МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт Факультет приборостроения, информационных технологий и электроники	Кафедра «Информационная безопасность систем и технологий»

Специальность 10.05.03 – Информационная безопасность автоматизированных систем

Специализация - Защищенные автоматизированные системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

МЕТОДИКА РАЗВЕРТЫВАНИЯ НА ПРЕДПРИЯТИИ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ

Студент _____ Логашов Владимир Алексеевич

Руководитель _____ Земсков Д.В.

Нормоконтролёр _____ Фатеев А.Г.

Рецензент инженер по защите информации ООО "ПЗТГ" _____ Крылов А.В.

Работа допущена к защите (протокол заседания кафедры от 15.06.20 № 13)

Заведующий кафедрой _____ С.Л. Зефиров

Работа защищена с отметкой удовлетворительно (протокол заседания ГЭК от 26.06.20г № 19)

Секретарь ГЭК _____ А.П. Иванов

Пенза 2020

Оглавление

Введение…….…..4
1 Анализ информационно-телекоммуникационной системы, входящей в состав автоматизированной системы управления…….....6
2 Обзор известных антивирусных средств с сетевым центром управления…...11
2.1 Антивирусные средства с сетевым центром управления…….11
2.2 Антивирусное средство Kaspersky Endpoint Security……....11
2.3 Антивирусное средство Symantec Endpoint Protection……..12
2.4 Антивирусное средство Dr.Web Enterprise Security……..13
3 Анализ возможных проблем при развертывании средств антивирусной защиты с сетевым центром управления…….19
4 Описание виртуального стенда……21
5 Методика развертывания средств антивирусной защиты с сетевым центром управления……23
5.1 Разработка методики развертывания средств антивирусной защиты с сетевым центром управления……..…23
5.2 Установка консоли администрирования и сетевого центра управления……...23
5.3 Создание групп компьютеров с различными версиями антивирусных средств……..28
5.4 Добавление компьютеров в группы…….…...……..30
5.5 Создание политик для групп компьютеров с различными версиями антивирусного средства……..32
5.6 Создание задач для групп компьютеров с различными версиями антивирусного средства……..39
5.7 Распределение трафика генерируемого в системе в процессе функционирования антивирусного средства……45
6 Вредные психофизиологические факторы, влияющие на опорно-двигательный аппарат специалиста по защите информации. Методы и средства

физической культуры, снижающие их воздействие…….……..…..46
6.1 Общие сведения……46
6.2 Обзор вредных психофизиологические факторов, влияющих на опорно-двигательный аппарат специалиста по защите информации.……47
6.3 Обзор методов и средств физической культуры.……...47
Заключение…...…….51
Список использованных источников……..52

Введение

В настоящее время компьютерные вирусы являются одной из наиболее опасных и значимых угроз безопасности.

Основными видами угроз антивирусной безопасности являются различные типы вредоносного программного обеспечения, способного нанести определённый вред автоматизированной системе или её пользователям. Вредоносное программное обеспечение представляет собой компьютерные вирусы, а также программы типа «Троянский конь», «adware», «spyware» и др.

Сегодня сети компаний находятся в постоянном развитии. Однако вместе с ним постоянно растет и число точек проникновения вирусов в корпоративные сети Интернет/интранет. Как правило, такими точками являются: шлюзы и серверы Интернет, серверы файл-приложений, серверы групповой работы и электронной почты, рабочие станции [1].

Для небольших предприятий, использующих до 10 узлов, целесообразны решения по антивирусной защите, имеющие удобный графический интерфейс и допускающие локальное конфигурирование без применения централизованного управления. Для крупных предприятий предпочтительнее системы антивирусной защиты с несколькими консолями и менеджерами управления, подчиненными некоторому единому общему центру. Такие решения позволяют обеспечить оперативное централизованное управление локальными антивирусными клиентами и дают возможность при необходимости интегрироваться с другими решениями в области безопасности корпоративных сетей.

Целью дипломного проекта является разработка методики развертывания на предприятии средств антивирусной защиты с сетевым центром управления.

В процессе выполнения дипломного проекта осуществляется:

– анализ информационно-телекоммуникационной системы, входящей в состав автоматизированной системы организации;

– обзор известных средств антивирусной защиты с сетевым центром управления;

– анализ возможных проблем при развертывании на предприятии средств антивирусной защиты с сетевым центром управления;

– разработка методики развертывания на предприятии средств антивирусной защиты с сетевым центром управления;

– технология развертывания на предприятии средств антивирусной защиты с сетевым центром управления;

– мероприятия по обеспечению комфортных условий труда при разработке методики развертывания на предприятии средств антивирусной защиты с сетевым центром управления;

– проектирование и расчет сетевого графика разработки методики развертывания на предприятии средств антивирусной защиты с сетевым центром управления.

1 Анализ информационно-телекоммуникационной системы, входящей в состав автоматизированной системы управления

Антивирусная защита является неотъемлемой частью системы защиты автоматизированной системы управления. Организационные и технические меры защиты информации, реализуемые в автоматизированной системе управления в рамках ее системы защиты, в зависимости от класса защищенности, угроз безопасности информации, используемых технологий и структурно-функциональных характеристик автоматизированной системы управления и особенностей ее функционирования, должны обеспечивать антивирусную защиту [2].

Информационно-телекоммуникационная подсистема автоматизированной системы организации состоит из 21 автоматизированного рабочего места, имеющие связь между собой. Автоматизированные рабочие места в организации разбиты на группы, согласно выполняемых ими функций. Структурная схема информационно-телекоммуникационная подсистема автоматизированной системы приведена на рисунке 1.

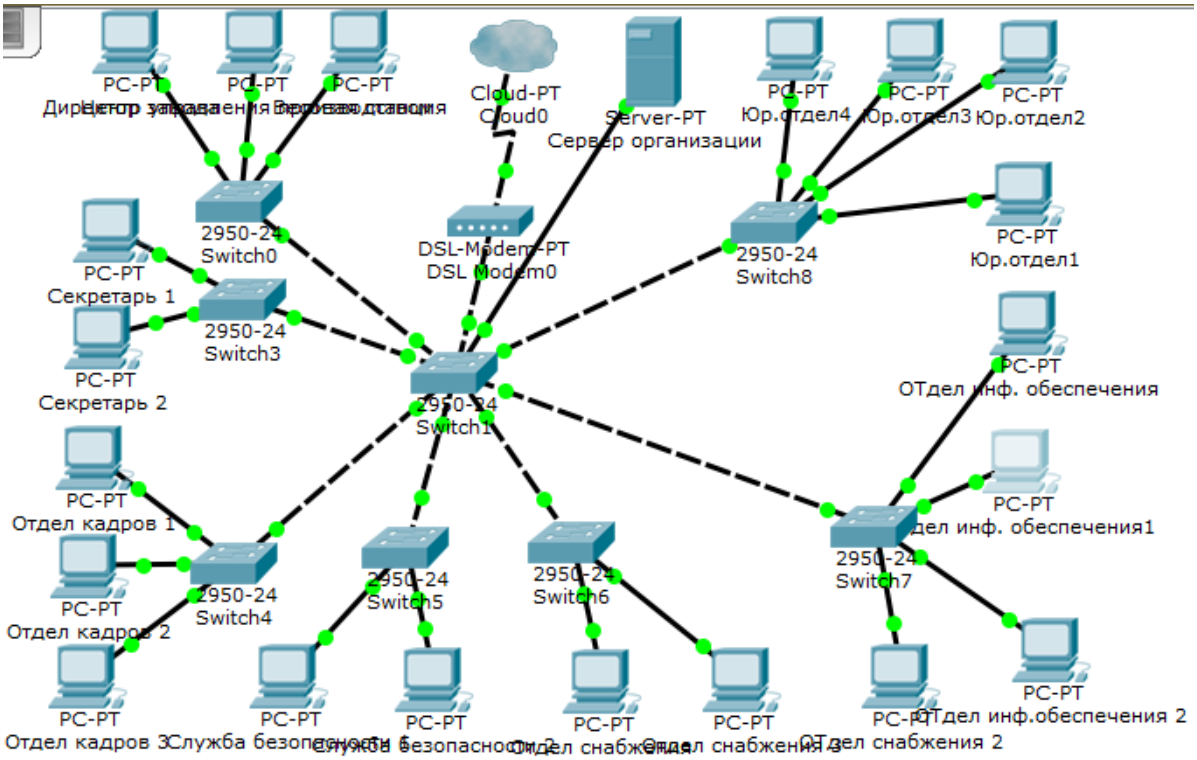

Рисунок 1 – Структурная схема ИТКС организации

Далее, было определено время работы узлов, с целью выявления оптимального времени для выполнения практических работ и реализации задач антивирусного средства. Данные о времени работы узлов представлены в таблице 1.

Таблица 1 – Время работы узлов

Название узла	Время работы
Директор завода	С 8.00 до 17.00
Секретарь 1	С 8.00 до 17.00
Секретарь 2	
Отдел кадров 1	С 8.00 до 17.00
Отдел кадров 2	
Отдел кадров 3	
Служба безопасности 1	Круглосуточно
Служба безопасности 2	
Отдел снабжения 1	С 8.00 до 17.00
Отдел снабжения 2	
Отдел снабжения 3	
Отдел информационного обеспечения 1	Круглосуточно
Отдел информационного обеспечения 2	
Отдел информационного обеспечения 3	
Юридический отдел 1	С 8.00 до 17.00
Юридический отдел 2	
Юридический отдел 3	
Центр управления производством	Круглосуточно
Весовая станция	Круглосуточно

Были описаны основные бизнес-процессы протекающие в организации, а так же основные информационные потоки. Общий вид и декомпозиция процесса при помощи диаграммы IDEF0 были показаны на рисунках 2 и 3 соответственно.

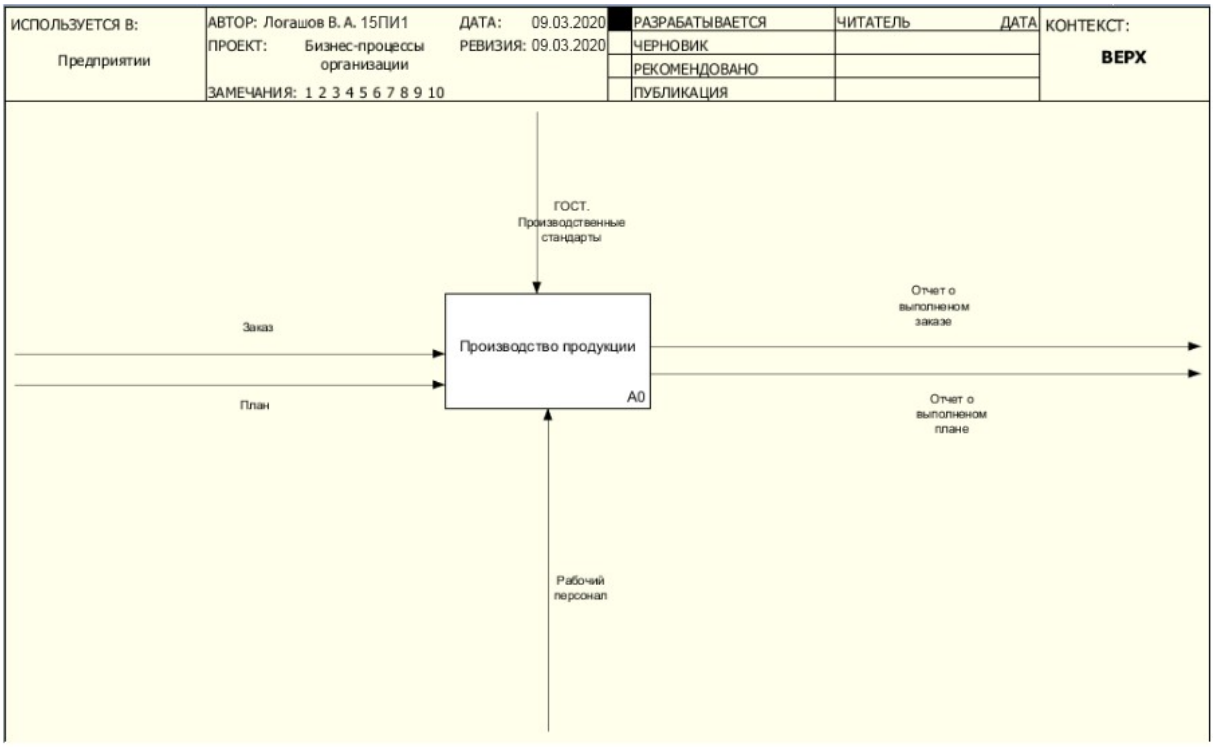

Рисунок 2 – Основной бизнес-процесс

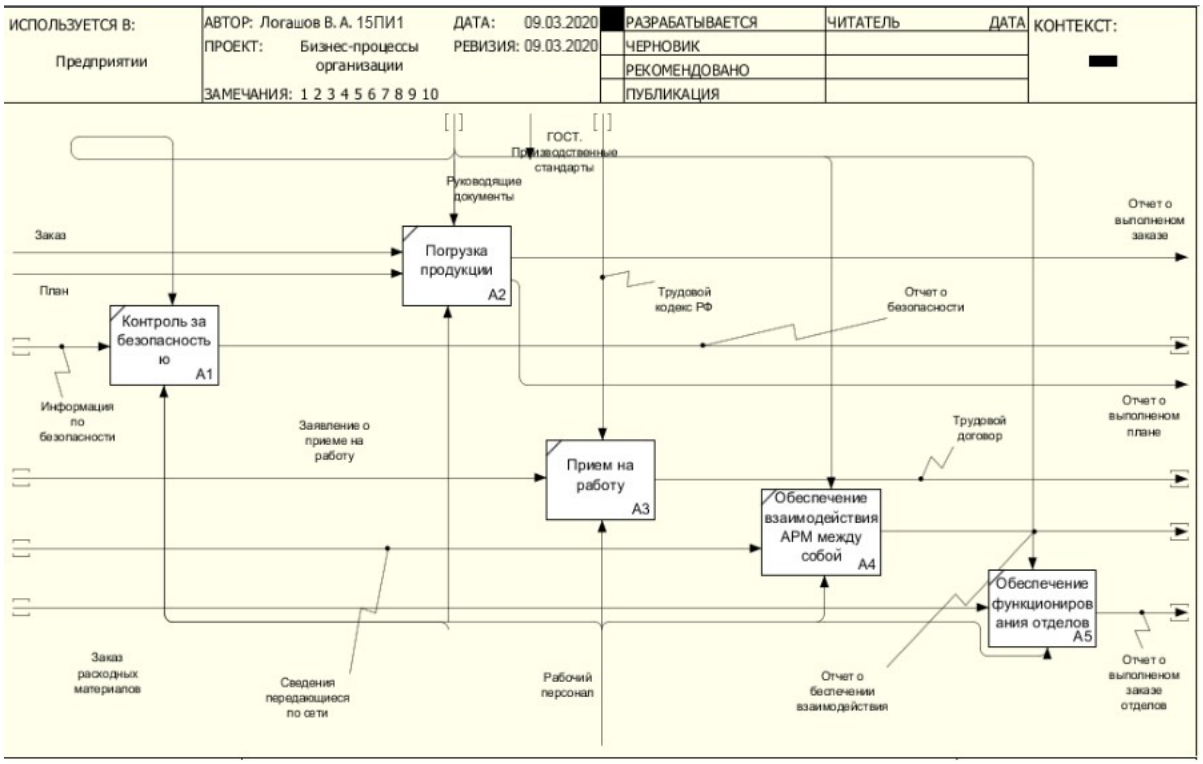

Рисунок 3 – Декомпозиция основного бизнес-процесса

Исходя из основных бизнес-процессов, были определены основные потоки информации в организации. Информационные потоки представлены в таблице 2.

