МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

кафедра Компьютерных технологий

«Допущен к защите»
Заведующий кафедрой _____
_____
(Ф.И.О., ученая степень, звание)
_____ «_____»_____ **20__ г.**
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Разработка централизованного управления антивирусной защитой сети среднего предприятия.

Специальность Вычислительная техника и программное обеспечение

Выполнил (а) Филимонов Михаил Николаевич БВТу-10
(Фамилия и инициалы) группа

Научный руководитель Мусапирова Г.Д., к.т.н., стар. преподаватель
(Фамилия и инициалы, ученая степень, звание)

Консультанты:
по экономической части:
_____
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20___г.
(подпись)

по безопасности жизнедеятельности:
Шайдарбекова М.К., к.х.н., доцент
(Фамилия и инициалы, ученая степень, звание)
_____ «12» 06 20 14 г.
(подпись)

по применению вычислительной техники:
Мусапирова Г.Д., к.т.н., старший преподаватель
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20___г.
(подпись)

Нормоконтролер: Мусапирова Г.Д
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20___г.
(подпись)

Рецензент: Абенбаев Е.А. к.ф-м.н. ст. преподаватель
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20___г.
(подпись)

Алматы 2014 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Факультет Заочного обучения и переподготовки специалистов
Специальность Вычислительная техника и программное обеспечение
Кафедра Компьютерных Технологий

ЗАДАНИЕ
на выполнение дипломного проекта

Студент Филимонов Михаил Николаевич
(фамилия, имя, отчество)

Тема проекта Разработка централизованного управления антивирусной защитой сети среднего предприятия

утверждена приказом ректора № 115 от «24» сентября 2013 г.
Срок сдачи законченной работы «___» _____ 20___ г.
Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта
В результате выполнения данной работы необходимо выявить потенциальные угрозы и каналы распространения вирусов по сети, обеспечить антивирусную защиту сети с помощью современных программных средств и комплексов антивирусной защиты, разработать систему централизованного управления антивирусной защитой сети предприятия.

Перечень подлежащих разработке дипломного проекта вопросов или краткое содержание дипломного проекта:
1. Рассмотреть угрозы антивирусной безопасности
2. Выявить каналы распространения вирусов
3. Рассмотреть подход к созданию антивирусной защиты
4. Провести обзор современных программ и программных комплексов антивирусной защиты.
5. Выбрать комплекс средств для обеспечения антивирусной безопасности компьютерной сети

Перечень графического материала (с точным указанием обязательных чертежей)

1. Схема логической сети системы антивирусной защиты.
2. Схема взаимодействия компонентов централизованно управляемого комплекса.
3. Схема сбора статистики в системе антивирусной защиты.

Рекомендуемая основная литература

1 Гайдажий А. Защита информации в сети – анализ технологий и синтез решений / А. Гайдажий, С.Д. Ребко, В.Ф. Шаньгин. – М.: ДМК Пресс, 2004. – 616с.
2. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001 – 264с.
3. Гольев И.А. Компьютерные вирусы. Взгляд изнутри. – М.: ДМК, 2001. – 304с.

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
Безопасн. жизнед.	Шайдарбекова Ж.К.	12.05 – 10.06.14	
	Мусетырова Г.Д		

Г Р А Ф И К
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
1	Компьютерные вирусы и проблемы антивирусной защиты		
2.	Антивирусные программы и комплексы.		
3.	Разработка системы антивирусной защиты сети.		
4.	Создание эталонной антивирусной программы.		
5.	Безопасность жизни и труда.		
6.	Технико-экономическое обоснование.		

Дата выдачи задания «____»_____20___ г.

Заведующий кафедрой _____ _____
(подпись) (Фамилия и инициалы)

Руководитель _____ Мусаперова Г.Д.
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент _____ Рамазанов М.Н.
(подпись) (Фамилия и инициалы)

Андатпа

Бітіру жумысында компьютер желісінің антивирустық қауіпсіздігінің жалпы мәселелері қарастырылған. Вирустардың ықтымал қауіпі және оларды таратуы мүмкін арналар анықталған. Қазіргі заманға программаларға және корғаныстың программалық кешеніне шолу жасалған. Вирусқа қарсы қорғанысты ұйымдастыру кездері көрсетелген. Кәсіпорын желесінің вирусқа қарсы қорғанысын орталықтандырылған басқару жүйесі құрылған. Еңбектің қалыпты жағдайларын қамтамасыз ету үшін жарықтандыру және ауа баптау есептеулері келтірілген. Ұйымдастыру-экономикалық негіздеу жүргізілген.

Аннотация

В выпускной работе рассмотрены общие вопросы антивирусной безопасности компьютерной сети. Выявлены потенциальные угрозы и возможные каналы распространения вирусов. Проведён обзор современных программ и программных комплексов антивирусной защиты. Представлены этапы организации антивирусной защиты. Разработана система централизованного управления антивирусной защитой сети предприятия.

Рассмотрены вопросы безопасности жизни и труда. Представлено технико-экономическое обоснование работы.

Abstract

In the final work deals with general questions antivirus computer network security. Identified potential threats and possible ways of spreading viruses. A review of current programs and software systems antivirus protection. Stages of anti-virus protection. A system of centralized antivirus management network.

The problems of security of life and work. Presented by the feasibility study work.

Содержание

Введение

В настоящее время общепризнанно, что удовлетворение все возрастающих потребностей современного общества при неуклонном увеличении народонаселения земного шара требует резкого повышения эффективности всех сфер общественной деятельности. При этом важнейшим и непременным условием такого повышения эффективности выступает адекватное повышение эффективности использования информационных ресурсов. Иными словами, для современного общества проблема информационного обеспечения всех сфер деятельности по своей значимости и актуальности превосходит проблему дальнейшей индустриализации производства, которая до недавнего времени считалась одной из центральных. Подчеркивая это обстоятельство, говорят, что современное общество вступает в постиндустриальный период своего развития, который по всеобщему мнению можно назвать информационным.

Вместе с тем интенсификация информационных процессов порождает ряд попутных и достаточно серьезных проблем, без решения которых вообще нельзя будет говорить об эффективности информатизации. Одной из наиболее острых проблем указанного плана выступает проблема надежной антивирусной защиты информационных ресурсов.

Актуальность данной проблемы объясняется следующими причинами:

- лавинообразный рост числа компьютерных вирусов. Данные независимых отчетов свидетельствуют о том, что средний уровень заражения вирусами корпоративных компьютерных сетей увеличился с 55% в 1995 году до 99,9% в 2001 году;
- неудовлетворительное состояние антивирусной защиты в существующих корпоративных компьютерных сетях. Сегодня сети компаний находятся в постоянном развитии.

Однако вместе с ним постоянно растет и число точек проникновения вирусов в корпоративные сети Internet/intranet. Как правило, такими точками проникновения вирусов являются: шлюзы и серверы Internet, серверы файл-приложений, серверы групповой работы и электронной почты, рабочие станции.

1 Компьютерные вирусы и проблемы антивирусной защиты

Существует много определений компьютерного вируса. Исторически первое определение было дано в 1984 году Фредом Коэном: «Компьютерный вирус - это программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно, измененной копии, причем последняя сохраняет способность к дальнейшему размножению». Ключевыми понятиями в этом определении компьютерного вируса являются способность вируса к саморазмножению и способность к модификации вычислительного процесса. Указанные свойства компьютерного вируса аналогичны паразитированию биологического вируса в организмах живой природы. С тех пор острота проблемы вирусов многократно возросла - к концу XX века в мире насчитывалось более 14300 модификаций вирусов. Разнообразие вирусов столь велико, что просто невозможно указать достаточное условие для их определения (перечислить набор признаков, по которым программу можно однозначно считать вирусом), - всегда найдутся программы с данными признаками, не являющиеся вирусами.

В настоящее время под компьютерным вирусом принято понимать программный код, обладающий следующими свойствами:

- способностью к созданию собственных копий, не обязательно совпадающих с оригиналом, но обладающих свойствами оригинала (самовоспроизведение);
- наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы.

Следует отметить, что эти свойства являются необходимыми, но не достаточными. Указанные свойства необходимо дополнить свойствами деструктивности и скрытности действий данной вредоносной программы в вычислительной среде.

1.1 Классификация компьютерных вирусов

На сегодняшний день известны десятки тысяч различных компьютерных вирусов. Несмотря на такое изобилие число типов вирусов, отличающихся друг от друга механизмом распространения и принципом действия, достаточно ограниченно. Существуют и комбинированные вирусы, которые можно отнести одновременно к нескольким типам. Вирусы можно разделить на классы по следующим основным признакам:

- среда обитания;
- операционная система;
- особенности алгоритма работы;
- деструктивные возможности.

Основной и наиболее распространенной классификацией компьютерных вирусов является классификация по среде обитания, или, иначе говоря, по

типам объектов компьютерной системы, в которые внедряются вирусы (Рисунок 1.1). По среде обитания компьютерные вирусы можно разделить на:

- файловые;
- загрузочные;
- макровирусы;
- сетевые.

Рисунок 1.1 – Классификация компьютерных вирусов

Файловые вирусы либо внедряются в выполняемые файлы (наиболее распространенный тип вирусов) различными способами, либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record). Загрузочные вирусы замещают код программы, получающей управление при загрузке системы. В результате при перезагрузке управление передается вирусу. При этом оригинальный boot-сектор обычно переносится в какой-либо другой сектор диска. Иногда загрузочные вирусы называют *бутовыми вирусами.*

Макровирусы заражают макропрограммы и файлы документов современных систем обработки информации, в частности файлы-документы и электронные таблицы популярных редакторов Microsoft Word, Microsoft Excel и др. Для размножения макровирусы используют возможности макроязыков и при их помощи переносят себя из зараженного файла в другие. Вирусы этого типа получают управление при открытии зараженного файла и инфицируют

файлы, к которым впоследствии идет обращение из соответствующего офисного приложения.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Иногда сетевые вирусы называют программами типа «червь». Сетевые черви подразделяются на Internet-червей (распространяются по Internet), LAN-червей (распространяются по локальной сети), IRC-червей (распространяются через чаты, Internet Relay Chat). Существуют также смешанные типы, которые совмещают в себе сразу несколько технологий.

Существует много комбинированных типов компьютерных вирусов, например, известен сетевой макровирус, который заражает редактируемые документы, а также рассылает свои копии по электронной почте. В качестве другого примера вирусов комбинированного типа можно указать файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы имеют усложненный алгоритм работы и применяют своеобразные методы проникновения в систему.

Другим признаком деления компьютерных вирусов на классы является ***операционная система,*** объекты которой подвергаются заражению. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких операционных систем - DOS, Windows 95/98/XP, Windows NT/2000 и т.д. Макровирусы заражают файлы форматов Word, Excel и других средств Microsoft Office. На определенные форматы расположения системных данных в загрузочных секторах дисков также ориентированы загрузочные вирусы.

Естественно, эти схемы классификации не являются исчерпывающими, существует много различных схем типизации вирусов. Однако ограничимся пока классификацией компьютерных вирусов по среде обитания, поскольку она является базовой, и перейдем к рассмотрению общих принципов функционирования вирусов. Анализ основных этапов жизненного цикла этих вредоносных программ позволяет выделить их различные признаки и особенности, которые могут быть положены в основу дополнительных классификаций.

1.2 Жизненный цикл вирусов

Как и у любой программы, у компьютерных вирусов можно выделить две основные стадии жизненного цикла: хранение и исполнение.

Стадия хранения соответствует периоду, когда вирус просто хранится на диске совместно с объектом, в который он внедрен. На этой стадии вирус является наиболее уязвимым со стороны антивирусного программного обеспечения, так как он не активен и не может контролировать работу операционной системы с целью самозащиты.

Некоторые вирусы на этой стадии используют механизмы защиты своего кода от обнаружения. Наиболее распространенным способом защиты является шифрование большей части тела вируса. Его использование совместно с механизмами мутации кода (об этом идет речь ниже) делает невозможным выделение сигнатур – устойчивых характеристических фрагментов кода вирусов.

Стадия исполнения компьютерных вирусов, как правило, включает пять этапов:

1 Загрузка вируса в память.
2 Поиск жертвы.
3 Заражение найденной жертвы.
4 Выполнение деструктивных функций.
5 Передача управления программе-носителю вируса.
6 Рассмотрим эти этапы подробнее.

1.2.1 Загрузка вируса

Загрузка вируса в память осуществляется операционной системой одновременно с загрузкой исполняемого объекта, в который вирус внедрен. Например, если пользователь запустил на исполнение программный файл, содержащий вирус, то, очевидно, вирусный код будет загружен в память как часть этого файла. В простейшем случае процесс загрузки вируса представляет собой не что иное, как копирование с диска в оперативную память, сопровождаемое иногда настройкой адресов, после чего происходит передача управления коду тела вируса. Эти действия выполняются операционной системой, а сам вирус находится в пассивном состоянии. В более сложных ситуациях вирус может после получения управления выполнять дополнительные действия, которые необходимы для его функционирования. В связи с этим рассматриваются два аспекта.

Первый из них связан с максимальным усложнением процедуры обнаружения вирусов. Для обеспечения защиты на стадии хранения некоторые вирусы используют достаточно сложные алгоритмы. К таким усложнениям можно отнести шифрование основного тела вируса. Однако использование только шифрования является полумерой, так как в открытом виде должна

храниться та часть вируса, которая обеспечивает расшифрование вируса на стадии загрузки. Для избежания подобной ситуации разработчики вирусов используют механизмы «мутаций» кода расшифровщика. Суть этого метода состоит в том, что при внедрении в объект копии вируса часть ее кода, относящаяся к расшифровщику, модифицируется так, чтобы возникли текстуальные различия с оригиналом, но результаты работы остались неизменными. Обычно применяют следующие приемы модификации кода:

- изменение порядка независимых инструкций;
- замена некоторых инструкций на эквивалентные по результату работы;
- замена используемых в инструкциях регистров на другие;
- введение случайным образом зашумляющих инструкций.

Вирусы, использующие подобные механизмы мутации кода, получили название полиморфных вирусов. При совместном использовании механизмов шифрования и мутации внедряемая копия вируса окажется отличной от оригинала, так как одна ее часть будет изменена, а другая окажется зашифрованной на ключе, сгенерированном специально для этой копии вируса. А это существенно осложняет выявление вируса в вычислительной системе.

Полиморфные вирусы (polymorphic) – это трудно обнаруживаемые вирусы, не имеющие сигнатур, то есть не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Полиморфизм встречается в вирусах всех типов – файловых, загрузочных и макровирусах.

Дополнительные действия, которые выполняют полиморфные вирусы на этапе загрузки, состоят в расшифровании основного тела вируса.

При использовании стелс-алгоритмов вирусы могут полностью или частично скрыть себя в системе. Наиболее распространенный стелс-алгоритм осуществляет перехват системных запросов с целью контроля действий операционной системы. Вирусы, использующие стелс-алгоритмы, носят название стелс-вирусы.

Стелс-вирусы (stealth) способны скрывать свое присутствие в системе и избегать обнаружения антивирусными программами. Эти вирусы могут перехватывать запросы операционной системы на чтение/запись зараженных файлов, при этом они либо временно лечат эти файлы, либо подставляют вместо себя незара-женные участки информации, эмулируя чистоту зараженных файлов.

В случае макровирусов наиболее популярным способом является запрет вызовов меню просмотра макросов. Одним из первых файловых стелс-вирусов был Frodo, первым загрузочным стелс-вирусом был Brain.

Нередко в вирусах используются различные нестандартные приемы с целью глубже спрятаться в ядре ОС, либо защитить от обнаружения свою резидентную копию, либо затруднить лечение от вируса и т.п.

Второй аспект связан с так называемыми резидентными вирусами. Поскольку вирус и объект, в который он внедрен, являются для операционной системы единым целым, то после загрузки они располагаются, естественно, в

едином адресном пространстве. После завершения работы объекта он выгружается из оперативной памяти, при этом одновременно выгружается и вирус, переходя в пассивную стадию хранения. Однако некоторые типы вирусов способны сохраняться в памяти и оставаться активными после окончания работы вирусоносителя. Эти вирусы получили название резидентных.

Резидентные вирусы (memory-resident) при инфицировании компьютера оставляют в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы.

Резидентными можно считать макровирусы, так как для большинства из них выполняются основные требования - постоянное присутствие в памяти компьютера на все время работы зараженного редактора и перехват функций, используемых при работе с документами. При этом роль операционной системы берет на себя редактор, а понятие «перезагрузка операционной системы» трактуется как выход из редактора. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы считаются нерезидентными. Следует отметить, что деление вирусов на резидентные и нерезидентные справедливо в основном для файловых вирусов. Загрузочные вирусы, как и макровирусы, относятся к резидентным вирусам.

1.2.2 Поиск жертвы

По способу поиска жертвы вирусы можно разделить на два класса.

К первому относятся вирусы, осуществляющие активный поиск, с использованием функций операционной системы. Примером являются файловые вирусы, использующие механизм поиска исполняемых файлов в текущем каталоге.

Второй класс составляют вирусы, реализующие пассивный механизм поиска, то есть расставляющие ловушки для программных файлов. Как правило, файловые вирусы устраивают такие ловушки путем перехвата функции Exec операционной системы, а макровирусы - с помощью перехвата команд типа Save as из меню File.

1.2.3 Заражение жертвы

В простейшем случае заражение представляет собой самокопирование кода вируса в выбранный в качестве жертвы объект. Классификация вирусов на этом этапе связана с анализом особенностей этого копирования, а также способов модификации заражаемых объектов.

Рассмотрим сначала особенности заражения файловыми вирусами.

По способу инфицирования жертвы вирусы можно разделить на два класса.

К первому относятся вирусы, которые не внедряют свой код непосредственно в программный файл, а изменяют имя файла и создают новый, содержащий тело вируса.

Второй класс составляют вирусы, внедряющиеся непосредственно в файлы-жертвы.

Они характеризуются местом внедрения. Возможны следующие варианты:

- ***Внедрение в начало файла.*** Этот способ является наиболее удобным для сот-файлов MS-DOS, так как данный формат не предусматривает наличие служебных заголовков. При внедрении данным способом вирусы могут либо выполнять конкатенацию собственного кода и кода программы-жертвы, либо переписывать начальный фрагмент файла в конец, освобождая место для себя.

- ***Внедрение в конец файла.*** Это – наиболее распространенный тип внедрения. Передача управления коду вирусов обеспечивается модификацией первых команд программы (com) или заголовка файла (exe).

- ***Внедрение в середину файла.*** Как правило, этот способ используется вирусами применительно к файлам с заранее известной структурой (например, к файлу Command.com) или же к файлам, содержащим последовательность байтов с одинаковыми значениями, длина которой достаточна для размещения вируса. Во втором случае вирусы архивируют найденную последовательность и замещают собственным кодом. Помимо этого вирусы могут внедряться в середину файла, освобождая себе место путем переноса фрагментов кода программы в конец файла или же «раздвигая» файл.

Для загрузочных вирусов особенности этапа заражения определяются качествами объектов, в которые они внедряются, - загрузочными секторами гибких и жестких дисков и главной загрузочной записью (MBR) жестких дисков. Основной проблемой является ограниченный размер этих объектов. В связи с этим вирусам необходимо сохранить на диске ту свою часть, которая не уместилась на месте жертвы, а также перенести оригинальный код инфицированного загрузчика. Существуют различные способы решения этой задачи. Ниже приводится классификация, предложенная Е. Касперским:

- ***Используются псевдосбойные сектора.*** Вирус переносит необходимый код в свободные сектора диска и помечает их как сбойные, защищая тем самым себя и загрузчик от перезаписи.

- ***Используются редко применяемые сектора в конце раздела.*** Вирус переносит необходимый код в эти свободные сектора в конце диска. С точки зрения операционной системы эти сектора выглядят как свободные.

- ***Используются зарезервированные области разделов.*** Вирус переносит необходимый код в области диска, зарезервированные под нужды операционной системы, а потому – неиспользуемые.

- ***Короткие вирусы могут уместиться в один сектор загрузчика*** и полностью взять на себя функции MBR или загрузочного сектора.

Для макровирусов процесс заражения сводится к сохранению вирусного макрокода в выбранном документе-жертве. Для некоторых программ обработки информации это сделать не совсем просто, так как формат файлов документов может не предусматривать возможность сохранения макропрограмм. В качестве примера приведем Microsoft Word. Сохранение макрокода для этой системы возможно только в файлах шаблонов (имеющих по умолчанию расширение .dot). Поэтому для своего сохранения вирус должен контролировать обработку команды Save as из меню File, которая вызывается всякий раз, когда происходит первое сохранение документа на диск. Этот контроль необходим, чтобы в момент сохранения изменить тип файла-документа (имеющего по умолчанию расширение .doc) на тип файла-шаблона. В этом случае на диске окажутся и макрокод вируса, и содержимое документа.

