	0,5	1	1

2	Анализ поведения программ	0,2	1	1	1	1
3	Проверка макросов	0,17	1	1	0	0
4	Проверка скрипов	0,13	1	1	1	1
5	Структура программной системы	0,08	1	0,5	0,5	1
6	Число поддерживаемых семейств ОС	0,12	0,7	0,33	0,33	1
7	Объем дистрибутива (Мб)	0,05	0,27	0,16	0,18	0,6
8	Критерий J	1	0,7581	0,7126	0,6686	0,81

Из таблицы 3 видно, что оптимальным антивирусным средством по указанному критерию является NOD 32. Следующим по значимости идет Антивирус Касперского, чуть хуже - Trend Micro ServerProtect, следом Panda Security.

3.6. Программно-аппаратный МЭ

Межсетевой экран (МЭ) (firewalls) или брандмауэр предназначен для контроля над исходящей и входящей в систему информацией, то есть он занимается фильтрацией потока данных на заранее оговоренных условиях. Эти условия задаются системным администратором сети и способствует предотвращению атак со стороны внешней сети. Кроме внешних МЭ существуют и внутренние, которые занимаются контролем над потоком между сегментами локальной сети.

Межсетевые экраны можно классифицировать по тому на каком уровне они работают: канальном, сетевом, транспортном, прикладном. В зависимости от уровня различаются и задачи МЭ. Чем ниже уровень, тем выше производительность и ниже стоимость. Чем выше уровень, тем больше задач способен решать межсетевой экран. Например, при фильтрации на сетевом уровне возможно просмотреть структуру локальной сети из глобальной.

Сегодня на российском рынке МЭ присутствует огромное количество их наименований, но рекомендуется при их выборе исходить из того, что приобретаемые средства должны быть сертифицированы Гостехкомиссией при Президенте РФ или ФАПСИ. В таблице 4 представлены некоторые из сертифицированных межсетевых экранов.

Как видно из таблицы все МЭ разделены на классы. Всего установлено 5 классов защищенности. Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации. Например, для автоматизированных систем (АС):

2 класс, работа с грифом СС;

3 класс, работа с грифом С.

Таблица 4- Сертифицированные межсетевые экраны

Название МЭ	**Класс защищенности по руководящему документу (РД) и номер сертификата**
Аппаратно-программный комплекс МЭ “Застава-Джет” под управлением ОС Solaris 2.5.1.	Сертификат СЗИ №146 выдан 14.01.1998 г. Гостехкомиссией России. (По классу 2 СВТ)
МЭ “CyberGuard” версии 4.0	Сертификат СЗИ №171 выдан 24.04.1998 г. Гостехкомиссией России. (По классу 3 СВТ)
Аппаратно-программные комплексы на базе маршрутизаторов Bay Networks: Advanced Remote Node, Access Stack Node 2 (ASN2), BackBone Node (BN)	4 по РД “МЭ” - № 175
Программный комплекс “Межсетевой экран FireWall-1/VPN-1” версии 4.0, Service Pack 2	4 по РД “МЭ” - № 230
Программно-аппаратный комплекс ФПСУ-IP	по 3 классу для МЭ - № 233

Название МЭ	**Класс защищенности по руководящему документу (РД) и номер сертификата**
Аппаратно-программные комплекс “МЭ WatchGuard”	4 по РД “МЭ” - № 236
СКЗИ от НСД в сетях передачи данных по протоколу TCP/IP - МЭ “Пандора” (на базе МЭ “Gauntlet” версии 3.1.1.)	Сертификат СЗИ №73 выдан 16.01.1997 г. Гостехкомиссией России. (По классу 3Б АС) Сертификат СЗИ №183 выдан 10.06.1998 г. Гостехкомиссией России. (По классу 3 МЭ)

Системы уровня сети занимаются тем, что анализируют проходящий трафик, сравнивают его с известными сигнатурами атак и принимают решение о вторжении в случае совпадения кода. В этом случае делается запись журнале и извещается системный администратор. Ну и конечно же СОВ пытается сама противодействовать атаке.

Процедурная же модель систем обнаружения вторжений занимается тем же, что и система сетевого уровня, а также фиксирует и исследует проходящую работу, пытаются адаптироваться к данной сети.

Система обнаружения вторжений является неплохим дополнением к МЭ и в ряде случаев занимаются облегчением труда системных администраторов, но в тоже время обладает существенным недостатком: СОВ не способны обнаружить неизвестные вторжения, пока не будут обновлены сигнатуры.

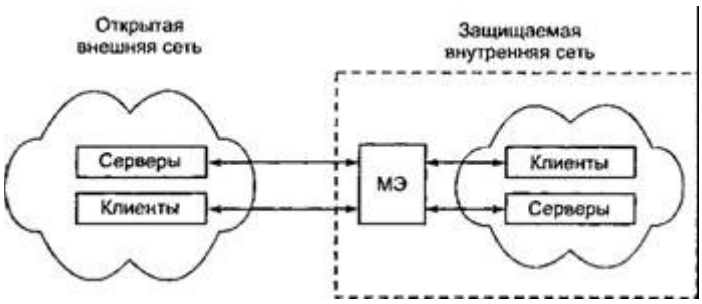

Рисунок 4.3- Защита МЭ

3.7.Выбор программно-аппаратного МЭ

3.7.1. Cisco ASA 5520

Адаптивная Security Appliance поставляет широкий спектр охранных услуг Gigabit Ethernet для подключения средних предприятий сетей, в модульных, высокую производительность устройства. С помощью своих четырех Gigabit Ethernet интерфейсов и поддержкой до 25 VLANs, предприятия могут легко развертывать эти службы безопасности на несколько зон, в пределах своей сети. Cisco ASA 5520 Адаптивная Security Appliance в масштабе предприятия, как их сети требованиям безопасности будет возрвстать, обеспечивая прочную защиту инвестиций. Предприятия могут увеличить свой IPSec и SSL VPN потенциал через многочисленные средства для поддержки большего числа мобильных работников на удаленных объектах, а также деловых партнеров. VPN потенциал может быть увеличен за счет использования комплексной кластеризации VPN и балансировки нагрузки, возможности Cisco ASA 5520 Адаптивная Security Appliance, а также более чем в два раза каждой платформы VPN потенциала путем установки VPN обновлении лицензии. Advanced прикладного уровня безопасности представленной Cisco ASA 5520 Адаптивная Security Appliance может быть увеличен путем размещения высокопроизводительных служб безопасности модуля.

С помощью факультативной безопасности контексте возможности Cisco ASA 5520 Адаптивная Security Appliance, предприятия могут разместить до 10 виртуальных межсетевых экранов на устройстве, чтобы характер контроля политик безопасности на уровне департаментов. Это позволяет укрепить безопасность сети.

3.7.2. D-Link - DFL-2500 [DFL-2500]

По мере того, как бизнес-процессы становятся все более зависимыми от сетевой инфраструктуры, капиталовложения, сделанные в решения по безопасности, становятся все более значимыми. D-Link представляет межсетевые экраны серии NetDefend нового поколения, являющиеся комплексным решением по обеспечению безопасности сетей предприятий. Серия NetDefend учитывает растущие требования, предъявляемые к сетевой безопасности, защите от атак хакеров, вирусным угрозам и повышению конфиденциальности информации. Каждый межсетевой экран этой серии обеспечивает высокий процент возврата инвестиций, благодаря поддержке широкого набора функций, гибкой настройке и высокому уровню защиты сети.

Устройства серии NetDefend представляют собой законченное решение в области безопасности, включающее встроенную поддержку межсетевого экрана, балансировки нагрузки, функций отказоустойчивости, механизма Zone-Defense, фильтрации содержимого, аутентификации пользователей, блокировки «мгновенных» сообщений и приложений P2P, защиты от атак «отказ в обслуживании» DoS. Эти устройства соответствуют требованиям предприятий к безопасности и удаленному доступу, обеспечивая высокопроизводительное решение по разумной цене. В межсетевых экранах гармонично объединены расширенные функции, предоставляющие администраторам сетей решение безопасности «все в одном» business-класса.