Таблица 2 – Информационные потоки

Отдел	Взаимодействие	Объем информации	Передаваемые данные
Директор завода	Весовая станция	Средний	Отчет о погрузке
	Цент управления	Высокий	Отчет о производстве
	Отдел кадров	Средний	Отчет о принятых работниках
	Служба безопасности	Средний	Отчет о происшествиях
	Снабжение	Средний	Отчет о закупках
Весовая станция	Центр управления	Высокий	Отчет о произведенной продукции

Была описана производительность компьютеров в организации. Перечень компьютеров и их характеристик приведена в таблице 3.

Таблица 3 – Производительность компьютеров, находящихся в организации

Компонент автоматизированной системы	Производительность
Секретарь 1	Microsoft Windows 2000 Professional (SP 4 Rollup1). Процессор Intel Pentium 300 МГц. 256 МБ RAM. KAV 6.0
Секретарь 2	
Отдел кадров 1	Microsoft Windows XP Professional (SP 2). Процессор Intel Pentium 300 МГц. 256 МБ RAM. KAV 6.0
Отдел кадров 2	
Отдел кадров 3	

Продолжение таблицы 3

Компонент автоматизированной системы	Производительность
Служба безопасности 1	Microsoft Windows 2000 Professional (SP 4 Rollup1). Процессор Intel Pentium 300 МГц. 256 МБ RAM. KAV 6.0
Служба безопасности 2	
Отдел снабжения 1	Microsoft Windows 7 Professional/ Enterprise/ Ultimate SP1. Процессор Intel Pentium 800 МГц. 512 МБ RAM. KES v.10
Отдел снабжения 2	
Отдел снабжения 3	
Юридический отдел 1	Microsoft Windows 7 Professional/ Enterprise/ Ultimate SP1. Процессор Intel Pentium 800 МГц. 512 МБ RAM. KES v.10
Юридический отдел 2	
Юридический отдел 3	
Весовая станция	Microsoft Windows 2000 Professional (SP 4 Rollup1). Процессор Intel Pentium 300 МГц. 256 МБ RAM. KAV 6.0
Директор завода	Microsoft Windows 7. Процессор с частотой 1ГГц. При 64-разрядной ОС 1.4 ГГц. Оперативная память 4 ГБ. HDD 10 ГБ. KES v.10
Центр управления производством	
Отдел информационных технологий 1	
Отдел информационных технологий 2	
Отдел информационных технологий 3	

2 Обзор известных антивирусных средств с сетевым центром управления

2.1 Антивирусные средства с сетевым центром управления

На данном этапе дипломного проектирования проводился обзор известных антивирусных средств с сетевым центром управления. Выбор надежного антивирусного продукта очень важен для достижения целей информационной безопасности.

Сетевой центр управления является средством управления антивирусной защитой корпоративной сети. Сетевой центр управления позволяет централизованно инсталлировать и управлять всеми компонентами антивирусного комплекса, установленными на различных уровнях корпоративной сети: на переносных компьютерах мобильных пользователей, рабочих станциях, файловых серверах, серверах приложений, почтовых системах, Web-серверах, межсетевых экранах.

Управление может осуществляться как с выделенного компьютера в рамках корпоративной сети, так и с удаленного компьютера.

При помощи сетевого центра управления возможно централизованно обновлять антивирусные базы, инсталлировать новые версии продуктов на всех участках сети; составлять гибкое расписание запусков, защищать параметры работы модулей антивируса на каждой отдельной рабочей станции или сервере и многое другое. В рамках дипломного проектирования было выбрано три антивирусных средства с сетевым центром управления:

- Kaspersky Endpoint Security;
- Symantec Endpoint Protection;
- Dr. Web Enterprise Security.

2.2 Антивирусное средство Kaspersky Endpoint Security

Kaspersky Endpoint Security для Windows это современная многоуровневая защита компьютеров и ноутбуков под управлением Windows в локальной сети организации. Комплексная защита от всех видов угроз обеспечивается

многоуровневой системой, включающей контроль запуска и активности программ, контроль внешних устройств, веб-контроль доступа к ресурсам сети Интернет и защиту от вредоносных программ, онлайн и сетевых угроз. Каждый тип угроз контролируется и обрабатывается отдельным компонентом Kaspersky Endpoint Security. Компоненты можно включать и выключать независимо друг от друга, а также настраивать различные параметры их работы, обеспечивая оптимальный уровень защиты. Инструмент централизованного управления защитой в локальной сети организации Kaspersky Security Center позволяет удаленно установить антивирусное решение на рабочие станции, настроить параметры защиты для компьютеров сети, управлять обновлениями ПО и антивирусных баз, контролировать статус защиты и оперативно реагировать на события. Корпоративная платформа «Лаборатории Касперского» Kaspersky Security для бизнеса включает в себя множество новейших инструментов и технологий для защиты всей IT-инфраструктуры, обеспечивая сохранность конфиденциальной информации и безопасный доступ пользователей к сетевым ресурсам. Помимо полноценной защиты традиционных рабочих станций и серверов решение Kaspersky Security для бизнеса позволяет контролировать и защищать мобильные устройства, предоставляет передовые антиспам-технологии, дает возможность шифровать наиболее важную информацию, а также помогает управлять удаленным доступом к корпоративной сети [3].

2.3 Антивирусное средство Symantec Endpoint Protection

Symantec Endpoint Protection гарантирует высокий уровень безопасности, быстродействие и интеллектуальное управление в физических и виртуальных средах. Благодаря использованию преимуществ крупнейшей в мире глобальной информационной сети Symantec обеспечивает превентивное выявление подверженных угрозам файлов и защиту от новейших атак без замедления работы. Symantec Endpoint Protection предназначен для защиты рабочих станций и серверов, работающих под управлением ОС Windows, Mac OS X и Linux (как 32-битных редакций, так и 64-битных). Компьютеры, работающие

под управлением этих операционных систем, составляют подавляющее большинство технического парка находящегося в локальных сетях предприятий.

Основная документация по Symantec Endpoint Protection переведена на русский язык и выполнена достаточно качественно. Основной документ «Руководство по внедрению Symantec Endpoint Protection и Symantec Network Access Control» имеет объём 1167 страниц. Тем не менее, это достаточно структурированный документ, в котором администратор антивирусной сети может найти ответы на большинство вопросов, возникающие в процессе развёртывания и эксплуатации Symantec Endpoint Protection . Для начинающих администраторов Symantec Endpoint Protection предлагается документ «Руководство по началу работы с Symantec Endpoint Protection», который имеет объём 32 страницы и содержит необходимую базовую информацию по началу работы с Symantec Endpoint Protection. Некоторые документы, относящиеся к описанию работы с клиентами Symantec Endpoint Protection, предлагаются только на английском языке. Например, это касается документации на антивирусный пакет для Linux-систем. Интерфейс клиентов для Windows полностью русифицирован. Инсталляционный пакет для Mac OS X русифицирован частично (имеются англоязычные окна), а интерфейс самого клиента доступен сугубо на английском языке. Клиент для защиты компьютеров, работающих под управлением Linux-систем, доступен только на английском языке, что, в общем-то, не должно быть препятствием для администраторов Linux-систем [4].

2.4 Антивирусное средство Dr.Web Enterprise Security

Dr.Web Enterprise Security Suite обеспечивает процесс построения и централизованного управления антивирусной защитой компьютеров и устройств пользователя. Администратор безопасности может управлять антивирусной системой защиты корпоративной сети из любой точки мира и практически с любого компьютера или устройства, имеющего выход в сеть

Интернет. Для его работы достаточно компьютера с любой операционной системой и выходом в Интернет. При этом для управления защитой не требуется устанавливать какое-либо дополнительное программное обеспечение. Единственным требованием является наличие интернет браузера. Интуитивно понятный интерфейс позволяет развернуть всю антивирусную сеть за рекордно короткие сроки. При этом система защиты может быть развернута практически в любой корпоративной сети организации, вне зависимости от ее размера и особенностей – общего количества сотрудников и филиалов, топологии, наличия или отсутствия сервера Active Directory. Развертывание антивирусной системы с легкостью можно провести из любой точки мира, причем для этого от администратора не потребуется никаких специальных навыков. Центр управления позволяет администратору, работающему внутри сети или на удаленном компьютере, централизованно управлять всеми компонентами защиты компьютера пользователя, отслеживать состояние всех защищенных узлов, получать уведомления о произошедших вирусных инцидентах, лечить или удалять зараженные файлы, а также настраивать автоматическую реакцию на них. Для этого достаточно лишь наличия связи между рабочим местом администратора и антивирусным сервером [5]. Было произведено сравнение антивирусных средств в таблице 4.

Таблица 4 – Сравнение антивирусных средств

Антивирусное средство/Параметр сравнения	Kaspersky Endpoint Security	Symantec Endpoint Protection	Dr.Web Enterprise Security
Поддержка мультиплатформенных сред	+	+	+
Простота управления и оформление отчетов	+	+	+
Возможность удаления конкурирующих продуктов	-	+	-

Продолжение таблицы 4

Антивирусное средство/Параметр сравнения	Kaspersky Endpoint Security	Symantec Endpoint Protection	Dr.Web Enterprise Security
Возможность поддержки виртуализации	+	-	-
Использование шифрования	+	-	-
Динамические белые списки	+	-	-
Наличие единой консоли управления	+	+	+
Сокращение сетевого трафика	+	+	+
Цена за базовую версию продукта	1265 рублей	2218 рублей	1100 рублей

При сравнении были определены основные параметры, по которым можно определить уровень возможностей различного антивирусных средств и качество их работы:

– поддержка мультиплатформенных сред – возможность корректной установки антивирусного программного обеспечения на различные операционные системы, такие как MacOS, Windows, Linux;

– простота управления и оформления отчетов – простой и понятный интерфейс антивирусного программного обеспечения, простая фильтрация и удобное создание отчетов по выборкам, необходимым в данный момент;

– возможность удаления конкурирующих продуктов – возможность удаления уже установленных антивирусных средств, при установке нового антивирусного средства;

– сокращение сетевого трафика – возможность антивирусного средства разгружать сеть при функционировании, с целью не нарушения работоспособности сети;

– цена базовой версии продукта – стоимость базовой версии антивирусного программного обеспечения, на год, для использования на одном компьютере;

– возможность поддержки виртуализации – возможность установки антивирусного программного обеспечения на виртуальные машины (Oracle Virtual Box, VMWare);

– использование шифрования - предназначено для защиты конфиденциальной информации пользователя от несанкционированного доступа и предотвращения утечки данных при сохранении операционной системой служебной информации на диске или неполном уничтожении файлов пользователя;

– динамические белые списки – создание списков разрешенного программного обеспечения, которое может быть установлено пользователем или администратором на компьютер;

– наличие единой консоли управления – возможность использования единой консоли управления на все антивирусное средства, которые установлены на компьютерах пользователей организации, и состоят в одной сети.

Как можно заметить из таблицы, у каждого антивирусного программного обеспечения есть свои плюсы и минусы, которые необходимо учитывать при использовании.

Результат тестирования антивирусных средств приведен на рисунке 4.

Антивирусные программы	Обнаружение	Динамика	Веб-защита	Самозащита	Ложные	Оценка
Qihoo 360 Internet Security 2014	98.1%	100%	100%	50%	3	9.2
BullGuard Internet Security 2014	97.0%	75%	100%	100%	0	9.2
Kaspersky Internet Security 2014	92.4%	87.5%	86.7%	100%	0	9.1
G Data InternetSecurity 2014	98.0%	87.5%	100%	50%	1	9.0
Emsisoft Internet Security Pack 8	97.3%	100%	73.3%	50%	0	8.9
F-Secure Internet Security 2014	97.1%	87.5%	93.3%	50%	0	8.9
Bitdefender Antivirus Free Edition	96.7%	75%	100%	50%	0	8.7
McAfee Internet Security 2014	98.2%	75%	73.3%	100%	2	8.5
Norton Internet Security 2014	96.2%	62.5%	73.3%	100%	1	8.2
Bitdefender Internet Security 2014	96.6%	75%	100%	0%	0	8.2
avast! Internet Security 2014	91.9%	50%	80%	100%	0	7.9
TrustPort Internet Security 2014	98.1%	87.5%	60%	0%	0	7.8
Ad-Aware PRO Security 11	96.1%	62.5%	93.3%	0%	0	7.6
Avira Internet Security Suite 2014	96.1%	75%	46.7%	50%	1	7.5
Comodo Internet Security Premium 6.3	90.8%	100%	20%	50%	4	7.3
ESET NOD32 Smart Security 7	95.2%	37.5%	86.7%	50%	0	7.2
Avira Free Antivirus 2014	96.1%	75%	26.7%	50%	0	7.2
Ashampoo Anti-Virus 2014	97.2%	62.5%	66.7%	0%	1	7.1
Trend Micro Titanium Internet Security	92.6%	50%	100%	0%	2	7.1
IObit Advanced SystemCare Ultimate	97.1%	62.5%	40%	50%	2	7.0
Panda Cloud Antivirus PRO 2.3	96.1%	75%	6.7%	50%	0	6.8
Panda Internet Security 2014	96.7%	75%	13.3%	0%	0	6.4
eScan Internet Security Suite	97.6%	37.5%	40%	50%	0	6.4
Microsoft Windows Defender 4.3	72.1%	12.5%	86.7%	100%	0	6.3
Outpost Security Suite PRO 9.0	93.7%	50%	20%	50%	0	6.2
Avast! Antivirus Free 2014	91.9%	0%	66.7%	100%	0	6.1
Ad-Aware Free Antivirus+ 11	96.2%	62.5%	13.3%	0%	0	6.0
ZoneAlarm Free Antivirus + Firewall	90.7%	0%	86.7%	50%	0	6.0
Norman Security Suite PRO 10	96.4%	37.5%	46.7%	0%	0	6.0
AVG Internet Security 2014	91.2%	0%	60%	100%	0	5.9
ZoneAlarm Internet Security Suite	90.8%	0%	80%	50%	0	5.8
AVG Anti-Virus Free 2014	91.2%	0%	46.7%	100%	1	5.6
Quick Heal Internet Security 2014	68.0%	25%	66.7%	50%	1	5.6
Webroot SecureAnywhere AntiVirus 2014	58.7%	37.5%	73.3%	100%	8	5.2
Dr.Web Security Space 9	94.7%	0%	33.3%	50%	0	5.0
Immunet Protect Free	61.0%	37.5%	26.7%	0%	0	4.5
NANO Антивирус	51.2%	0%	26.7%	50%	5	3.2
VIRUSfighter + SPYWAREfighter	40.6%	0%	13.3%	50%	0	3.0
ArcaVir Internet Security 2013	52.3%	0%	6.7%	50%	12	2.2

Рисунок 4 – Результаты тестирования антивирусных средств

Сравнение проводилось по 5 параметрам:

– обнаружение - общий уровень обнаружения антивируса (количество обнаруженных угроз) в процентах при проверке 3039 вредоносных файлов;

– динамика – процент угроз нейтрализованных при запуске от оставшихся нераспознанных вредоносных файлов после сканирования;

– веб-защита – процент заблокированных фишинговых и вредоносных веб-сайтов;

– самозащита – уровень самозащиты антивируса при проверке с помощью Process Hacker;

– ложные – количество ложных срабатываний при проверке 761335 чистых файлов после установки 160 приложений в систему;

– оценка – общая оценка антивируса по итогам тестирования на основе указанных выше параметров.

Как видно из таблицы 3 и результатов тестирования антивирусных средств, приведенного на рисунке 4, для достижения поставленных в дипломном проекте целей, подходит антивирусное средство Kaspersky Endpoint Security.

