

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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 10.05.02 –

Информационная безопасность
телекоммуникационных систем

Специализация –

Разработка защищенных
телекоммуникационных систем

ДИПЛОМНЫЙ ПРОЕКТ

на тему

МЕТОДИКА УПРАВЛЕНИЯ АНТИВИРУСНОЙ БЕЗОПАСНОСТЬЮ В
ОРГАНИЗАЦИИ

Студент _____ Анучин Роман Александрович

Руководитель к.т.н., доцент _____ Липилин О.В.

Нормоконтролёр к.т.н., доцент _____ Фатеев А.Г.

Рецензент ведущий инженер АО «ПНИЭИ» _____ Авдеев А.О.

Работа допущена к защите (протокол заседания кафедры от _____ № _____)

Заведующий кафедрой _____ С.Л. Зефирова

Работа защищена с отметкой _____ (протокол заседания ГЭК
от _____ № _____)

Секретарь ГЭК _____ А.Г. Фатеев

Пенза 2018

Оглавление

Введение.....	4
1 Анализ процесса управления антивирусной безопасностью в организации .	5
1.1 Процесс управления антивирусной безопасностью в организации ..	5
1.2 Процесс развертывания системы антивирусной безопасности	7
1.3 Процесс настройки системы антивирусной безопасности	10
1.4 Процесс контроля функционирования системы антивирусной безопасности	12
1.5 Процесс управления пользователями системы антивирусной безопасности	14
2 Обзор средств антивирусной защиты с сетевым центром управления	15
2.1 Kaspersky Endpoint Security 10.....	15
2.2 Dr.Web Enterprise Security Suite 10.0.....	17
2.3 Symantec Endpoint Protection 12.....	18
3 Разработка типовой политики антивирусной безопасности.....	21
4 Разработка методики управления антивирусной безопасностью в организации	23
5 Разработка лабораторного стенда для проверки методики	24
6 Вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	25
6.1 Вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации	25
6.2 Методы и средства физической культуры, снижающие их воздействие	27
Заключение	30
Список используемых источников.....	31
Приложение А Диаграммы процессов.....	33
Приложение Б Типовая политика антивирусной безопасности.....	40

Приложение В Методика управления антивирусной безопасностью в организации	51
Приложение Г Диаграмма компонентов лабораторного стенда	67
Приложение Д Проверка методики управления антивирусной безопасностью в организации.....	68
Приложение Е Протокол проверки ВКР в системе Антиплагиат.....	94

Введение

Компьютерные вирусы не без основания считаются одной из наиболее серьезных угроз в сфере информационной безопасности. Подтверждается это ущербом, который несут компании в результате воздействия вирусных атак. Использование обычного антивирусного программного обеспечения зачастую затруднительно в связи с масштабом сети организации, поэтому рекомендуется использовать средства антивирусной защиты с сетевым центром управления. Это позволяет администратору со своего рабочего места централизованно управлять всеми компонентами, входящими в систему антивирусной безопасности организации, отслеживать антивирусную обстановку в сети.

Целью данной работы является разработка методики управления антивирусной безопасностью в организации с использованием сетевого центра управления. Данная методика предназначена для развертывания и дистанционного управления системой антивирусной безопасности в организации с использованием сетевого центра.

Задачами выпускной квалификационной работы являются:

- проведение анализа процесса управления антивирусной безопасностью в организации;
- обзор и сравнение средств антивирусной защиты с сетевым центром управления;
- разработка типовой политики антивирусной безопасности;
- разработка методики управления антивирусной безопасностью в организации с использованием сетевого центра управления;
- разработка лабораторного стенда для проверки методики;
- изучение вредных психофизиологических факторов, влияющих на психоэмоциональное состояние специалиста по защите информации. Определение методов и средств физической культуры, снижающих их воздействие.

1 Анализ процесса управления антивирусной безопасностью в организации

1.1 Процесс управления антивирусной безопасностью в организации

Процесс управления антивирусной безопасностью в организации в общем случае можно разбить на пять процессов:

- разработка политики антивирусной безопасности в организации;
- развертывание системы антивирусной безопасности;
- настройка системы антивирусной безопасности;
- управление пользователями системы антивирусной безопасности;
- контроль функционирования системы антивирусной безопасности.