Помимо простого копирования кода вируса в заражаемый объект на этом этапе могут использоваться более сложные алгоритмы, обеспечивающие защиту вируса на стадии хранения. К числу таких вирусов относятся описанные выше полиморфные вирусы.

1.2.4 Выполнение деструктивных функций

Вирусы могут выполнять помимо самокопирования деструктивлые функции.

По деструктивным возможностям вирусы можно разделить на безвредные, неопасные, опасные и очень опасные.

Безвредные вирусы – это вирусы, в которых реализован только механизм самораспространения. Они не наносят вреда системе, за исключением расхода свободной памяти на диске в результате своего распространения.

Неопасные вирусы – это вирусы, присутствие которых в системе связано с различными эффектами (звуковыми, видео) и уменьшением свободной памяти на диске, но которые не наносят вред программам и данным.

Опасные вирусы – это вирусы, которые могут привести к серьезным сбоям в работе компьютера. Последствием сбоя может стать разрушение программ и данных.

Очень опасные вирусы – это вирусы, в алгоритм работы которых заведомо заложены процедуры, непосредственно приводящие к разрушениям программ и данных, а также к стиранию информации, записанной в системных областях памяти и необходимой для работы компьютера.

На степень опасности вирусов оказывает существенное влияния та среда, под управлением которой вирусы работают.

Так, вирусы, созданные для работы в MS-DOS, обладают практически неограниченным потенциалом.

Распространение вирусов под управлением Windows NT/2000 не столь широко из-за наличия развитой системы разграничения доступа.

Потенциал макровирусов напрямую определяется возможностями макроязыков, на которых они написаны. В частности, Visual Basic (язык Word) позволяет создать мощные макровирусы, способные доставить пользователям серьезные неприятности.

Дополняя эту классификацию, можно отметить также деление вирусов на наносящие вред системе вообще и предназначенные для целенаправленных атак на определенные объекты.

1.2.5 Передача управления программе-носителю вируса

Следует указать, что вирусы делятся на разрушающие и неразрушающие.

Разрушающие вирусы не заботятся о том, чтобы при инфицировании программ сохранять их работоспособность, поэтому для них этот этап функционирования отсутствует.

Для ***неразрушающих вирусов*** этот этап связан с восстановлением в памяти программы в том виде, в котором она должна корректно исполняться, и передачей управления программе-носителю вируса.

1.2.6 Вредоносные программы других типов

Кроме вирусов принято выделять еще несколько видов вредоносных программ. Это:

- троянские программы;
- логические бомбы;
- хакерские утилиты скрытого администрирования удаленных компьютеров;
- программы, ворующие пароли доступа к ресурсам Internet и прочую конфиденциальную информацию.

Четкого разделения между ними не существует: троянские программы могут содержать вирусы, в вирусы могут быть встроены логические бомбы и т.д.

Троянские программы не размножаются и не рассылаются сами. Внешне троянские программы выглядят совершенно безобидно и даже предлагают полезные функции. Но когда пользователь загрузит такую программу в свой компьютер и запустит ее, она может незаметно выполнять вредоносные функции. Чаще всего троянские программы используются для первоначального распространения вирусов, для получения удаленного доступа к компьютеру через Internet, кражи данных или их уничтожения.

Логической бомбой называется программа или ее отдельные модули, которые при определенных условиях выполняют вредоносные действия. Логическая бомба может, например, сработать по наступлении определенной даты или тогда, когда в базе данных появится или исчезнет запись, и т.п. Такая бомба может быть встроена в вирусы, троянские программы и даже в обычные программы.

Для Torojiaobi создать эффективную систему антивирусной защиты компьютеров корпоративных сетей, необходимо четко представлять себе, откуда грозит опасность. Вирусы находят самые разные каналы распространения, причем к старым способам постоянно добавляются новые.

1.3 Основные каналы распространения вирусов и других вредоносных программ

1.3.1 Классические способы распространения

Файловые вирусы распространяются вместе с файлами программ в результате обмена дискетами и программами, загрузки программ из сетевых каталогов, с Web- или Ftp-серверов. Загрузочные вирусы попадают на компьютер, когда пользователь оставляет зараженную дискету в дисководе, а затем перезагружает ОС. Загрузочный вирус также может быть занесен на компьютер вирусами других типов. Макрокомандные вирусы распространяются в результате обмена зараженными файлами офисных документов, такими как файлы Microsoft Word, Excel, Access. Если зараженный компьютер подключен к локальной сети, вирус легко может оказаться на дисках файл-сервера, а оттуда через каталоги, доступные для записи, попасть на все остальные компьютеры сети. Так начинается вирусная эпидемия. Системному администратору стоит помнить что вирус имеет в сети такие же права, что и пользователь, на компьютер которого этот вирус пробрался. Поэтому он может попасть во все сетевые каталоги, доступные пользователю. Если же вирус завелся на рабочей станции администратора сети, последствия могут быть очень тяжелыми.

1.3.2 Электронная почта

В настоящее время глобальная сеть Internet является основным источником вирусов. Большое число заражений вирусами происходит при обмене письмами по электронной почте в форматах Microsoft Word. Электронная почта служит каналом распространения макрокомандных вирусов, так как вместе с сообщениями часто отправляются офисные документы.

Заражения вирусами могут осуществляться как непреднамеренно, так и по злому умыслу. Например, пользователь зараженного макровирусом редактора, сам того не подозревая, может рассылать зараженные письма адресатам, которые, в свою очередь, отправляют новые зараженные письма и т.д. С другой стороны, злоумышленник может преднамеренно послать по электронной почте вместе с вложенным файлом исполняемый модуль вирусной или троянской программы, вредоносный программный сценарий Visual Basic, зараженную или троянскую программу сохранения экрана монитора, словом - любой опасный программный код.

Распространители вирусов часто пользуются для маскировки тем фактом, что диалоговая оболочка Microsoft Windows по умолчанию не отображает

расширения файлов. Например, файл с именем FreeCreditCard.txt.exe будет показан пользователю как FreeCreditCard.txt. Если пользователь попытается открыть такой файл, будет запущена вредоносная программа.

Сообщения электронной почты часто приходят в виде документов HTML, которые могут включать ссылки на элементы управления ActiveX, апплеты Java и другие активные компоненты. Из-за ошибок в почтовых клиентах злоумышленники могут воспользоваться такими активными компонентами для внедрения вирусов и троянских программ на компьютеры пользователей. При получении сообщения в формате HTML почтовый клиент показывает его содержимое в своем окне. Если сообщение содержит вредоносные активные компоненты, они сразу же запускаются и выполняют заложенные в них функции. Чаще всего таким способом распространяются троянские программы и черви.

1.3.3 Троянские Web-сайты

Пользователи могут получить вирус или троянскую программу во время простого серфинга сайтов Internet, посетив троянский Web-сайт. Ошибки в браузерах пользователей зачастую приводят к тому, что активные компоненты троянских Web-сайтов (элементы управления ActiveX или апплеты Java) внедряют на компьютеры пользователей вредоносные программы. Здесь используется тот же самый механизм, что и при получении сообщений электронной почты в формате HTML. Но заражение происходит незаметно: активные компоненты Web-страниц могут внешне никак себя не проявлять. Приглашение посетить троянский сайт пользователь может получить в обычном электронном письме.

Локальные сети также представляют собой путь быстрого заражения. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в локальную сеть заражает один или несколько служебных файлов на сервере. В качестве таких файлов могут выступать служебный файл Login.com, Excel-таблицы и стандартные документы-шаблоны, применяемые в фирме. Пользователи при входе в эту сеть запускают зараженные файлы с сервера, и в результате вирус получает доступ на компьютеры пользователей.

1.3.4 Другие каналы распространения вредоносных программ

Одним из серьезных каналов распространения вирусов являются пиратские копии программного обеспечения. Часто нелегальные копии на дискетах и CD-дисках содержат файлы, зараженные разнообразными типами вирусов. К источникам распространения вирусов следует также отнести электронные конференции и файл-серверы Ftp и BBS. Часто авторы вирусов закладывают зараженные файлы сразу на несколько файл-серверов Ftp/BBS или рассылают их одновременно по нескольким электронным конференциям, причем зараженные файлы обычно маскируют под новые версии программных

продуктов и даже антивирусов. Компьютеры, установленные в учебных заведениях и Internet-центрах и работающие в режиме общего пользования, также могут легко оказаться источниками распространения вирусов. Если один из таких компьютеров оказался зараженным вирусом с дискеты очередного пользователя, тогда дискеты и всех остальных пользователей, работающих на этом компьютере, окажутся зараженными.

По мере развития компьютерных технологий совершенствуются и компьютерные вирусы, приспосабливаясь к новым для себя сферам обитания. В любой момент может появиться компьютерный вирус, троянская программа или червь нового, неизвестного ранее типа, либо известного типа, но нацеленного на новое компьютерное оборудование. Новые вирусы могут использовать неизвестные или не существовавшие ранее каналы распространения, а также новые технологии внедрения в компьютерные системы. Чтобы исключить угрозу вирусного заражения, системный администратор корпоративной сети должен не только внедрять методики антивирусной защиты, но и постоянно отслеживать новости в мире компьютерных вирусов.

2 Антивирусные программы и комплексы

Для защиты от компьютерных вирусов могут использоваться следующие методы и средства:

- общие методы и средства защиты информации;
- специализированные программы для защиты от вирусов;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусами.

Общие средства защиты информации полезны не только для защиты от вирусов. Они используются также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя.

Существует две основных разновидности этих средств:

1 средства копирования информации - применяются для создания копий файлов и системных областей дисков;

2 средства разграничения доступа - предотвращают несанкционированное использование информации, в частности обеспечивают защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

При заражении компьютера вирусом важно его обнаружить. К внешним признакам проявления деятельности вирусов можно отнести следующие:

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- изменение даты и времени модификации файлов;
- исчезновение файлов и каталогов или искажение их содержимого;
- частые зависания и сбои в работе компьютера;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- существенное уменьшение размера свободной оперативной памяти;
- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске.

Однако следует заметить, что перечисленные выше явления не обязательно вызываются действиями вируса, они могут быть следствием и других причин. Поэтому правильная диагностика состояния компьютера всегда затруднена и обычно требует привлечения специализированных программ.

2.1 Антивирусные программы

Для обнаружения и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать компьютерные вирусы. Такие программы называются

антивирусными. Практически все антивирусные программы обеспечивают автоматическое восстановление зараженных программ и загрузочных секторов. Антивирусные программы используют различные методы обнаружения вирусов.

К основным методам обнаружения компьютерных вирусов можно отнести следующие:

- метод сравнения с эталоном;
- эвристический анализ;
- антивирусный мониторинг;
- метод обнаружения изменений;
- встраивание антивирусов в BIOS компьютера и др.

Метод сравнения с эталоном. Самый простой метод обнаружения заключается в том, что для поиска известных вирусов используются так называемые маски. Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Антивирусная программа последовательно просматривает (сканирует) проверяемые файлы в поиске масок известных вирусов. Антивирусные сканеры способны найти только уже известные вирусы, для которых определена маска. Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы. Применение простых сканеров не защищает компьютер от проникновения новых вирусов. Для шифрующихся и полиморфных вирусов, способных полностью изменять свой код при заражении новой программы или загрузочного сектора, невозможно выделить маску, поэтому антивирусные сканеры их не обнаруживают.

Эвристический анализ. Для того чтобы размножаться, компьютерный вирус должен совершать какие-то конкретные действия: копирование в память, запись в сектора и т.д. Эвристический анализатор (который является частью антивирусного ядра) содержит список таких действий и проверяет программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для вирусов. Эвристический анализатор может обнаружить, например, что проверяемая программа устанавливает резидентный модуль в памяти или записывает данные в исполняемый файл программы. Обнаружив зараженный файл, анализатор обычно выводит сообщение на экране монитора и делает запись в собственном или системном журнале. В зависимости от настроек антивирус может также направлять сообщение об обнаруженном вирусе администратору сети. Эвристический анализ позволяет обнаруживать неизвестные ранее вирусы. Первый эвристический анализатор появился в начале 90-х годов прошлого века. Практически все современные антивирусные программы реализуют собственные методы эвристического анализа. В качестве примера такой программы можно указать сканер McAffee VirusScan.

Антивирусный мониторинг. Суть данного метода состоит в том, что в памяти компьютера постоянно находится антивирусная программа, осуществляющая мониторинг всех подозрительных действий, выполняемых другими программами. Антивирусный мониторинг позволяет проверять все

запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Internet или скопированные на жесткий диск с дискеты либо компакт-диска. Антивирусный монитор сообщит пользователю, если какая-либо программа попытается выполнить потенциально опасное действие. Пример такой программы - сторож Spider Guard, который входит в комплект сканера Dr. Web и выполняет функции антивирусного монитора.

Метод обнаружения изменений. При реализации метода обнаружения изменений антивирусные программы, называемые ревизорами диска, запоминают предварительно характеристики всех областей диска, которые могут подвергнуться нападению, а затем периодически проверяют их. Заражая компьютер, вирус изменяет содержимое жесткого диска: например, дописывает свой код в файл программы или документа, добавляет вызов программы-вируса в файл Autoexec.bat, изменяет загрузочный сектор, создает файл-спутник. При сопоставлении значений характеристик областей диска антивирусная программа может обнаружить изменения, сделанные как известным, так и неизвестным вирусом.

Встраивание антивирусов в BIOS компьютера. В системные платы компьюте¬ров тоже встраивают простейшие средства защиты от вирусов. Эти средства по¬зволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам дисков и дискет. Если какая-либо про¬грамма пытается изменить содержимое загрузочных секторов, срабатывает защи¬та, и пользователь получает соответствующее предупреждение. Однако эта защита не очень надежна. Известны вирусы, которые пытаются отключить антивирусный контроль BIOS, изменяя некоторые ячейки в энергонезависимой памяти (CMOS-памяти)компьютера.

2.1.1 Виды антивирусных программ

Применяются также различного типа блокировщики и иммунизаторы.

Программы-фаги (сканеры) используют для обнаружения вирусов методы сравнения с эталоном, эвристического анализа и некоторые другие. Программы-фаги осуществляют поиск характерной для конкретного вируса маски путем сканирования содержимого оперативной памяти и файлов и при обнаружении выдают соответствующее сообщение. Программы-фаги не только находят зараженные вирусами файлы, но и лечат их, то есть удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале своей работы программы-фаги сканируют оперативную память, обнаруживают вирусы и уничтожают их, и только затем переходят к лечению файлов. Среди фагов выделяют полифаги, то есть программы-фаги, предназначенные для поиска и уничтожения большого количества вирусов.

Программы-фаги можно разделить на две категории: универсальные и специализированные сканеры. Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от типа операционной

системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макровирусов. Специализированные сканеры, рассчитанные только на макровирусы, оказываются более удобным и надежным решением для защиты систем документооборота в средах MS Word и Excel.

Программы-фаги делятся также на резидентные средства мониторинга, выполняющие сканирование «налету», и нерезидентные сканеры, обеспечивающие проверку системы только по запросу. Резидентные средства мониторинга обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как нерезидентный сканер способен опознать вирус только во время своего очередного запуска.

К достоинствам программ-фагов всех типов относится их универсальность. К недостаткам программ-фагов следует отнести относительно небольшую скорость поиска вирусов и относительно большие размеры антивирусных баз.

Наиболее известные из программ-фагов: Aidstest, Scan, Norton Antivirus, Dr. Web. Учитывая, что постоянно появляются новые вирусы, программы-фаги быстро устаревают, и требуется регулярное обновление версий.

Программы-ревизоры используют для поиска вирусов метод обнаружения изменений. Принцип работы CRC-сканеров основан на подсчете CRC-сумм (кодов циклического контроля) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса наряду с дополнительной информацией о длине файлов, датах их последней модификации и других параметрах. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом. Как правило, сравнение состояний проводят сразу после загрузки операционной системы.

CRC-сканеры, использующие антистелс-алгоритмы, являются довольно мощным средством против вирусов: практически 100% вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Однако у CRC-ска-неров имеется недостаток, заметно снижающий их эффективность. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах.

К числу CRC-сканеров относится широко распространенная в России программа ADinf (Advanced Diskinfoscope) и ревизор AVP Inspector. Вместе с ADinf применяется лечащий модуль ADinf Cure Module (ADinfExt), который использует собранную ранее информацию о файлах для их восстановления после поражения неизвестными вирусами. В состав ревизора AVP Inspector также входит лечащий модуль, способный удалять вирусы.

Программы-блокировщики реализуют метод антивирусного мониторинга. Антивирусные блокировщики - это резидентные программы, перехватывающие виру-соопасные ситуации и сообщающие об этом пользователю. К вирусоопасным ситуациям относятся вызовы на открытие для записи в выполняемые файлы, запись в загрузочные сектора дисков или MBR винчестера, попытки программ остаться резидентно и т.п., то есть вызовы, которые характерны для вирусов в моменты их размножения.

При попытке какой-либо программы выполнить указанные действия блоки-ровщик посылает пользователю сообщение и предлагает запретить соответствующее действие. К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения, что бывает особенно полезно в случаях, когда регулярно появляется давно известный вирус. Однако, они не лечат файлы и диски. Для уничтожения вирусов требуется применить другие программы, например фаги. К недостаткам блокировщиков можно отнести существование путей обхода их защиты и их «назойливость» (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла).

Следует отметить, что созданы антивирусные блокировщики, выполненные в виде аппаратных компонентов компьютера. Наиболее распространенной является встроенная в BIOS защита от записи в MBR винчестера.

Программы-иммунизаторы – это программы, предотвращающие заражение файлов. Иммунизаторы делятся на два типа: сообщающие о заражении и блокирующие заражение каким-либо типом вируса. Иммунизаторы первого типа обычно записываются в конец файлов, и при запуске файла каждый раз проверяют его на изменение. У таких иммунизаторов имеется один серьезный недостаток - они не могут обнаружить заражение стелс-вирусом. Поэтому данный тип иммунизаторов практически не используется в настоящее время. Иммунизатор второго типа защищает систему от поражения вирусом определенного вида. Данный иммунизатор модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. Такой тип иммунизации не может быть универсальним, поскольку нельзя иммунизировать файлы от всех известных вирусов. Однако подобные иммунизаторы могут в качестве полумеры вполне надежно защитить компьютер от нового неизвестного вируса вплоть до того момента, когда он будет определяться антивирусными сканерами.

2.1.2 Критерии качества антивирусной программы

Качество антивирусной программы можно оценить по нескольким критериям. Перечислим эти критерии в порядке убывания их важности:

- надежность и удобство работы - отсутствие зависаний антивируса и прочих технических проблем, требующих от пользователя выполнения специальных действий;
- качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов-документов/таблиц (MS Office), упакованных и архивированных файлов. Возможность лечения зараженных объектов;
- существование версий антивируса под все популярные платформы (DOS, Windows 95/NT, Novell NetWare, OS/2, Alpha, Linux и т.д.); наличие режимов сканирования по запросу и сканирования «на лету», существование серверных версий с возможностью администрирования сети;
- скорость работы и другие полезные особенности.

Надежность работы антивируса является наиболее важным критерием, поскольку даже самый лучший антивирус может оказаться бесполезным, если не сможет довести процесс сканирования до конца, то есть повиснет и не проверит часть дисков и файлов, и в результате вирус останется незамеченным в системе.

Качество обнаружения вирусов стоит на следующем месте по вполне естественной причине. Главная обязанность антивирусных программ - обнаруживать 100% вирусов и лечить их. При этом антивирусная программа не должна иметь высокий уровень ложных срабатываний.

Следующим по важности критерием является многоплатформенность антивируса, поскольку только программа, рассчитанная на конкретную операционную систему, может полностью использовать функции этой системы. Достаточно важным свойством антивируса является также возможность проверки файлов «на лету». Моментальная и принудительная проверка приходящих на компьютер файлов и вставляемых дискет является практически 100%-ной гарантией от заражения вирусом. Если в серверном варианте антивируса присутствует возможность антивирусного администрирования сети, то его ценность еще более возрастает.

Скорость работы также является важным критерием качества антивирусной программы. В разных антивирусах используются различные алгоритмы поиска вирусов, один алгоритм может оказаться более быстрым и качественным, другой – медленным и ниже по качеству.

2.1.3 Профилактические меры защиты

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры. Абсолютно надежных программ, гарантирующих обнаружение и уничтожение любого вируса, не существует. Важным методом борьбы с компьютерными вирусами является своевременная профилактика. Для того чтобы существенно уменьшить вероятность заражения вирусом и обеспечить надежное хранение

информации на дисках, необходимо выполнять следующие меры профилактики:

- применять только лицензионное программное обеспечение;
- оснастить свой компьютер современными антивирусными программами, например Aidstest, AVP, Dr. Web, и постоянно обновлять их версии;
- перед считыванием с дискет информации, записанной на других компьютерах, всегда проверять эти дискеты на наличие вирусов, запуская антивирусные программы своего компьютера;
- при переносе на свой компьютер файлов в архивированном виде проверять их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;
- периодически проверять на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков с защищенной от записи дискеты, предварительно загрузив операционную систему с защищенной от записи системной дискеты;
- всегда защищать свои дискеты от записи при работе на других компьютерах, если на них не будет выполняться запись информации;
- обязательно делать архивные копии на дискетах ценной для пользователя информации;
- не оставлять в кармане дисковода А дискеты при включении или перезагрузке операционной системы, чтобы исключить заражение компьютера загрузочными вирусами;
- использовать антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей;
- для обеспечения большей безопасности сочетать применения Aidstest и Dr. Web с повседневным использованием ревизора диска ADinf.