3 Анализ возможных проблем при развертывании средств антивирусной защиты с сетевым центром управления

В этом разделе дипломного проекта проведен анализ возможных проблем при развертывании средств антивирусной защиты с сетевым центром управления. К наиболее важным проблемам были отнесены следующие проблемы:

– распределение сетевого трафика;
– рациональное использование рабочего времени;
– несовместимость различных антивирусных программ между собой.

Проблема совместимости различных версий антивирусных средств заключается в том, что на компьютерах в организации установлены старые и более новые версии антивирусного средства. Для устранения этой проблемы можно было бы удалить старую версию антивируса и установить более новую. Но тут возникает следующая проблема – характеристики компьютера не удовлетворяют требованиям новой версии антивирусного средства. Kaspersky Enpoint Security позволяет устранить эту проблему путем обновления старой версии до новой, без удаления, через сетевой центр управления. Администратор выбирает в сети компьютер на котором требуется обновить версию антивируса и выбирает действие.

Проблемы рационального использования работы компонентов АС и загруженности сети заключается в том, что обновление занимает достаточно длительный процесс времени и создают большую нагрузку на сеть. Увеличение пропускной способности сети достаточно затратно, поэтому данным путем устранить проблему невозможно. Для решения этой проблемы в Kaspersky Endpoint Security существует такая возможность, как сокращение сетевого трафика. Регулирование пропускной способности позволяет сократить сетевой трафик за счет гибкого управления соединениями и пропускной способностью, что позволяет распределять нагрузку на сеть без помех для функционирования других узлов.

Для решения проблемы, которая связана с рациональным использованием времени работы компонентов АС, была использована таблица 1. Как видно из таблицы, самое оптимальное время с 17.00 до 8.00. В это время можно проводить обновление антивирусных средств.

4 Описание виртуального стенда

Для разработки методики и ее проверки был создан виртуальный стенд. Модель виртуального стенда показана на рисунке 5.

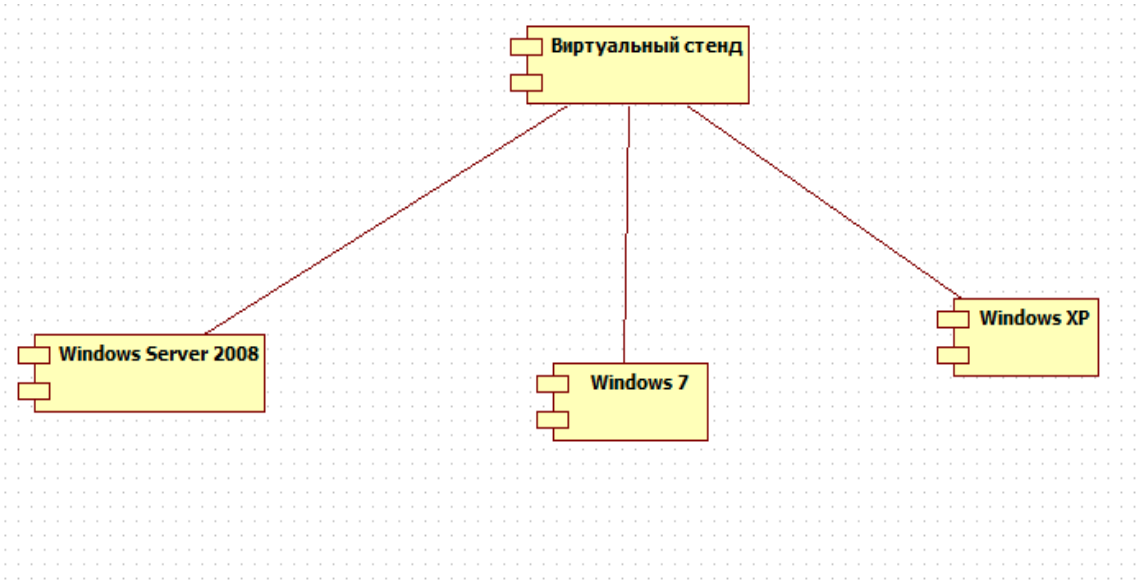

Рисунок 5 - Модель виртуального стенда

Виртуальный стенд создавался с помощью средства виртуализации Oracle VM Virtual Box. Использовалось три рабочие машины:

– рабочая станция с операционной системой Windows Server 2008 R2;

– рабочая станция с операционной системой Windows 7 с установленным на ней антивирусным средством Kaspersky Endpoint Protection 10;

– рабочая станция с операционной системой Windows XP с установленным на ней антивирусным средством Kaspersky AntiVirus 6.0.

Для переноса компьютера с Windows XP на новый центр администрирования, необходимо провести следующие действия:

– на рабочей станции с Windows XP, необходимо зайти в управление сетью, и присвоить необходимый адрес. В рамках дипломного проекта IP адрес 10.0.2.6;

– далее в командной строке в папке Network Agent, которая находится по умолчанию по следующему пути: «C:\Program Files\Kaspersky Lab\

NetworkAgent, запустить утилиту klmover.exe со следующим параметром: `klmover.exe -address 10.0.2.4`, где указанный адрес, это адрес машины с центром управления;

– для проверки соединения необходимо запустить утилиту klnagchk.exe. При успешном переносе, результат работы этой утилиты показан на рисунке 6.

Рисунок 6 – Результат проверки соединения

5 Методика развертывания средств антивирусной защиты с сетевым центром управления

5.1 Разработка методики развертывания средств антивирусной защиты с сетевым центром управления

На данном этапе разрабатывалась методика развертывания средств антивирусной защиты с сетевым центром управления. Поскольку на предприятии может быть большие количество сотрудников, которые будут выполнять различные задачи, необходимо уделить особое внимание правильной настройке антивирусного программного обеспечения. Методика развертывания представляет собой определенный порядок действий по настройке и управлению антивирусными средствами в корпоративной среде. При разработке методики рассматриваются следующие вопросы:

– установка консоли администрирования и сетевого центра управления;

– создание групп компьютеров с различными версиями антивирусных средств;

– добавление компьютеров в группы;

– создание политик для групп компьютеров с различными версиями антивирусного средства;

– создание задач для групп компьютеров с различными версиями антивирусного средства;

– распределение трафика генерируемого в системе в процессе функционирования антивирусного средства.

5.2 Установка консоли администрирования и сетевого центра управления

В данном параграфе описывается процесс установки консоли администрирования и сетевого центра управления на сервер организации. Консоль администрирования – Kaspersky Security Center, представляет собой

единую консоль управления всеми продуктами «Лаборатории Касперского». Kaspersky Security Centre, упрощает управление безопасностью и IT-системами, включает в себя:

- управление защитой рабочих мест;
- управление мобильными устройствами и их защита;
- управление безопасностью виртуальных сред;
- системное администрирование.

Установка консоли администрирования приведена на рисунках с 8 по 13.