Для того чтобы минимизировать влияние аварийной ситуации на всю сеть, межсетевые экраны поддерживают специальную функцию - Zone-Defense, представляющую собой механизм, позволяющий им работать с коммутаторами локальных сетей D-Link и обеспечивающий активную сетевую безопасность. Функция Zone-Defense автоматически изолирует инфицированные компьютеры сети и предотвращает распространение ими вредоносного трафика.

Аппаратная спецификация межсетевых экранов NetDefend включает высокоскоростные процессоры, большие базы данных и вычислительные мощности, позволяющие обрабатывать до миллиона параллельных сессий. Устройства поставляются с несколькими, настраиваемыми пользователями интерфейсами, включая порты Gigabit Ethernet, позволяя развертывать гибкие, масштабируемые и свободные от «узких» мест сети, объединяющие между собой различные рабочие группы и предприятия.

Все межсетевые экраны данной серии поддерживают удаленное управление через Web-интерфейс или выделенное соединение. Они включают набор функций для мониторинга и поддержания состояния и безопасности сети, в том числе отправку уведомлений по email, ведение журнала системных событий и предоставление статистики в режиме реального времени. Эти функции, наряду с возможностью обновления программного обеспечения, гарантируют, что межсетевой экран сможет предоставить максимальную производительность и безопасность для сети.

3.7.3. D-Link - DFL-260 [DFL-260]

D-Link, лидер в предоставлении комплексных сетевых решений для SOHO и SMB, поставляющий широкий набор оборудования (от широкополосных модемов/маршрутизаторов до управляемых коммутаторов Fast/Gigabit Ethernet, а также оборудование для беспроводных LAN, IP-камеры и NAS), представляет высокопроизводительный межсетевой экран NetDefend

UTM, полностью удовлетворяющий потребностям бизнеса в создании интегрированной сети, включающей различные продуктовые линейки.

Межсетевой экран D-Link серии NetDefend UTM DFL-260 является надежным решением для обеспечения безопасности, позволяющим защитить офисы SMB от различных сетевых угроз. Этот межсетевой экран поддерживает трансляцию сетевых адресов (NAT), виртуальные частные сети (VPN), активную сетевую безопасность, систему предотвращении вторжений (IPS), фильтрацию Web-содержимого (WCF), антивирусную (AV) защиту и управление полосой пропускания – и весь этот функционал реализован в едином компактном настольном корпусе. При этом устройство может легко интегрироваться в существующую сеть.

Межсетевой экран для сетей SOHO DFL-260 обеспечивает законченное решение для управления, мониторинга и обслуживания безопасной сети. Среди функций управления: удаленное управление, политики управления полосой пропускания, блокировка по URL/ключевым словам, политики доступа и SNMP. Также поддерживаются такие функции сетевого мониторинга, как уведомление по e-mail, системный журнал, проверка устойчивости и статистика в реальном времени.

Производительность VPN DFL-260 поддерживает встроенный VPN-клиент и сервер, что позволяет работать практически с любой политикой VPN и осуществлять подключение филиалов к головному офису по безопасной сети. Пользователи, работающие на дому, также могут безопасно подключиться к сети для доступа к внутренним данным компании и получения электронной почты. DFL-260 поддерживает аппаратный VPN engine для поддержки и управления широким диапазоном сетей VPN. Это устройство поддерживает протоколы IPSec, PPTP и L2TP в режиме Клиент/Сервер и осуществляет обработку проходящего через него трафика.

Расширенные опции настройки VPN включают: шифрование ES/3DES/AES/Twofish/Blowfish/CAST-128, управление ключами IKE/ISAKMP или вручную, согласование режимов Quick/Main/Aggressive и поддержка

аутентификации VPN, используя внешний RADIUS-сервер или базу данных пользователей.

Unified Threat Management (UTM) DFL-260 оснащен системой обнаружения и предотвращения вторжений (IDP/IPS), антивирусом (AV) и фильтрацией Web-содержимого для проверки и защиты содержимого на 7 уровне. Используемый в данном устройстве аппаратный ускоритель увеличивает производительность IPS и AV, управляющей базы поиска в Web, содержащей миллионы URL для фильтрации Web-содержимого (WCF). Сервисы обновления IPS, антивируса и базы данных URL защищают офисную сеть от вторжений, червей, вредоносных кодов и удовлетворяют потребностям бизнеса по управлению доступом сотрудников к Интернет.

Мощная система предотвращения атак (IPS), использует уникальную технологию IPS – компонентные сигнатуры, которые позволяют распознавать и обеспечивать защиту, как против известных, так и против новых атак. В результате данное устройство помогает при атаках (реальных или потенциальных) значительно снизить влияние на такие важные аспекты, как полезная нагрузка, закрытая информация, а также предотвратить распространение инфекций и компьютерные вторжения. База данных IPS включает информацию о глобальных атак и вторжениях, собранную на публичных сайтах (например, National Vulnerability Database и Bugtrax). DFL-260 обеспечивает высокую эффективность сигнатур IPS, постоянно создавая и оптимизируя сигнатуры NetDefend через D-Link Auto-Signature Sensor System. Эти сигнатуры обеспечивают высокую точность обнаружения при минимальном количестве ошибочных срабатываний.

Фильтрация Web-содержимого помогает работодателям осуществлять мониторинг, управление и контроль использования сотрудниками предоставленного им доступа к Интернет. DFL-260 поддерживает несколько серверов глобальных индексов с миллионами URL и информацией в реальном времени о Web-сайтах, что позволяет увеличить производительность и обеспечить максимальную доступность сервиса. В этом межсетевом экране

используются политики с множеством параметров, а также белые и черные списки, что позволяет запретить или разрешить доступ в заданное время к Web-сайтам для любой комбинации пользователей, интерфейсов и IP-сетей. Эти устройства также позволяют обходить потенциально опасные объекты, включая Java-апплеты, Java-скрипты/VBS-скрипты, объекты ActiveX и cookies, активно обрабатывая содержимое Интернет.

Аппаратный ускоритель. Благодаря встроенным аппаратным ускорителям, межсетевой экран DFL-260 позволяет одновременно выполнять функции IPS и антивирусного сканирования, не снижая производительность межсетевого экрана и VPN. Помимо этого, аппаратные ускорители обеспечивают работу межсетевого экрана DFL-260 с большей производительностью, по сравнению с аналогичными межсетевыми экранами UTM, представленными на рынке.

3.7.4. D-Link - DFL-210 [DFL-210]

По мере того, как бизнес-процессы становятся все более зависимыми от сетевой инфраструктуры, капиталовложения, сделанные в решения по безопасности становятся все более значимыми. D-Link представляет ряд мощных решений нового поколения для защиты сетей предприятий Серия NetDefend учитывает растущие требования, предъявляемые к сетевой безопасности, защите от атак хакеров, вирусным угрозам и повышению конфиденциальности информации. Каждый межсетевой экран этой серии обеспечивает высокий процент возврата инвестиций, благодаря поддержке широкого набора функций, гибкой настройке и высокому уровню защиты сети.

Устройства серии NetDefend представляют собой законченное решение в области безопасности, включающее встроенную поддержку межсетевого экрана, балансировку нагрузки, функции отказоустойчивости, механизм Zone-Defense, фильтрацию содержимого, аутентификацию пользователей,

блокировку «мгновенных» сообщений и приложений P2P, защиту от атак «отказ в обслуживании» DoS и поддержку виртуальных локальных сетей VPN. Эти устройства соответствуют требованиям предприятий различного масштаба, от SOHO до Enterprise к безопасности и удаленному доступу, обеспечивая высокопроизводительное решение по разумной цене. В межсетевых экранах эффективно объединены расширенные функции, предоставляющие администраторам сетей решение безопасности business-класса «все в одном».

Для того, чтобы минимизировать влияние аварийной ситуации на всю сеть, межсетевые экраны поддерживают специальную функцию - Zone-Defense, представляющую собой механизм, позволяющий им работать совместно с управляемыми коммутаторами D-Link и обеспечивающий активную сетевую безопасность. Функция Zone-Defense автоматически изолирует инфицированные компьютеры сети и предотвращает распространение ими вредоносного трафика.