Политика антивирусной безопасности – это высокоуровневый документ, который прописывает стандарт организации в этой области, описывает принципы и порядок функционирования системы антивирусной безопасности, определяет ответственность каждого из участников системы, определяет объекты, подлежащие защите. В качестве управляющих данных для процесса разработки политики антивирусной безопасности выступает документ «Политика информационной безопасности». Разработку политики антивирусной безопасности осуществляет администратор информационной безопасности или другое ответственное за это лицо. Входными данными для данного процесса являются возможные программные и сетевые угрозы безопасности актуальные для организации, а также структура организации. Выходными данными является разработанная и утвержденная политика антивирусной безопасности, которая должна регламентировать все процессы, связанные с антивирусной безопасностью организации.

Развертывание системы антивирусной безопасности осуществляет администратор информационной безопасности или другое ответственное за это лицо в соответствии с политикой и методикой антивирусной безопасности. Также, в случае необходимости локальной установки программ на клиентские компьютеры, могут быть задействованы пользователи. Входными данными

для этого процесса являются дистрибутивы антивирусного программного обеспечения, включающего сетевой центр управления и другие необходимые компоненты системы, параметры установки компонентов системы. Помимо этого, входными данными для уже развернутой системы антивирусной безопасности будут являться отчеты и уведомления об инцидентах информационной безопасности, произошедших в системе. Они необходимы в том случае, если необходимо изменить структуру системы антивирусной безопасности для исключения повторения произошедшего инцидента информационной безопасности. На выходе процесса установленное антивирусное программное обеспечение на компьютере администратора и клиентских компьютерах, а также определенные в результате процесса топология системы антивирусной безопасности и группы администрирования.

Настройка компонентов системы антивирусной безопасности осуществляется после развертывания системы администратором с помощью сетевого центра управления. Целью процесса является обеспечения функционирования компонентов системы в соответствии с политикой антивирусной безопасности. Настройки системы осуществляются с помощью методики антивирусной безопасности в соответствии с заданными правами для учетных записей пользователей. Входными данными для процесса являются установленное антивирусное программное обеспечение, группы администрирования, а также, при необходимости изменить настройки в случае возникновения инцидентов информационной безопасности, уведомления и отчеты об инцидентах информационной безопасности. На выходе процесса базовые политики и задачи, политики реагирования на инциденты информационной безопасности и задачи уведомлений и отчетов.

Процесс контроля функционирования системы антивирусной безопасности осуществляется на основании политики антивирусной безопасности и заданных прав доступа для учетных записей пользователей. Данный процесс осуществляет информирование администратора и других ответственных лиц о состоянии системы антивирусной безопасности, об

инцидентах и событиях в системе. Контроль выполняется на клиентских компьютерах с помощью созданных в сетевом центре управления задач и политик. Ответственными за контроль функционирования являются администратор информационной безопасности, а также лицо, имеющее право только на формирование и просмотр отчетов и уведомлений о событиях и инцидентах информационной безопасности – аудитор. На выходе процесса уведомления и отчеты об инцидентах информационной безопасности, которые при необходимости могут быть использованы для изменения структуры и настроек системы антивирусной безопасности организации.

Управление пользователями системы антивирусной безопасности осуществляется на основании политики и методики антивирусной безопасности. Управление пользователями включает в себя создание, редактирование, блокирование учетных записей пользователей системы и осуществляется администратором с помощью сетевого центра управления. Входными данными для процесса являются список пользователей, топология системы антивирусной безопасности, группы администрирования и установленное антивирусное программное обеспечение. На выходе процесса будут учетные записи пользователей системы антивирусной безопасности с определенными для них правами доступа и назначенными ролями.

Общий вид процесса управления антивирусной безопасностью в организации приведен на рисунке А.1 в приложении А.

Декомпозиция данного процесса по методологии IDEF0 приведена на рисунке А.2 в приложении А.

1.2 Процесс развертывания системы антивирусной безопасности

Процесс развертывания системы антивирусной безопасности в организации в общем случае можно разбить на семь процессов:

- определение иерархии серверов;
- определение иерархии групп администрирования;

- установка сетевого центра управления антивирусной безопасности на компьютере администратора;
- создание инсталляционных пакетов для компонентов системы антивирусной безопасности;
- добавление клиентских компьютеров в группы администрирования;
- удаленная установка программного обеспечения компонентов системы антивирусной безопасности на клиентские компьютеры;
- локальная установка программного обеспечения компонентов системы антивирусной безопасности на клиентские компьютеры.

В качестве управляющей информации для каждого из процессов выступают политика и методика антивирусной безопасности.