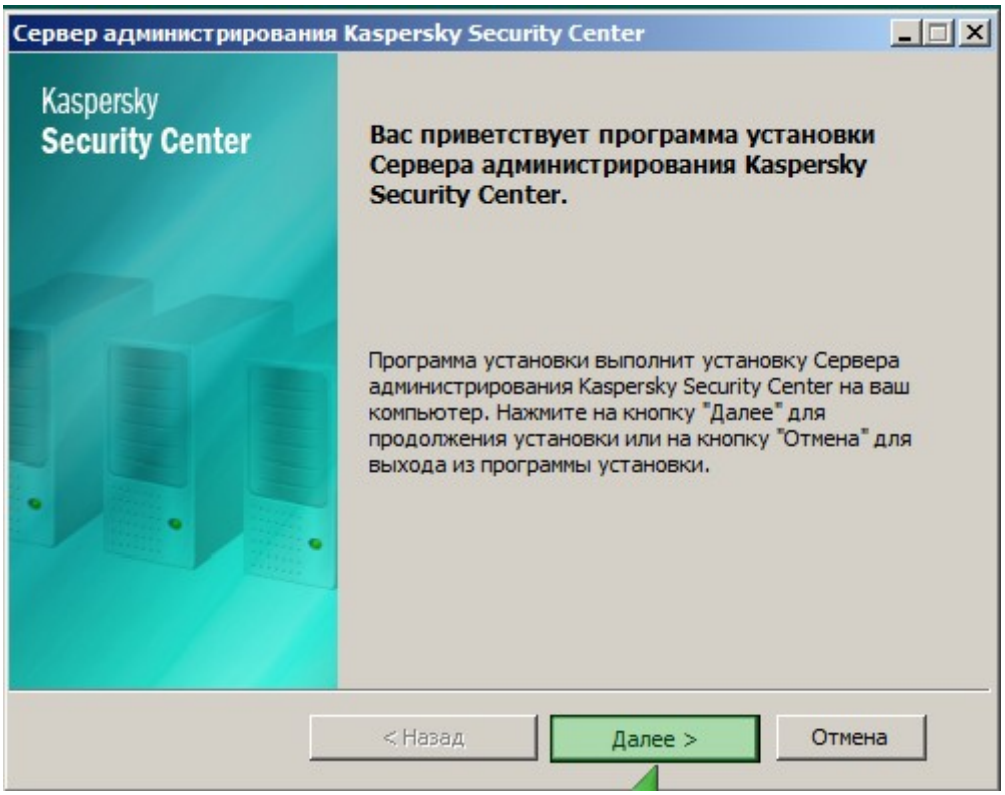

Рисунок 8 – Начало установки

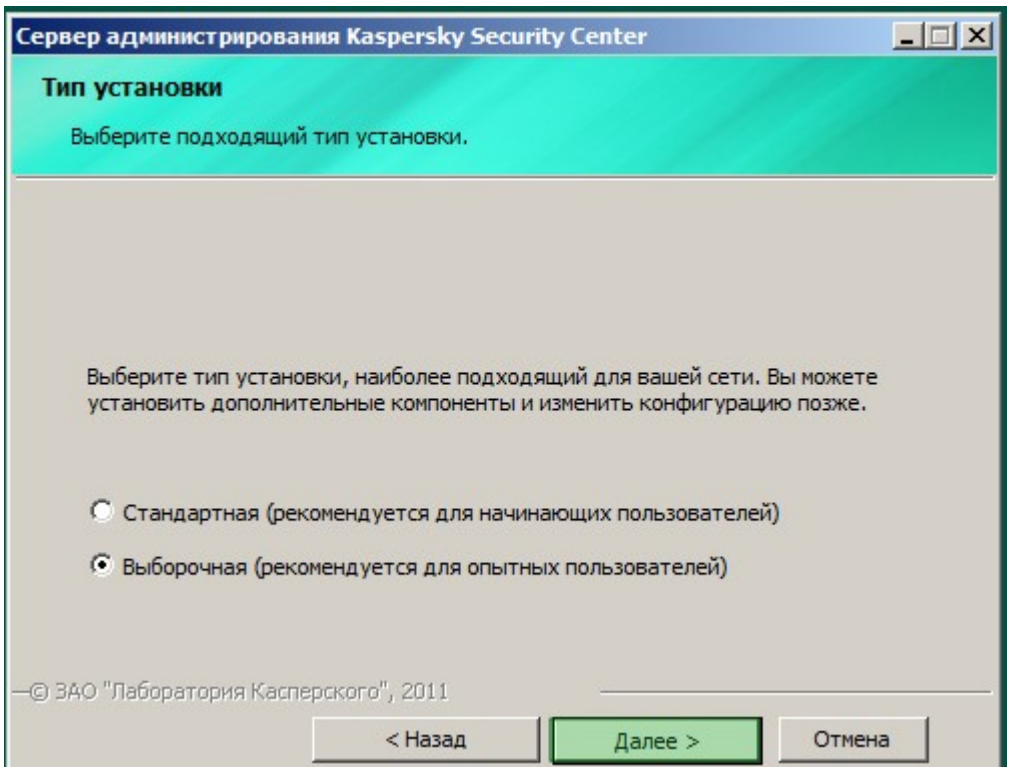

Рисунок 9 – Выбор типа установки

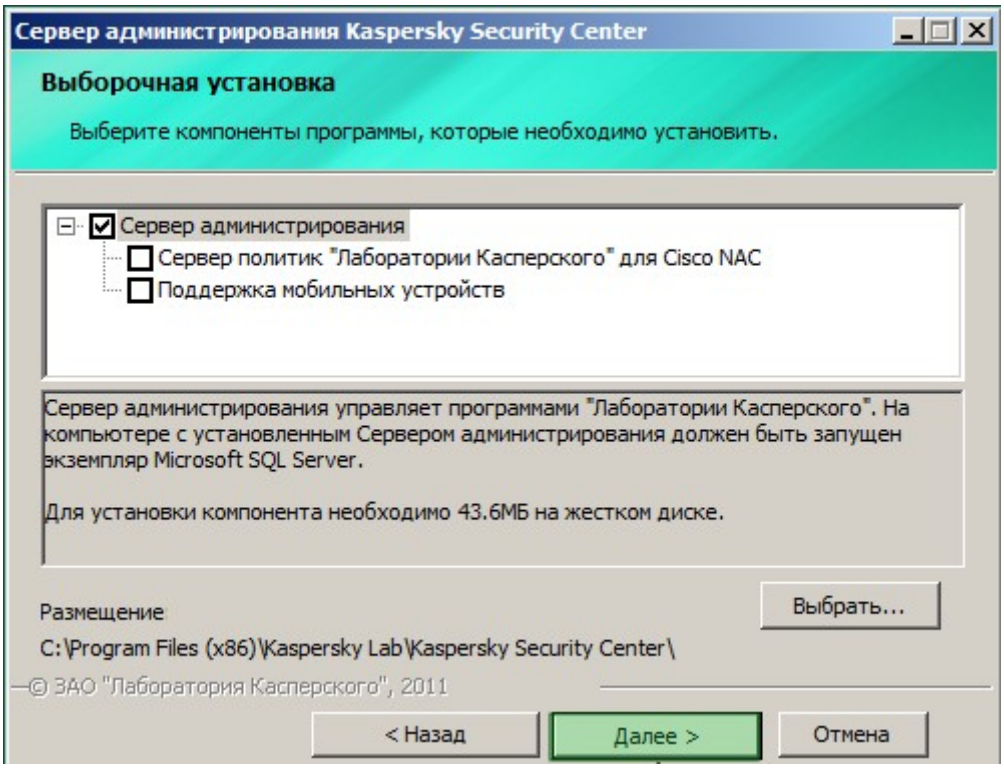

Рисунок 10 – Компоненты установки

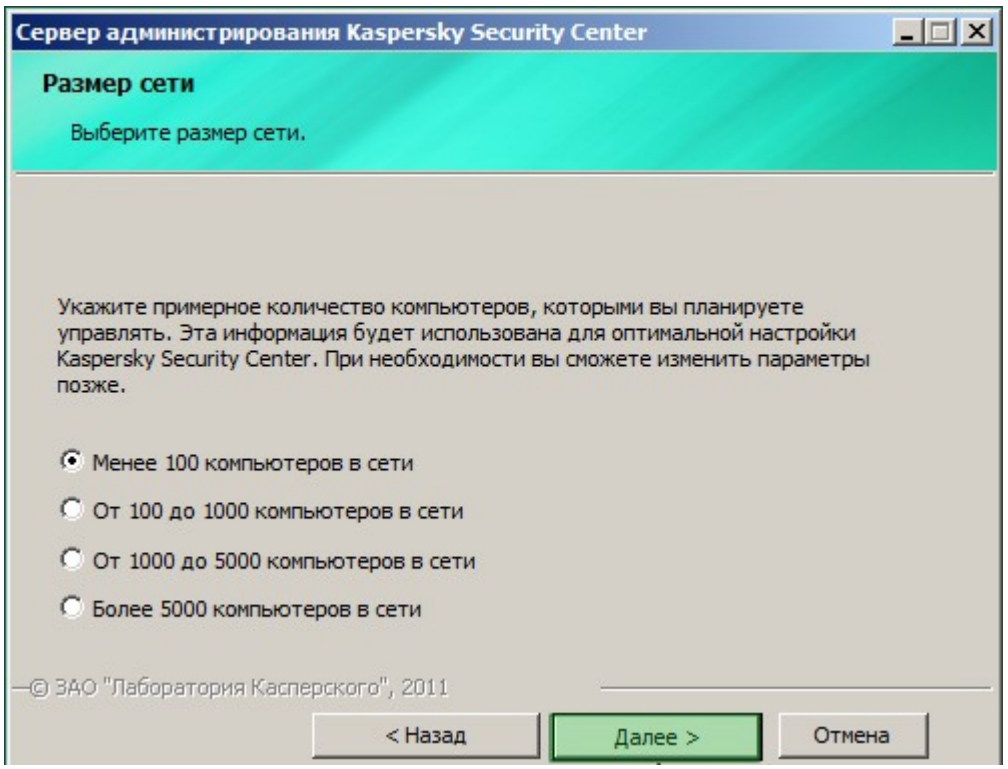

Рисунок 11 – Выбор размера сети

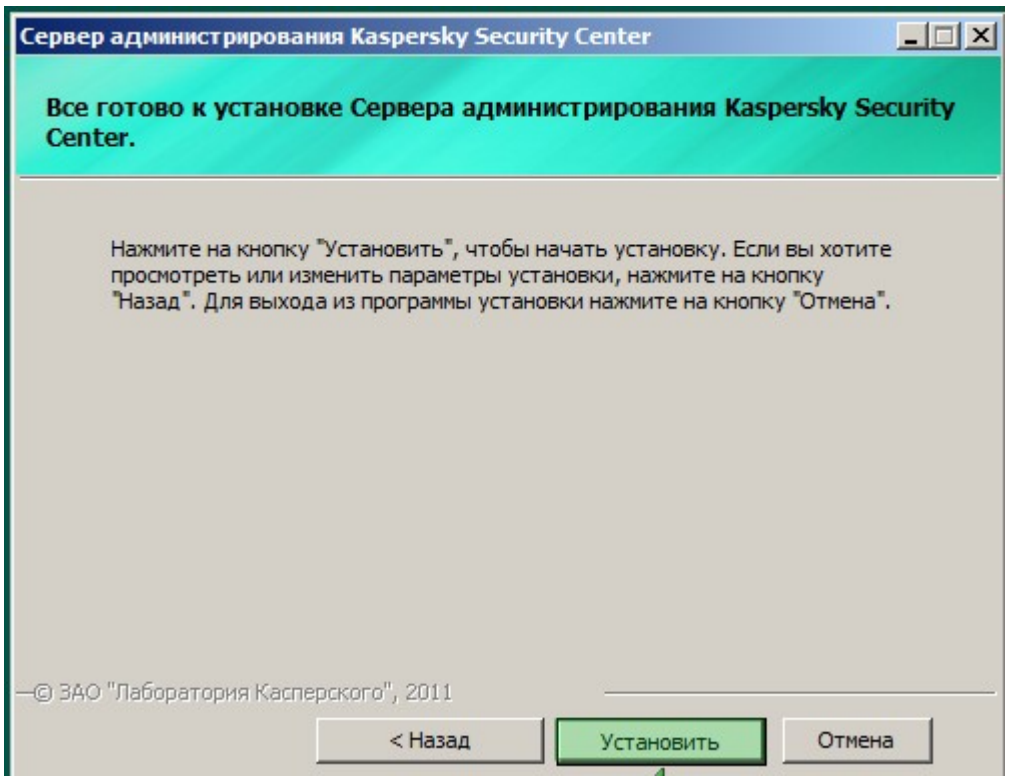

Рисунок 12 – Завершение настройки параметров установщика

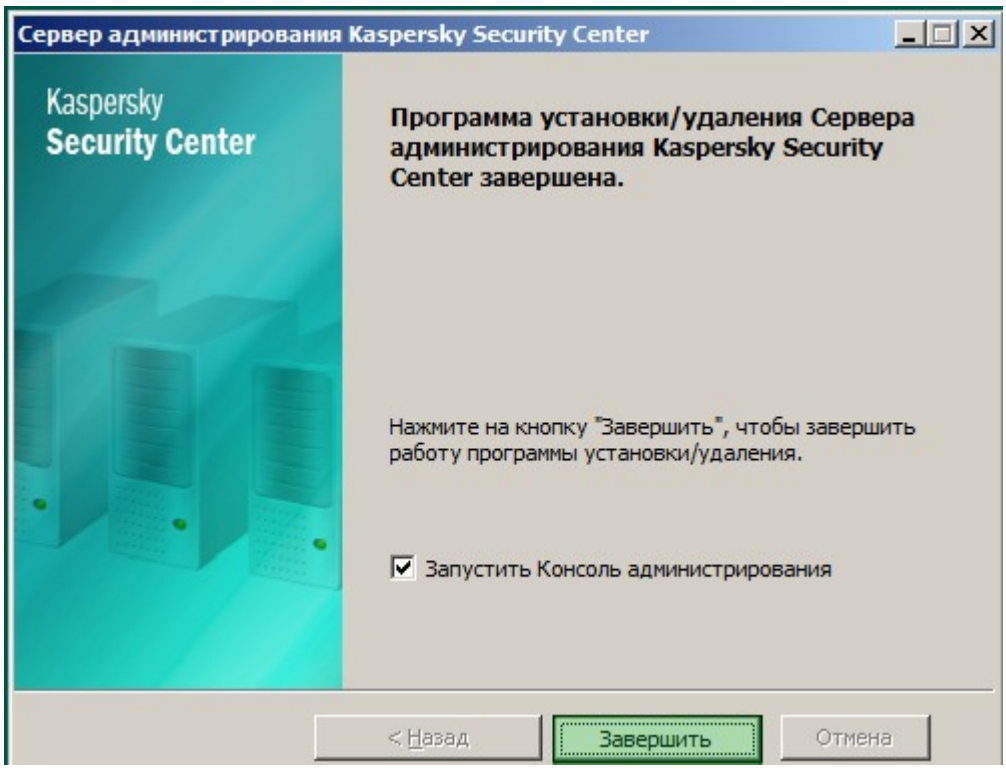

Рисунок 13 – Завершение установки консоли администрирования

На рисунке 14 показан общий вид консоли администрирования.

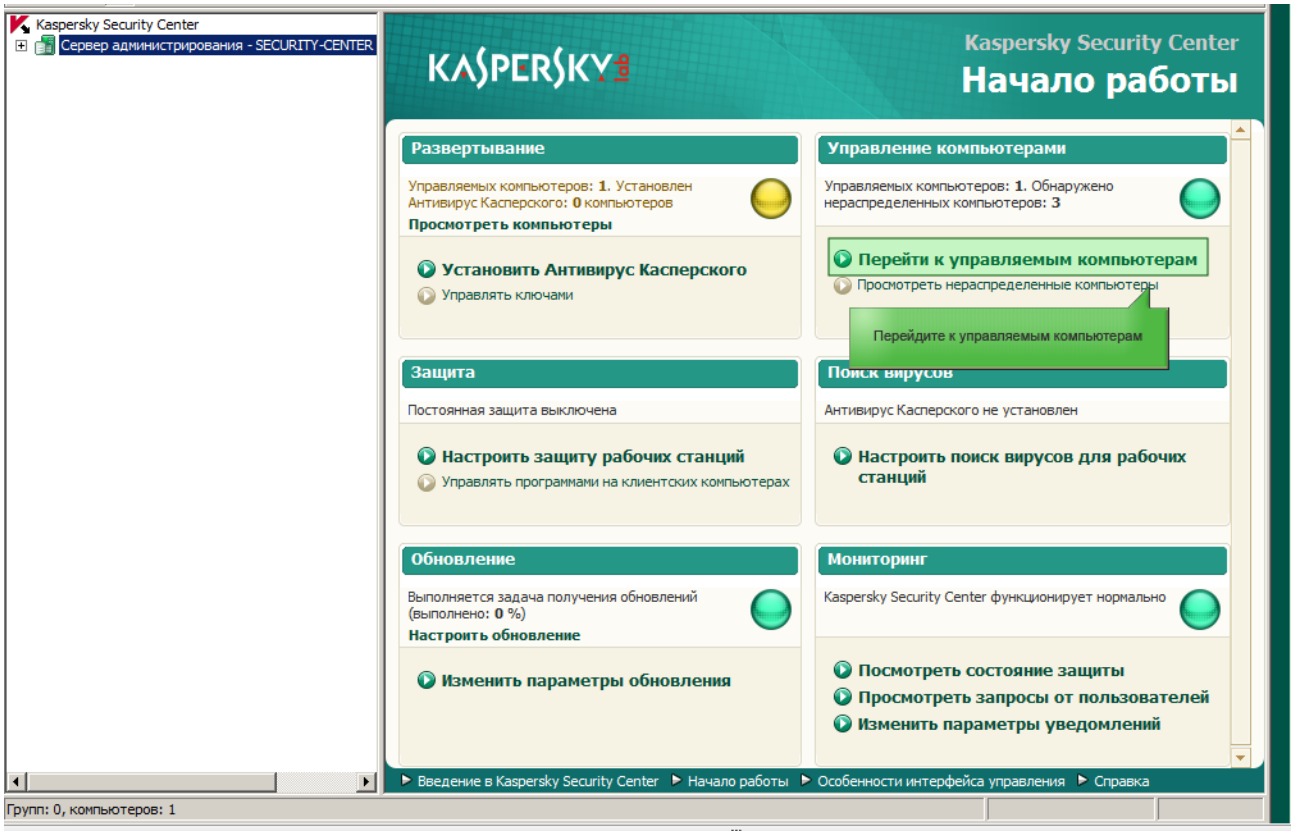

Рисунок 14 – Общий вид консоли администрирования

Программные и аппаратные требования для установки консоли администрирования:

- Windows Server 2003;
- Windows Server 2003 x64;
- Windows Server 2008 (в режиме ядра);
- Windows Server 2008 x64 Service Pack 1 (требуется Windows Installer 4.5);
- Windows Server 2008 R2;
- Windows Server 2008 R2 (в режиме ядра).

Кроме этого, на выбранном для Сервера администрирования компьютере не должно быть установленного Агента администрирования. Программа установки автоматически обнаруживает установленный Агент и просит администратора удалить его.

Минимальные требования к аппаратной конфигурации:

- процессор с частотой не менее 1 ГГц;
- 512 Мб свободной оперативной памяти (сверх того, что требуется операционной системе и другим приложениям, установленным на компьютере);
- 1 Гб свободного дискового пространства.

5.3 Создание групп компьютеров с различными версиями антивирусных средств

После установки на Сервере администрирования есть только одна группа - управляемые компьютеры. При такой организации администратор вынужден использовать одну политику защиты для всех компьютеров, что не всегда удобно.

Даже в небольших сетях бывает удобно или даже необходимо использовать разные настройки защиты для серверов и пользовательских компьютеров. А в крупных сетях, где разные группы пользователей используют разные специализированные программы, возможность создавать политики с разными исключениями для разных пользователей очень удобна. А для того,

чтобы применять разные политики, нужно поместить компьютеры в разные группы. С практической точки зрения бывает удобно, когда компьютеры в Kaspersky Security Center организованы в такие же группы, как и в Active Directory, или в группы, соответствующие IP-подсетям, используемым в организации. В этом случае принадлежность компьютера к группе сразу же дает администратору понимание того, где физически расположен компьютер, чтобы послать к нему сотрудника ИТ-отдела.

Порядок создания групп:

- развернуть дерево «Сервер администрирования»;
- выбрать вкладку «Управляемые компьютеры»;
- перейти во вкладку группы;
- выбрать действие «Создать группу»;
- в появившемся окне ввести имя группы;
- нажать «ОК».

Порядок создания групп приведен на рисунке 15.

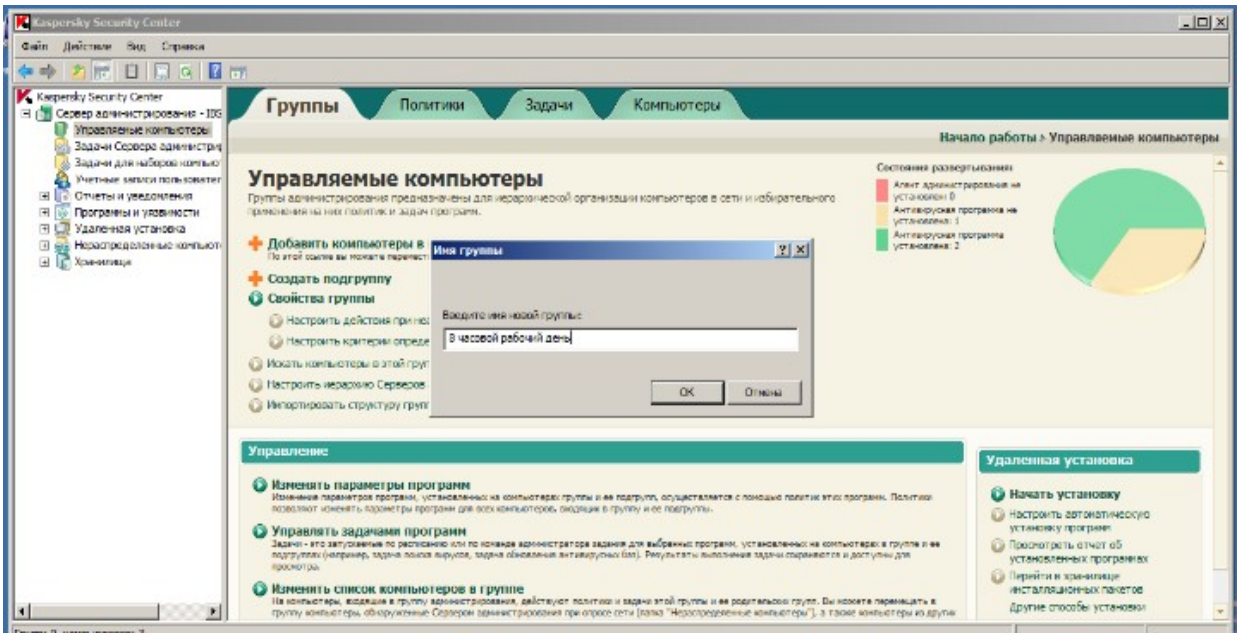

Рисунок 15 – Создание группы

В рамках дипломного проекта было решено создать группы для пользователей. В Kaspersky Security Center были созданы две группы по времени работы сотрудников и одна группа по версии установленного

антивирусного программного обеспечения на компьютерах. Результат создания групп пользователей приведен на рисунке 16.