Аппаратная спецификация межсетевых экранов NetDefend включает высокоскоростные процессоры, базы данных и вычислительные мощности, позволяющие обрабатывать до миллиона параллельных сессий. Эти межсетевые экраны поставляются с несколькими сетевыми интерфейсами, настраиваемыми пользователями, включая порты Gigabit Ethernet, позволяя развертывать гибкие, масштабируемые и свободные от «узких» мест сети, объединяющие между собой различные рабочие группы и предприятия.

Все межсетевые экраны серии NetDefend поддерживают удаленное управление через Web-интерфейс, как из локальной подсети, так и через выделенное VPN-соединение.

Устройства также включают в себя набор функций для мониторинга и поддержания состояния и безопасности сети, в том числе отправку уведомлений по электронной почте, ведение журнала системных событий и предоставление статистики в режиме реального времени. Эти функции, наряду с возможностью обновления программного обеспечения, гарантируют, что

межсетевой экран сможет предоставить максимальную производительность и безопасность для сети.

Основные характеристики МЭ, представлены в таблице 5.

Таблица 5 - Сравнительная таблица

Характиристики	**Название**			
	D-Link - DFL-2500	**2 D-Link - DFL-260**	**2 D-Link - DFL-210**	**Cisco ASA 5520**
Пропускная способность МСЭ, Мбит/с Пропускная способность VPN IPSec (AES), Мбит/с	150/60	80/25	80/25	100/30
Количество портов	40	25	25	25
Предотвращение DoS/DDoS-атак	есть	есть	есть	есть
Отказоустойчивость:	высокая	средняя	средняя	средняя
Балансировка нагрузки	есть	есть	есть	есть
Стоимость в руб.	154475 руб	20439 руб	16346 руб.	17540 руб.

Из таблицы 5 видно, что оптимальным средством Cisco ASA 5520. Это устройство соответствует требованиям предприятия к безопасности и удаленному доступу, обеспечивая высокопроизводительное решение по разумной цене.

Учитывает требования, предъявляемые к сетевой безопасности, защите от атак хакеров, вирусным угрозам и повышению конфиденциальности информации. Межсетевой экран этой серии обеспечивает высокий процент возврата инвестиций, благодаря поддержке широкого набора функций, гибкой настройке и высокому уровню защиты сети.

Вид антивирусной защиты частного компании, после монтажа, установки и настройки ПО.

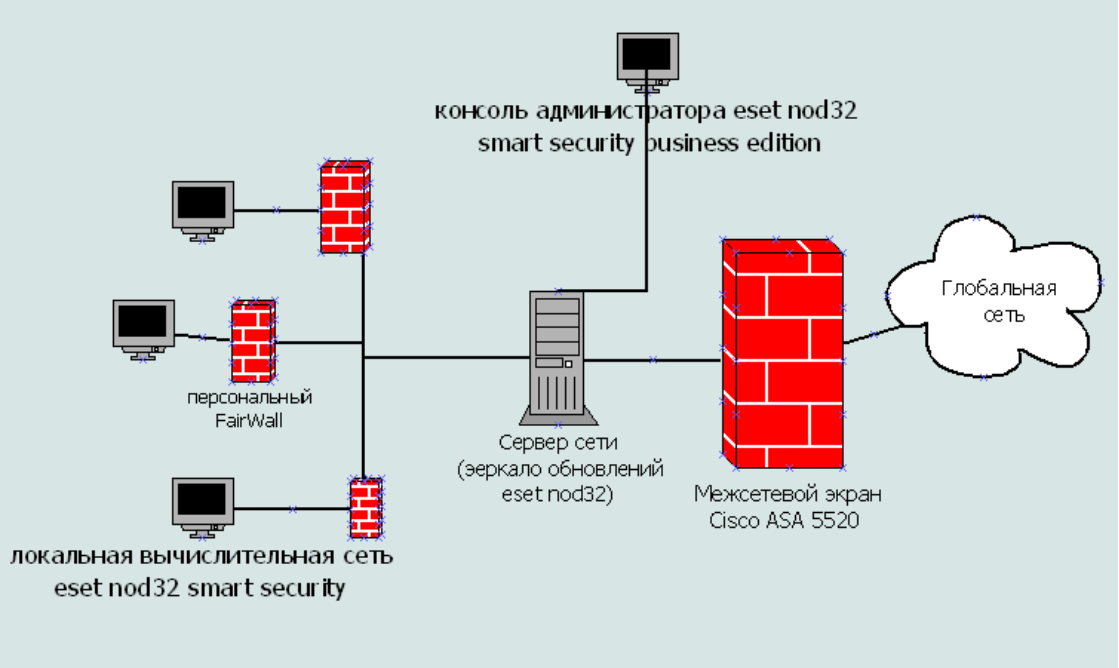

Рисунок 4.4 - Защищенная сеть

Выводы:

- Была построена система антивирусной защиты предприятия «Навиком»
- Выбран антивирусное программное обеспечение, по результатам анализа
- Выбран защита аппаратной части
- Не стал использовать антивирусы для Android так как на сегодняшний момент они не могут обеспечить надежную защиту телефонов, и покупка такого продукта является бес полезным.

3.8. РАСЧЁТ ЗАТРАТ НА РАЗРАБОТКУ И ВНЕДРЕНИЕ ИС.

3.8.1. Расчет затрат на разработку ИС

В состав затрат на разработку системы ($К_Р$) входят:

- затраты на заработную плату разработчиков, $FC_{зп}$, руб.;
- отчисления в Государственные внебюджетные фонды, $Н_{стр.в}$, руб.;
- затраты на материалы (без НДС), $FC_{МР}$, руб.;
- затраты на электроэнергию (без НДС), $FC_{ЭР}$, руб.;
- амортизационные отчисления, FA_t, руб.;
- накладные расходы, $FC_{НР}$;

3.8.2. Затраты на заработную плату разработчиков

Прежде, чем подсчитать затраты на заработную плату разработчиков, следует составить перечень работ, из которых складывается процесс разработки дипломного проекта. Перечень работ, соответствующий содержанию (плану) магистерской работы, следует представить в таблице 1.2. В этой же таблице приводятся остальные данные, необходимые для расчета.

Затраты на заработную плату разработчиков рассчитывают по следующей формуле:

$FC_{зп}= к_д * l_{дн(1400)} * t_Р$=85751,47 рублей (4.1)

где $k_д$ - коэффициент, учитывающий дополнительную заработную плату. Его принимают 1,1;

$t_Р$ – продолжительность выполнения работ по разработки ИС в днях;

$l_{дн}$ - среднедневная ставка заработной платы. (1400 рублей)

После этого следует определить ожидаемую трудоемкость выполнения i-й работы:

$T_i = (3T_{min} + 2T_{max})/5$, (4.2)

T_{min} – минимальная трудоемкость работы при наиболее благоприятных условиях,

T_{max} – максимальная трудоемкость работы при наиболее неблагоприятных условиях ее выполнения.

Таблица 6 - Ожидаемая трудоемкость работ

Наименование работ	τ_{min}чел. дни	τ_{max}чел. дни	τ_iчел. дни
затраты труда на подготовку описания задачи	1	3	1,8
затраты труда на исследование решения задачи	1	4	2,2
затраты труда на исследование сетевой архитектуры	1	2	1,4
затраты труда на настройку	10	18	13,2
затраты труда на отладку	2	5	3,2
затраты труда на подготовку документации	1	4	2,2
ИТОГО			37,2

Продолжительность работ рассчитывается по формуле:

$$t = \frac{\tau_i \cdot (1+\alpha)}{R_i \cdot k_B} \quad (4.3)$$

где α – доля дополнительных работ, выполняемых данной группой исполнителей, данный коэффициент может принимать значения от 0 до 0,4;

R_i – число исполнителей i–й работы, человек (определяется по фактическим данным, результаты заносятся в таблицу 7;

$k_в$ – коэффициент использования разработчиками сменного времени,

$k_в$ = $К_{р.д.}$/$К_{к.д.}$ = 247/365= 0,68.