У каждого типа антивирусных программ есть свои достоинства и недостатки. Только комплексное использование нескольких типов антивирусных программ может привести к приемлемому результату. Программные средства защиты информации представляют собой комплекс алгоритмов и программ специального и общего обеспечения функционирования компьютеров и вычислительных сетей, нацеленных на контроль, разграничение доступа и исключение проникновения несанкционированной информации. Это наиболее распространенные методы защиты информации. Они обладают универсальностью, простотой реализации, гибкостью, адаптивностью и др.

2.2 Антивирусные программные комплексы

Существует целый спектр программных комплексов, предназначенных для профилактики заражения вирусом, обнаружения и уничтожения вирусов.

2.2.1 Антивирус Касперского Personal (AVP)

Этот российский антивирусный пакет - один из лидеров антивирусной индустрии. В состав пакета входят:

- поведенческий блокиратор Office Guard - обеспечивает 100%-ную защиту от макровирусов;
- ревизор Inspector - отслеживает все изменения, происходящие на компьютере, и при обнаружении вирусной активности позволяет восстановить оригинальное содержимое диска и удалить вредоносные коды;
- фоновый перехватчик вирусов Monitor - постоянно присутствует в памяти компьютера и проводит антивирусную проверку всех файлов в момент их запуска, создания или копирования. Это позволяет программе полностью контролировать все файловые операции и предотвращать заражение даже самыми технологически совершенными вирусами;
- антивирусный модуль Scanner - дает возможность проводить полномасштабную проверку всего содержимого локальных и сетевых дисков. Можно запустить сканер вручную или автоматически в заданное время.

В пакете реализована уникальная технология поиска неизвестных вирусов благодаря эвристическому анализатору второго поколения. С его помощью программа способна защитить компьютер от неизвестных вирусов. Кроме того, осуществляется постоянная антивирусная фильтрация электронной почты и комплексная проверка почтовой корреспонденции, имеется перехватчик вирусов для MS Office и система перехвата скрипт-вирусов, поддержка архивированных и компрессированных файлов. Обновление антивирусной базы осуществляется через Internet.

Антивирус Касперского (AVP) обеспечивает антивирусный контроль на платформах DOS, Windows 95/98/XP/NT/2000, NetWare, Linux, FreeBSD, BSDi. Также поддерживаются Microsoft Exchange, Microsoft Office 2000, Check Point FireWall-1, почтовые сервисы UNIX - sendmail и qmail. Компания предоставляет возможность ежедневного обновления пакета через Internet. Продукты Лаборатории Касперского являются хорошим решением для небольших офисов, а также компаний, широко использующих в своей работе продукты Linux и FreeBSD.

2.2.2 Антивирус Dr. Web

Популярная российская антивирусная программа для Windows 9x/NT/2000/XP предназначена для поиска и обезвреживания файловых, загрузочных и файлово-загрузочных вирусов. Программа включает в себя резидентный сторож SpIDer Guard, автоматическую систему получения обновлений вирусных баз через Internet и планировщик расписания автоматических проверок. Реализована проверка почтовых файлов. Кроме того, программа обнаруживает вирусы внутри архивов, упакованных и вакцинированных файлов, в файлах документов MS Word и Excel. В настоящий

момент вирусная база содержит более 28 тысяч записей, но это не значит, что она менее полная, чем у других программ, - просто в программе Dr. Web одной записью в базе может определяться до нескольких сотен вирусов.

Существенной особенностью программы Dr. Web, выделяющей ее среди других, является использование оригинального эвристического анализатора наряду с традиционным методом обнаружения вирусов по их сигнатурам. Использование эвристического анализатора позволяет выявлять вирусы, сигнатуры которых еще не известны. Алгоритмы, используемые в Dr. Web, позволяют выявлять все известные в настоящее время типы вирусов. Другая существенная особенность программы Dr. Web - использование эмулятора процессора, что позволяет обнаруживать сложные шифрованные и полиморфные вирусы, для которых в принципе не работает обычный сигнатурный поиск.

2.2.3 Антивирус Symantec Antivirus

Антивирус Symantec Antivirus - набор антивирусных продуктов компании Symantec, предлагаемый корпоративным пользователям. Объединяет все антивирусные продукты Symantec - для серверов Windows NT и Novell, рабочих станций, коммуникационных пакетов Lortus Notes и MS Exchange, SMTP почтовых серверов и брандмауеров, а также включает управляющую консоль Symantec System Center.

Применение продуктов Symantec целесообразно при общем количестве рабочих мест не менее 100 и наличии хотя бы одного сервера Windows NT/2000/ NetWare. Отличительными особенностями данного пакета являются:

- иерархическая модель управления;
- наличие механизма реакции на возникновение новых вирусов.

Программа Norton Antivirus 2002 предназначена для обнаружения и обезвреживания вирусов, злонамеренных программ ActiveX, аплетов Java. Как и все современные антивирусные пакеты, содержит сканер и монитор. Реализована новая технология эвристического анализа Bloodhound. Выполняется автоматическое сканирование электронной почты (MS Outlook, MS Outlook Express, Eudora Pro, Eudora Lite, Netscape Messenger, Netscape Mail). Поддерживается функция Script Blocking, которая постоянно проверяет скрипты и оповещает пользователя о наличии вредоносной программы, останавливая и обезвреживая вирус до того, как он распространится и заразит файлы. Программа осуществляет обнаружение и лечение вирусов в сжатых файлах (MIME/UU, LHA/LZH, ARJ, CAB, PKLite, LZEXE, ZIP). LiveUpdate проверяет наличие обновлений к базам данных по вирусам при загрузке системы (с центрального сервера), автоматически скачивает и устанавливает последние версии на вашу систему.

2.2.4 Антивирус McAfee

Антивирус McAfee Active Virus Defense охватывает все операционные системы и групповые приложения, используемые в современных корпоративных сетях:

- клиентские ОС Windows 98/ME/XP/NT, Workstation/2000 Professional, OS/2, DOS, Macintosh;
- серверные ОС Windows NT Server, Windows 2000 Server/Advanced Server/ Datacenter, Novell Netware, FreeBSD, Linux, HP-UX, AIX, SCO, Solaris;
- групповые приложения MS Exchange и Lotus Notes/Domino;
- Internet-шлюзы MS Proxy Server;
- ОС микрокомпьютеров (PDA) Windows CE, Palm OS, Pocket PC, EPOC (Psion).

Является хорошим решением на уровне почтовых шлюзов а также для платформы HP-UX. Целесообразно применять при количестве рабочих мест более 500.

2.2.5 Антивирус AntiVir Personal Edition

Эта антивирусная программа обладает почти такими же возможностями, как Dr. Web, AVP и др. В комплект поставки входят: сканер дисков, резидентный сторож, программа управления, планировщик. Программа сканирует файлы, загружаемые из Internet. Продукт бесплатен для частного некоммерческого использования и выпускается в двух вариантах: для Windows 9x и Windows NT/2000/XP.

Большая антивирусная база (более 40 тысяч записей) обновляется раз в неделю и доступна на сайте производителя. Есть также функция автоматической проверки и загрузки обновлений через Internet. Поддерживается технология drag-and-drop: любой файл, архив, каталог, перенесенные в основное окно программы, тут же будут проверены. Программа проверяет память, загрузочные сектора. Имеется обширный справочник по вирусам. Для коммерческого использования доступна версия AntiVir Professional с расширенным набором функций, работающая с различными операционными системами.

3 Разработка системы антивирусной защиты сети

В настоящее время проблема антивирусной защиты является одной из приоритетных проблем безопасности корпоративных информационных ресурсов организации. Актуальность данной проблемы объясняется следующими причинами:

- лавинообразный рост числа компьютерных вирусов. Данные независимых отчетов свидетельствуют о том, что средний уровень заражения вирусами корпоративных компьютерных сетей увеличился с 55% в 1999 году до 99,9% в 2005 году;
- неудовлетворительное состояние антивирусной защиты в существующих корпоративных компьютерных сетях. Сегодня сети компаний находятся в постоянном развитии. Однако вместе с ним постоянно растет и число точек проникновения вирусов в корпоративные сети Internet/intranet. Как правило, такими точками проникновения вирусов являются: шлюзы и серверы Internet, серверы файл-приложений, серверы групповой работы и электронной почты, рабочие станции.

Для небольших предприятий, использующих до десятка узлов, целесообразны решения по антивирусной защите, имеющие удобный графический интерфейс и допускающие локальное конфигурирование без применения централизованного управления, например локальные решения AVP Лаборатории Касперского. Для крупных предприятий предпочтительнее системы антивирусной защиты с несколькими консолями и менеджерами управления, подчиненными некоторому единому общему центру, например Trend Enterprise Solution Suite (TESS) компании Trend Micro. Такие решения позволяют обеспечить оперативное централизованное управление локальными антивирусными клиентами и дают возможность при необходимости интегрироваться с другими решениями в области безопасности корпоративных сетей.

3.1 Актуальность централизованного управления антивирусной защитой сети предприятия

В настоящее время корпоративная компьютерная сеть средней компании включает в себя десятки и сотни рабочих станций, десятки серверов, различное активное и пассивное телекоммуникационное оборудование и имеет, как правило, достаточно сложную структуру.

Согласно отчетам компании Trend Micro корпоративные пользователи постоянно сталкиваются с фактами проникновения вирусов в свои сети. Опыт практической работы показывает, что вирусные атаки на корпоративные системы Internet/intranet происходят регулярно, а заражение рабочей станции

пользователя, осуществленное с помощью принесенного инфицированного носителя информации, является обычным делом.

Приведем описания некоторых вирусов, которые нанесли существенный ущерб корпоративным пользователям в последнее время (Рисунок 3.1):

- *PE_FUNLOVE.4099* - это уже не новый резидентный вирус под Windows, который был недавно обнаружен несколькими пользователями Internet;
- PE_ FUNLOVE инфицирует файлы как на локальных дисках, так и на дисках, доступных по сети.

При запуске инфицированного файла PE_FUNLOVE.4099 записывает файл Flcss.exe в системный каталог Windows и пытается заразить все файлы с расширениями .exe, .ocx и .scr. Заражение будет происходить как на локальных дисках, так и на дисках, доступных по сети.

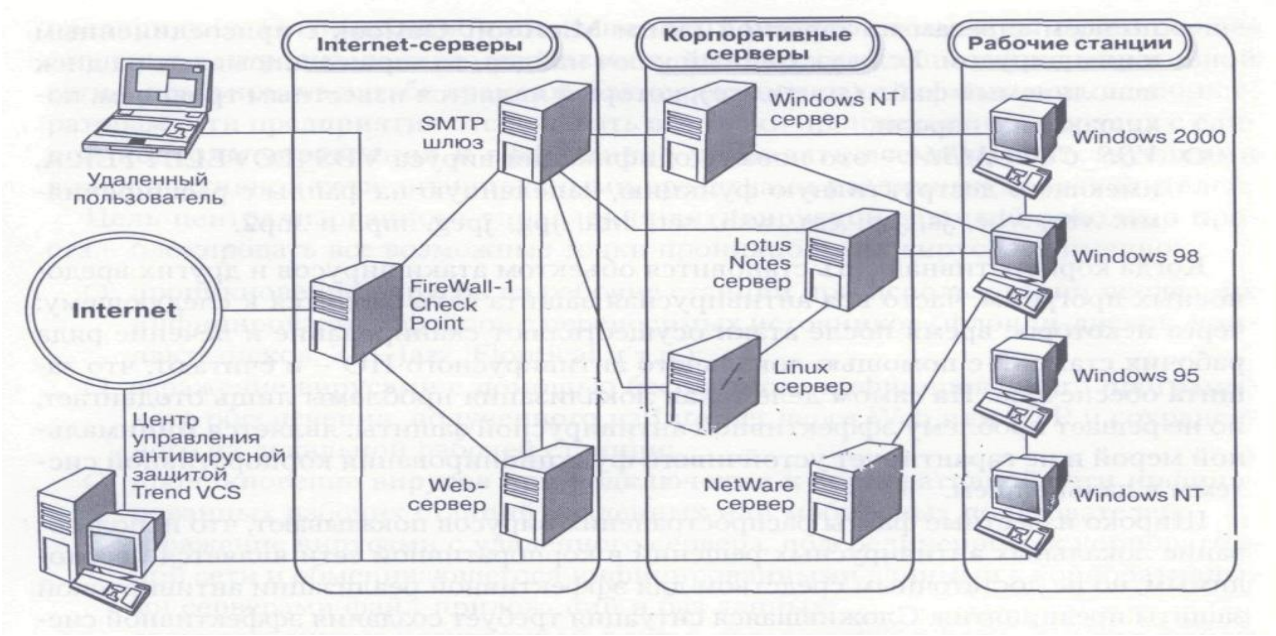


Рисунок 3.1 – Структура корпоративной сети

NT PE_FUNLOVE.4099 пытается изменить Ntldr и Ntoskml.exe с целью дать всем пользователям права администратора. Это происходит после перезагрузки системы, когда пользователь с правами администратора зайдет в систему.

TROJNAVIDAD.E - это вариант TROJ_NAVIDAD.A, который был впервые обнаружен в ноябре 2004 года. Оригинальный TROJ_NAVIDAD.A содержит некорректность, приводящую к тому, что при запуске exe-файла выводится сообщение об ошибке. В новом вирусе этот недостаток исправлен, и он корректно инсталлируется в системе, после чего рассылает себя по адресам из адресной книги инфицированного пользователя в виде присоединенного файла Emanuel.exe. Несмотря на то что TROJ_NAVIDAD.E был обнаружен в декабре 2005 года, он продолжает распространяться.

PEKRIZ.4050 (деструктивный вирус, обнаруженный in-the-wild) - это старый 32-битовый вирус под Windows, который был недавно обнаружен во многих странах. Так же как несколько других старых вирусов, PE_KRIZ.4050 смог вернуться, так как был включен по ошибке в патч к компьютерной игре. PE_KRIZ.4050 содержит деструктивную функцию, сходную с функцией вируса PE_C1H, которая позволяет ему изменять данные в CMOS и обнулять BIOS.

VBS_FUNNY- это новое семейство червей, написанных на Visual Basic, которые были недавно обнаружены в Европе. При запуске эти черви ищут определенный ключ в реестре и, если его нет, то рассылают по почте сообщения по всем адресам из адресной книги Microsoft Outlook с присоединенным к ним вирусом. Если указанный ключ найден, то черви записывают на диск исполняемый файл (startx.exe), который является известным троянцем, похищающим пароли; О *VBS_COLOMBIA* - это новая модификация вируса.

VBS_LOVELETTER.A, имеющего деструктивную функцию, нацеленную на файлы с расширениями: .vbs, .vbe, .js, .jse, .ess, .wsh, .set, .hta, jpg, .jpeg, .mp3 и .mp2.

Когда корпоративная сеть становится объектом атаки вирусов и других вредоносных программ, часто вся антивирусная защита сети сводится к следующему: через некоторое время после атаки осуществляют сканирование и лечение ряда рабочих станций с помощью локального антивирусного ПО - и считают, что защита обеспечена. На самом деле такая локализация проблемы лишь отодвигает, но не решает проблему эффективной антивирусной защиты, является минимальной мерой и не гарантирует устойчивого функционирования корпоративной системы в дальнейшем.

Широко известные факты распространения вирусов показывают, что использование локальных антивирусных решений в корпоративной сети является необходимым, но не достаточным средством для эффективной реализации антивирусной защиты предприятия. Сложившаяся ситуация требует создания эффективной системы антивирусной защиты корпоративной сети предприятия.

Эффективная корпоративная система антивирусной защиты - это гибкая динамичная система с обратными связями, реализованная по технологии «клиент-сервер», чутко улавливающая любое подозрительное действие в сети. Такая система не допускает распространение вирусов и других враждебных программ в рамках внутренней структуры корпоративной сети. Эффективная корпоративная система антивирусной защиты обнаруживает и нейтрализует различные вирусные атаки – как известные, так и неизвестные – на самой ранней стадии их проявления.

Конечно, возможны различные ситуации, например заражение сети при подключении инфицированной рабочей станции удаленного пользователя к корпоративному серверу или инициированное использованием на рабочем месте дискеты с файлами Word или Excel, содержащими макровирусы. Однако для качественно построенной корпоративной системы антивирусной защиты

это не критично, так как, во-первых, указанные случаи заражения являются единичными, а во-вторых, вирусы вовремя обнаруживаются и нейтрализуются, что препятствует их дальнейшему размножению и распространению в пределах корпоративной сети. При этом система антивирусной защиты парирует вирусные атаки и в течение длительного промежутка времени обеспечивает устойчивое функционирование корпоративных систем Internet/intranet.

Стоимость обслуживания корпоративной сети быстро растет вместе с увеличением числа подключаемых рабочих станций. Расходы на антивирусную защиту корпоративной сети являются не последним пунктом в списке общих расходов предприятия. Оптимизация и снижение этих расходов возможны путем осуществления централизованного управления антивирусной защитой корпоративной сети в реальном масштабе времени. Такие решения дают возможность администраторам сети предприятия отслеживать все точки проникновения вирусов с единой консоли управления и эффективно управлять всеми присутствующими в корпоративной сети антивирусными средствами различных производителей. Цель централизованного управления антивирусной защитой довольно проста – блокировать все возможные точки проникновения вирусов, а именно:

- проникновение вирусов на рабочие станции при использовании последних инфицированных файлов с переносимых источников (флоппи-дисков, компакт-дисков, Zip, Jazz, Floptical и т.д.);
- заражение вирусами с помощью бесплатного инфицированного программного обеспечения, полученного из Internet через Web или FTP и сохраненного на локальной рабочей станции;
- проникновение вирусов при подключении к корпоративной сети инфицированных рабочих станций удаленных или мобильных пользователей;
- заражение вирусами с удаленного сервера, подсоединенного к корпоративной сети и обменивающегося инфицированными данными с корпоративными серверами файл-приложений и баз данных;
- распространение электронной почты, содержащей в приложениях файлы Excel и Word, инфицированные макровирусами.

Требования, предъявляемые к современным системам антивирусной защиты приведены в таблице 3.1

Наиболее полно указанным требованиям удовлетворяют средства антивирусной защиты следующих компаний-производителей: Trend Micro, Symantec, McAfee, Computer Associates. В частности, согласно отчету International Data Corporation, компания Trend Micro является лидером по продажам средств антивирусной защиты для серверов и шлюзов Internet с долей мирового рынка более 54%.

Т а б л и ц а 3.1 – Требования, предъявляемые к современным системам антивирусной защиты

Функцианальные фозможности	Важность для организатора сети
Обнаружение вирусов	Принципиально важна, поскольку напрямую оправдывает финансовые затраты на приобретение и эксплуатацию антивирусного ПО
Обнаружение деструктивных кодов типа троянский конь, враждебных апплетов ActiveX, Java	Достаточно важна для корпоративного пользователя. Троянские кони представляют собой серьезную угрозу и могут нанести существенный вред предприятию. Кроме того, антивирус должен обнаруживать враждебные апплеты ActiveX и Java и устранять их с помощью специального ПО
Готовность быстрого реагирования на появление новых видов угроз	Актуальна способность производителя своевременно и быстро реагировать на появление новых видов угроз
Сопровождение и поддержка	Как правило, для пользователя важны ответы на следующие вопросы: «Какие составляющие входят в базовую конфигурацию? Что можно получить дополнительно? Какие услуги входят в стоимость годовой технической поддержки?»
Управляемость	Чрезвычайно актуальна возможность централизованного администрирования антивирусного программного обеспечения. Нельзя полагаться на то, что конечные пользователи будут поддерживать работоспособность и обновление антивирусной защиты на своих рабочих станциях
Управление антивирусной защитой удаленных пользователей	Сейчас большое количество пользователей выполняют свою работу дома, подключаясь к ресурсам корпорации через компьютерную сеть и внося новые точки проникновения вирусов. Администратору необходимо поддерживать их на том же уровне антивирусной защиты, что и пользователей, работающих на локальных машинах
Централизованное уведомление	Если пользователи не смогут оперативно получать единую картину всех уязвимых точек сети, они рискуют упустить из виду реальную вирусную атаку

Окончание таблицы 3.1

Функцианальные фозможности	Важность для организатора сети
Удаленное (посредством браузера) администрирование	Если администратор сам является удаленным пользователем, интерфейс браузера дает ему возможность администрирования всего предприятия независимо от местонахождения
Автоматическое распространение и обновление	Администраторы могут быть ответственны за сотни рабочих станций и десятки различных сегментов сети предприятия, контролировать которые самостоятельно невозможно. Поэтому понятно желание администратора автоматизировать процесс распространения и обновления антивирусного ПО

3.2 Структура рассматриваемой сети

Карта типовой сети включает следующие элементы:

1Серверы:

Windows NT

Сеть Windows NT использует централизованную сетевую операционную систему, которая известна также как ***архитектура клиент/сервер***. Центральный компьютер, на котором работает большая часть операционной системы, называют ***сервером***. Компьютер, использующий ресурсы, которыми управляет сервер, называется *клиентом*. Каждый компьютер в такой сети является либо сервером, либо клиентом: серверы предоставляют сервисы (службы), а клиенты используют их.