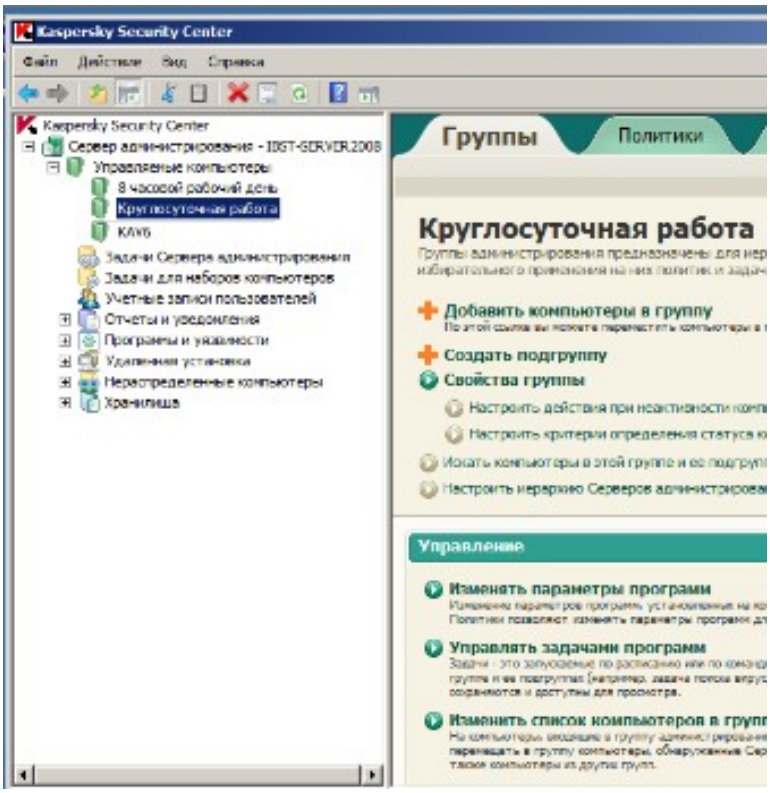

Рисунок 16 – Созданные группы

5.4 Добавление компьютеров в группы

Далее необходимо распределить компьютеры в созданные группы. В рамках дипломного проекта, из-за недостаточных возможностей аппаратных ресурсов виртуального стенда, нераспределенных компьютеров всего два. В реальной организации компьютеров может быть намного больше. Все компьютеры которые подключены к серверу находятся в ветке «Нераспределенные компьютеры». Компьютеры можно добавить несколькими способами. В рамках дипломного проекта был выбран наиболее удобный и простой способ.

Порядок добавления компьютеров в группы:

– в дереве выбрать ветку «Управляемые компьютеры» и выбрать нужную группу;

– во вкладке «Группы» выбрать действие «Добавить компьютеры»;

– в мастере добавления компьютеров выбрать «Выбрать компьютеры, обнаруженные в сети Сервером администрирования»;

– включить «Нераспределенные компьютеры»;

– по завершению, мастер добавления выдаст сообщение.

Порядок добавления компьютеров в группы приведен на рисунках ниже

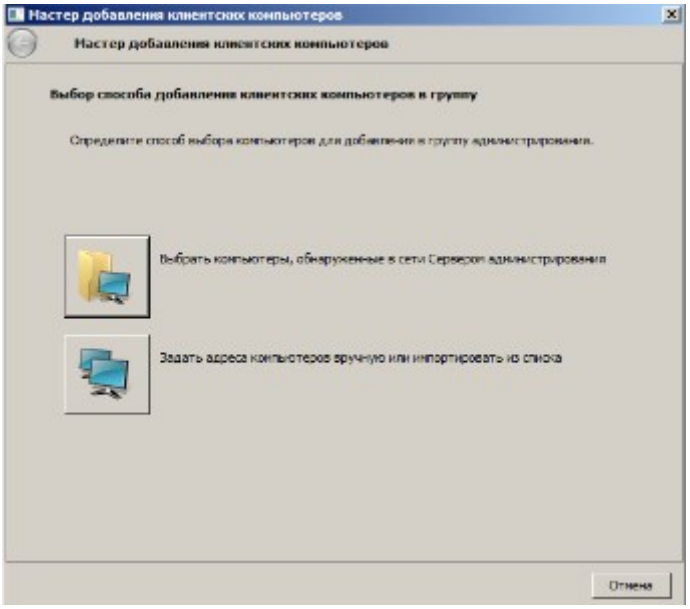

Рисунок 17 – Выбор режима поиска

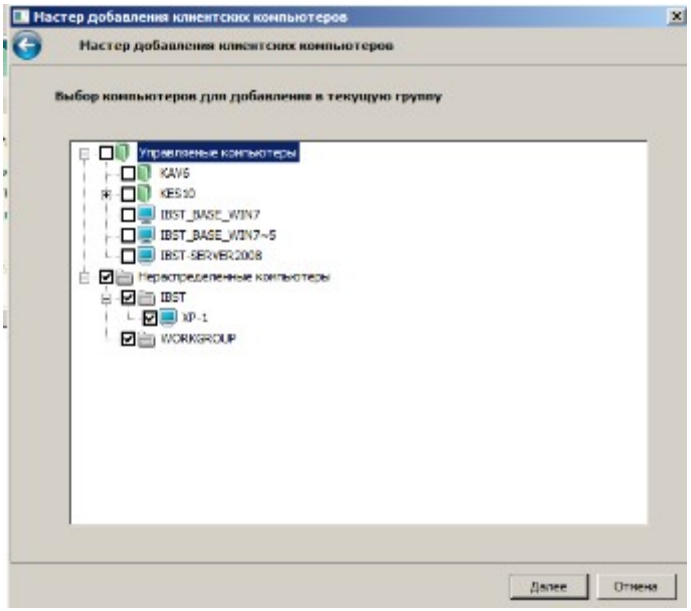

Рисунок 18 – Выбор нераспределенных компьютеров

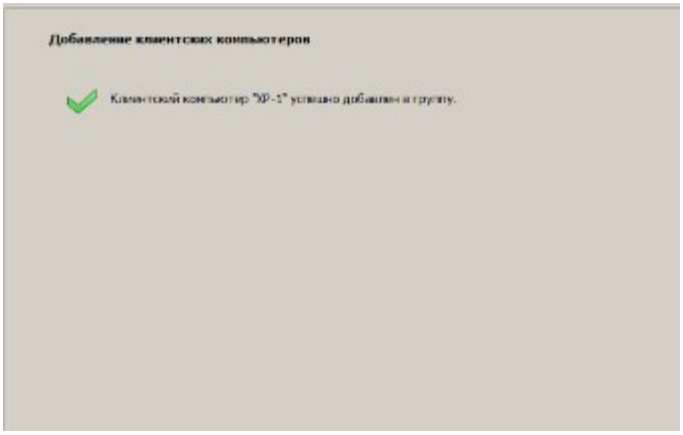

Рисунок 19 – Добавление клиентских компьютеров

Аналогично, добавляются компьютеры в необходимые группы.

5.5 Создание политик для групп компьютеров с различными версиями антивирусного средства

Политика — это инструмент управления постоянно действующими настройками управляемого продукта. В политике Антивируса Касперского задаются параметры, касающиеся антивируса в целом, параметры интерфейса, параметры компонентов постоянной защиты и параметры, являющиеся общими для нескольких компонентов защиты либо для компонентов защиты и задач.

Политика служит одновременно для настройки параметров и для контроля их применения на компьютерах. Администратор отмечает настройки в политике как обязательные, и после этого пользователь не может изменить эти настройки через локальный интерфейс антивируса.

Требуется выбрать необходимую группу, для этого необходимо зайти во вкладку «Политики» и выбрать «Создать политику». Запустится мастер создания политик, показанный на рисунке 20.

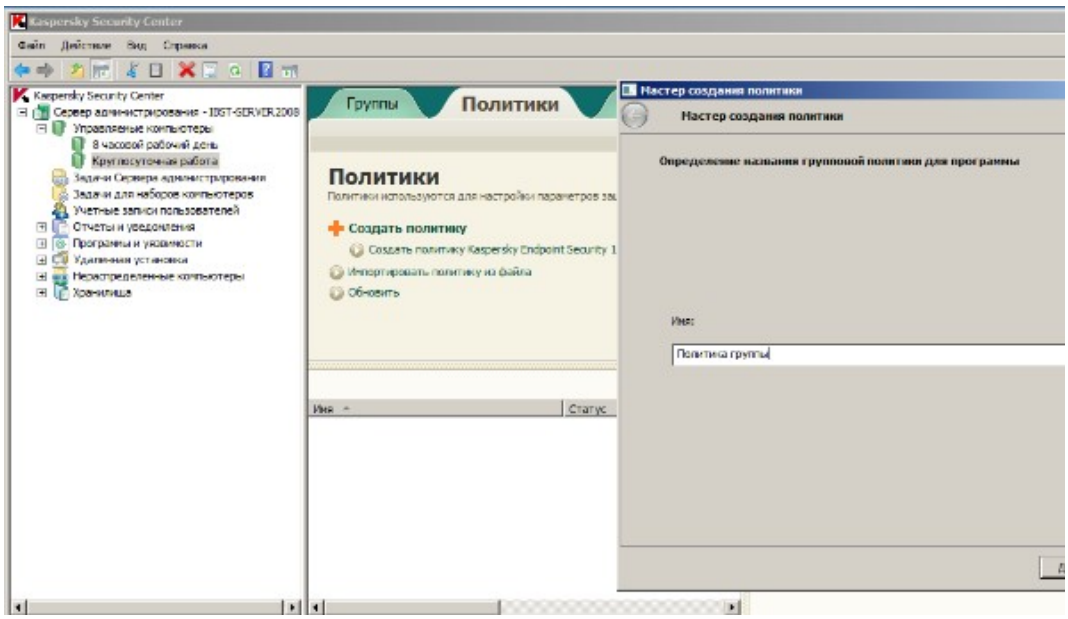

Рисунок 20 – Мастер создания политики

В строке «Имя» вводится название создаваемой политики и следует нажать «Далее». Затем предложено выбрать средство для создания групповой политики. Необходимо выбрать «Kaspersky Endpoint Security 10». Результат приведен на рисунке 21.

Как видно из рисунка 21, к выбору доступно не более трех программ для создания групповой политики. Программа «Сервер администрирования Kaspersky Security Center» создает политику для сервера администрирования, а программа «Агент администрирования Kaspersky Security Center» создает политику для агентов администрирования. Далее идет настройка параметров защиты. Настройка параметров защиты зависит от функционала компьютера пользователя, т.е. чем больше функций выполняет компьютер, тем больше надо настроить параметров. Что бы можно было настроить параметр в дальнейшем, необходимо нажать иконку замка для разблокировки.

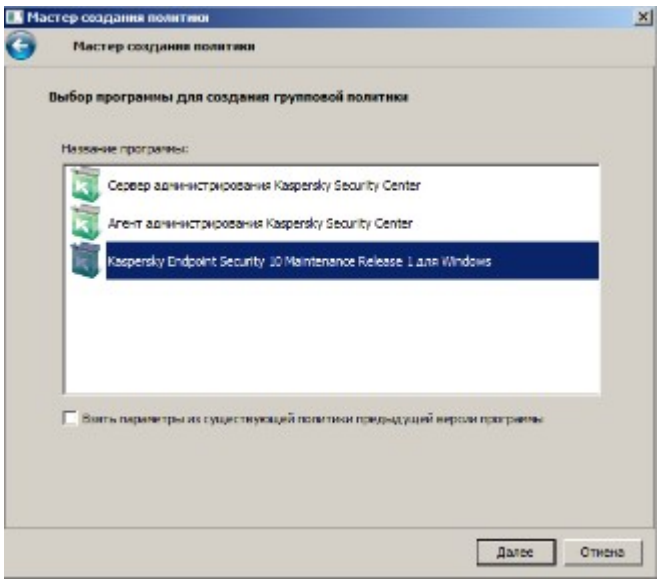

Рисунок 21 – Выбор программы для создания групповой политики

Как видно из рисунка 21, можно выбрать не более трех программ для создания групповой политики. Программа «Сервер администрирования Kaspersky Security Center» создает политику для сервера администрирования, а программа «Агент администрирования Kaspersky Security Center» создает политику для агентов администрирования. Далее идет настройка параметров защиты. Настройка параметров защиты зависит от функционала компьютера, т.е. чем больше компьютер выполняет функций, тем больше надо настроить параметров. Что бы можно было настроить параметр в дальнейшем, необходимо нажать иконку замка для разблокировки.

Настройки защиты для разных групп пользователей будут различны. Для группы «8 часовой рабочий день» необходимо подключить все параметры, так как к этим компьютерам могут быть подключены отчуждаемые носители, которые могут быть заражены, имеется выход в интернет, в котором есть вероятность скачивания зараженного файла или перехода на фишинговый сайт, пользователи получают и отправляют почту, так же возможен риск сетевых атак. Мастер создания политик показан на рисунке 23.

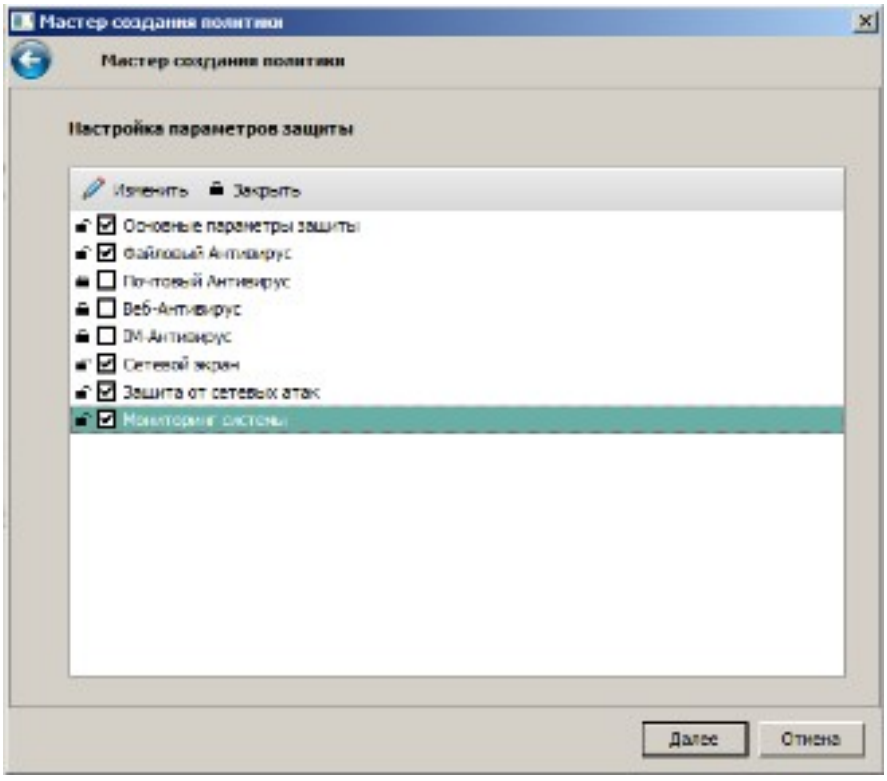

Рисунок 23 – Мастер создания политики

Далее следует настройка правил. Окно настройки показано на рисунке 24.

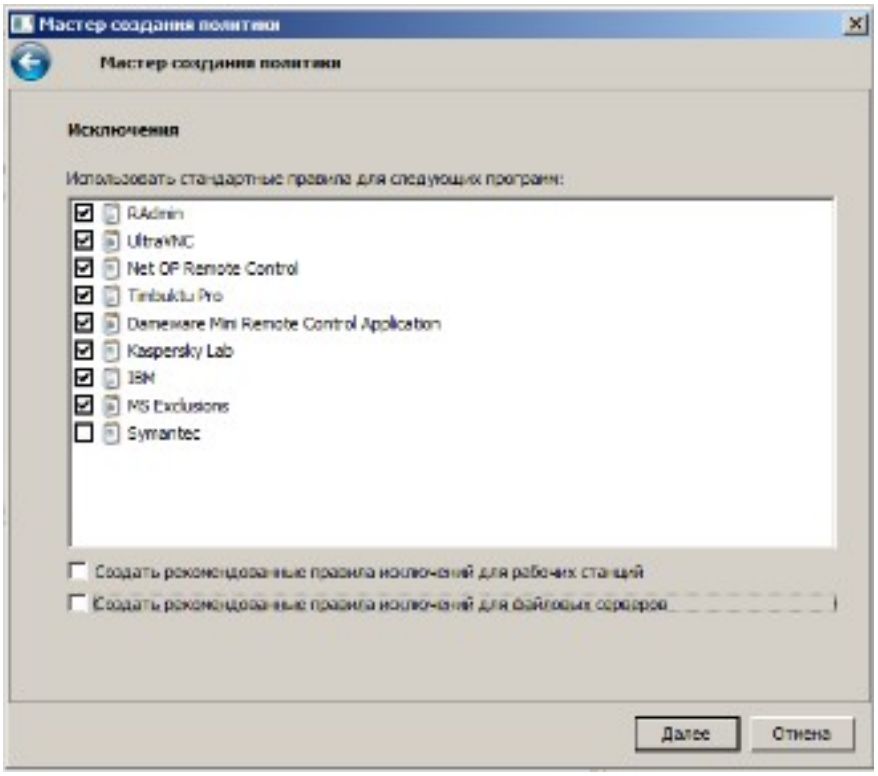

Рисунок 24 – Настройка правил исключения

Далее идет настройка системного аудита. Для группы «8 часовой рабочий день» необходимо настроить детальный аудит. Необходимо установить галочки напротив всех событий. Настройка аудита показана на рисунке 25.