Таблица 7 - Состав, трудоемкость и продолжительность работ

Наименование работ	τ_iчел. дни	R_iчел.	t_iдни
затраты труда на подготовку описания задачи	1,8	1	3,17
затраты труда на исследование решения задачи	2,2	1	3,88
затраты труда на исследование сетевой архитектуры	1,4	1	2,47
затраты труда на настройку			
затраты труда на отладку	13,2	1	23,29
затраты труда на подготовку документации	3,2	1	5,64

ИТОГО:$t_P = \sum t_i$			65,6

4.1.3 Затраты на материалы

В данной статье учитываются затраты на расходные материалы, комплектующие, канцелярские товары и технические средства, стоимостью менее 40 тысяч рублей, которые необходимы разработчикам для осуществления проекта.Эти затраты рассчитывают по формуле:

$$FC_{MP} = \sum_{i=1}^{n} P_{Mi} \cdot m_i = 27\ 717 \quad \text{рублей (4.4)}$$

где P_{Mi} – цена i–го вида материала без НДС, руб./ед.;

m_i – количество используемого материала i–го вида, ед.

Исходные данные для расчета следует представить в таблице 8.

Таблица 8 - Цена материалов, покупных изделий и технических средств (стоимостью менее 40 тыс. рублей) для разработки системы

№	Наименование материалов	Кол-во, единиц	Цена, руб./ед.*	Сумма, рублей
1	Бумага SvetoCopyA4	1	190	190
2	Картридж EpsoC13T	1	1299	1299
Итого FC_M				1489
№	Наименование технических средств, стоимостью менее 40 тыс.руб.	Кол-во, единиц	Цена, руб./ед.*	Сумма, рублей
1	Ноутбук Lenovo IdeaPad G700	1	25190	25190
2	Компьютерная мышь A4TECH R4 Black	1	1599	1599
3	Принтер Epson L210	1	12799	6099
Итого FC_{TC}				39 588
Итого FCмр = FCм + FCтс				41 077

Бумага SvetoCopyA4 - http://mkontora.com/shop/UID_845.html?from=yandexmarket

Картридж Epson C13T - http://www.komus.ru/product/95669/?utm_campaign=GMC-msk&utm_source=google_gmc&utm_medium=cpc&utm_content=95669&utm_term=95669

Ноутбук Lenovo IdeaPad G700 - http://www.mvideo.ru/products/noutbuk-lenovo-ideapad-g700-59387364-30022034

Компьютерная мышь A4TECH R4 - http://www.eldorado.ru/cat/detail/71088096/?category=2582505

Принтер Epson L210 - https://market.yandex.ru/product--epson-l210/8527156?ncrnd=6286

4.1.4.Затраты на электроэнергию

Эти затраты рассчитывают по формуле

$$FC_{эр} = C_э * \sum (W_{Эi} * t^ч_i) = 1628{,}07 \text{ рублей} \quad (4.5)$$

где $C_э$ – тариф на электроэнергию без НДС, руб./кВтч (Указывается тариф, сложившийся на дату расчета в соответствии нормативами, можно принять 4,78 руб);

$W_{Эj}$ – потребляемая используемыми на i-й работе техническими средствами мощность, кВт;

$t^ч_i$ – время выполнения i-й работы в часах, для определения $t^ч_i$можно использовать данные таблицы 9 и среднее время работы техники за день в часах (из табл.1.3 t_i*8).

Таблица 9 - Затраты на электроэнергию

Наименование работ	$t^ч_i$	$W_{Эi}$	$W_{Эi} * t^ч_i$ кВт
затраты труда на подготовку описания задачи	21,18	0,65	13,76
затраты труда на исследование решения задачи	25,88	0,65	16,82
затраты труда на исследование сетевой архитектуры	16,47	0,65	10,71

Наименование работ	$t^ч_i$	$W_{Эi}$	$W_{Эi} * t^ч_i$ кВт
затраты труда на настройку	155,29	0,65	100,94
затраты труда на отладку	37,65	0,65	24,47
затраты труда на подготовку документации	25,88	0,65	16,82
Установка системы	21,18	0,65	16,25
Тестирование	37,65	0,65	29,25
ИТОГО: $\sum (W_{Эi} * t^ч_i)$			340,6

4.1.6. Накладные расходы при разработке

Под накладными расходами понимаются следующие расходы разработчика. Коммунальные платежи: водоснабжение, отопление, освещение; затраты на заработную плату административно-управленческого, вспомогательного и обслуживающего персонала (АУП и ВОП) с отчислениями во внебюджетные государственные фонды; контрагентские расходы, т.е. оплата работ, выполняемых сторонними организациями, налоги, начисленные в установленном законом порядке, арендные платежи, расходы на техническое обслуживание и ремонт технических средств.

$FC_{нр} = 0,5* (FC_{мр} + FC_{эр} + 1,3* FC_{зп}) = 76\,956,84$ рублей (4.6)

Таблица 10 - Затраты на разработку ИС

№ п/п	Статьи затрат	Условные обозначения	Значение
1	Затраты на заработную плату разработчиков	$FC_{зп}$	85 751,47
2	Отчисления в Государственные внебюджетные фонды от затрат на заработную плату разработчиков	$Н_{стр.в}$	25 725,44
3	Затраты на материалы	$FC_{мр}$	41 077,00
4	Затраты на электроэнергию	$FC_{эр}$	1 359,77
5	Накладные расходы	$FC_{нр}$	76 956,84
	Итого затрат на разработку	$К_Р$	230 870,52

Цена разработки при использовании ИС рассчитывается по формуле:

$$Ц_{разр} = К_{р} \cdot (1 + \frac{Р_{разр}}{100}) = 288550{,}65 \quad (4.7)$$

где $Р_{разр}$ – рентабельность разработчика. Может приниматься от 25 до 30%.

3.8.3. Расчёт затрат на внедрение ИС

В состав затрат на внедрение следует включать:

- затраты на приобретение дополнительного оборудования для внедрения ИС, стоимостью более 40 тысяч рублей;
- затраты на приобретение дополнительных производственных площадей для внедрения ИС, руб.;
- затраты на подготовку персонала для работы с ИС, руб.

В этом разделе экономической части следует указать, что необходимо приобрести и подготовить пользователю ИС, для того, чтобы предлагаемая информационная система успешно функционировала.

3.8.4. Затраты на подготовку персонала

Эти затраты рассчитывают по формуле

$FC_{пп} = Ц_{подг} * R_{спец}$ = 7000 рублей (4.8)

где $Ц_{подг}$ – цена подготовки одного специалиста. $Ц_{подг}$ = 7000 руб.;

Результаты расчета затрат на внедрение следует привести в таблице 11

Таблица 11 - Затраты на внедрение системы

№ п/п	Статьи затрат	Условные обозначения	Сумма, руб.
1	Затраты на подготовку персонала	$FC_{пп}$	7 000
	Итого	$К_{внед}$	7 000

Необходимая сумма инвестиций на разработку и внедрение подсистемы на предприятии определяется по формуле, в зависимости от варианта проекта:

$К_{инв}=Ц_р + К_{внед}$= 237 870,52 рублей (4.9)

4.2.3 Расчет изменения эксплуатационных расходов в плановом периоде при внедрении системы на предприятии.

При расчете проекта необходимо определить изменение в расходах потребителя при использовании ИС ($ТС_и$). Расходы необходимо разделить на постоянные ($FC_и$) и переменные ($VC_и$).

$ТС_и = FC_и + VC_и$ (4.10)

Внутри каждой группы выделяются следующие статьи расходов: материальные, оплату труда и страховые взносы во внебюджетные фонды, амортизацию.

При расчете необходимо все изменения расходов потребителя разделить на две группы. Первая группа, дополнительные расходы потребителя при внедрении информационной системы ($ТС^{доп}$). Вторая – экономия на расходах за счет использования ИС ($ТС^{эк}$). В каждой группе расходы также подразделяются на постоянные и переменные.