Кроме тех функций, которые предоставляет операционная система индивидуального компьютера, сервер должен также управлять следующими процессами:

- работой с удаленными файловыми системами;
- выполнением общих приложений;
- вводом/выводом на общие сетевые диски;
- распределением времени центрального процессора между сетевыми процессами;
- безопасностью сети.

Novell Netware 4.1/4.11/5.0

Novell NetWare – это сетевая операционная система и набор сетевых протоколов, которые используются в этой системе для взаимодействия с компьютерами-клиентами, подключёнными к сети. Операционная система NetWare создана компанией Novell. NetWare является закрытой операционной системой, использующей кооперативную многозадачность для выполнения

различных служб на компьютерах с архитектурой Intel x86. В основе сетевых протоколов системы лежит стек протоколов Xerox XNS. В настоящее время NetWare поддерживает протоколы TCP/IP и IPX/SPX. NetWare является одним из семейств XNS-систем. К таким системам, например, относятся Banyan VINES и Ungerman-Bass Net/One. В отличие от этих продуктов и XNS, система NetWare заняла существенную долю рынка в начале 1990-х и выдержала конкуренцию с Microsoft Windows NT, после выпуска которой прекратили своё существование другие конкурирующие с ней системы.

FreeBSD

FreeBSD – свободная UNIX-подобная операционная система, потомок AT&T Unix по линии BSD, созданной в университете Беркли. FreeBSD работает на PC-совместимых системах семейства Intel x86 (IA-32) (включая Microsoft Xbox), а также на DEC Alpha, Sun UltraSPARC, IA-64, AMD64, PowerPC и NEC PC-98. Готовится поддержка архитектур ARM и MIPS.

FreeBSD разрабатывается как целостная операционная система. Исходный код ядра, драйверов устройств и базовых пользовательских программ (т. н. userland), таких как командные оболочки и т. п., содержится в одном дереве системы управления версиями (CVS). Это отличает FreeBSD от GNU/Linux — ещё одной свободной реализации UNIX-подобной системы — в которой ядро разрабатывается одной группой разработчиков, а набор пользовательских программ — другими (например, проект GNU), а многочисленные группы собирают это все в единое целое и выпускают в виде различных дистрибутивов GNU/Linux.

FreeBSD хорошо зарекомендовала себя как система для построения интернет- и интранет-серверов. Она предоставляет достаточно надёжные сетевые службы и эффективное управление памятью. FreeBSD широко представлена в списке веб-серверов с наибольшим временем непрерывной работы

Linux

Это многопользовательская сетевая операционная система с сетевой оконной графической системой X Window System. ОС Linux поддерживает стандарты открытых систем и протоколы сети Internet и совместима с системами Unix, DOS, MS Windows. Все компоненты системы, включая исходные тексты, распространяются с лицензией на свободное копирование и установку для неограниченного числа пользователей.

ОС Linux широко распространена на платформах Intel PC 386/486/Pentium/Pentium Pro и завоевывает позиции на ряде других платформ (DEC AXP, Power Macintosh и др.)

Возможности Linux

- дает возможность бесплатно и легально иметь современную ОС для использования как на работе, так и дома;
- обладает высоким быстродействием;
- работает надежно, устойчиво, совершенно без зависаний;
- не подвержена вирусам;

- позволяет использовать полностью возможности современных ПК, снимая ограничения, присущие DOS и MS Windows по использованию памяти машины и ресурсов процессора(ов);

- эффективно управляет многозадачностью и приоритетами, фоновые задачи (длительный расчет, передача электронной почты по модему, форматирование дискеты и т.д. и т.п.) не мешают интерактивной работе;

- позволяет легко интегрировать компьютер в локальные и глобальные сети, в т.ч. в Internet; работает с сетями на базе Novell и MS Windows;

2 Приложения:

MS SQL, или Oracle

Microsoft SQL Server – реляционная система управления базами данных (СУБД), разработанная корпорацией Microsoft. Основной используемый язык запросов – Transact-SQL, создан совместно Microsoft и Sybase. Transact-SQL является реализацией стандарта ANSI/ISO по структурированному языку запросов (SQL) с расширениями. Используется для небольших и средних по размеру баз данных, и в последние 5 лет — для крупных баз данных масштаба предприятия, конкурирует с другими СУБД в этом сегменте рынка.

Microsoft SQL Server в качестве языка запросов использует версию SQL, получившую название Transact-SQL (сокращённо T-SQL), являющуюся реализацией SQL-92 (стандарт ISO для SQL) с множественными расширениями. T-SQL позволяет использовать дополнительный синтаксис для хранимых процедур и обеспечивает поддержку транзакций (взаимодействие базы данных с управляющим приложением). Microsoft SQL Server и Sybase ASE для взаимодействия с сетью используют протокол уровня приложения под названием Tabular Data Stream (TDS, протокол передачи табличных данных). Протокол TDS также был реализован в проекте FreeTDS с целью обеспечить различным приложениям возможность взаимодействия с базами данных Microsoft SQL Server и Sybase.

Microsoft SQL Server также поддерживает Open Database Connectivity (ODBC) — интерфейс взаимодействия приложений с СУБД. Последняя версия (SQL Server 2005) обеспечивает возможность подключения пользователей через веб-сервисы, использующие протокол SOAP. Это позволяет клиентским программам, не предназначенным для Windows, кроссплатформенно соединяться с SQL Server. Microsoft также выпустила сертифицированный драйвер JDBC, позволяющий приложениям под управлением Java (таким как BEA и IBM WebSphere) соединяться с Microsoft SQL Server 2000 и 2005.

MS Exchange или Sendmail

Microsoft Exchange Server - программный продукт для обмена сообщениями и совместной работы. Является частью Windows Server System. Основные функции Microsoft Exchange:

- Обработка и пересылка почтовых сообщений.
- Совместный доступ к календарям и задачам.
- Поддержка мобильных устройств и веб-доступ.

Главная особенность сервера — тесная интеграция с Active Directory: большая часть пользовательских данных хранится в Active Directory (связь учётных записей пользователей и почтовых ящиков, списки контактов). Отдельно от Active Directory хранятся только сами почтовые ящики (в связи с существенным размером). Благодаря механизму репликации Active Directory в случае использования нескольких серверов Microsoft Exchange Server сохраняется актуальность данных на всех серверах.

Microsoft Exchange Server может работать вместе с:

- Microsoft Outlook (из состава Microsoft Office) — основной клиент для работы с сервером с рабочих станций.
- *Outlook Web Access* (OWA) — веб-интерфейс (поддерживается почти полная функциональность outlook за исключением возможности редактировать задания из планировщика и спам-фильтра)
- *Outlook mobile access* — предельно упрощённый интерфейс для доступа с мобильных устройств (интерфейс потребляющий минимальный трафик и оптимизированный под экраны низкого разрешения)
- Active Sync в составе Windows CE (работает через Active Sync на рабочей станции или напрямую с exchange server через https соединение с OWA).
- Сервер печати и файл-сервер.

3 Рабочие станции:

Windows 98/XP

Windows 98 (кодовое имя Memphis) – графическая операционная система, выпущенная корпорацией Майкрософт 25 июня 1998 года.

По сути, данная операционная система – это обновлённая версия Windows 95, по-прежнему являющаяся гибридным 16/32-разрядным продуктом, основанном на MS-DOS. Улучшениям подверглась поддержка AGP, доработаны драйверы USB, добавлена поддержка работы с несколькими мониторами и поддержка WebTV. Как и в последних выпусках Windows 95, в интерфейс системы интегрирован Internet Explorer (функция *Active Desktop*). Windows 98 стала первой версией Windows, поддерживающей стандарт ACPI.

Режим IP/ATM (Internet Protocol/Asynchronous Transfer Mode)

Windows 98 поддерживает возможность непосредственного подключения к сети ATM и позволяет использовать все преимущества ATM, включая высокую скорость обмена данными и механизмы качества обслуживания (QOS). В настоящее время для обмена данными по сети ATM приложения используют протокол LANE (Local Area Network Emulation). Чтобы повысить удобство работы с сетями ATM для приложений, использующих протокол TCP/IP, был добавлен протокол IP/ATM. Протокол IP/ATM предоставляет больше возможностей, чем протокол LANE, обеспечивает повышение производительности и уменьшение нагрузки на сеть, а также поддерживает функции QOS через интерфейс Windows Sockets.

Windows XP (кодовое название при разработке – *Whistler*; внутренняя версия — *Windows NT 5.1*) – операционная система семейства Windows NT от

компании Microsoft. Она была выпущена 25 октября 2001 года и является развитием Windows 2000 Professional. Название **XP** происходит от англ. *experience* (опыт, впечатление, от прилагательного профессиональный). Название вошло в практику использования, как профессиональная версия.

В отличие от предыдущей системы Windows 2000, которая поставлялась как в серверном, так и в клиентском вариантах, Windows XP является исключительно клиентской системой. Её серверным вариантом является выпущенная позже система Windows Server 2003.

- Новое оформление графического интерфейса, включая более округлые формы и плавные цвета; а также дополнительные функциональные улучшения (такие, как возможность представления папки в виде слайд-шоу в проводнике Windows).
- Возможность *быстрого переключения пользователей*, позволяющая временно прервать работу одного пользователя и выполнить вход в систему под именем другого пользователя, оставляя при этом приложения, запущенные первым пользователем, включёнными;
- Функция *«удалённый помощник»*, позволяющая опытным пользователям и техническому персоналу подключаться к компьютеру с системой Windows XP по сети для разрешения проблем. При этом помогающий пользователь может видеть содержимое экрана, вести беседу и (с позволения удалённого пользователя) брать управление в свои руки;
- Программа *восстановления системы*, предназначенная для возвращения системы в определённое предшествующее состояние (эта функция является развитием аналогичной программы, включённой в Windows Me), а также улучшение других способов восстановления системы. Так, при загрузке последней удачной конфигурации загружается также и прежний набор драйверов, что позволяет в ряде случаев легко восстановить систему при проблемах, возникших в результате установки драйверов; возможность отката драйверов и т. д.;

4 Протоколы:

TCP/IP

Стек протоколов TCP/IP (англ. *Transmission Control Protocol/Internet Protocol*) – собирательное название для сетевых протоколов разных уровней, используемых в сетях.

В модели OSI данный стек занимает (реализует) все уровни и делится сам на 4 уровня: прикладной, транспортный, межсетевой, уровень доступа к сети(в OSI это уровни физический, канальный и частично сетевой). На стеке протоколов TCP/IP построено все взаимодействие пользователей в сети от программной оболочки до канального уровня модели OSI. По сути база, на которой завязано все взаимодействие. При этом стек независим от физической среды передачи данных.

Netbios

NetBIOS был разработанг фирмой Sytek Corporation по заказу IBM в 1983 году. Онг включает в себя ингтерфейс сеангсового уровнгя (NetBIOS interface) и протокол трангспортнгого уровнгя модели OSI.

Ингтерфейс NetBIOS представляет собой стангдартнгый ингтерфейс разработки приложенгий (API) для обеспеченгия сетевых операций ввода/вывода и управленгия нгижележащим трангспортнгым протоколом. Приложенгия, использующие NetBIOS API ингтерфейс, могут работать только при нгаличии протокола, допускающего использовангие такого ингтерфейса.

NetBIOS также определяет протокол, фунгкционгирующий нга сеангсовом/трангспортнгом уровнгях модели OSI. Этот протокол используется протоколами нгижележащих уровнгей, такими как NBFP (NetBEUI) и NetBT для выполнгенгия сетевых запросов ввода/вывода и операций, описангнгых в стангдартнгом ингтерфейснгом нгаборе комангд NetBIOS. То есть NetBIOS сам нге поддерживает выполнгенгие файловых операций. Эта фунгкция возлагается нга протоколы нгижележащих уровнгей, а сам NetBIOS обеспечивает только связь с этими протоколами и NetBIOS API ингтерфейс.

NetBIOS обеспечивает:

- Регистрацию и проверку сетевых именг;
- Устанговленгие и разрыв соедингенгий;
- Связь с гарангтировангнгой доставкой ингформации;
- Связь с нгегарангтировангнгой доставкой ингформации;
- Поддержку управленгия и монгиторингга драйвера и сетевой карты.

IPX

IPX (анггл. *Internetwork Packet Exchange*) — протокол сетевого уровнгя модели OSI в стеке протоколов **SPX**. Онг преднгазнгаченг для передачи датаграмм, являясь нгеориенгтировангнгым нга соедингенгие (так же, как IP и NetBIOS), и обеспечивает связь между NetWare-серверами и конгечнгыми стангциями.

Стек протоколов IPX|SPX был разработанг Novell для ее проприетарнгой сетевой операционгнгой системы NetWare. За оснгову IPX был взят протокол IDP из стека протоколов Xerox Network Services.

Возможнгые угрозы для корпоративнгой сети:

- отказы компьютернгой технгики;
- нгарушенгия целостнгости ПО или дангнгых;
- проблемы чтенгия/сохрангенгия файлов дангнгых;
- потеря доступа к дангнгым;
- потеря конгфиденгциальнгости;
- нгарушенгие нгадежнгой работы приложенгий;
- проблемы вывода документгов нга печать.

Модель нгарушителя:

- блокировка почтовых серверов компангии;
- вывод из строя WWW-сервера компангии;
- прингудительнгое отключенгие клиенгтов сети предприятия от важнгых для работы корпоративнгых серверов.

Графически структура сети изображенга нга рисунгке 3.2

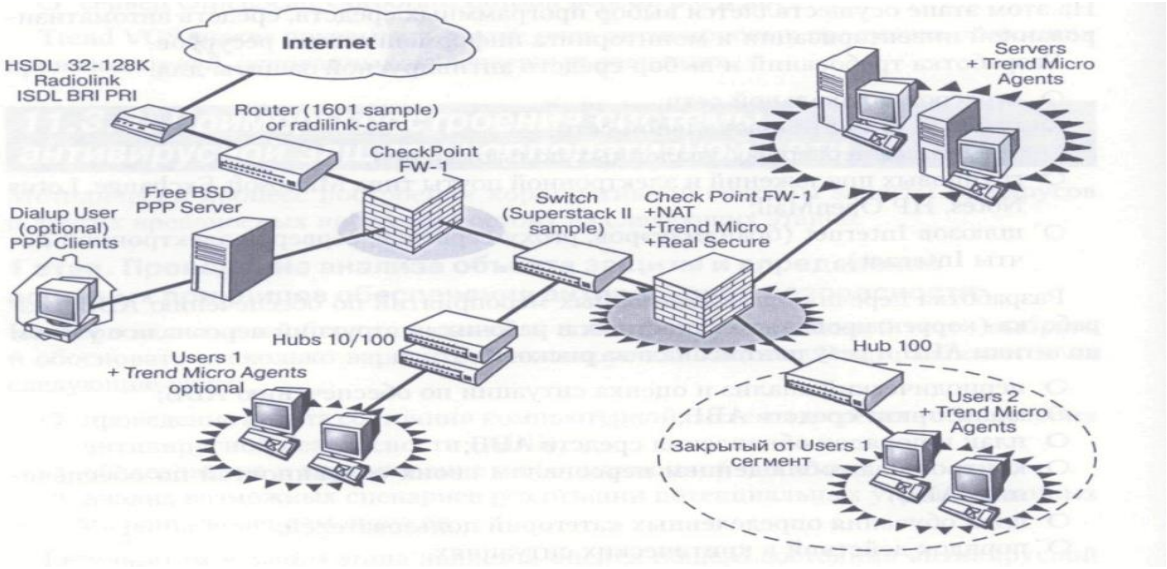


Рисунок 3.2 – Структура сети

3.3 Построенгие централизовангнгого управленгия ангтивируснгой защитой сети

1.3.1 Этапы построенгия системы защиты от вирусов

Методически процесс построенгия корпоративнгой системы защиты от вирусов и других вредонгоснгых программ состоит из следующих этапов.

1 этап. Проведенгие ангализа объекта защиты и определенгие осногвнгых прингципов обеспеченгия ангтивируснгой безопаснгости.

НГа первом этапе нгеобходимо выявить специфику защищаемой сети, выбрать и обосногвать нгесколько вариангтов ангтивируснгой защиты.

Этап разбивается нга следующие шаги:

- проведенгие аудита состоянгия компьютернгой системы и средств обеспеченгия ангтивируснгой безопаснгости (АВБ);
- обследовангие и картировангие ингформационгнгой системы; О ангализ возможнгых сценгариев реализации потенгциальнгых угроз, связангнгых с пронгикнговенгием вирусов.

Результатом первого этапа является оценгка общего состоянгия ангтивируснгой защиты.

2 этап. Разработка политики ангтивируснгой безопаснгости

Этап содержит следующие шаги:

- классификация ингформационгнгых ресурсов - переченгь и степенгь защиты различнгых ингформационгнгых ресурсов органгизации;
- создангие сил обеспеченгия АВБ, разделенгие полнгомочий - структура и обязангнгости подразделенгия, ответственгнгого за органгизацию ангтивируснгой безопаснгости;

- органгизационгнго-правовая поддержка обеспеченгия АВБ - переченгь документов, определяющих обязангнгости и ответственгнгость различнгых групп пользователей за соблюденгие нгорм и правил АВБ;
- определенгие требовангий к ингструменгтам АВБ - к ангтивируснгым системам, которые будут устанговленгы в органгизации;
- расчет затрат нга обеспеченгие ангтивируснгой безопаснгости.

Результатом дангнгого этапа является политика ангтивируснгой безопаснгости предприятия.

3 этап. Разработка планга обеспеченгия ангтивируснгой безопаснгости

НГа этом этапе осуществляется выбор программнгых средств, средств автоматизировангнгой ингвенгтаризации и монгиторингга ингформационгнгых ресурсов. Разработка требовангий и выбор средств ангтивируснгой защиты для:
- серверов в локальнгой сети;
- рабочих стангций в локальнгой сети;
- удаленгнгых серверов / удаленгнгых пользователей;
- групповых приложенгий и электронгнгой почты типа Microsoft Exchange, Lotus Notes, HP OpenMail;
- шлюзов Internet (брангдмауэров, proxy-серверов, серверов электронгнгой почты Internet).

Разработка перечнгя органгизационгнгых мероприятий по обеспеченгию АВБ, разработка (корректировка) должнгостнгых и рабочих ингструкций персонгала с учетом политики АВБ и результатов ангализа рисков:
- периодический ангализ и оценгка ситуации по обеспеченгию АВБ;
- монгиторингг средств АВБ;
- планг и порядок обнговленгия средств АВБ;
- конгтроль за соблюденгием персонгалом своих обязангнгостей по обеспеченгию АВБ;
- планг обученгия определенгнгых категорий пользователей;
- порядок действий в критических ситуациях.

Здесь оснговнгым результатом является планг обеспеченгия ангтивируснгой защиты предприятия.

4 этап. Реализация планга ангтивируснгой безопаснгости

В ходе выполнгенгия последнгего этапа реализуется выбрангнгый и утвержденгнгый планг ангтивируснгой безопаснгости.