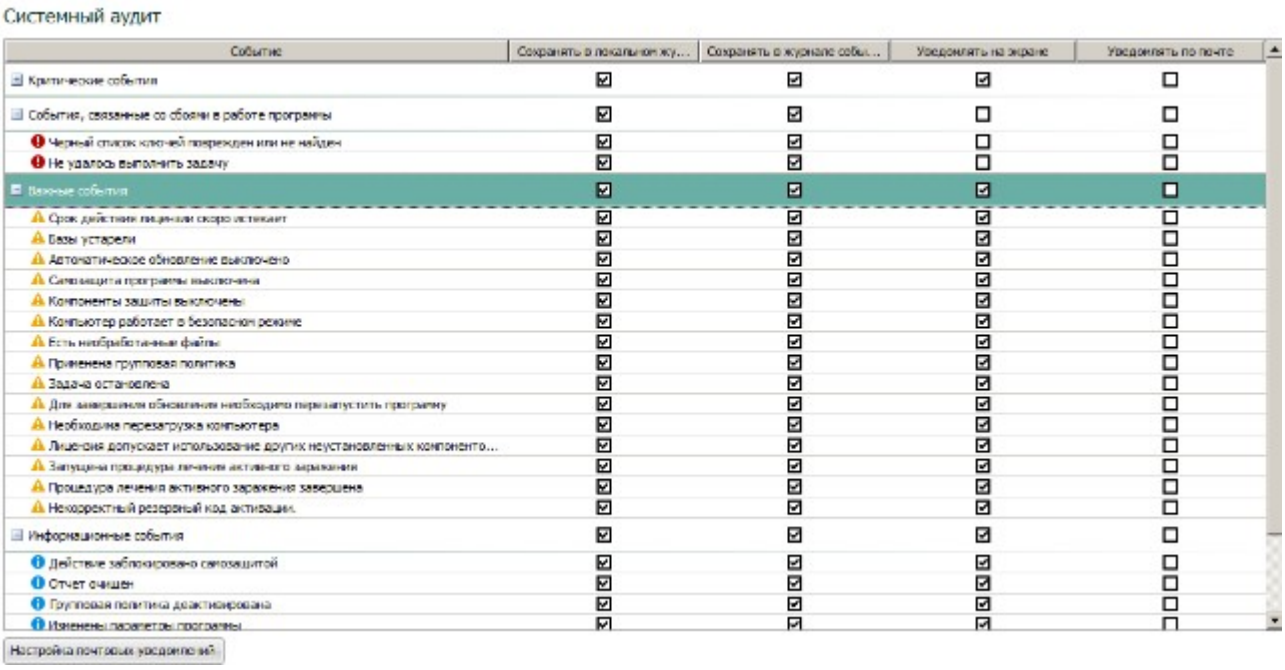

Рисунок 25 – Настройки системного аудита

После завершения создания политики, необходимо перейти к детальной настройке.

На рисунке 26 показано окно настройки.

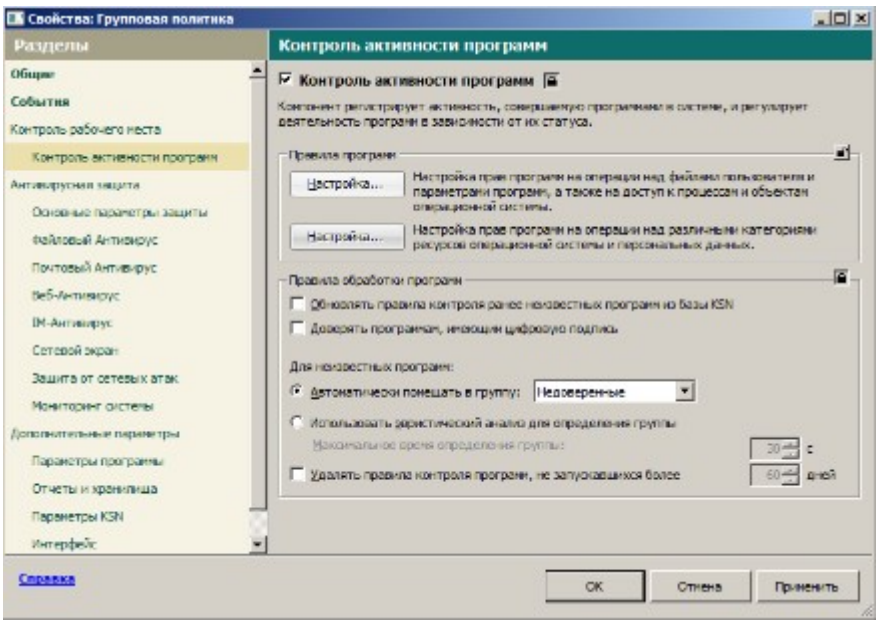

Рисунок 26 – Окно настройки

В окне настройки в разделе активность программ необходимо настроить автоматическое перемещение программ в группу «Недоверенные». Это необходимо для того, что бы исключить возможность пользователей устанавливать различные программы для развлечения, без ведома администратора. Далее требуется перейти в раздел «Файловый антивирус» и установить «Уровень безопасности» в положение «Высокий». Так будет обеспечен максимальный уровень безопасности для группы. Окно настройки файлового антивируса показано на рисунке 27. Аналогично требуется выставить высокий уровень безопасности в других компонентах антивирусной защиты. Далее мастер предлагает настроить параметры программ. Настройка показана на рисунке 28. В этом разделе необходимо установить галочки «Включить самозащиту» и «Выключить внешнее управление системной службы». Далее надо установить галочки в разделе «Режимы работы». Тут необходимо активировать функцию «Уступать ресурсы другим программам». Данная функция очень полезна, когда компьютер и без того с низким уровнем производительности, выполняет какую либо задачу антивируса, и при этом пользователь выполняет на компьютере рабочие обязанности.

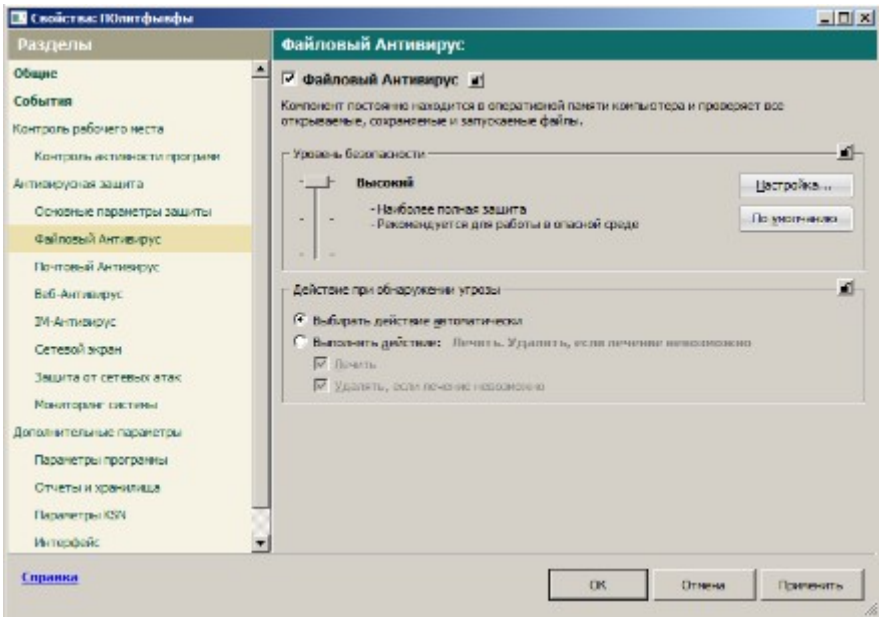

Рисунок 27 – Настройки файлового антивируса

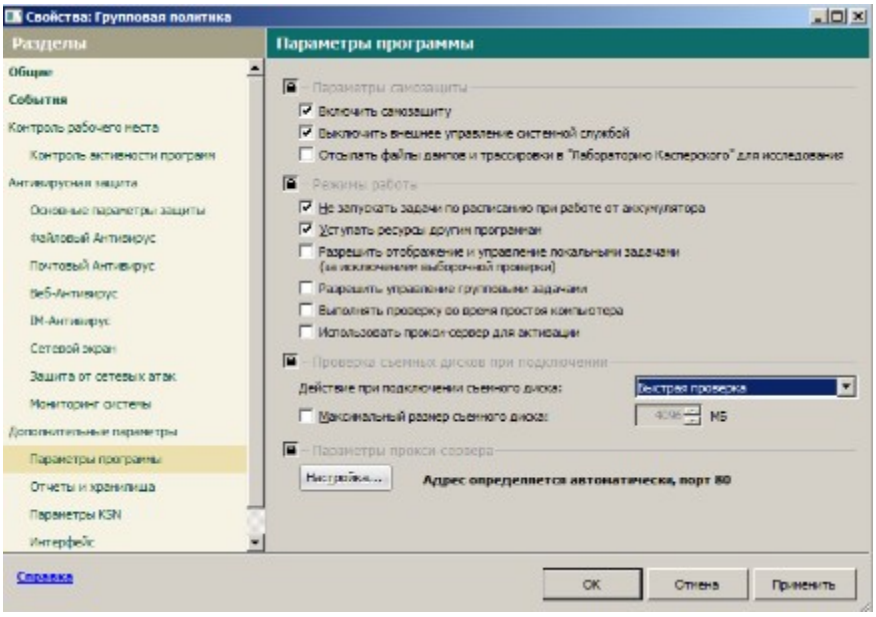

Рисунок 28 – Настройка параметров программ

Таким образом этот режим позволяет распределить ресурсы компьютера. После создания политики можно наблюдать на какие компьютеры пользователей распространяется политика безопасности. На рисунке 29 показаны результаты создания политики.

Аналогично политики создаются для других групп, которые администратор создаст в сетевом центре управления.

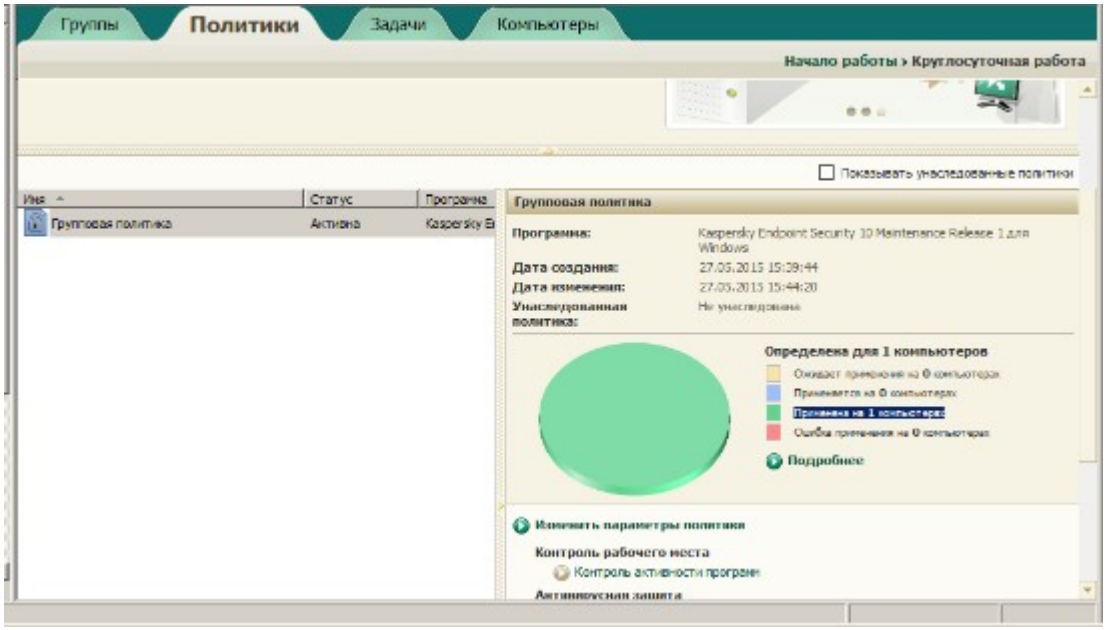

Рисунок 29 – Созданные политики

5.6 Создание задач для групп компьютеров с различными версиями антивирусного средства

В этом разделе дипломного проекта создавались задачи для групп компьютеров пользователей. Задача создается для удобства администратора, т. к. сотрудников в организации может быть большое количество, то собственноручно на каждом компьютере активировать задачи будет проблематично, поэтому необходимо запустить одну общую задачу, которая будет запущена на необходимых компьютерах пользователей. Чтобы создать задачу, необходимо перейти во вкладку «Задачи». Далее нужно выбрать действие «Создать задачу». Мастер создания задач просит ввести имя создаваемой задачи. Мастер создания задач показан на рисунке 30.

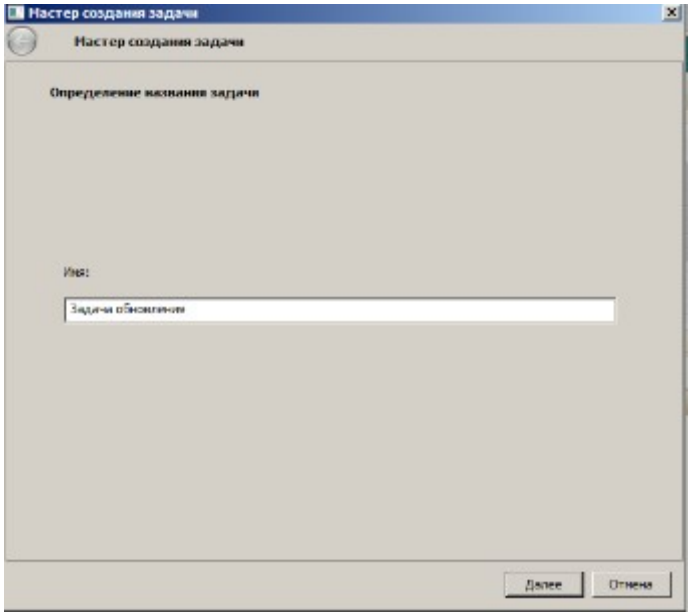

Рисунок 30 – Мастер создания задач

Далее необходимо выбрать тип задачи. Предложенных типов задач может быть несколько. Они подразделяются на задачи для сервера администрирования и задачи для агента администрирования. Далее необходимо выбрать задачу «Обновление» в разделе «Задачи для агента администрирования». Результат показан на рисунке 31.