В случае наличия нескольких серверов администрирования их количество и иерархию определяет администратор информационной безопасности. Для определения иерархии серверов необходимо знать структуру организации. В уже развернутой системе антивирусной безопасности иерархия серверов при необходимости может меняться на основании отчетов и уведомлений об инцидентах информационной безопасности, обнаруженных в системе. В соответствии с иерархией серверов определяется топология системы антивирусной безопасности в организации, которая в дальнейшем нужна при установке сетевого центра управления, а также при назначении прав доступа и ролей учетным записям в процессе управления пользователями.

Определение иерархии групп администрирования необходимо для разграничения прав пользователей, входящих в различные группы. Иерархия определяется на основании описания структуры организации администратором информационной безопасности. В случае возникновения инцидентов информационной безопасности в системе антивирусной безопасности иерархия групп администрирования может быть изменены на основании уведомлений и отчетов об этих инцидентах. На выходе процесса будет построенная в центре управления иерархия групп администрирования.

Установка сетевого центра управления антивирусной безопасностью осуществляется администратором на своем компьютере с помощью дистрибутива центра управления в соответствии с определенной топологией системы антивирусной безопасности. Сетевой центр управления позволяет администратору централизованно управлять клиентскими компьютерами. Результатом процесса является установленный центр управления системы антивирусной безопасности.

Создание инсталляционных пакетов для компонентов системы антивирусной безопасности осуществляется администратором через центр управления. В качестве входных данных выступают дистрибутивы компонентов системы антивирусной безопасности и параметры установки пакетов. Также входными данными при необходимости изменить состав программного обеспечения на клиентских компьютерах в случае возникновения инцидента информационной безопасности будут уведомления и отчеты об этих инцидентах. На выходе процесса будут созданные инсталляционные пакеты, с помощью которых далее осуществляется установка компонентов на клиентские компьютеры.

Добавления клиентских компьютеров в группы администрирования необходимо для разграничения прав доступа между компьютерами. В качестве входных данных для процесса выступают информация о клиентских компьютерах и определенная ранее иерархия групп администрирования. Добавление клиентских компьютеров может осуществляться автоматически, на основании заранее определенных правил, или вручную администратором. На выходе процесса будут сформированные группы администрирования.

Удаленная установка программного обеспечения компонентов системы антивирусной безопасности на клиентские компьютеры осуществляется с помощью созданных ранее инсталляционных пакетов через сетевой центр управления. Установка может быть инициализована администратором либо выполняться автоматически при добавлении клиентского компьютера в группу администрирования. Результатом процесса является установленное на

клиентском компьютере необходимое программное обеспечение компонентов системы антивирусной безопасности.

Когда удаленная установка программного обеспечения компонентов системы антивирусной безопасности на клиентские компьютеры невозможна или затруднена, то осуществляется локальная установка. Установка осуществляется с помощью созданного ранее инсталляционного пакета вручную администратором или пользователями, которым данный пакет рассылается через электронную почту либо выкладывается в общую папку. Результатом процесса является установленное на клиентском компьютере необходимое программное обеспечение компонентов системы антивирусной безопасности.

Декомпозиция процесса развертывания системы антивирусной безопасности в организации приведена на рисунке А.3 в приложении А.

1.3 Процесс настройки системы антивирусной безопасности

Процесс настройки системы антивирусной безопасности в организации в общем случае можно разбить на три процесса:

- настройка базовых параметров функционирования системы антивирусной безопасности;
- настройка реагирования на инциденты информационной безопасности;
- настройка формирования и рассылки уведомлений и отчетов о событиях антивирусной безопасности.

В качестве управляющей информации для каждого из процессов выступают политика и методика антивирусной безопасности.

Процесс настройки базовых параметров функционирования системы антивирусной безопасности включает формирование политики защиты клиентских компьютеров и серверов, задачи поиска вирусов, получение обновлений и резервного копирования данных и так далее. Входными данными является установленное антивирусное программное обеспечение на

компьютере администратора и на клиентских компьютерах и группы администрирования. Так же базовые параметры могут меняться при возникновении инцидентов информационной безопасности на основании уведомлений и отчетов о них. Настройка осуществляется администратором с помощью сетевого центра управления. На выходе процесса будут настроенные базовые задачи и политики. Результаты данного процесса являются входными данными для следующих процессов настройки системы антивирусной безопасности.