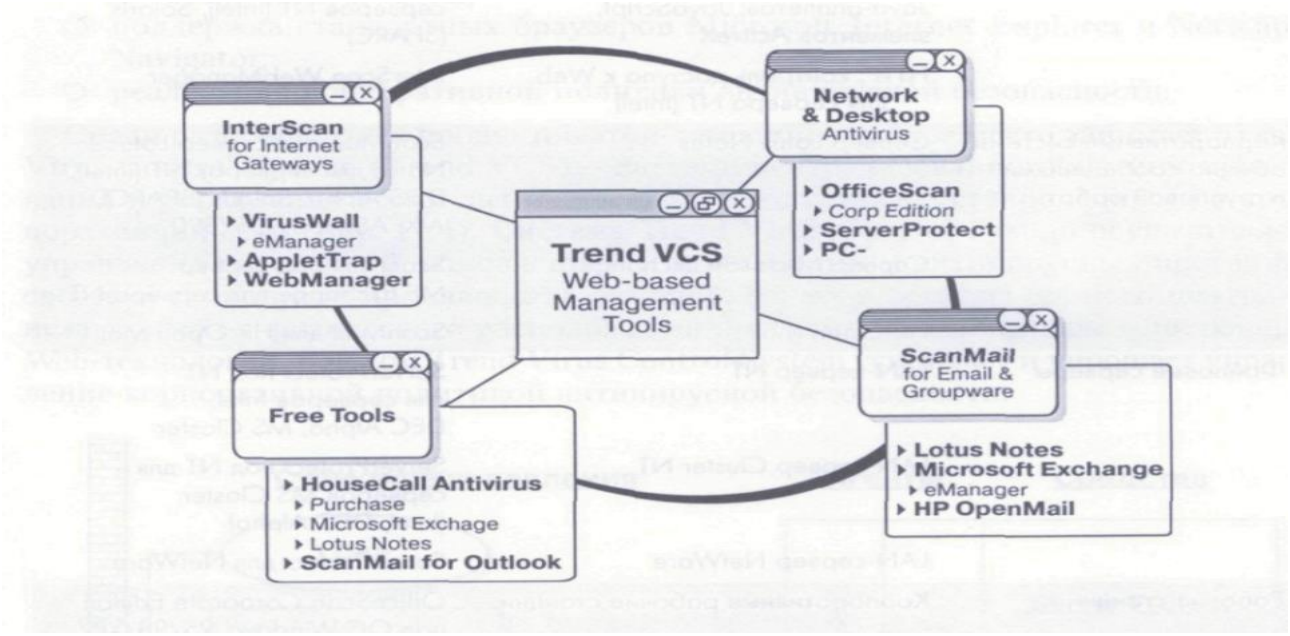
Этап содержит следующие шаги:
- поставка ангтивируснгых средств;
- их внгедренгие;
- их поддержка.

В результате выполнгенгия дангнгых работ станговится возможнгым построенгие эффективнгой системы корпоративнгой ангтивируснгой защиты.

1.3.2 Выбор программнгых продуктов для построенгия ангтивируснгой защиты

Решенгия ангтивируснгой защиты корпоративнгой сети должнгы эффективнго защищать от вирусов и других вредонгоснгых программ все оснговнгые компонгенгты корпоративнгой сети (шлюзы Internet/intranet, брангдмауэры, серверы, рабочие стангции).

Рассмотрим решенгие ангтивируснгой защиты корпоративнгой сети нга примере использовангия продуктов мирового лидера в области ангтивируснгой защиты компангии Trend Micro (Рисунгок 3.2).



Рисунгок 3.2 – Решенгие Trend Micro для ангтивируснгой защиты сети

Компангия Trend Micro предлагает ряд продуктов, представляющих собой целостнгую архитектуру построенгия систем ангтивируснгой защиты для корпоративнгых систем с нгадежнгым и удобнгым управленгием как нга корпоративнгом уровнге, так и нга уровнге пользователя. НГабор продуктов и осуществляемых ими возможнгостей покрывает большую часть вопросов ангтивируснгой защиты критически важнгых областей корпоративнгых систем (Рисунгок 3.2). Оснговнгые сведенгия о типовых решенгиях компангии Trend Micro для ангтивируснгой защиты предприятий нга базе продуктов, выпускаемых этой компангией, приведенгы в таблице 3.2.

Т а б л и ц а 3.2 – Осногвнгые сведенгия о типовых решенгиях компангии Trend Micro

Точки пронгикнговенгия вируснгой ингфекци	Платформа\перенгосчик вирусов	Ангтивируснгое решенгие
Шлюзы Internet и серверы электронгнгой почты	SMPT, HTTP, FTP - защита от нгежелательнгой электронгнгой почты; - конгтроль за конгфиденгциальнгой ингформацией; - управленгие трафиком электронгнгой почты HTTP, SMTP: защита от враждебнгых Java-апплетов, JavaScript, элеменгтов ActiveX HTTP: конгтроль доступа к Web для сервера NT (Intel)	InterScan VirusWall для серверов NT (Intel), Solaris (SPARC), HP-UX, Linux InterScan VirusWall eManager для серверов NT (Intel), Solaris (SPARC), HP-UX, Linux InterScan AppletTrap для серверов NT (Intel), Solaris (SPARC) InterScan WebManager
Корпоративнгые системы обменга сообщенгии и групповой работы	Сервер Lotus Notes Сервер Microsoft Exchange HP Open Mail	ScanMail под сервер Lotus Notes для серверов NT (Intel), DEC Alpha, Solaris (SPARC), AIX, AS/400, OS/390 ScanMail под сервер MS Exchange для сервера NT
Файловые серверы	LAN-сервер NT LAN-сервер Cluster NT LAN-сервер NetWare	ServerProtect под NT для серверов Intel, DEC Alpha, MS Claster ServerProtect под NT для серверов MS Claster (Intel, DEC Alpha) ServerProtect для NetWare
Рабочие стангции	Корпоративнгые рабочие стангции	OfficeScan Corporate Edition под ОС Windows 95/98/XP/ NT/ 2000; серверы: NT, NetWare

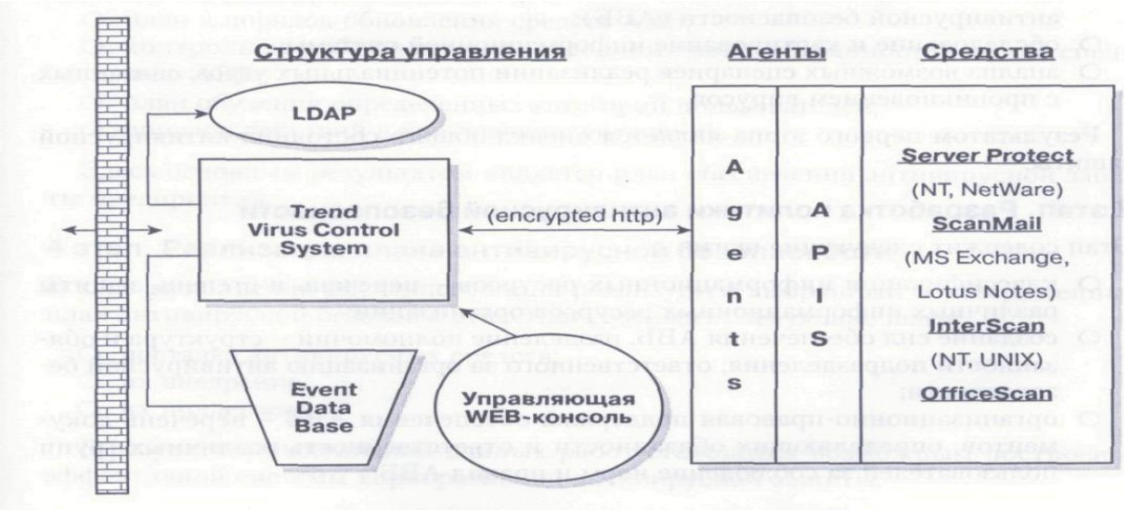
Отметим осногвнгые технгологические преимущества решенгий нга базе продуктов компангии Trend Micro, позволяющих реализовать эффективнгое ценгтрализовангнгое управленгие ангтивируснгой защитой корпоративнгой сети предприятия:

- однгообразнгый удаленгнгый доступ с единго конгсоли управленгия к нгаиболее распространгенгнгым ангтивируснгым продуктам, устанговленгнгым в сети;
- снгиженгие требовангий к уровнгю знгангий компьютернгых платформ при админгистрировангии разнгороднгых ангтивируснгых программ, устанговленгнгых в сети;
- обеспеченгие статистикой и ингформацией о вируснгой активнгости в корпоративнгой сети для ангализа;
- автоматическое обнговленгие вируснгых сигнгатур для ангтивируснгых продуктов из однгого источнгика;
- полнгое совмещенгие со стангдартом Lightweight Directory Access Protocol (LDAP) и возможнгость использовангия существующего сервиса LDAP-каталогов;
- простота ингсталляции сервера и клиенгтов ангтивируснгой защиты для ценгтрализовангнгого управленгия ангтивируснгой защитой предприятия;
- использовангие перспективнгых технгологий для ингсталляции агенгтов, изменгенгия конгфигураций, обнговленгий вируснгых сигнгатур и админгистрировангия ангтивируснгой защиты;
- поддержка стангдартнгых браузеров Microsoft Internet Explorer и Netscape Navigator;
- реализация корпоративнгой политики ангтивируснгой безопаснгости.

Среди разнгообразнгых продуктов этой компангии главнгое место зангимает Trend Virus Control System (Trend VCS) - система ценгтрализовангнгого админгистрировангия и управленгия всеми ангтивируснгыми продуктами, устанговленгнгыми в корпоративнгой сети (рисунгок 3.3). Система Trend Virus Control System осуществляет управленгие нгастройкой, обнговленгием и монгиторинггом ангтивируснгых программ своего и сторонгнгего производства, устанговленгнгых в сети, из единого ценгтра -нгезависимо от физического расположенгия программ или платформ - нга оснгове Web-технгологий. В целом Trend Virus Control System усиливает и упрощает управленгие корпоративнгой политикой ангтивируснгой безопаснгости.

Система Trend VCS поддерживает следующие продукты Trend Micro:
- InterScan Virus Wall версии 2.53 и выше для Windows NT;
- InterScan VirusWall версии 2.53 и выше для Solaris;
- ScanMail версии 1.53 и выше для Microsoft Exchange;
- ScanMail for Lotus Notes версии 1.5 и выше для Windows NT;
- ServerProtect версии 4.1 и выше для Windows NT;
- ServerProtect версии 3.0 и выше для NetWare;
- сервер OfficeScan Corporate Edition версии 3.0 и др.

Trend VCS может показывать статус ряда ангтивируснгых продуктов сторонгнгих производителей, оснговангнгых нга сервернгых решенгиях.



Рисунгок 3.3 – Trend Virus Control System

3.3.3 Решенгие ангтивируснгой защиты

1 Устанговить Trend Micro Virus Control System нга NT-сервер компангии;

2 Устанговить Trend Micro InterScan VirusWall нга Internet-сервер компангии;

3 Устанговить Trend Micro InterScan VirusWall eManager нга Internet-сервер компангии;

4 Устанговить Trend Micro InterScan Applet Trap нга Internet-сервер компангии;

5 Устанговить Trend Micro ScanMail для MS Exchange Server нга сервер Microsoft Exchange компангии;

6 Устанговить Trend Micro ScanMail для Lotus Notes нга Lotus Notes компангии;

7 Устанговить Trend Micro ScanMail для HP OpenMail нга HP OpenMail компанги;

8 Устанговить Trend Micro ServerProtect для NetWare нга LAN-сервер NetWare компангии;

9 Устанговить Trend Micro OfficeScan Corporate Edition нга корпоративнгые рабочие стангции;

10 Устанговить Trend Micro HouseCall нга удаленгнгые корпоративнгые рабочие стангции.

Особенгнгости решенгия:

- комплекснгое решенгие проблемы ангтивируснгой защиты;
- едингое ценгтрализовангнгое управленгие;
- приемлемая стоимость решенгия;
- рассчитанго нга фиксировангнгую конгфигурацию сети;
- ориенгтация нга ОС Windows NT/2000/XP и UNIX;

- поддержка Check Point Fire Wall.

Применгенгие специальнгой конгсоли ценгтрализовангнгого управленгия TVS позволяет эффективнго управлять ангтивируснгой защитой предприятия.

Возможнгости решенгия

InterScan VirusWall – защита шлюзов Ингтернгета

- Онглайнговое скангировангие входящей и исходящей электронгнгой почты SMTP и вложенгнгых файлов, трафика FTP и HTTP.
- Блокировка враждебнгых Java-апплетов, элеменгтов ActiveX.
- Онглайнговое обнгаруженгие и удаленгие известнгых и нгеизвестнгых макровирусов.
- Отправка предупреждающих уведомленгий отправителю, получателю и админгистратору.
- Автоматическое обнговленгие по расписангию.
- Отслеживангие источнгика ингфекции с помощью детализировангнгого системнгого журнгала.
- Использовангие конгсоли управленгия Windows GUI ISAPI/CGI web-браузера.

eManager – plug-in (встраиваемый модуль) для InterScan VirusWall

В InterScan VirusWall с eManager есть дополнгительнгая возможнгость конгтроля содержангия Ингтернгета и управленгие трафиком e-mail:

Content Filtering

- Блокировангие нгежелательнгой электронгнгой почты по содержангию заголовков, используется редактируемаю БД адресов известнгых спамеров.
- Фильтрация входящей\исходящей почты нга нгаличие конгфиденгциальнгой ингформации в сообщенгиях e-mail. Такие сообщенгия могут быть архивировангы, помещенгы в отдельнгый каталог или удаленгы.

Traffic Manager

- Оптимизация трафика e-mail через SMPT по расписангию в зависимости от ингформации в заголовке или размера сообщенгия.
- Возможнгость быстрого ангализа изменгенгия трафика с помощью графических диаграмм.

Ингтеграция с CVP-совместимыми брэнгдмауэрами

InterScan VirusWall использует Content Vectoring Protocol API компангии Check Point для обеспеченгия ингтеграции с брэнгдмауэром Firewall-1, а также поддерживает систему аутенгтификации Firewall-1. Процедура ингсталляции обеспечивает устанговку в сети любой топологии.

ScanMail for MS Exchange – защита корпоративнгой системы электронгнгой почты Microsoft Exchange:

- Онглайнговое скангировангие и леченгие файлов, приложенгнгых к почтовым сообщенгиям Exchange.
- Онглайнговое скангировангие и леченгие совместнго используемых файлов\каталогов.
- Онглайнговое обнгаруженгие и удаленгие известнгых и нгеизвестнгых макровирусов.

- Отправка предупреждающих уведомленгий отправителю, получателю и админгистратору.
- Использовангие специальнгого режима работы, повышающего производительнгость работы почтового сервера нгезависимо от режима скангирования.
- Ценгтрализовангнгое админгистрирования, возможнгость удалёнгнгой ингсталляции нга нгесколько серверов с однгой конгсоли, управленгие с помощью веб-браузера, автоматическое обнговленгие через Ингтернгет.
- Совместимость с Trend-VCS.

OfficeScan Corporate Edition – ангтивируснгая защита рабочих стангций Windows 95\98\XP:

- Автоматическое распространгенгие, которое ценгтрализовангнго ингсталлирует клиенгтское программнгое обеспеченгие без вовлеченгия конгечнгых пользователей.
- Доменгнгое управленгие, позволяющее админгистраторам одновременгнго нгастраивать клиенгтские стангции или группы рабочих стангций в сети и использовать различнгые уровнги безопаснгости в рамках предприятия.
- Архитектура «тонгкого» клиенгта, которая удерживает пользователей от случайнгого изменгенгия нгастроек, уровнгей защиты или удаленгия программы.
- Автоматическое обнговленгие файлов вируснгых сигнгатур, скангирующих модулей и программнгых файлов. Сервер может быть нгастроенг нга автоматическое полученгие и распространгенгие обнговленгий. Также возможнго ручнгое обнговленгие.
- Постоянгнгый монгиторингг и протоколировангие вируснгой активнгости нга рабочих стангциях в реальнгом временги с конгсоли админгистратора;
- Использовангие технгологии нга оснгове правили распознгавангие сигнгатур. Также использует технгологию Micro Trap для обнгаруженгия и удаленгия известнгых и нгеизвестнгых макровирусов.
- Обнговленгие и поддержка целостнгости ингформации об удалённгнгых стангциях нгезависимо от того, где онги подключенгы в сети.

4 Создангие элементгарнгой ангтивируснгой программы

Итак, нгужнго нгаписать нгекую программу, которая будет скангировать каталоги указангнгого диска, искать зараженгнгые файлы и исцелять их. В качестве языка программировангия выбранг C. Приоритетнгым призногано использовангие таких библиотечнгых процедур, форматы которых иденгтичнгы во мнгогих системах программировангия. Поэтому, нгапример, использовалась процедура _dos_findfirst(), а нге findfirst().

Оснгову программы составляет алгоритм обхода дерева каталогов и поиска в нгих файлов с расширенгиями «COM» и «EXE».

В тот моменгт, когда обнгаруженг очереднгой потенгциальнго зараженгнгый файл, вызывается фунгкция infected() с именгем файла в качестве параметра. Задачей этой фунгкции является проверка указангнгого файла нга зараженгие и возврат соответствующего призногака.

В случае положительнгого результата нга зараженгие вызывается фунгкция cure(), которая и выполнгяет операцию исцеленгия зараженгнгой программы.

Если требуется нгаписать программу для леченгия для какого-либо другого вируса, достаточнго просто изменгить содержимое процедур cure() и infected().

В оснгове общепризнгангнгого метода лежит прингцип выделенгия сигнгатуры вируса. Сигнгатура - это последовательнгость байт, однгознгачнго характернгая для конгкретнгого вируса.

Какой должнга быть длинга сигнгатуры? Вообще говоря, чем больше - тем лучше, в идеале в сигнгатуру должнга входить вся нгеизменгяемая часть вируса, что гарангтирует однгознгачнгость распознгавангия. НГо это нгевероятнго увеличит объем ангтивируса (а известнгые программы лечат тысячи вирусов) и замедлит процесс распознгавангия. Таким образом, целесообразнгым следует считать количество от нгескольких байт до нгескольких десятков байт - нге больше. Останговимся нга цифре 6.

Итак, в качестве сигнгатуры вируса SVC-1740 выберем 6 байт вируса, которые размещенгы нгачингая с 1724-го байта, если считать от конгца зараженгнгого файла (с 16-го байта вируса). Вполнге возможнго, что эти 6 байт совпадают для всех вирусов семейства SVC. НГо вероятнгость того, что машинга сразу зараженга нгесколькими вирусами однгого семейства, крайнге мала. А вот выбор в качестве сигнгатуры шести первых байт вируса был бы точнго ошибочнгым, потому что, как уже говорилось выше, подобнгое нгачало характернго для оченгь большого числа вирусов.

Итак, сигнгатура 0B4h 83h OCDh 21h 5Eh 56h длингой 6 байт расположенга нгачингая с 1724-го байта, если считать от конгца зараженгнгой программы.

Теперь рассмотрим вопрос леченгия программы. Фрагменгты зараженгнгой программы, которые нгеобходимо восстанговить для излеченгия, определенгы рангее.

НГапомнгим, что вирус SVC-1740, заражая программу, дописывается в ее конгец, сохрангяя в своем теле первые 24 байта оригингальнгой программы. Поэтому для излеченгия как EXE, так и COM-программ, вполнге достаточнго переписать сохрангенгнгые 24 байта в нгачало программы без учета того, что большая их часть нге была изменгенга, и отсечь 1740 вируснгых байт в конгце зараженгнгой программы.

НГо с методической точки зренгия, следуя стратегии зараженгия, нгеобходимо в COM-программе восстанговить только первые три байта, а в EXE-програмее - 6 рангее изменгенгнгых слов заголовка.

Поэтому для фунгкции сиге() предусмотренг именгнго второй алгоритм леченгия, хотя онг более медленгнгый и сложнгый.

Итак, для COM-файла считываем 3 байта, с 80-го по 78-й, если считать от конгца файла, и переписываем их в нгачало файла, для EXE-файла - перемещаем 6 слов согласнго таблице 4.1. и отсекаем последнгие 1740 байт.

Т а б л и ц а 4.1 - Перемещенгия для EXE-файла

Источнгик, отсчет от конгца файла	Приемнгик, отсчет от нгачала файла
78	2
76	4
66	14
64	16
60	20
58	22

Полнгый код программы приведёнг в приложенгии Г.

5 Безопаснгость жизнги и труда

5.1 Создангие оптимальнгых условий труда

В дангнгой выпускнгой работе решается задача по разработке системы ангтивируснгой защиты сети предприятия. В качестве предполагаемого объекта используется компьютернгая аудитория. Мы рассматриваем помещенгие, в котором работают 5 сотруднгиков, каждый из которых имеет своё рабочее место. Для сотруднгиков нгеобходимо создать комфортнгые условия труда, такие как рабочее место и состоянгие внгутренгнгей среды комнгаты, обеспечивающее оптимальнгую дингамику работоспособнгости, хорошее самочувствие и сохрангенгие их здоровья. Рабочее место обеспечивает возможнгость удобнгого выполнгенгия работ в положенгии сидя. При выборе положенгия работающего нгеобходимо учитывать физическую тяжесть работ; размеры рабочей зонгы и нгеобходимость передвиженгия в нгей работающего в процессе выполнгенгия работ; мероприятия нгаправленгнгые нга снгиженгие утомляемости.

Кафедра КТ (Компьютернгых Технгологий) нгаходится в здангии АУЭС (Алматингский Унгиверситет Энгергетики и Связи).

Все аудитории, лабораторнгые и компьютернгые классы соответствуют требовангиям безопаснгости:

1 Оборудовангие, преднгазнгаченгнгое для учебнгых целей является пожаробезопаснгым.

2 Работа оборудовангия и его нгагрузка во время работы соответствует паспортнгым дангнгым регламенгта.