$ТС_и = ТС^{доп} - ТС^{эк}$ (4.11)

Расчет первой группы показателей проводится в следующей последовательности.

$ТС^{доп} = FC^{доп} + VC^{доп}$ (4.12)

3.8.5. Дополнительные затраты на заработную плату персонала, обслуживающего ИС.

Эти затраты рассчитывают по следующей формуле:

$VC_{зи}^{доп} = 1,1* t * l_{дн} *R =$ 1.1*46,93*1400*1 = 72 272,2 рублей (4.13)

где t - продолжительность выполнения функций с использованием ИС, дн.;

R – количество дополнительного персонала для работы с ИС, чел.;

$l_{дн}$ - средняя дневная ставка персонала, руб.

1 человек 3 раза в неделю по 3 часа рабочего времени

8*6 = 48 час. раб.

3*3 = 9 час. раб.

$$\alpha = \frac{9}{48} = 0.19$$

$$t = \alpha * 247 = 46{,}93$$

3.8.6. Отчисления в Государственные внебюджетные фонды от затрат на заработную плату персонала

Их рассчитывают по следующей формуле:

$VH_{стр.в}^{доп} = 0{,}3 * VC_{зп}^{доп}$ = 21 681,66 рублей (4.14)

3.8.7. Дополнительные затраты на электроэнергию, связанные с выполнением функций ИС

Затраты на электроэнергию рассчитывают по формуле:

$VC_{эи}^{доп} = C_э * \sum (W_{Эi} * t^ч_i)$, (4.15)

где $C_Э$ – тариф на электроэнергию без НДС, руб./кВтч;

$W_Э$ – потребляемая мощность, кВт;

t - продолжительность использования системы в течение года, час.

Результаты расчетов представлены в таблице 12.

Таблица 12 - Расход электроэнергии на выполнение функций системы

№	Название прибора	Кол-во, единиц	Потребляемая мощность, $W_{эi}$, кВт	Время работы, t_i час	$W_{эi} * t_i$, кВтч
1	Персональный	30	0,65	44,46	202,29

№	Название прибора	Кол-во, единиц	Потребляемая мощность, $W_{эi}$, кВт	Время работы, t_i час	$W_{эi} * t_i$, кВтч
	компьютер				
2	Сервер	1	4	44,46	177,84
Итого:					200,2

t = 46,93 * 8 * 0.19= 71,33

$VC_{эи}^{доп}$ = 4.78 *380,13= 956,95рубля

3.8.8. Амортизационные отчисления

$FA_{и}^{доп} = FC_{об} * На/100 + Ц_{разр} / Т_{ис}$ = 0 + 422740,76/10 = 42274,08 рублей (4.16)

где $FC_{об}$ - балансовая стоимость оборудования (стоимостью более 40 тыс.руб.), используемого при функционировании системы ($FC_{об}$ = 0**)**

$Т_{ис}$ - срок полезного использования системы, годы, если данный срок не регламентирован соглашение или другими нормативными актами, принимаем 10 лет.

Если в процессе анализа будут выявлены дополнительные виды затрат, обусловленные спецификой деятельности потребителя, их также необходимо будет учесть в данном расчете.

$FC^{доп} = FA_{и}^{доп}$ (4.15)

$VC^{доп} = VC_{зи}^{доп} + VH_{стр.в}^{доп} + VC_{ми}^{доп} + VC_{эи}^{доп}$ (4.16)

$VC^{доп}$ = 72 272,2 + 21 681,66 + 0 1817,02 = 95770,88 рублей

3.8.9. Расчет экономии на расходах потребителя.

Расчет второй группы показателей проводится в следующей последовательности.

$TC^{эк} = FC^{эк} + VC^{эк}$ (4.17)

Основными возможными источниками экономии на расходах потребителя являются снижение трудоемкости выполнения работ и, следовательно, снижения заработной платы исполнителей и соответственно

отчислений в государственные внебюджетные фонды, а также снижение нормы расхода основных материалов. Например, внедрение ИС позволит автоматизировать ежемесячный отчет по продажам потребителя. До внедрения системы данную отчетность формировали 3 исполнителя в течении 5 рабочих дней. Среднедневная ставка исполнителя 1500 руб/дн. Тогда ежегодная экономия на заработной плате исполнителей составит:

$VC_{зи}^{эк} = 1,1* t * l_{дн} *R* m = 1,1*5*1400*7*12 = 646\ 800$ рублей.

где m – количество месяцев в году.

Ежегодная экономия на страховых взносах во внебюджетные государственные фонды исполнителей составит:

$VH_{стр.в}^{эк} = 0,3* VC_{зи}^{эк} = 194040$ рублей.

$VC_{и} = VC^{доп} - VC^{эк}$

$FC_{и} = FC^{доп} - FC^{эк}$

Результаты расчета изменения расходов потребителя с использованием ИС приведены в таблице 13.

Таблица 13-Изменение расходов потребителя с использованием ИС

№	Статьи затрат	Сумма, руб.
1	Дополнительные переменные расходы потребителя	110995,456
2	Дополнительные постоянные расходы потребителя	23787,05218
3	Итого дополнительные расходы потребителя	134782,5082
4	Экономия на переменных расходах потребителя	1467180
5	Экономия на постоянных расходах потребителя	840840
6	Итого экономия на расходах потребителя	491557,4918

3.9.Расчет экономической эффективности проекта

3.8.10. Финансовый план (расчет эффективности инвестиций в разработку и внедрение системы) расчет ЧДД проекта

Одним из основных показателей оценки эффективности реализации проекта (инвестиций) является показатель чистого дисконтированного дохода (ЧДД). Дисконтирование — приведение экономических показателей разных лет к сопоставимому по времени виду (в бакалаврской работе к началу реализации проекта) путем умножения этих показателей на коэффициент дисконтирования.

Коэффициент дисконтирования, рассчитываемый по формуле:

$$\alpha_{t=} \quad \frac{1}{(1+E)^t} \qquad (4.18)$$

где α_t — коэффициент дисконтирования;

t — расчетный период (в годах);

E — норма дисконта, которая может быть, как единой для всех шагов расчета, так и переменной.

Величина ЧДД для постоянной нормы, дисконта вычисляется по формуле:

$$ЧДД=\sum_{t=0}\{(Пч_t+FA_t)*\alpha_t\}-\sum_{t=0}(K_t*\alpha_t) \qquad (4.19)$$

При этом величины FA_t и K_t принимаются постоянными:

$$K_t = K_0 = K_{инв} \quad (4.20)$$

$$FA_t = FA_и^{доп} \quad (4.21)$$

Таблица 14 - Расчет ЧДД

Наименование	Годы расчетного периода		
	0	1	2
Капиталовложения, K_t	237 870,52	0,00	0,00
TRдоп	0,00	0,00	0,00
TCи	0,00	-491 557,49	-491 557,49
Чистая прибыль, $Пч_t$	0,00	393 245,99	393 245,99
Амортизационные отчисления, A_t	0,00	23 787,05	23 787,05
Пчt+At	0,00	417 033,05	417 033,05
Пчt+At-Kt	-237 870,52	417 033,05	417 033,05
ЧД= $\sum (П_{чt}+A_t-Kt)$	-237 870,52	179 162,52	596 195,57
Коэффициент дисконтирования, α_t	1,000	0,901	0,812
Дисконтированые капвложения, $K_t*\alpha_t$	237 870,52	0,00	0,00
Дисконтированная прибыль,(Пчt+At)*α_t	0,00	375 705,45	338 473,38
(Пчt+At)*αt-Kt*αt	-237870,5218	375705,4465	338473,3752
ЧДД=∑((Пчt+At)*αt-Kt*αt)	-237 870,52	137 834,92	476 308,30
Коэф-т дисконтирования	1,000	0,901	0,812

Проект признается эффективным, если значение ЧДД>0.

Сроком окупаемости (с учетом дисконтирования - $Т^{Д}_{ок}$), называется период времени от начального момента, до момента после которого текущий чистый дисконтированный доход ЧДД становится неотрицательным.