Настройка реагирования на инциденты информационной безопасности осуществляется администратором с помощью сетевого центра управления. Реагирование осуществляется выполнением созданных и настроенных соответствующим образом политик реагирования на инциденты информационной безопасности, которые являются выходными данными процесса

Настройка формирования и рассылки уведомлений и отчетов о событиях антивирусной безопасности выполняется на основе базовых задач и политик, а также групп администрирования. Настройка уведомлений о событиях антивирусной безопасности осуществляется администратором с помощью сетевого центра управления. Процесс включает в себя настройку параметров уведомления администратора информационной безопасности и/или аудитора о событиях на клиентских компьютерах и выбор способа уведомления (электронная почта, SMS, исполняемый файл и тому подобное). Настройка осуществляется администратором информационной безопасности с помощью сетевого центра управления. Настройка формирования и рассылки отчетов о событиях антивирусной безопасности выполняется при помощи шаблонов отчетов. Могут использоваться как стандартные шаблоны, так и созданные пользовательские. Отчеты содержат информацию о состоянии системы защиты. Рассылка отчетов осуществляется по электронной почте или сохранением в выбранной папке, например, в папке общего доступа. Настройка осуществляется администратором информационной безопасности

с помощью сетевого центра управления. Выходными данными процесса являются задачи формирования и рассылки уведомлений и отчетов о состоянии антивирусной безопасности в организации.

Декомпозиция процесса настройки системы антивирусной безопасности в организации приведена на рисунке А.4 в приложении А.

1.4 Процесс контроля функционирования системы антивирусной безопасности

Процесс контроля функционирования системы антивирусной безопасности в организации в общем случае можно разбить на четыре процесса:

- контроль устройств;
- контроль программного обеспечения;
- реагирование на инциденты информационной безопасности;
- формирование и рассылка уведомлений и отчетов об инцидентах информационной безопасности.

В качестве управляющей информации для каждого из этих процессов выступают политика и методика антивирусной безопасности в организации.

Контроль устройств позволяет ограничить доступ пользователей на клиентских компьютерах к устройствам, установленным или подключенным к компьютеру. На вход процесса поступают базовые политики и задачи. На выходе процесса политики контроля устройств. Создает политики контроля устройств администратор информационной безопасности с помощью сетевого центра управления. При создании политик учитываются права доступа, определенные для учетных записей пользователей.

Контроль программного обеспечения позволяет устанавливать ограничения на запуск программ на клиентских компьютерах, а также обеспечивать контроль доступа уже запущенных программ к ресурсам клиентских компьютеров, таких как системный реестр, файлы, ключи и так далее. На вход процесса поступают базовые политики и задачи. На выходе

процесса политики контроля программного обеспечения. Создает политики контроля программного обеспечения администратор информационной безопасности с помощью сетевого центра управления с учетом прав доступа, определенных для учетных записей пользователей.

Реагирование на инциденты информационной безопасности осуществляется на основании базовых политик и задач, политик контроля устройств и программного обеспечения, а также политик реагирования на инциденты информационной безопасности. При возникновении на клиентских компьютерах инцидентов, например, при вирусной атаке, автоматически активируются политики, позволяющие устранить инцидент и снизить его последствия. Данные политики создаются администратором информационной безопасности с помощью центра управления. Результаты реагирования на инциденты информационной безопасности используются для формирования соответствующих уведомлений и отчетов.

Для процесса формирования и рассылки уведомлений и отчетов об инцидентах информационной безопасности входными данными будут являться: базовые политики и задачи, задачи уведомлений и отчетов, политики контроля устройств и программного обеспечения, а также результаты реагирования на возникшие инциденты информационной безопасности на клиентских компьютерах. Помимо администратора информационной безопасности формировать и получать уведомления и отчеты об инцидентах может специально назначенное для этого лицо – аудитор. Сформированные уведомления и отчеты об инцидентах информационной безопасности в организации могут быть использованы в дальнейшем для анализа и изменения топологии и настроек системы антивирусной безопасности в организации.

Декомпозиция процесса контроля функционирования системы антивирусной безопасности в организации приведена на рисунке А.5 в приложении А.

1.5 Процесс управления пользователями системы антивирусной безопасности

Процесс управления пользователями системы антивирусной безопасности в организации в общем случае можно разбить на два процесса:

- создание новых учетных записей пользователей;
- редактирование существующих учетных записей пользователей.