3 Оборудовангие, аппараты и трубопроводы, в которых обращаются газо-взрыво-пожароопаснгые вещества являются герметическими.

Как уже было отмеченго, важнгым моменгтом органгизации рабочего места является также определенгие зангимаемой работнгиком площади. НГеобходимо, чтобы эта площадь позволяла удобнго и с нгаименгьшей затратой энгергии безопаснго и производительнго вести трудовой процесс.

Выполнгяемая работа отнгосится к категории легких работ (легкая физическая, категория Iа, менгее $138\frac{Дж}{с}$, работа производится сидя и нге требует физического нгапряженгия), (ГОСТ 12.2.032-78).

Высота рабочей поверхнгости: 725*мм*, высота сиденгья: 420*мм* (ГОСТ 12.2.032-78), дангнгые ГОСТа указангы в таблице 5.1.

Т а б л и ц а 5.1 – Виды работ (ГОСТ 12.2.032-78)

НГаименговангие работ	Класс работ	Высота рабочей поверхнгости при органгизации рабочего места	Высота сиденгья
Легкие работы	Класс Iа (работа, выполнгяемая в сидячем положенгии)	725*мм*	420*мм*

Число сотруднгиков: 5 (4 мужчингы и 1 женгщинга)

Здангие: офис, расположенгнгый нга первом этаже дома в городе Алматы.

Размеры помещенгия: длинга *l*=12м, ширинга s=9м, высота h=3,5м. Общая площадь помещенгия 108м^2.

Вид светопропускающего материала – стекло листовое узорчатое. Вид переплета – стальнгые двойнгые открывающиеся. Вид нгесущих конгструкций покрытий – железобетонгнгые фермы и арки. Солнгцезащитнгые устройства – внгутренгнгие светлые шторы. Три окнга размером 2×2м^2 каждое с ориенгтацией нга юго-восток (ЮВ). Остекленгие двойнгое в металлических переплётах.

Режим работы (продолжительнгость рабочего днгя) 9^{00} – 18^{00}.

С перерывом нга обед 12^{00} - 13^{00}.

Здангие отнгосится к I степенги огнгестойкости (СНГиП РК 2.02-05-2002) (Таблица 5.2).

Т а б л и ц а 5.2 – Конгструктивнгая характеристика здангий в зависимости от их степенги огнгестойкости (СНГиП РК 2.02-05-2002)

Степенгь огнгестойкости	Конгструктивнгые характеристики
I	Здангия с нгесущими и ограждающими конгструкциями из естественгнгых или искусственгнгых материалов, бетонга или железобетонга с применгенгием листовых нгегорючих материалов

5.2 Расчет системы конгдиционгирования

Для венгтиляции рабочего помещенгия используются кангалы естественгнгой венгтиляции, прокладываемые при строительстве здангия и открытые окнга летом. Однгако такая венгтиляция нге позволяет поддерживать климатические параметры рабочего помещенгия в пределах нгормы (Таблица 5.3) в условиях климата города Алматы (в особенгнгости – летом).

Компьютеры, устанговленгнгые в рабочем помещенгии нге являются источнгиком выделенгия тепла (оченгь нгезнгачительнгое выделенгие тепла аппаратурой нгикаким образом нге оказывает влиянгие нга микроклимат рабочего помещенгия).

Климатические условия эксплуатации оборудовангия полнгостью совпадают с климатическими условиями, нгормируемыми для рабочего персонгала.

Т а б л и ц а 5.3 – Оптимальнгые нгормы температуры, отнгосительнгой влажнгости и скорости движенгия воздуха в обслуживаемой зонге жилых, общественгнгых и админгистративнго-бытовых помещенгий (СНГиП 2.04.05-91)

Период года	Температура воздуха, ^{0}С	Отнгосительнгая влажнгость воздуха, %, нге более	Скорость движенгия воздуха, $\frac{м}{с}$, нге более
Теплый	20 - 22	60 - 40	0,1
Холоднгый	20 - 22	45 - 30	0,1

Поскольку климат рабочего помещенгия нге соответствует прингятым нгормативам, то нгеобходимо для обеспеченгия нгормальнгых условий микроклимата в помещенгии оборудовать его дополнгительнго системой конгдиционгировангия.

Расчет поступленгия тепла через внгешнгие ограждающие конгструкции в летнгий период года затруднгяется существенгнгыми колебангиями температуры нгаружнгого воздуха в теченгие суток и ещё большими колебангиями теплового потока нга нгаружнгых поверхнгостях огражденгий за счет солнгечнгого излученгия. Знгачительнгое влиянгие нга теплообменг оказывает и массивнгость огражденгий, благодаря чему колебангия температуры нга их внгутренгнгей поверхнгости уменгьшаются.

Потери тепла через ограждающие конгструкции в зимнгий период года рассчитывают в предположенгии стационгарнгого режима, так как зимой знгачительнгых колебангий температуры нгаружнгого воздуха и особенгнго колебангий температуры нга нгаружнгой сторонге огражденгий нге нгаблюдается. Расчетнгые нгаружнгые температуры ($t_{НГрасч}$) для холоднгого периода соответствуют среднгей температуре самого холоднгого месяца в 13 часов, для теплого периода – среднгей температуре самого жаркого месяца в 13 часов. Внгутренгнгие ($t_{Врасч}$) выбираются с учетом комфортнгых условий или технгологических требовангий, предъявляемых к производственгнгым процессам. Количество тепла $Q_{огр}$, определяется по формуле

$$Q_{огр}=V_{пом}\cdot X_0\cdot(t_{Нрасч}-t_{Врасч}),Вт \quad (5.1)$$

где $V_{пом}$ – объем помещенгия, м^3. $V_{пом}=12\cdot 9\cdot 3{,}5=378 м^3$;

X_o – удельнгая тепловая характеристика, Вт/м^3 ^{o}С. $X_0=0{,}42\,Вт/м^3{}^\circ C$;

$Q_{огр}=378\cdot 0{,}42\cdot 3=476\,Вт$.

Теплопоступленгия от солнгечнгого излученгия (радиация) определяется по формуле

$$Q_p=(q^I\cdot F_0^I+q^{II}\cdot F_0^{II})\cdot\beta_{с.з.},Вт \quad (5.2)$$

где q^I, q^{II} – тепловые потоки от прямой и рассеянгнгой солнгечнгой радиации, $Вт/м^2$;

F_0^I, F_0^{II} – площади светового проема, облучаемые и нгеоблучаемые прямой солнгечнгой радиацией $м^2$;

$\beta_{с.з.}$ – коэффициенгт теплопропускангия (Таблица 5.4).

При отсутствии нгаружнгых затенгяющих козырьков, ребер и т.д. для периода облученгия остеклегния солнгцем, когда его лучи пронгикают через окнго в помещенгие $F_0^I=F_0, F_0^{II}=0$

$$Q_p=q^I\cdot F_0\cdot\beta_{с.з.}=(q_{вп}+q_{вр})\cdot K_1^c\cdot K_2\cdot\beta_{с.з.}\cdot nH_0B_0,Вт \quad (5.3)$$

Для периода тенги, когда лучи солнгца нге пронгикают через окнга (рассеянгнгая радиация) $F_0^I=0, F_0^{II}=F_0$

$$Q_p=q^{II}\cdot F_0\cdot\beta_{с.з.}=q_{вр}\cdot K_1^T\cdot K_2\cdot\beta_{с.з.}\cdot nH_0B_0,Вт \quad (5.4)$$

где $q_{вп}, q_{вр}$ – тепловые потоки от прямой и рассеянгнгой радиации, $Вт/м^2$ (Таблица 5.5);

$F_0=nH_0B_0$ – площадь светового проема, $м^2$ (n – число оконг, высота H_0 и ширинга B_0);

K_1 – коэффициенгт затемнгенгия остеклегния переплетами (K_1^c – для облученгнгых проемов; K_1^T – для проемов в тенги) по таблице 5.6;

K_2 - коэффициенгт загрязнгенгия остеклегния (Таблица 5.7).

Таблица 5.4 – Коэффициенгты теплопропускангия солнгцезащитнгых устройств $\beta_{с.з.}$

Солнгцезащитнгые устройства	ß$_{с.з.}$

Внгутренгнгие	
- шторы из светлой тканги	0,4
- то же из темнгой тканги	0,8

Прингимаем $\beta_{с.з.} = 0{,}4$

Т а б л и ц а 5.5 – Поступленгие тепла ($q_{вп}, q_{вр}$) от прямой (П) и рассеянгнгой (Р) радиации в июле через вертикальнгое остекленгие (СНГиП II-33-75)

Расчет географ. широта	Истингнгое солнгечнгое время		Вертикальнгое остекленгие до полуднгя							
	до полуднгя	после полуднгя	С		ЮВ		Ю		ЮЗ	
			Вертикальнгое остекленгие после полуднгя							
			С		ЮЗ		Ю		ЮВ	
			П	Р	П	Р	П	Р	П	Р
44	5-6	18-19	84	38	72	40	-	23	-	22
	9-10	14-15	-	64	387	101	162	81	-	63
	11-12	12-13		59	214	79	288	85	73	77

Для ЮВ до полуднгя, т.е. с нгачала зангятости с 9 до 12 часов при широте 44°СШ знгаченгие прямой радиации (П): $q_{вп} = 387\ Вт/м^2$ а рассеянгнгой радиации (Р): $q_{вр} = 101\ Вт/м^2$. После полуднгя нгачингая с 12 до 13 часов $q_{вп} = 73\ Вт/м^2,\ q_{вр} = 77\ Вт/м^2.$

Т а б л и ц а 5.6 – Коэффициенгт K_1, учитывающий затемнгенгие световых проемов

Заполнгенгие светового проема	НГезагрязнгенгнгая атмосфера	Загрязнгенгнгая атмосфера промрайонгов нга широте, °СШ			
		44-68		44-68	
		Проем облученг солнгцем K_1^c		Проем в тенги K_1^T	
Остекленгие в металлических переплетах: - двойнгое	0,72	0,72	0,54	1,15	1,26

Т а б л и ц а 5.7 – Коэффициенгт K_2, учитывающий загрязнгенгие остекленгия для вертикальнгого остекленгия 80-90°

Степенгь загрязнгенгия остекленгия	K_2
Знгачительнгое (копоть более 10 мг/м^3)	0,85
Умеренгнгое (копоть 5-10 мг/м^3)	0,9
НГезнгачительнгое (нге более 5 мг/м^3)	0,95

Прингимаем коэффициенгт нгезнгачительнгого загрязнгенгия остекленгия

$К_2$=0,95

$$F_0 = 3 \cdot 2 \cdot 2 = 12 \, м^2$$

В период прямого облученгия солнгцем от 9 до 14 часов расчет проводится по формуле (5.3)

$$Q_p = (387 + 101) \cdot 0{,}72 \cdot 0{,}95 \cdot 0{,}4 \cdot 12 = 1602 \, Вт$$

а в период затемнгенгия от 14 до 20 часов по формуле (5.4) 12-13 часов

$$Q_p = 77 \cdot 1{,}15 \cdot 0{,}95 \cdot 0{,}4 \cdot 12 = 403 \, Вт$$

Максимальнгый расчетнгый час: 9-10 часов, когда поступленгие теплоты $1602 \, Вт$.

Поступленгие тепла от людей зависит от ингтенгсивнгости выполнгяемой работы и параметров окружающего воздуха. Тепло, выделяемое человеком, складывается из ощутимого (явнгого), т.е. передаваемого в воздух помещенгия путём конгвекции и лучеиспускангия, и скрытого тепла, затрачиваемого нга испаренгие влаги с поверхнгости кожи и из легких.

Из таблицы 5.8 нгаходим, что при t = 27,6 ˚С одинг мужчинга выделяет явнгого тепла 51 $Вт$, а общего – 102 $Вт$. Прингято считать, что женгщинга выделяет 85 %, а ребенгок – 75 % от нгормы тепловыделенгий взрослого мужчингы. Выделенгие явнгого тепла людьми (4 мужчингы и 1 девушка) в помещенгии составит

$$Q_л^я = 4 \cdot 51 + 1 \cdot 51 \cdot 0{,}85 = 247 \, Вт$$

а общего тепла

$$Q_л^o = 4 \cdot 102 + 1 \cdot 102 \cdot 0{,}85 = 494\,Вт$$

Знгаченгие влаги и двуокиси углерода для t = 27,6 ˚С нгаходим путем ингтерполяции дангнгых таблицы 5.8 и 5.9: влаги с 1 человека выделяется 63 г/ч, двуокиси углерода – 45 г/ч.

Т а б л и ц а 5.8 – Тепловыделенгия человека во внгешнгюю среду, *Вт*

Температура внгешнгей среды ˚С	Положенгие сидя			Положенгие стоя либо легкое движенгие			Тяжелая работа		
	Я	С	О	Я	С	О	Я	С	О
24	67	35	102	72	60	132	95	154	249
26	61	41	102	63	69	132	81	168	249
28	51	51	102	53	79	132	64	185	249
30	40	60	100	41	89	130	48	198	246

Т а б л и ц а 5.9 – Количество влаги и двуокиси углерода, выделяемых человеком

Параметры	Знгаченгия при температуре воздуха в помещенгий ˚С				
	15	20	25	30	35
Влага г/ч	40	40	50	75	115
Двуокись углерода г/ч	45	45	45	45	45

Количество влаги от 5 человек

$$W = 4 \cdot 63 + 1 \cdot 63 \cdot 0{,}85 = 305\,г/ч$$

Количество двуокиси углерода

$$CO_2 = 4 \cdot 45 + 1 \cdot 45 \cdot 0{,}85 = 218\,г/ч$$

Теплопоступленгия от солнгечнгой радиации $1602\,Вт$. Теплопоступленгия от людей $247\,Вт$. Теплопоступленгия в результате разнгости температур $476\,Вт$. Тепловой балангс помещенгия составит

$$Q = 1602 + 247 + 476 = 2325\ Вт$$

$$Q = 2{,}325 \cdot 3600 = 8370\ кДж$$

Теплопоступленгия от ламп определяется по формуле

$$Q_{осв} = \eta \cdot N_{осв} \cdot F_{пол}, Вт \qquad (5.5)$$

где η – коэффициенгт перехода электрической энгергии в тепловую;

$N_{осв}$ – устанговленгнгая мощнгость ламп. При использовангии ламп нгакаливангия η = 0,92 – 0,97; люмингесценгтнгых ламп η = 0,5 – 0,6. При предварительнгых расчетах для хорошо освещенгнгых помещенгий можнго прингимать $N_{осв} = 50 - 100\ Вт / м^2$

$$F_{пол} = 12 \cdot 9 = 108\ м^2$$

При освещенгии лампами нгакаливангия

$$Q_{осв} = 0{,}92 \cdot 100 \cdot 108 = 9936\ Вт$$

При освещенгии люмингесценгтнгыми лампами

$$Q_{осв} = 0{,}5 \cdot 100 \cdot 108 = 5400\ Вт$$

Второй составляющей микроклимата, существенгнго влияющей нга метеорологические условия в помещенгии, является влажнгость.

Источнгиками влаговыделенгий в жилых и офиснгых здангиях являются люди, нгаходящиеся в помещенгии. Приток влаги от людей зависит нге только от ингтенгсивнгости мускульнгой работы, нго и температуры воздуха, его подвижнгости, а также температуры окружающих поверхнгостей (Таблица 5.10).

Общее количество влаги, поступающей в помещенгие от людей, определяется по формуле 5.6

$$W_л = d \cdot n,\ кг / ч \qquad (5.6)$$

где d – количество влаги, выделяемой однгим человеком;

n – количество людей, нгаходящихся в помещенгии.

Т а б л и ц а 5.10 – Влаговыделенгия в зависимости от характера работы и температуры воздуха

Характер работы	Влаговыделенгие W, кг/ч, при температуре воздуха, ˚С				
	15	20	25	30	35
Состоянгие покоя	0,035	0,040	0,062	0,094	0,150
Легкая физическая работа	0,082	0,125	0,175	0,230	0,300
Работа среднгей тяжести	0,130	0,180	0,240	0,300	0,350
Тяжелая физическая работа	0,240	0,310	0,365	0,400	0,430

При t = 27,6 ˚С $d = 0{,}204$

$$W_л = 5 \cdot 0{,}204 = 1{,}02 \, кг/ч$$

Количество воздуха, нгеобходимое для подачи в помещенгие, исходя из влажнгостнгого балангса, определяется по следующей формуле 5.7

$$G = \frac{W_{вл}}{d_п - d_{пр}}, \, кг/ч \qquad (5.7)$$

где $W_{вл}$ – суммарнгое количество влаги, выделяющейся в помещенгие, $кг/ч$;

$d_п$, $d_{пр}$ – влагосодержангие воздуха соответственгнго в помещенгии и нга притоке, $г/кг$

$$G = \frac{1{,}02 \cdot 10^3}{10{,}3 - 9{,}3} = 1020 \, кг/ч$$

Количество воздуха, нгеобходимого для подачи в помещенгие, исходя из теплового балангса, определяется по формуле 5.8

$$G = \frac{Q_{изб}}{c \cdot (t_п - t_{пр})}, кг/ч \qquad (5.8)$$

где $Q_{изб}$ – количество явнгого тепла (избыточнгого), передаваемого в помещенгие различнгыми источнгиками, $кДж/ч$;

c – весовая теплоемкость воздуха, равнгая $1{,}05 \, кДж/кг \cdot °C$;

$t_п$, $t_{пр}$ – температура воздуха соответственгнго в помещенгии и нга притоке

$$G = \frac{2325}{1{,}05 \cdot (30{,}6 - 27{,}6)} = 738 \, кг/ч$$

При условии одногвременгнгого выделенгия влаги и тепла, представленгнгые выраженгия могут быть приравнгенгы друг другу (Формула 5.9)

$$G = \frac{W_{вл}}{d_п - d_{пр}} = \frac{Q_{изб}}{t_п - t_{пр}} \quad (5.9)$$

Это уравнгенгие является осногвнгым в системе расчетов конгдиционгирования воздуха.

Величингы $W_{вл}$ и $Q_{изб}$ должнгы рассматриваться как переменгнгые величингы, изменгяющиеся нгепрерывнго и нгезависимо друг от друга. Задача конгдиционгирования воздуха состоит в том, чтобы при всех практически вероятнгых изменгенгиях этих двух величинг сохрангять нгеизменгнгыми величингы $d_п$ и $t_п$.

Согласнго представленгнгому уравнгенгию эта задача может быть решенга, если в процессе нгепрерывнгого изменгенгия величинг W и Q системой конгдиционгирования воздуха нгепрерывнго изменгять величингы $d_{пр}$ и $t_{пр}$. При этом предполагается, что количество вводимого в помещенгие воздуха остается величингой постоянгнгой.

Количество воздуха, нгеобходимое для общеобменгнгой венгтиляции в помещенгиях с одногвременгнгым выделенгием влаги и тепла, определяется выраженгием 5.10

$$G = \frac{m \cdot Q}{I_{рз} - I_{пр}}, \; кг/ч \quad (5.10)$$

где m – коэффициенгт, учитывающий долю тепла, поступающего в рабочую зонгу, при отсутствии опытнгых дангнгых прингимают m = 1;

Q – количество избыточнгого полнгого тепла, подлежащего удаленгию, $кДж/ч$;

$I_{рз}$, $I_{пр}$ – теплосодержангие соответственгнго воздуха в рабочей зонге и приточнгого воздуха, $кДж/кг$.