Индекс доходности дисконтированных инвестиций (ИДД) представляет собой отношение суммы приведенных эффектов к величине капиталовложений

ИДД=$\Sigma(П_{чt}+FA_t)*\alpha_t/\Sigma(K_t*\alpha_t)$ = 3385217,72/ 429740,76= 4,87 (4.22)

Индекс доходности тесно связан с ЧДД: если ЧДД положителен, то ИДД>1 и наоборот. Если ИДД>1, проект эффективен, если ИИД<1 - неэффективен.

Выводы.

1. ЧДД =476 308,3 рублей.

2. Простой срок окупаемости проекта: $Т_{ок}$ = 1 году. Срок окупаемости с учетом дисконтирования: $Т^{Д}_{ок}$ = 1 году.

3. ИДД =4,87.
4. Проект признается эффективным.

4. ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ПОЛУЧЕННЫХ РЕШЕНИЙ (DISCUSSIONS)

В своей работе в качестве методов исследования руководствовался иностранными научными статьями. Многие авторы считаю, что одной из основных показателей для выбора антивирусного программного обеспечения является влияние его на скорость работы ПО. В рамках данного исследования проводил тесты, такие как:

- Влияние антивирусов на загрузку операционной системы
- Скорость работы антивирусных мониторов в реальном времени
- Среднее время открытия файлов и приложений

4.1.Влияние антивирусов на загрузку операционной системы.

Длительность запуска операционной системы является хорошим показателем влияния на время работы компьютера. Таким образом мною 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, я узнал, как они влияют на время загрузки ОС. Для каждой антивирусной продукции я провел тесны 10 раз для чистоты эксперимента. Результаты тестов представлены ниже на рисунке 5.1:

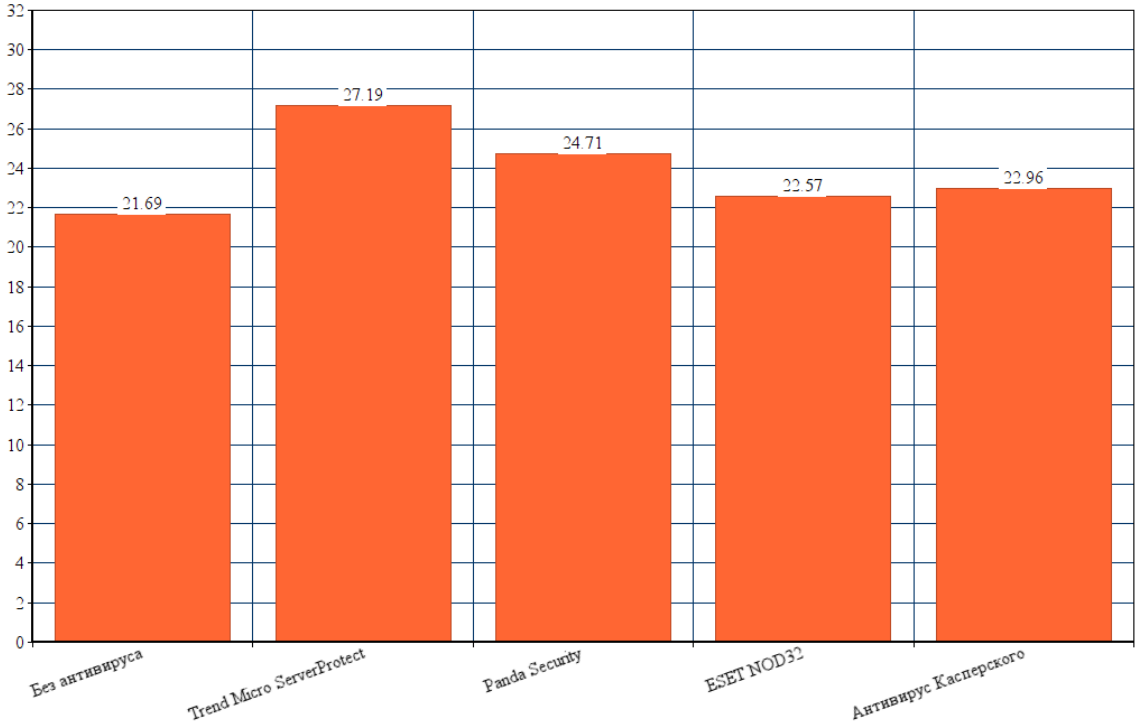

Рис. 5.1 - Влияние антивирусов на загрузку системы.

Из диаграммы следует что, Наименьшее время влияния на загрузку системы оказал ESET Nod32 антивирус, однако Антивирус Касперского показал приблизительно такие же результаты что и ESET Nod32. Самое плохое время оказалось у Антивируса Trend Micro ServerProtect.

4.2. Скорость работы антивирусных мониторов в реальном времени.

Важным элементом 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 защиты у выбранных мною антивирусов я провел следующий тест.

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 объём составил 6.06 Гб.

Результат теста представлен ниже на рисунке 5.2:

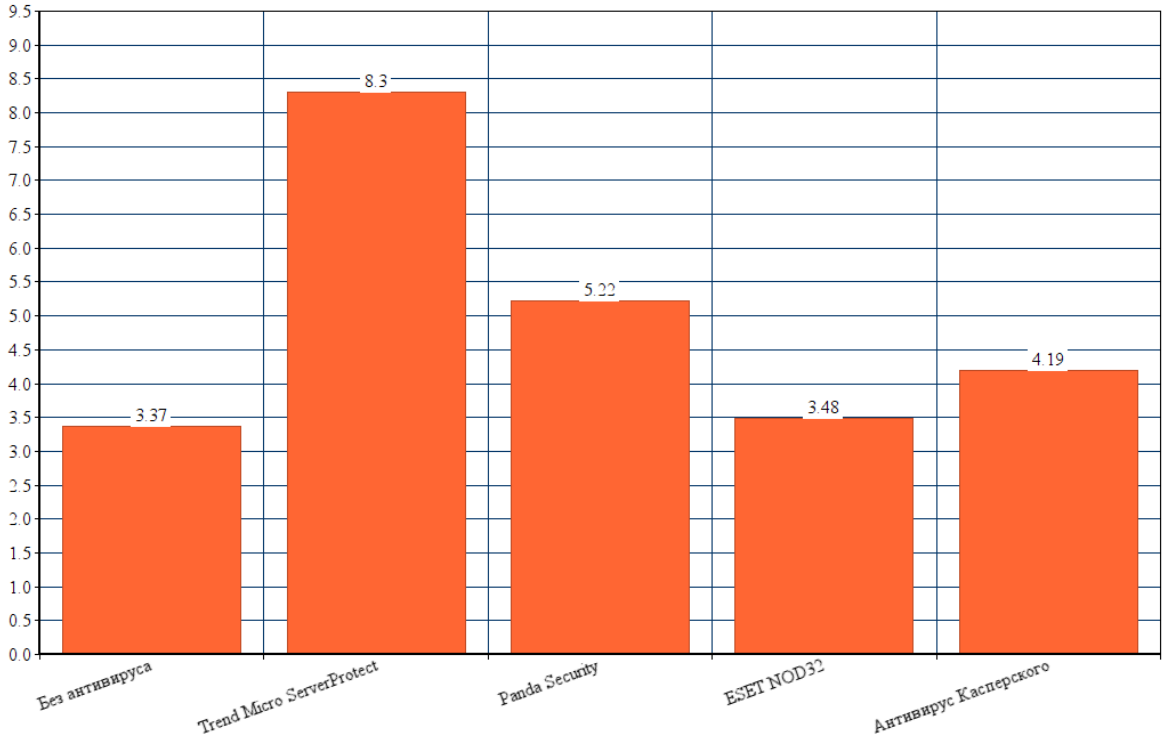

Рисунок 5.2 - Скорость работы антивирусных мониторов в реальном времени.

Наихудшим образом себя проявил Trend Micro ServerProtect антивирус, время копирования папки с установленным антивирусом и включенным монитором защиты в реальном времени по сравнения 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.