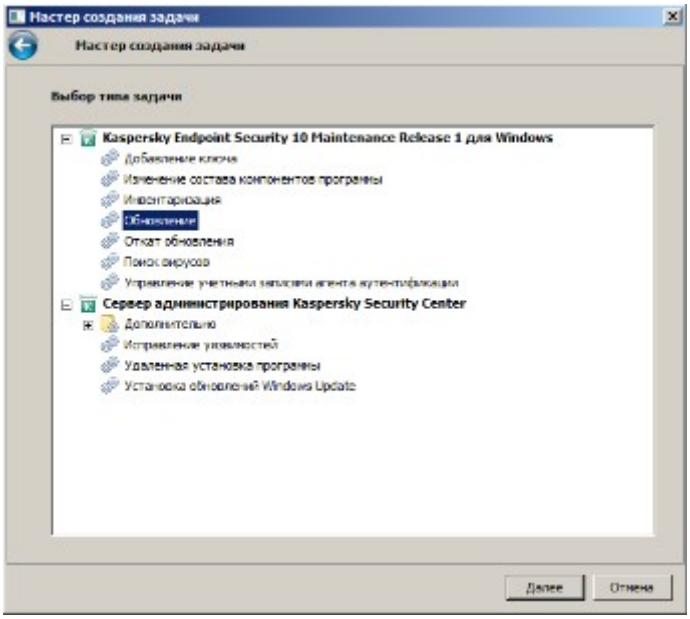

Рисунок 31 - Выбор типа задачи

Далее действие зависит от выбранной задачи. В данном случае требуется выбрать источник обновления. На рисунке 32 показан результат выбора источника.

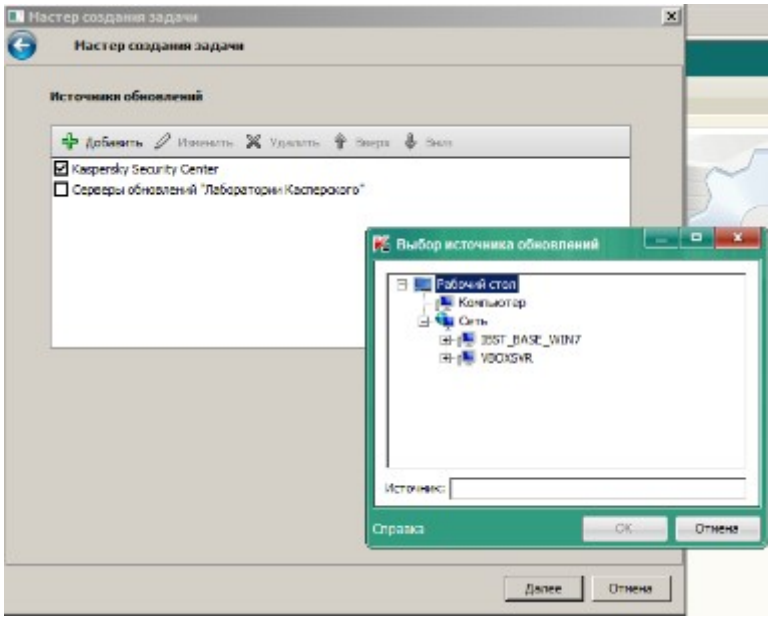

Рисунок 32 – Выбор источника обновления

Далее предлагается выбрать расписание запуска задач. Расписание можно выбрать любое. Расписание выбирается в зависимости от времени работы. В рамках дипломного проекта, удобно использовать ежемесячное расписание запуска задачи. Результат показан на рисунке 33.

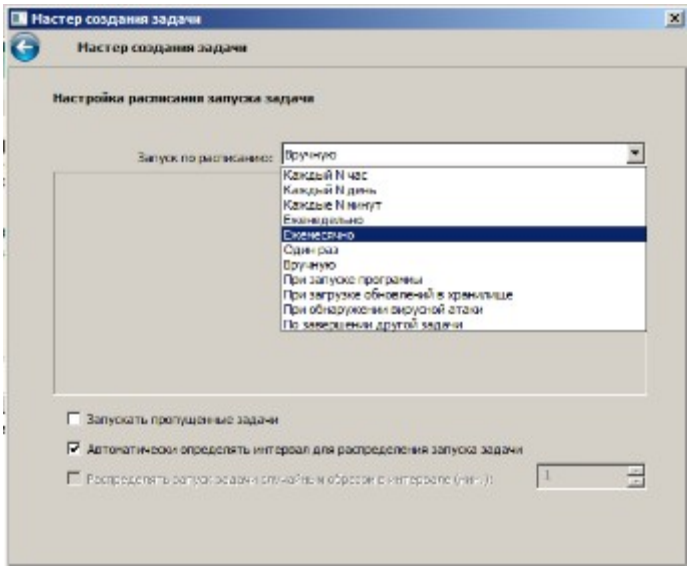

Рисунок 33 – Выбор расписания запуска задачи

После завершения создания задачи, созданная задача будет отображаться в списке задач для той группы, для которой она создавалась. Результат создания задачи показан на рисунке 34.

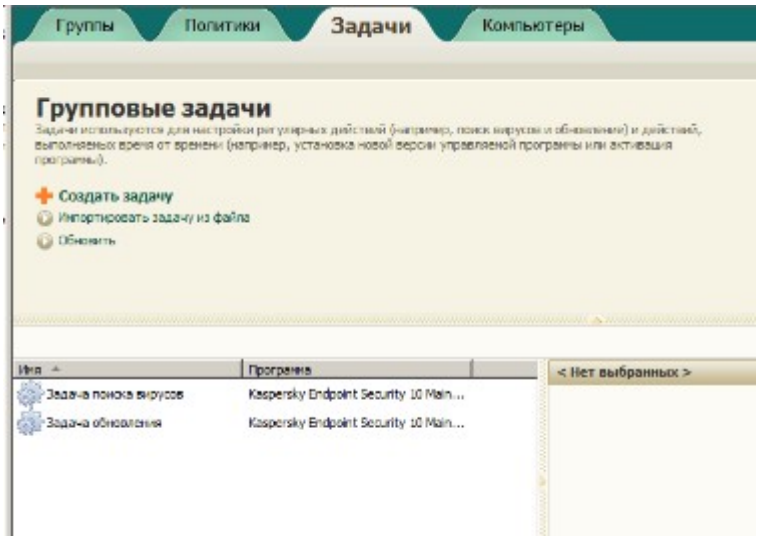

Рисунок 34 – Результат создания задач

Далее в рамках дипломного проекта была создана задача поиска вирусов для группы компьютеров. Создание задачи поиска вирусов аналогично созданию задачи обновления. После ввода имени задачи, предлагается выбрать тип задачи. В разделе «Kaspersky Endpoint Security 10 для Windows» следует выбирать тип «Поиск вирусов». Выбор типа задачи показан на рисунке 35.

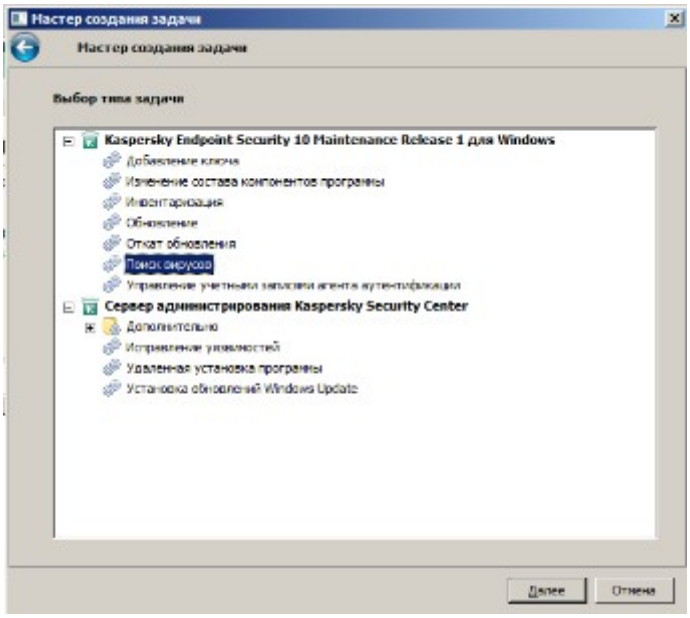

Рисунок 35 - Выбор типа задачи

Далее предлагается выбрать область проверки. Требуется выбрать существующую область, также можно создать свою. Создание и выбор области проверки показан на рисунке 36.

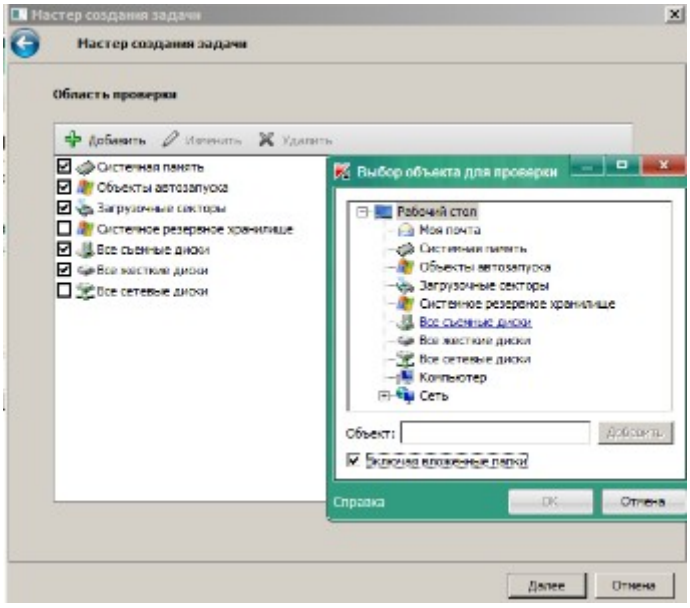

Рисунок 36 – Выбор области проверки

Далее предлагается выбрать действие, которое будет выполняться при обнаружении вирусной активности. Можно выбрать действие автоматически, при этом режиме компьютер сам будет решать лечить или удалять. Так же можно выбрать какое-то конкретное действие. В рамках дипломного проекта было выбрано конкретное действие. Выбор действия показан на рисунке 37.

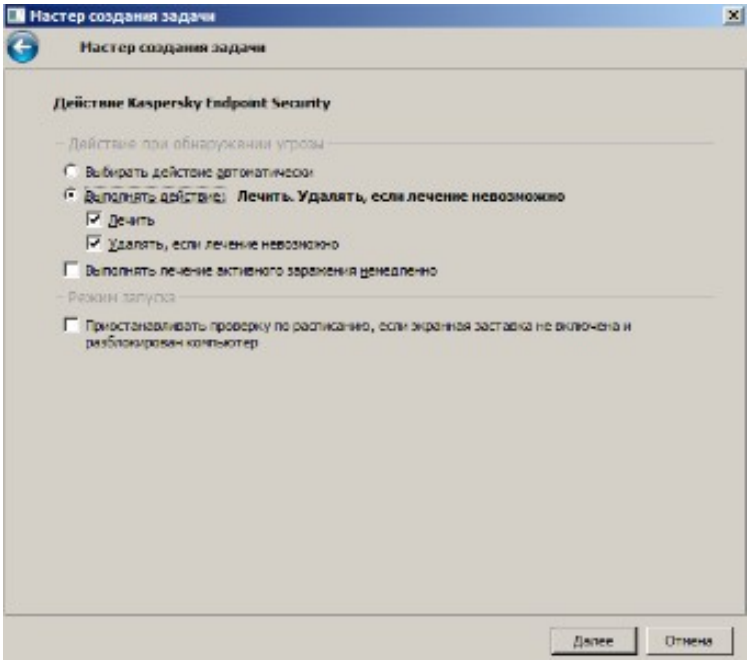

Рисунок 37 – Выбор действия при обнаружении угрозы

Затем предлагается выбрать расписание запуска задачи. В данном случае задача будет запускаться вручную. Таким образом требуется выбрать параметр «Вручную». Выбор расписания показан на рисунке 38.

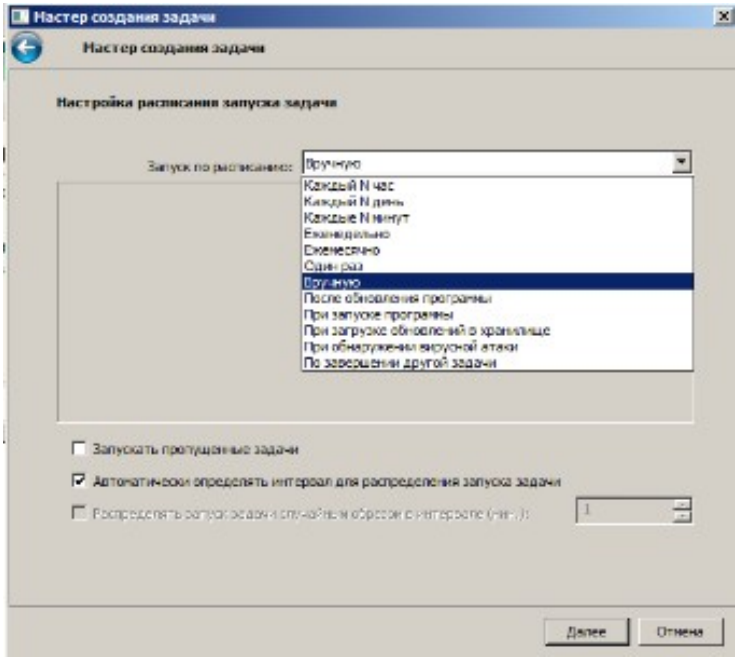

Рисунок 38 – Выбор расписания запуска

По завершению создания задачи, задача появится в списке. Результат показан на рисунке 39.

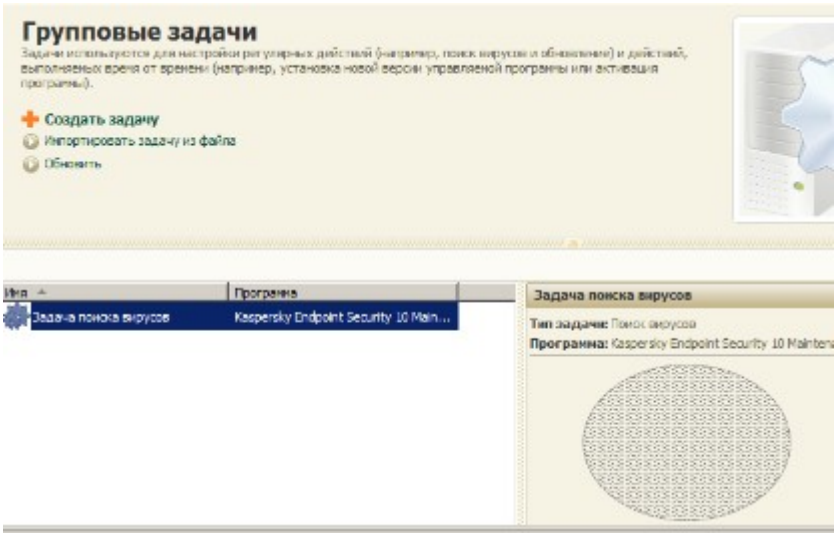

Рисунок 39 – Созданная задача

Функционирование созданных задач показано на рисунках 40 и 41.