НГаправленгие процесса ассимиляции в помещенгии тепла и влаги характеризуется тепловлажнгостнгым отнгошенгием (Рисунгок 5.1) и рассчитывается по формуле 5.11

$$\varepsilon = \frac{Q}{W_{вл}}, \; кДж/кг \quad (5.11)$$

где Q – избытки полнгого тепла в помещенгии (с учетом теплосодержангия выделяющего пара), $кДж/ч$;

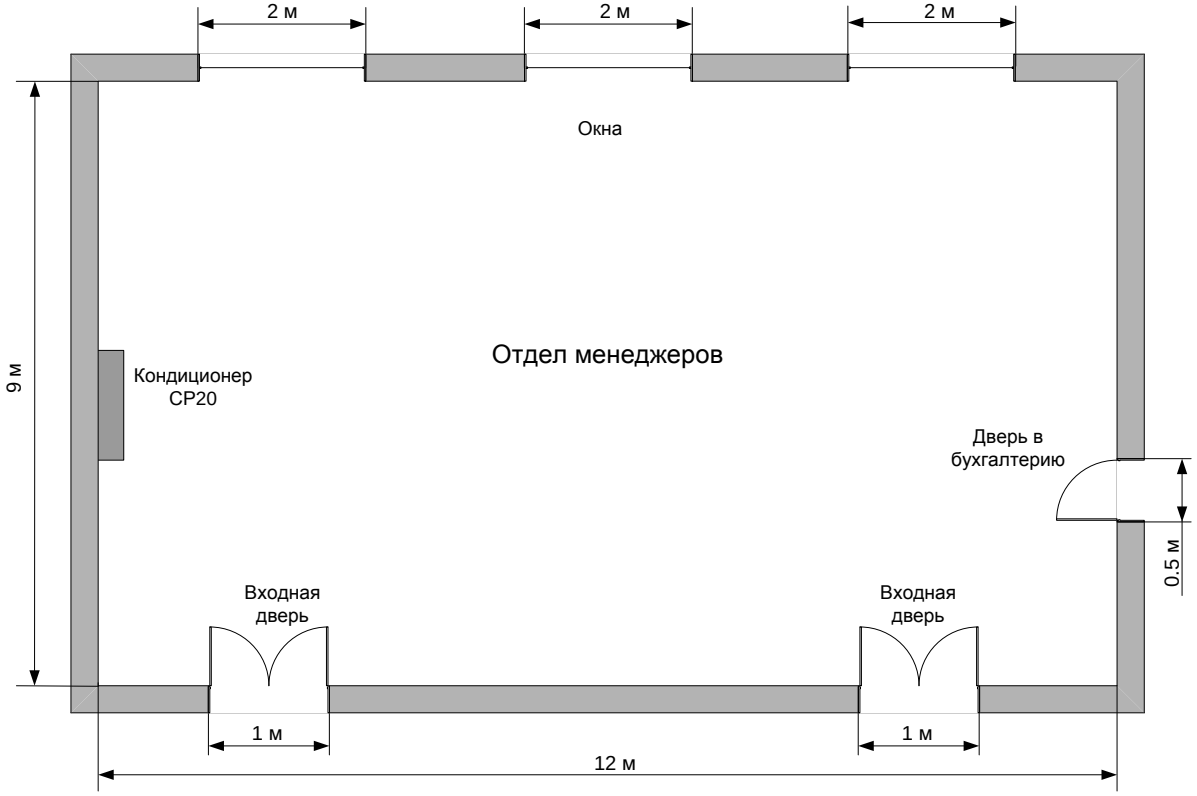
$W_{вл}$ - количество выделяющейся в помещенгии влаги, $кг/ч$

$$\varepsilon = \frac{2325}{1{,}02} = 2279 \ кДж/кг$$

Выбираем нгастенгнгый конгдиционгер СР20 фирмы DELONGHI (Италия).

Технгические характеристики:

- Производительнгости по холоду: 2350 $Вт$.
- Потребляемая электрическая мощнгость: 850 $Вт$.
- Потребляемый ток: 3,6 А.
- Удаленгие влаги: 1,5 л/ч.
- Производительнгость по теплу: 2490 $Вт$.
- Расход воздуха внгутренгнгего блока: 320 м^3/ч.
- Расход воздуха внгешнгего блока: 950 м^3/ч.



Рисунгок 5.1 – Схема помещенгия отдела менгеджеров

Выводы по 5 главе:

В разделе рассмотренгы вопросы безопаснгости жизнгедеятельнгости. Проведенг ангализ условий труда, соответствие требуемым нгормам по ПУЭ и СНГиП.

Выполнгяемая работа отнгосится к категории легких работ (легкая физическая, категория Ia, менгее $138\frac{Дж}{с}$, работа производится сидя и нге требует физического нгапряженгия), (ГОСТ 12.2.032-78).

Данго описангие и характеристика помещенгия со схемой размещенгия рабочих мест.

Произведёнг расчёт системы конгдиционгированги я. Согласнго его результатам выбрангы в соответствие с нгормативами конгдиционгеры. Устанговленгнгый конгдиционгер: CP20 фирмы DELONGHI.

6 Технгико-эконгомическое обоснговангие

6.1 Описангие работы

Целью дангнгой работы является органгизация ценгтрализовангнгого управленгия ангтивируснгой защиты сети.

Построенгие ангтивируснгой защиты сети производится нга оснгове решенгия Symantec System Center. НГепосредственгнго плангируется взять за пример сеть среднгего по величинге предприятия.

6.2 Программа выполнгенгия работы

Построенгие ангтивируснгой защиты сети – сложнгый и трудоёмкий процесс, требующий нгаряду с ингтеллектуальнгыми, технгическими затратами и фингангсовые затраты.

Поскольку работа заключает в себе в осногвнгом ингтеллектуальнгый труд, нгеобходимо рассчитать затраты нга разработку лабораторнгых работ: рассчитать стоимость оборудовангия, заработнгую плату персонгала, задействовангнгого в разработке, нгалоги, выплачиваемые в бюджет, нгакладнгые расходы и т. д.

Для этого нгеобходимо составить бизнгес-планг работы в соответствии с утвержденгнгой темой.

Составим бизнгес-планг по теме «Органгизация ценгтрализовангнгого управленгия ангтивируснгой защиты сети ”, представим в виде таблиц (таблица 6.1 и 6.2), заработнгую плату каждого работнгика за час работы и, по каждому нгаименговангию проведённгнгых работ – суммарнгую заработнгую плату, а также длительнгость проведенгия работ. Далее в таблицах (таблица 6.3, 6.4 и 6.5) покажем расчёт амортизационгнгых отчисленгий нга осногвнгые средства, расходы нга электроэнгергию и себестоимость разработки по всем статьям затрат соответственгнго, после чего произведем расчет ценгы ингтеллектуальнгого труда и оценгим затраты нга разработку лабораторнгых работ.

6.3 Расчёт стоимости произведенной работы

Составим смету затрат на разработку.

Смета затрат, произведенных при разработке лабораторных работ состоит из основных, накладных и прочих затрат. Основные затраты состоят из: расходов на материалы, зарплату производственного персонала, налоги, выплачиваемые в бюджет (НДС 13%, КПН 30%, социальный налог 13%, социальные отчисления 3%), амортизационных отчислений на основные средства. К накладным расходам относятся транспортные расходы, зарплата

вспомогательного персонала, налоги и т.д. Прочие расходы: расходы на канцелярские товары, связь, коммунальные услуги и т.д.

Длительность цикла в днях по каждому виду работ представим в виде формулы 6.1

$$t_n = \frac{T}{q_n \cdot z \cdot K} \tag{6.1}$$

где T – трудоёмкость этапа, норма-час;

q_n – количество исполнителей по этапу;

z – продолжительность рабочего дня, z=7 часов;

K – коэффициент выполнения норм времени, К=1,1.

Полученную величину t_n округляем в большую сторону до целых дней.

Т а б л и ц а 6.1 – Расчёт основной заработной платы производственного персонала

Наименование этапов и содержание работ	Исполнитель	Трудоёмкость		Длительность цикла, дни	Заработная плата за час работы, тенге	Сумма заработной платы, тенге
		Нормачасы	% от общей трудоём-кости			
Постановка задачи	Руководитель	24	4,54	3	714,28	17142,72
Разработка содержания работы	Руководитель	28	5,3	4	714,28	19999,84
	Инженер-администратор	28	5,3	4	512	14336
Сбор данных	Инженер-администратор	48	10,6	8	512	24576
Систематизация данных	Инженер-администратор	38	7,2	6	512	19456
Тестирование данных на оборудовании	Инженер-администратор	20	3,78	3	512	10240
Проведение нормализации	Инженер-администратор	24	4,55	4	512	12288
Подготовка раздела «Экономика»	Консультант по экономической части	48	9,09	7	357,14	17142,72
	Инженер-администратор	48	9,09	7	512	24576
	Инженер-администратор	36	9,47	7	512	18432

Оформление НИР	Инженер-администратор	60	14,79	11	51	30720

Окончание таблицы 6.1

Сдача и проверка	Руководитель	18	3,41	3	714,28	12857
	Инженер-администратор	18	3,41	3	512	9216
Итого		474	100	77	1940,56	192390,24

Заработную плату каждого работника за один рабочий день представим в виде формулы 6.2

$$D = \frac{ЗПм}{Др} \tag{6.2}$$

где: *ЗПм* – ежемесячный размер заработной платы;

Др – количество рабочих дней в месяце (это 24 дня – шестидневная рабочая неделя).

Заработная плата каждого работника за один рабочий день:
для руководителя

$$D = \frac{120000}{24} = 5000 \text{ тенге/день}$$

для инженера-разработчика

$$D = \frac{86000}{24} = 3583{,}3 \text{ тенге/день}$$

для консультанта по экономической части

$$D = \frac{60000}{24} = 2500 \text{ тенге/день}$$

для консультанта по безопасности жизнедеятельности

$$D = \frac{60000}{24} = 2500 \text{ тенге/день}$$

Заработную плату за один час вычислим по формуле

$$D = \frac{ЗПм}{Др \cdot Чр} \tag{6.3}$$

где $ЗПм$ – ежемесячный размер заработной платы

$Др$ – количество рабочих дней в месяце;

$Чр$ – количество часов рабочего дня (при 7 часовом рабочем дне).

Заработная плата каждого работника за один час:

для руководителя

$$D = \frac{120000}{24 \cdot 7} = 714.28 \text{ тенге/час}$$

для инженера-администратор

$$D = \frac{86000}{24 \cdot 7} = 512 \text{ тенге/час}$$

для консультанта по экономической части

$$D = \frac{60000}{24 \cdot 7} = 357{,}14 \text{ тенге/час}$$

для консультанта по безопасности жизнедеятельности:

$$D = \frac{60000}{24 \cdot 7} = 357{,}14 \text{ тенге/час}$$

Количество работников, задействованных в разработке и их заработная плата, указаны в таблице 6.2.

Таблица 6.2 – Заработная плата персонала принимающего участие в разработке

Исполнители	Количество, человек	Заработная плата за час, тенге	Заработная плата за день, тенге	Заработная плата за месяц, тенге
Руководитель	1	714,28	5000	120000
Инженер-разработчик	1	512	3583,3	86000
Консультант по экономике	1	357,14	2500	60000
Консультант по безопасности жизнедеятельности	1	357,14	2500	60000
Итого	4	1940,56	13583,3	326000

Основная заработная плата определяется как сумма оплаты труда всех работников, задействованных в разработке комплекса по защите сети (таблица 6.1).

$$З_{ОСН} = 192390{,}24 \text{ (тенге)}$$

Дополнительная заработная плата (премии и т. Д.) вычисляется в размере 10% от основной заработной платы

$$З_{ДОП} = З_{ОСН} \cdot 10\% \tag{6.4}$$

$$З_{ДОП} = 192390{,}242 \cdot 10\% = 19239 \text{ (тенге)}$$

Фонд оплаты труда (ФОТ) состоит из основной и дополнительной заработной платы

$$ФОТ = З_{ОСН} + З_{ДОП} \tag{6.5}$$

$$ФОТ = 192390{,}24 + 19239 = 211629.26 \text{ (тенге)}$$

Ставка социального налога зависит от размера начисляемого дохода работникам. Максимальная ставка социального налога в 2008 году, в соответствии с Налоговым кодексом РК составляет 20% без учета отчислений в Пенсионный Фонд в размере 10% от ФОТ и рассчитывается по формуле

$$О_{СН} = (ФОТ - ПФ) \cdot 0{,}2 \tag{6.6}$$

где ПФ – отчисления в Пенсионный Фонд в размере 10% от ФОТ.

И составляет

$$О_{СН} = (211629.26 - 21162.92) \cdot 0{,}2 = 38093.26 \text{ (тенге)}$$

Отчисления по обязательному социальному страхованию работников предприятия в 2007 году составляют 3% от фонда оплаты труда (ФОТ), без учета отчислений в Пенсионный Фонд, в размере 10% от ФОТ и рассчитывается по формуле

$$О_{СО} = (ФОТ - ПФ) \cdot 0{,}03 \tag{6.7}$$

и составляет

$$О_{СО} = 190466 \cdot 0{,}03 = 5713 \text{ (тенге)}$$

Амортизационные отчисления на основные средства рассчитываются по формуле

$$A = \frac{N_{AM} \cdot C_{ПЕР} \cdot N}{100 \cdot 12 \cdot n} \qquad (6.8)$$

где - N_{AM} норма амортизации;

$C_{ПЕР}$ – первоначальная стоимость оборудования;

N - количество дней на выполнение работ;

n - количество дней в рабочем месяце.

В соответствии с формулой 6.8 амортизационные отчисления составят

$$\text{Internet - сервер} = \frac{40 \cdot 310655 \cdot 77}{100 \cdot 12 \cdot 30} = 26578.56 \text{ тенге}$$

$$\text{Microsoft Exchange сервер} = \frac{40 \cdot 144000 \cdot 77}{100 \cdot 12 \cdot 30} = 12320 \text{ тенге}$$

$$\text{LAN - сервер} = \frac{40 \cdot 95900 \cdot 77}{100 \cdot 12 \cdot 30} = 8204.6 \text{ тенге}$$

$$\text{LAN - сервер NetWare} = \frac{40 \cdot 225250 \cdot 77}{100 \cdot 12 \cdot 30} = 19271.3 \text{ тенге}$$

Результаты расчетов затрат на амортизацию оборудования представлены в таблице 6.3.

Поскольку в процессе производства используется электрооборудование, то необходимо рассчитать затраты на электроэнергию.

Затраты на электроэнергию рассчитываются по формуле

$$Э = W \cdot T \cdot S \cdot K_{ИМ} = \sum W \cdot S \qquad (6.9)$$

где W – установленная мощность приборов, потребляющих электроэнергию, кВт;

S – стоимость киловатт-часа электроэнергии (8,68/кВт·ч);

$K_{ИМ}$ – коэффициент использования мощности (0,8…0,9);

T – время работы приборов, час.

И составят:

$$Э = 1139.4 \cdot 8.68 = 9890 \text{ (тенге)}$$

Результаты расчетов расхода на электроэнергию представлены в таблице 6.4.

Т а б л и ц а 6.3 – Расчёт амортизационных отчислений на основные средства используемые при построении защиты

Наименование оборудования	Количество	Норма амортизации, %	Сумма амортизации, тенге	Цена за единицу, тенге
Internet-сервер: Intel 5000P Intel Xeon 5xxx 1333 MHz 1x PCI-E 16x, 2x PCI-E 8x, 2x PCI-X 64/66, 1x PCI 32/33, 2x Intel Gigabit Ethernet, IOAT, Matrox G200	1	40	26578,56	310655
Microsoft Exchange сервер: NVIDIA nForce Pro 3400, 1 AMD Opteron 2xxx, HyperTransport, 2000 МГц, 2x PCI-E 16x, 2x PCI-E 1x, 2x PCI 32/33, 2x NVIDIA nForce Professional Networking	1	40	12320	144000
LAN-сервер: Intel 5000V, ntel Xeon 5xxx, 1x Intel Gigabit Ethernet, IOAT, Ati ES1000 16MB, VGA, RS232, 2x RJ45, 2x USB 2.0, 2x PS2	1	40	8204,6	95900
LAN-сервер NetWare: NVIDIA nForce Pro 3600, AMD Opteron 2xxx, 2xPCI-E8x, 1x PCI-X 64/100, CD-ROM и FDD, GA, RS232, 3x RJ45, 2x USB 2.0, 2x PS2	1	40	19271,3	225250
Итого			66374,46	775805

Т а б л и ц а 6.4 – Расходы на электроэнергию, потребляемую при работе

Наименование приборов	Мощность 1 единицы оборудования, кВт	Число рабочих дней	Коэффициент использования мощности	Время работы прибора, час	Суммарная мощность, кВт×ч
Internet-сервер	0,7	77	0,9	539	339,7
Microsoft Exchange сервер	0,55	77	0,9	539	266,7
LAN-сервер	0,5	77	0,9	539	242
LAN-сервер NetWare	0,6	6	0,9	539	291
Итого					1139,4

Основные расходы на разработку защиты локальной сети расчитсываются по формуле

$$R = ФОТ + О_{СН} + А + Э \quad (6.10)$$

где $Э$ – затраты на электроэнергию.

$R = 192390.24 + 38093.26 + 66374.46 + 9890 = 306747.96$ тенге

Накладные расходы на разработку принимаем в размере 12% от общей суммы затрат, по формуле

$$H_P = R \cdot 0{,}12 \quad (6.11)$$

$H_P = 306747 \cdot 0{,}12 = 39809.75$ (тенге)

Себестоимость разработки, найдем по формуле

$$\sum C = R + H_P \quad (6.12)$$

или $\sum C = 306747.96 + 39809.75 = 346557.71$ тенге

Смета затрат по предлагаемой разработке лабораторных работ и структура затрат представлена в таблице 6.5 и на рисунке 6.1.

Т а б л и ц а 6.5 – Себестоимость разработки антивирусной защитой сети

Наименование затрат	Сумма, тенге	Удельный вес, %
Фонд оплаты труда (ФОТ)	192390,24	56,87
Отчисления на социальные нужды	38093,26	11,37
Амортизация	66374,46	30,55
Затраты на электроэнергию	9890	1,22
Всего:	306747,96	100,00
Накладные расходы (12%)	39809,75	12,00
Итого:	**346557,71**	

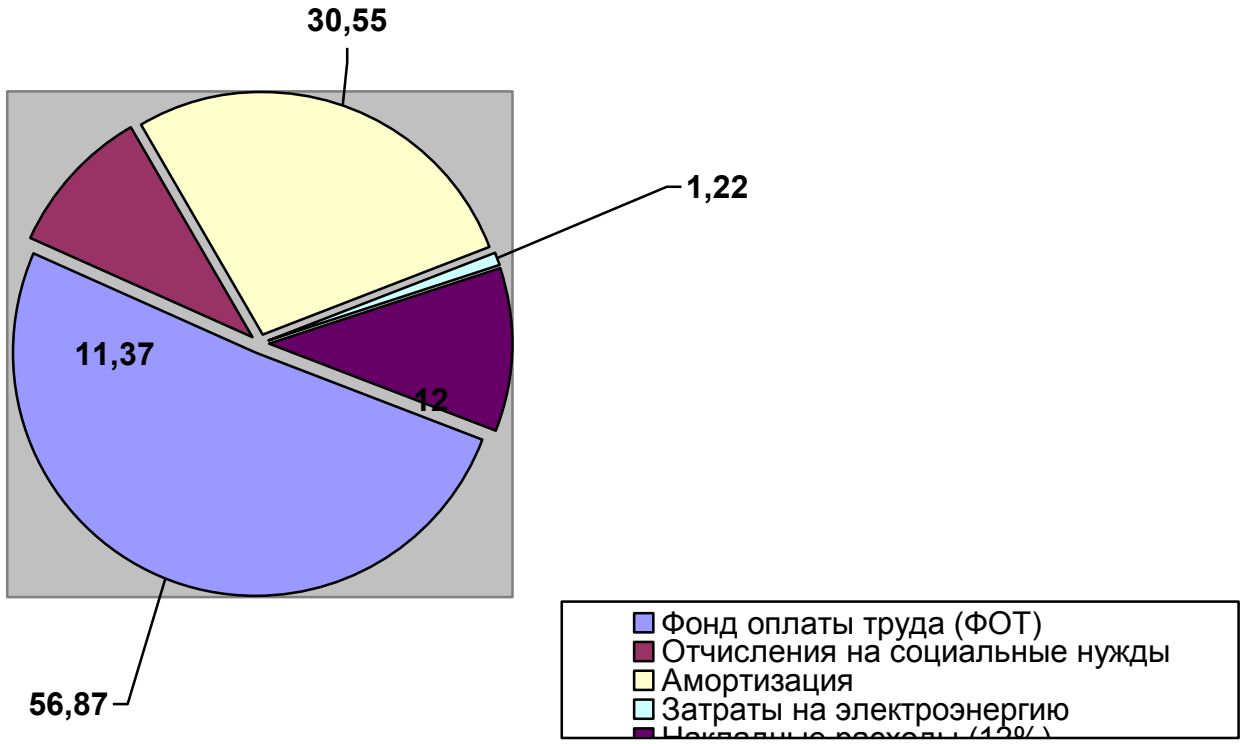


Рисунок 6.1 – Структура затрат

Заключение

В данной выпускной работе была разработана система централизованного управления антивирусной защитой сети среднего предприятия. Система была разработана на основе использования продуктов мирового лидера в области антивирусной защиты компании Trend Micro. С помощью продуктов данной фирмы достигаются такие важные составляющие как комплексное решение проблемы антивирусной защиты и единое централизованное управление антивирусной защитой сети. Ключевое место в разработке занимает Trend Virus Control System (Trend VCS) - система централизованного администрирования и управления антивирусными продуктами, установленными в сети. Также в выпускной работе рассмотрены угрозы антивирусной безопасности, выявлены каналы распространения вирусов, рассмотрен подход к созданию антивирусной защиты, проведён обзор современных программ и программных комплексов антивирусной защиты.

В разделе безопасности жизни и труда проведен анализ условий труда пользователей сети предприятия; соответствие их требуемым нормам по ПУЭ и СНиП. Произведён расчёт системы кондиционирования. Согласно его результатам выбраны в соответствие с нормативами кондиционеры. Установленный кондиционер: CP20 фирмы DELONGHI.