4.3. Среднее время открытия файлов и приложений.

Помимо сказанного ранее, антивирусное ПО может повлиять на время открытия приложений и файлов. Для этого были проведены измерения времени запуска приложений с помощью утилиты AppTimer. Так как большинство программ мы запускаем не вручную, а по открытию определенного файла, в проводимом тесте приложения использовались не напрямую, а с помощью пяти больших файлов. В качестве приложений использовались офисные программы: Microsoft Word и Microsoft Power Point,

просмотрщик pdf-файлов Adobe Reader, графический редактор Adobe Photoshop, а также программа для просмотра графических файлов WinDjView.

Так же хотелось бы отметить, что на скорость открытия файла сильно влияет запускается он первый раз после загрузки ОС или же нет. Дело в том, что при первом запуске все системные файлы приложения считываются с жесткого диска в оперативную память, а при повторном система помешает ваши файлы в оперативную память, что существенно увеличивает скорость их последующей загрузки. Для чистоты эксперимента все измерение времени всех файлов производилось сразу после загрузки ОС без повторного открытия.

Результаты представлены на рисунке 5.3.

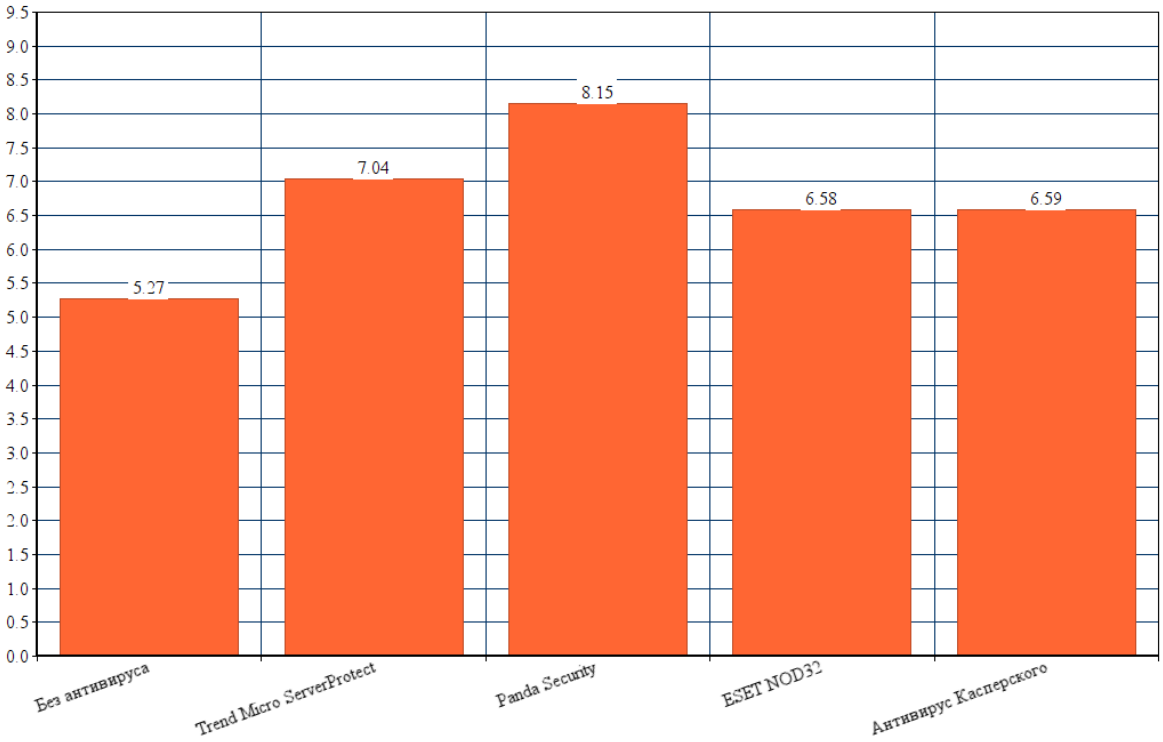

Рисунок 5.3 - Среднее время открытия файлов и приложений.

Различие между антивирусами Касперского и ESET Nod32 оказались минимальными, и пользователь вряд ли сможет почувствовать разницу. Однако антивирус Panda Security оторвался от всех остальных кандидатов, в худшую сторону.

4.4. Математическое исследование эффективности предложенных решений.

Одним из способов исследований является математическое моделирование распространения вредоносных программ. Оно лучше всего показывает статистику распространения вирусов в разработанной системе защиты сети.

Исследования показывают, что лучше всего заражение компьютерными вирусами описывают модели, из математической теории биологических эпидемий. Большинство авторов для описания компьютерной эпидемии пользуются моделями типа SI, SIR и SEIR. В данном исследовании рассмотрена модель MSEIRS, которая достаточно полно описывает развитие эпидемии для популяции людей. Например, модель MSEIRS предусматривает латентный период заболевания, то есть когда объект заражен, но вирус еще не распространяет. Данную биологическую модель можно модифицировать для лучшего описания разрушительных воздействий вируса на работу компьютерной сети организации если, подключаемые новые узлы изначально обеспечены антивирусной защитой. В такой системе, каждый компьютер в сети может находиться в одном из пяти состояний: уязвимом, вновь подключенном с установленным антивирусным ПО, инфицированном, латентном (инфицирован, но не распространяет вирус), невосприимчивом к вирусу. Работа этой системы схематично отображена на рисунке 5.4.

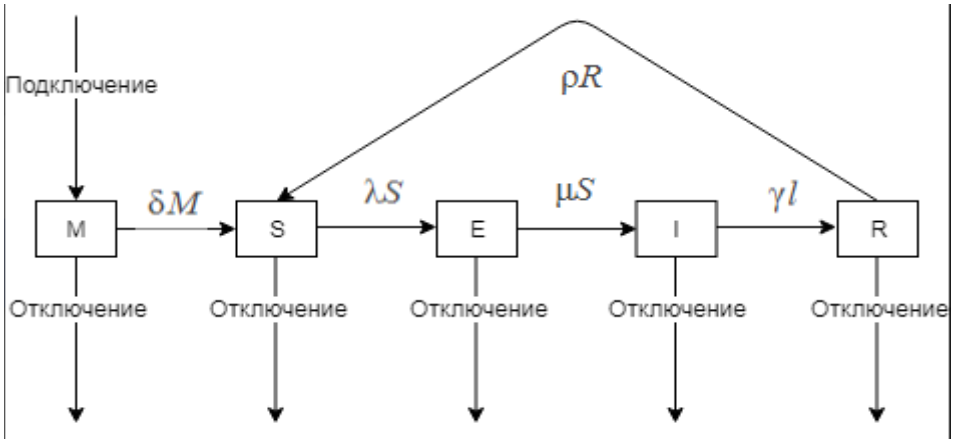

Рисунок 5.4 – Схема модели MSEIRS

Для описания модели использованы следующие переменные и постоянные величины: θ – параметр, скорости увеличения новых уязвимых компьютеров; β – характеристика скорости инфицирования уязвимых хостов; μ – параметр, определяющий частоту отключения узлов от сети (не зависит от вируса); δ – параметр, характеризующий скорость, с которой невосприимчивые хосты вновь становятся уязвимыми; ε – параметр, характеризующий средний период, когда компьютер является зараженным, но сам вирус не активен; γ – параметр, оценивающий скорость обновления антивирусных баз. N(t) – суммарное число компьютеров в сети в момент времени t; S(t) – число уязвимых компьютеров в момент времени t; M(t) – число новых машин в момент времени t; E(t) – число зараженных компьютеров (до того как компьютер повредил зараженный узел) в момент времени t (латентная стадия); I(t) – количество инфицированных узлов в момент времени t; R(t) – число компьютеров не подверженных заражения в момент времени t;

В любой момент времени будет выполняться условие M(t)+S(t)+E(t)+I(t)+R(t) = N(t).