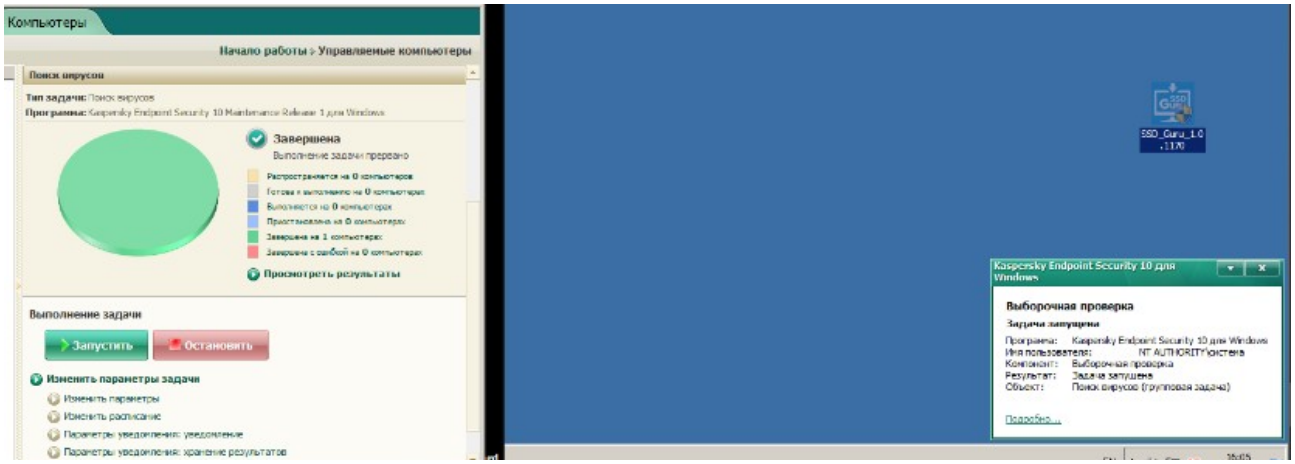

Рисунок 40 – Запуск задачи

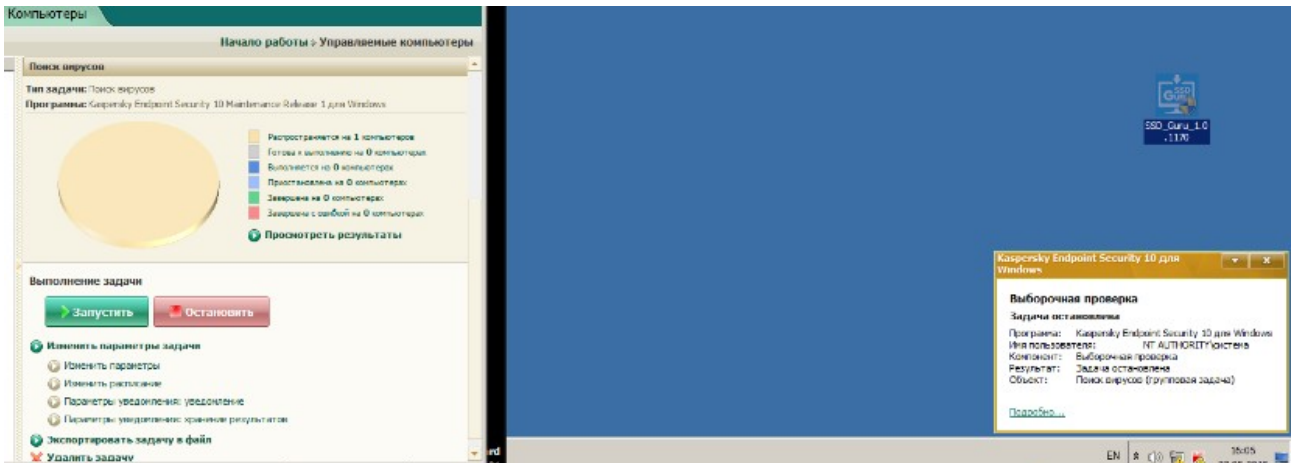

Рисунок 41 – Остановка задачи

5.7 Распределение трафика генерируемого в системе в процессе функционирования антивирусного средства

Уменьшение трафика происходит с помощью фильтров при скачивании обновлений утилитой Kaspersky Updater для Windows. Фильтры позволяют задавать более четкие условия, по которым определяется, нужно ли скачивать конкретный файл обновления или нет. Фильтры запускаются через графический интерфейс утилиты обновления. Запуск фильтра показан на рисунке 42. Стоит заметить, что все файлы обновления имеют признак, по которому можно задать подобную четкую фильтрацию. Использование фильтров описанных в этой статье, помогают уменьшить трафик, но не гарантирует максимально гибкой настройки списка файлов скачивания

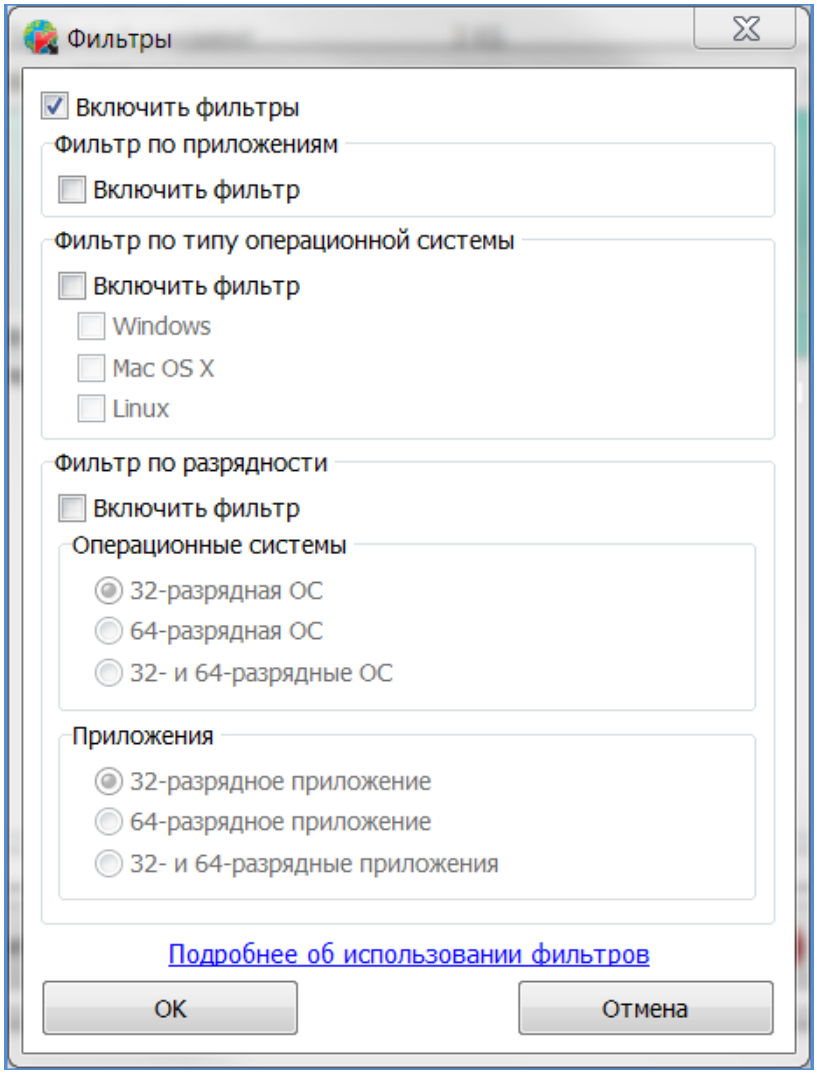

Рисунок 42 – Создание фильтра

6 Вредные психофизиологические факторы, влияющие на опорно-двигательный аппарат специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

6.1 Общие сведения

Безопасность жизнедеятельности представляет собой науку о комфортном и травмобезопасном взаимодействии человека со средой обитания. Является составной частью системы государственных, социальных и оборонных мероприятий, проводимых в целях защиты населения и хозяйства страны от последствий аварий, катастроф, стихийных бедствий, средств поражения противника. Целью БЖД также является снижение риска возникновения чрезвычайной ситуации по вине человеческого фактора. В современных организациях едва ли не большинство сотрудников проводят свой рабочий день за компьютером. Такой сотрудник зачастую является работником умственного труда. Однако он, так же как и работники труда физического, подвергается воздействию вредных факторов, обусловленных особенностями производственного процесса. Работа по разработке методики развертывания на предприятии средств антивирусной защиты с сетевым центром управления требует большого количества времени, проведенного за компьютером. При разработке методики администратор осуществляет следующие виды деятельности:

- работа по считыванию информации с экрана по предварительным запросам;
- работа по вводу информации;
- творческая работа в режиме диалога с компьютером.

В связи с этим необходимы повышенные условия комфортности рабочего места, на котором разрабатывается методика. Для этого необходимо осуществить мероприятия по обеспечению комфортных условий труда.

В данном разделе дипломного проекта были выявлены вредные психофизиологические факторы, влияющие на опорно-двигательный аппарат

специалиста по защите информации, а также определены методы и средства физической культуры, снижающие их воздействие.

6.2 Обзор вредных психофизиологические факторов, влияющих на опорно-двигательный аппарат специалиста по защите информации

Малоподвижность, монотонность движений и длительное пребывание в одном и том же положении приводят синдрому длительных статических нагрузок, вызывающему мышечные боли и воспалительные процессы, затрудненное дыхание, вызываемое выставленными вперед локтями, искривление позвоночника, а так же боли кистевых суставах из-за многочисленных мелких и монотонных движений. Недостаточный по времени отдых или же чрезмерная нагрузка в течение длительного времени приводят к переутомлению. При переутомлении отмечаются головная боль, рассеянность, снижение памяти, внимания, нарушение сна, которые приводят к снижению работоспособности, а в дальнейшем могут привести в хроническим заболеваниям. Для успешного труда пользователя ПЭВМ необходима рационально организованная окружающая среда, включающая в себя удобное расположение сигнализации, клавиш управления, сидения и т.п.

6.3 Обзор методов и средств физической культуры

Работа по разработке лабораторного практикума для изучения работы со средствами антивирусной защиты требует большого количества времени, проведенного за компьютером. В связи с этим были определены методы и средства физической культуры, снижающие вредное воздействие на опорно-двигательный аппарат. Конструкция рабочего стула обеспечивает поддержание рациональной рабочей позы при работе на ПЭВМ и позволяет изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Рабочий стул является подъемно- поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, при этом

регулировка каждого параметра является независимой, легко осуществляемой и имеет надежную фиксацию. Поверхность сиденья, спинки и других элементов стула является полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений. Высота рабочей поверхности стола составляет 725 мм, ширина – 1000 мм, глубина – 800 мм. Рабочий стол должен иметь пространство для ног высотой 600 мм, шириной – 550 мм, глубиной на уровне колен – 500 мм и на уровне вытянутых ног – 700 мм.

Конструкция рабочего стула обеспечивает:

- ширину и глубину поверхности сиденья 400 мм;
- поверхность сиденья с закругленным передним краем;
- регулировку высоты поверхности сиденья в пределах от 400 до 550 мм и углам наклона вперед до 15 град, и назад до 5 град.;
- высоту опорной поверхности спинки 310 мм, ширину - 400 мм и радиус кривизны горизонтальной плоскости - 400 мм;
- угол наклона спинки в вертикальной плоскости в пределах около 30 градусов;
- регулировку расстояния спинки от переднего края в пределах от 260 до 400 мм;
- стационарные или съемные подлокотники длиной 270 мм и шириной – 70 мм;
- регулировку подлокотников по высоте над сиденьем в пределах 230 мм и внутреннего расстояния между подлокотниками в пределах 500 мм.

Клавиатура расположена на поверхности стола на расстоянии 200 мм от края, обращенного к пользователю или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

Для профилактики заболеваний опорно-двигательного аппарата рекомендуется правильно организовать график работы с ПЭВМ. Организация работы с ПЭВМ осуществляется в зависимости от вида и категории трудовой деятельности.

Виды трудовой деятельности приведены в таблице 5: группа А - работа по считыванию информации с экрана ВДТ с предварительным запросом; группа Б - работа по вводу информации; группа В - творческая работа в режиме диалога с ПЭВМ, При выполнении в течение рабочей смены работ, относящихся к разным видам трудовой деятельности, за основную работу с ПЭВМ следует принимать такую, которая занимает не менее 50% времени в течение рабочей смены или рабочего дня. Для видов трудовой деятельности устанавливается 3 категории тяжести и напряженности работы с ПЭВМ, которые определяются: для группы А - по суммарному числу считываемых знаков за рабочую смену, но не более 60 000 знаков за смену; для группы Б - по суммарному числу считываемых или вводимых знаков за рабочую смену, но не более 40 000 знаков за смену; для группы В - по суммарному времени непосредственной работы с ПЭВМ за рабочую смену, но не более 6 часов за смену.

В зависимости от категории трудовой деятельности и уровня нагрузки за рабочую смену при работе с ПЭВМ устанавливается суммарное время регламентированных перерывов.

Таблица 5 - Суммарное время регламентированных перерывов в зависимости от продолжительности работы, вида и категории трудовой деятельности с ПЭВМ

Категория работы с ПЭВМ	Уровень нагрузки за рабочую смену при видах работ с ПЭВМ			Суммарное время регламентированных перерывов, мин	
	группа А, количество знаков	группа Б, количество знаков	группа В, ч	при 8-часовой смене	при 12-часовой смене
1	до 20 000	до 15 000	до 2	50	80
2	до 40 000	до 30 000	до 4	70	110
3	до 60 000	до 40 000	до 6	90	140

Перед началом работы на ПЭВМ, рекомендуются в течении 5 минут произвольные движения умеренной или средней интенсивности, направленные на дополнительное напряжение мышц конечностей. В процессе напряженной продолжительной умственной деятельности, сопровождаемой к тому же эмоциональным стрессом, рекомендуется проделать произвольные упражнения на общее расслабление и снижение тонуса скелетных мышц, желательно в сочетании с ритмичным сокращением небольших мышечных групп (разгибателей и сгибателей пальцев кисти, мимических мышц лица и т. п.).

Заключение

В результате дипломного проектирования была разработана методика развертывания на предприятии средств антивирусной защиты с сетевым центром управления. В процессе проектирования проведены анализ информационно-телекоммуникационной системы организации, обзор средств антивирусной защиты с сетевым центром управления и анализ возможных проблем при развертывании методики. На основании результатов была создана методика развертывания на предприятии средств антивирусной защиты с сетевым центром управления.

В рамках выполнения технологического раздела описан процесс методики развертывания на предприятии средств антивирусной защиты с сетевым центром управления.

В рамках выполнения раздела по безопасности жизнедеятельности разработаны мероприятия по обеспечению комфортных условий труда при разработке методики.

Таким образом, все задание на дипломное проектирование было выполнено в полном объеме.

Список использованных источников

1 Kaspersky Endpoint Security 10 for Windows (for workstation) [Электронный ресурс]. – Режим доступа: https://support.kaspersky.ru/kes10wks, свободный. – Загл. с экрана.

2 Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 – ФСТЭК России [Электронный ресурс]. – Режим доступа: http://fstec.ru/tekhnicheskaya-zashchitainformatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru0001-01bi00, свободный. – Загл. с экрана.

3 Сертификация [Электронный ресурс]. – Режим доступа: http://clsz.fsb.ru/certification.htm, свободный. – Загл. с экрана.

4 Санитарная обработка офиса. Выбираем корпоративный антивирус - "Хакер" [Электронный ресурс]. – Режим доступа: https://xakep.ru/2010/11/01/53650/, свободный. – Загл. с экрана.

5 Антивирусное программное обеспечение | Symantec [Электронный ресурс]. – Режим доступа: https://www.symantec.com/ru/ru/endpointprotection/system-requirements, свободный. – Загл. с экрана.

6 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности – М.: Стандартинформ, 2014 год. – 96 с.

7 ГОСТ 12.0.003-2015. Система стандартов по безопасности труда. Опасные и вредные производственные факторы. Классификация. М.: Стандартинформ, 2016 год. – 10 с.

8 Опасные и вредные факторы при работе с ПЭВМ [Электронный ресурс]. – Режим доступа: http://rgrtu-640.narod.ru/bezopasnostzhiznedeyatelnosti/45.html, свободный. – Загл. с экрана.

9 Вредные и опасные факторы при работе с компьютером [Электронный

ресурс]. – Режим доступа: http://www.grandars.ru/shkola/bezopasnostzhiznedeyatelnosti/vrednye-faktory-pri-rabote-na-pk.html, свободный. – Загл. С экрана.

10 Экзамен по физической культуре в вузе / Коваль Л.Н., Богданов О.Г., Ярошенко Е.В., Алексеева Е.Н., М.-Берлин: Директ-Медиа, 2015.

11 Физическая культура студента / Под ред. Ильинича В.И. М.: Гардарики, 2000.