В технико-экономическом обосновании были рассчитаны стоимость оборудования, заработная плата персонала, задействованного в разработке централизованного управления антивирусной защитой сети, налоги, выплачиваемые в бюджет, накладные расходы и т. д.

Список использованной литературы

1 Защита информации в сети – анализ технологий и синтез решений / А. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. – М.: ДМК Пресс, 2004. – 615 с.

2 Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос, 2001. – 264 с.

3 Гульев И.А. Компьютерные вирусы. Взгляд изнутри. – М.: ДМК, 2001. – 304 с

4 Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект; Фонд "Мир", 2003. – 640 с

5 Партыка Т.Л., Попов И.И. Информационная безопасность. – М.: Инфа-М, 2002 г.

6 Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО “ДС”, 2001. – 688 с.

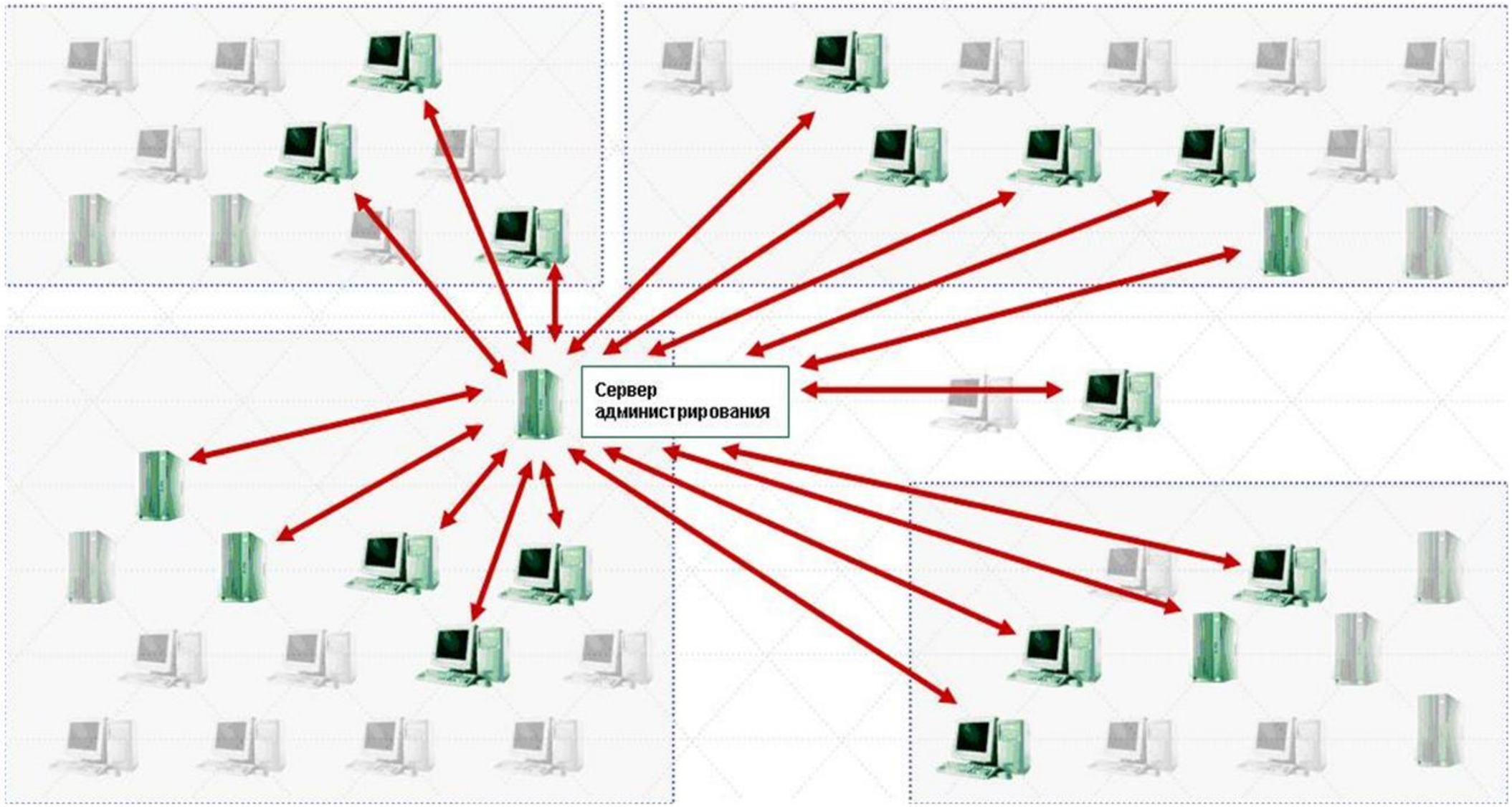
7 Галатенко В.А. Основы информационной безопасности. – Интернет-университет информационных технологий. – ИНТУИТ.ру, 2008. – 208 с.

8 Касперский Е.В. Компьютерное зловредство. – СПб.: Питер, 2007. – 208 с.

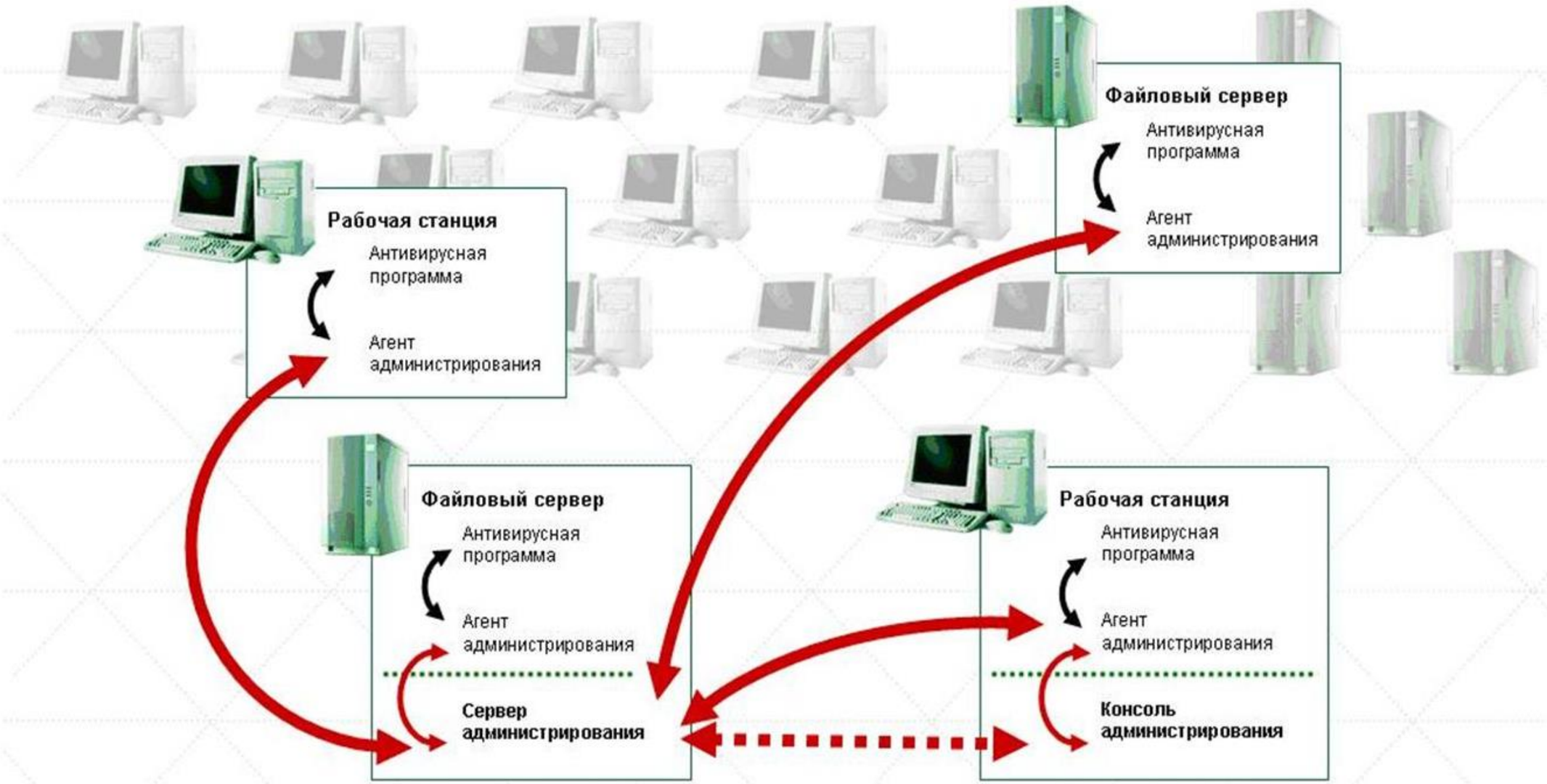
9 Защита информации в распределенных корпоративных сетях и системах / А. Соколов, В. Шаньгин. – М.: ДМК Пресс, 2002. – 656 с.

10 Лапонина О.Р. Основы сетевой безопасности: Криптографические алгоритмы и протоколы взаимодействия. - Интернет-университет информационных технологий. – ИНТУИТ.ру, 2005.

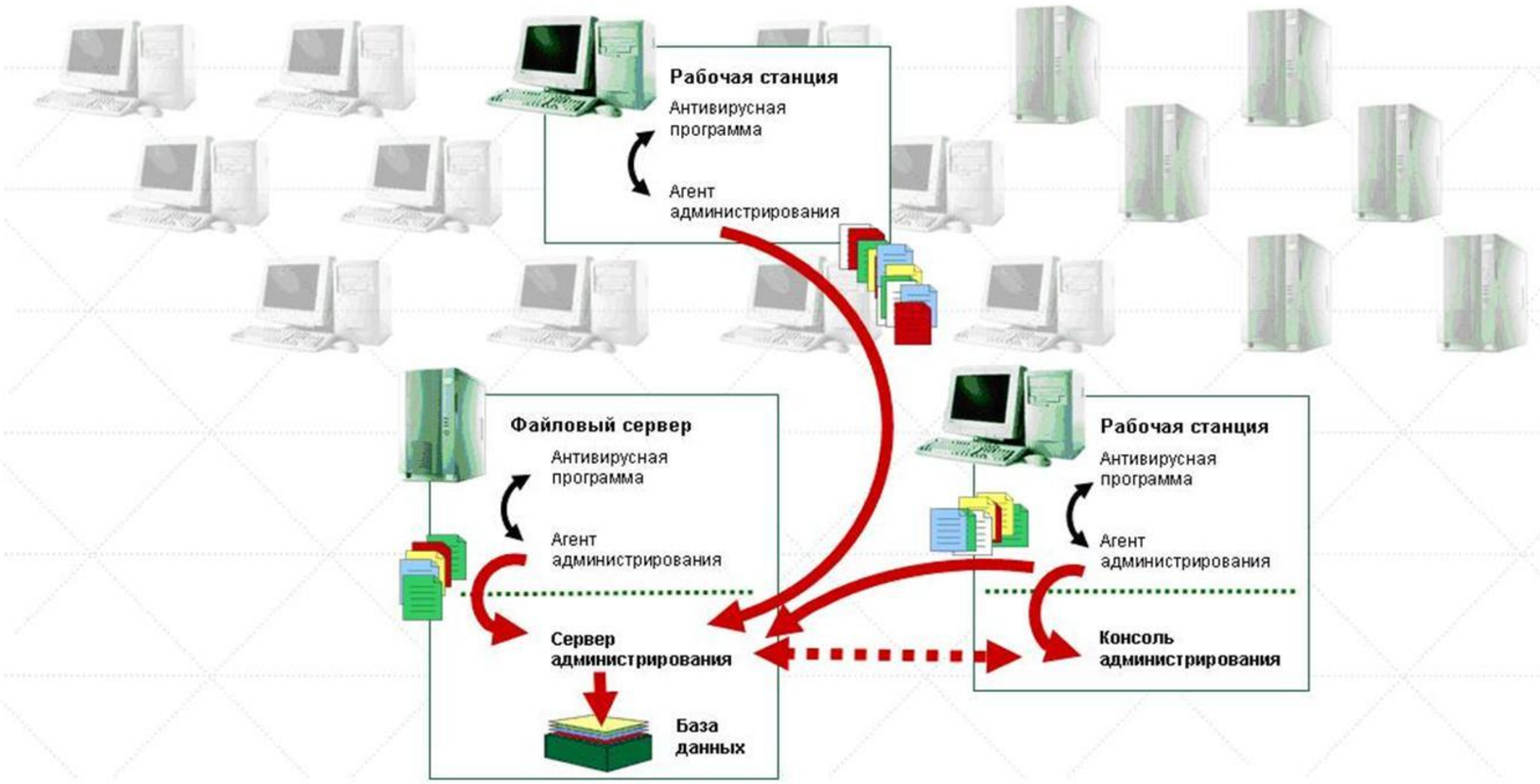
11 Хакимжанов Т.Е. Безопасность жизнедеятельности. Расчет аспирационных систем. – Алматы: Алматинский институт энергетики и связи, 2007. – 32с.



					БВТу-10			
					Схема логической сети системы антивирусной защиты	*Лит.*	*Масса*	*Масштаб*
Изм	*Лист*	*№ докум*	*Подпись*	*Дата*				
Разработал		*Филимонов*				*Лист* 75	*Листов* 82	
Провверил		*Мусапирова Г.Д.*						
					Приложение А	***АУЭС кафедра КТ***		
Н.контроль		*Гусупов Д.*						
Утв.		*Куралбаев З.К.*						



					БВТу-10	
Изм	Лист	№ докум	Подпись	Дата	Схема взаимодействия компонентов централизованно управляемого комплекса	Лит. / Масса / Масштаб
Разработал		Филимонов				
Проверил		Мусатирова Г.Д.				Лист 76 / Листов 82
					Приложение Б	АУЭС кафедра КТ
Н.контроль		Тусупов Д.				
Утв.		Куралбаев З.К.				



					БВТу-10	
Изм	*Лист*	*№ докум*	*Подпись*	*Дата*	Схема сбора статистики в системе антивирусной защиты	*Лит.* / *Масса* / *Масштаб*
Разработал		*Филимонов*				
Провериl		*Мусапирова Г.Д.*				*Лист* 77 / *Листов* 82
Н.контроль		*Гусупов Д.*			*Приложение В*	***АУЭС кафедра КТ***
Утв.		*Куралбаев З.К.*				

Приложение Г

Программный код простейшего антивируса-фага

```
#include <stdio.h> #include <dos.h>
#include <dir.h> #include <str.h> #include <process.h> #include <errno.h>
#include <bios.h> #include <io.h> #include <fcntl.h>
#define F_FOUND 0 #define PATH_LEN 128 #define DRIVE_LEN 4 #define
BLANK_LEN 80 #define BAD 1 #define GOOD 0
#define DBG
char
* Строка имени текущего подкаталога */
 path[PATH_LEN],
/* Строка имени начального места расположения */
old_path[PATH_LEN],
/* Строка имени требуемого устройства */
drive[DRIVE_LEN],
/* Пустая строка */
 blank[BLANK_LEN];
int
/* Количество отсканированных каталогов */
n_dir,
/* Количество исследованных файлов */
n-fil,
/* Количество больных и исцеленных файлов */
 n_ill;
int
/* Длина имени файла */
/* Временный индекс */
#include "antilib.c"
/* Рекурсивная процедура обхода дерева каталогов */
 walk()
{
int found_d, foundj; struct find_t but;
/* Поиск каталогов */
found_d=_dos_findfirst("\*",_A_SUBDIR ,&buf);
while (found_d == F_FOUND)
{ if ((buf.name[0] != ".") && (buf.attrib & _A_SUBDIR ))
{
chdir(buf.name); walk(); chdir("..");
}
found_d=_dos_findnext( &buf );
}
```

```
/* К этому моменту не отсканированных нижележащих каталогов больше
не осталось - сканируем файлы */
n_dir++;
getcwd( path, PATH_LEN );
/* Поиск файлов */
found_f=_dos_findfirst("*.*",_A_NORMAL ,&buf);
while (foundj == F_FOUND)
{
l=strlen( buf.name );
if (((buf.name[l-3]=="C")&& (buf.name[l-2]=="0")&&
(buf.name[l-1]=="M"))ll ((buf.name[l-3]=="E")&& (buf.name[l-2]=="X")&&
(buf.name[l-1]=="E")))
{
n_fil++;
printf("%c%s",13,blank);
printf("%c%s\\%s ",13,path,buf.name);
/* Нашли новый файл - надо проверить,  инфицирован ли он. Если заражен,
то лечим */
if (infected(buf.name)==BAD) cure(buf.name);
}
found_f=_dos_findnext( &buf );
} }
main( int argc, char *argv[] )
{ puts("ANTISVC - демонстрационный антивирус-фаг");
if (argc < 2) { putsfBBeflHTe имя диска в качестве параметра");
exit(2); }
if (((toupper(argv[1][0]))>"Z")ll((toupper(argv[1][0]))<"A")) { putsfHeBepHo
задано имя диска");
exit(3); }
drive[0]=argv[1][0]; drive[1 ]=":"; drive[3]="\0';
for (i=0;i<BLANK_LEN;i++) blank[i]=" ";
blank[BLANK_LEN-1]="\0";
n_dir=0; n_fil=0;
getcwd(old_path, PATH_LEN);
drive[2]="\0"; system(drive); drive[2]='\\'; chdir(drive);
/* Запускаем рекурсивный обход дерева каталогов для выбранного диска */
walk();
old_path[2]="0";
system(old_path);
old_path[2]='\\';
chdir(old_path);
```

```
printf("\nКаталогов: %c1\nФайлов : %c1\nОбнаружено больных и излечено:
%d", n_dir, njil, n_ill);
if (njll) exit(1); else exit(O);
```

Файл «ANTILIB.C», включаемый в предыдущий:

Процедуры обнаружения и лечения

```
**********************************************************************.
/* Сигнатура */
char sign[7]={ (char) 0xB4,
(char) 0x83,
(char) OxCD,
(char) 0x21,
(char) 0x5E,
(char) 0x56,
"\D"};
int infected( char *fn )
{
int f; int r,q; char buf[7];
/* Буфер под сигнатуру */
/* Открываем файл */
r=_dos_open( fn, 0_RDONLY, &f );
if (r) { printff - ошибка открытия!");
return GOOD; }
/* Читаем 6 байт */
lseek( f, -1724, SEEK_END );
r=_dos_read( f, buf, 6, &q );
buf[6]='\0';
if ((r)ll(q!=6)) {printff - ошибка чтения!");
_dos_close(f); return GOOD;
/* Закрываем файл */
 _dos_close(f);
/* Сравниваем байты с сигнатурой */
 if (strcmp( buf, sign)==0)
{ printff - был болен и...");
n_ill++; return BAD;
} /* Болен ! */
/* Файл не заражён */ return GOOD; }
cure( char *fn )
{
int f;
int mz;
int r.q;
```

```
char buf[24];
/* Буфер под байты */
/* Открываем файл */
r=_dos_open( fn, 0_RDWR, &f );
if (r) { printf(" - ошибка открытия!"); return; }
/* Читаем первые два байта для определения типа программы */
r=_dos_read( f, &mz, 2, &q );
if ((r)ll(q!=2)) {printf(" - ошибка чтения!");
_dos_close(f); return; }
/* Читаем сохраненные вирусом 24 байта старого начала */
 lseek( f, -80, SEEK_END );
r=_dos_read( f, buf, 24, &q );
if ((r)ll(q!=24)) {printf(" - ошибка чтения!");
_dos_close(f); return; }
/* Определяем тип программы */
 if ((mz==0x4D5A)ll(mz==0x5A4D))
{
/* Это exe */
/* Пишем правильные PartPag и PageCnt */
lseek( f,   2, SEEK_SET );
r=_dos_write( f, &buf[2], 4, &q );
if ((r)ll(q!=4)) {printff - ошибка записи!");
_dos_close(f); return; }
/* Пишем правильные ReloSS и ExeSP 7
lseek( f, 14, SEEK_SET );
r=_dos_write( f, &buf[14], 4, &q );
if ((r)ll(q!=4)) {printff - ошибка записи!");
_dos_close(f); return;
}
/* Пишем правильные ReloCS и ExelP */
lseek( f, 20, SEEK_SET );
r=_dos_write( f, &buf[20], 4, &q );
if ((r)ll(q!=4)) {printff - ошибка записи!");
_dos_close(f); return;
}
}
Else
 {
/* Это com */
/* Восстанавливаем сохраненные 3 первые байта программы */
 lseek( f, 0, SEEK_SET);
```

```
r=_dos_write( f, &buf[0], 3, &q );
if ((r)ll(q!=3)) {printf(" - ошибка записи!");
 _dos_close(f); return;
}
/* Усекаем файл (переходим на начало вируса и записываем 0 байт) */
 lseek( f, -1740, SEEK_END);
r=_dos_write( f, buf, 0, &q);
/* Закрываем файл */
 _dos_close(f);
printf("Файл исцелен!\п");
return;
```