Процесс вредоносных воздействий вируса на сеть компании описывается системой дифференциальных уравнений со следующими начальными условиями:

$$\frac{\partial M}{\partial r} = \theta N - (\delta + \mu)M \quad M(0) = M0,$$

$$\frac{\partial S}{\partial r} = \delta M - \frac{\beta SI}{N} - \mu S + \delta R \quad S(0) = S0,$$

$$\frac{\partial E}{\partial t} = \frac{\beta SI}{N} - (\varepsilon + \mu)E \quad E(0) = E0, \qquad (5.1)$$

$$\frac{\partial I}{\partial t} = \epsilon E - (\gamma + \mu) I \quad I(0) = I0,$$

$$\frac{\partial R}{\partial t} = \gamma I - (\delta + \mu) R \quad R(0) = R0.$$

Непрерывные функции M(t), S(t), E(t), I(t), R(t) можно считать фазовыми переменными. Будем рассматривать коэффициент γ как кусочно-непрерывную функцию управления, которая имеет следующие ограничения

0£g(t)£Ymax£1, tÎ[0, T], (5.2)

где Ymax – характеризует экономические и технические возможности организации и является максимальной нормой управления.

Для определения защищенности компьютерной сети будем исходить из условия, что в конечный момент времени данного нам периода большее количество узлов в сети (более 80 %) невосприимчивы к заражению. в таком случае будем использовать метод штрафных функций [7], и вся задача управления будет заключаться в минимизации функционала

$$I(\gamma) = Amax((0, 8N(T) - R(T)), 0)^2 \quad (5.3)$$

где N(T) = M(T)+S(T)+E(T)+I(T)+R(T) – суммарное количество компьютеров в сети в конечный момент времени, где A > 0 – штрафной параметр.

В результате получаем непрерывную задачу оптимального управления (5.1)–(5.3). С помощью принципа максимума Понтрягина можно свести исходную задачу (5.1)–(5.3) к решению краевой. Однако получение решения краевой задачи в аналитическом виде довольно сложно и поэтому требует применения численных методов.

Для численного решения задачи (5.1)–(5.3) построим ее дискретную аппроксимацию, используя явную разностную схему. На отрезке [0, T] введем равномерную сетку {tk = Dtk, 0 £ k £ L} с шагом Dt = T/L. Обозначим значения фазовых функций и функции управления в точках разбиения

следующим образом: M(tk) = Mk, S(tk) = Sk, E(tk) = Ek, I(tk) = Ik, R(tk) = Rk, γ(tk) = γk, k=$\overline{0,L}$.

Дискретная задача оптимального управления при k=$\overline{0,L-1}$примет вид

$$I = A[max\{0,8N^L - R^L;0\}]^2 \to inf$$

$$M^{k+1} = M^k + \Delta t(\Theta N^k - (\delta + \mu)M^k)$$

$$S^{k+1} = S^k + \Delta t(\frac{\beta S^k I^k}{N^k} - \mu S^k + \delta R^k)$$

$$E^{k+1} = E^k + \Delta t(\delta M^k - \frac{\beta S^k I^k}{N^k} - \mu S^k + \delta R^k)$$

$$E^{k+1} = E^k + \Delta t(\frac{\beta S^k I^k}{N^k} - (\varepsilon + \mu)E^k$$

$$I^{k+1} = I^k + \Delta t(\varepsilon E^k - (\gamma^k + \mu)I^k)$$

$$R^{k+1} = R^k + \Delta t(\gamma^t I^k - (\delta + \mu)R^k)$$

$$M^\theta = M_\theta,\ S^\theta = S_\theta,\ S^\theta = S_\theta,\ I^\theta = I_\theta,\ R^\theta = R_\theta$$

$$0 \le \gamma^E \le Y_{max} \le 1$$

Для построения приближенного оптимального решения воспользуемся методом проекции градиента. При этом рекуррентные формулы для определения сопряженных векторов получаем из условий стационарности функции Лагранжа.

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. В таблицах 14 и 15 представлены вводимые экспериментальные данные.

Таблица 14 - 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

Таблица 14 - Параметры антивирусного 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

На рисунке 5.5 показаны траектории динамики функций, характеризующие количество компьютеров разных типов, и функции управления.

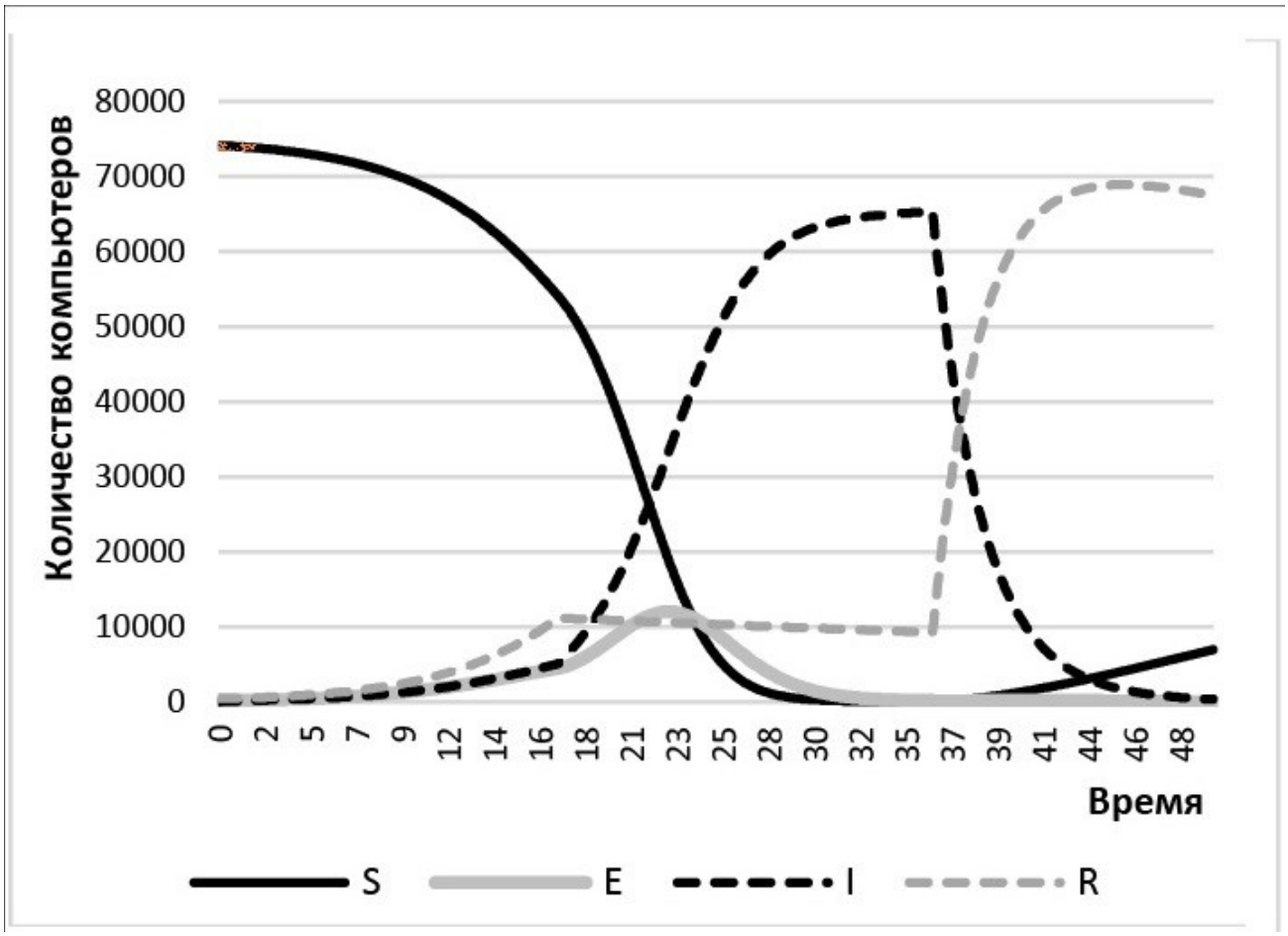

Рисунок 5.5 – График распространения вирусов.

На приведенном графике можно заметить, что при большой скорости распространения вредоносного кода за рассматриваемый период удается 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