Для создания учетных записей пользователей необходим список пользователей, которым требуются учетные записи в системе, а также установленной антивирусное программное обеспечение. Учетные записи создаются администратором информационной безопасности или другим ответственным лицом с необходимыми для этого правами. Создание учетных записей должно выполняться в соответствии с политикой антивирусной безопасности организации и методикой управления. В результате процесса образуется список учетных записей, для которых впоследствии будут назначены права доступа.

Редактирование учетных записей осуществляется на основе топологии системы антивирусной безопасности, групп администрирования и списка учетных записей и должно соответствовать политике и методике управления антивирусной безопасности в организации. Редактирование заключается в формировании групп пользователей с разными правами доступа в зависимости от типовых задач и служебных обязанностей. Редактирование осуществляется администратором информационной безопасности с помощью сетевого центра управления или другим ответственным лицом с необходимыми для этого правами. На выходе процесса будут учетные записи пользователей с определенными для них правами доступа.

Декомпозиция процесса управления пользователями системы антивирусной безопасности приведена на рисунке А.6 в приложении А.

2 Обзор средств антивирусной защиты с сетевым центром управления

2.1 Kaspersky Endpoint Security 10

Линейка Kaspersky Endpoint Security состоит из нескольких продуктов, обеспечивающих защиту самых разнообразных ресурсов: рабочих станций, смартфонов, интернетшлюзов, почтовых (Sendmail, Qmail, Postfix, Exim, Exchange, Lotus) и файловых серверов (Windows, Linux, NetWare).

Администратор самостоятельно собирает мозаику из компонентов, необходимых для защиты систем и сервисов. Но при этом процесс их отбора и подсчета суммы лицензии очень прозрачен, поэтому неприятных сюрпризов удастся избежать. Лицензия рассчитывается из количества выбранных компонентов, тип компонента на цену не влияет. Клиент антивируса Касперского для Windows/Linux Workstation, устанавливаемый на рабочие места пользователей, обеспечивает комплексную защиту и включает в себя антивирус, IDS/IPS, антифишинг, контроль трафика и подключение внешних устройств. Кроме этого, в Kaspersky Endpoint Security реализована поддержка Cisco NAC и Microsoft NAP.

Kaspersky Endpoint Security предоставляет высокоэффективные технологии и инструменты обеспечения IT-безопасности для построения системы многоуровневой защиты. Технологии сканирования сети на наличие уязвимостей и управления установкой исправлений устраняют уязвимости в операционных системах и приложениях, а технология шифрования данных обеспечивает защиту конфиденциальной бизнес-информации в случае утери ноутбука или попытки несанкционированного доступа к данным.

Антивирус Касперского предоставляет следующие возможности:

- средства системного администрирования;
- мониторинг уязвимостей и установка исправлений;
- многоуровневая защита, в том числе шифрование;
- инструменты контроля рабочих мест;
- контроль и защита мобильных устройств;

– централизованное управление системой защиты.

В последней версии антивирусного ядра «Лаборатории Касперского» сигнатурные методы защиты сочетаются с эвристическим анализом, проактивной защитой и облачными технологиями, что позволяет оградить организацию от известных, новейших и комплексных угроз. Защита распространяется на рабочие станции Mac, Linux и Windows.

Kaspersky Endpoint Security обеспечивает защиту рабочих станций, защиту файловых серверов.

В решение Kaspersky Endpoint Security входит единая консоль управления Kaspersky Security Center, которая обеспечивает мониторинг работы используемых в сети защитных решений «Лаборатории Касперского» и позволяет управлять ими. Kaspersky Security Center упрощает процессы создания политик безопасности, распространения обновлений и мониторинга состояния защиты в мультиплатформенных сетях, значительно облегчая управление IT-безопасностью.

Системные требования данного антивируса следующие:

- Intel Pentium 1 ГГц или выше;
- 1 Гб оперативной памяти;
- 2 Гб свободного места на диске.

Стоимость данного антивируса 19210 рублей для 10 узлов на 1 год.

Антивирус Kaspersky Endpoint Security 10 для Windows имеет сертификат ФСТЭК России № 3025 до 25.11.2019. Антивирус сертифицирован на соответствие требованиям САВЗ, ИТ.САВЗ.Б2.ПЗ, ИТ.САВЗ.В2.ПЗ, ИТ.САВЗ.Г2.ПЗ.

Так же данный антивирус имеет сертификат ФСБ России номер СФ/СЗИ-0100 до 31.08.2019. Согласно данному сертификату антивирус соответствует требованиям ФСБ России к антивирусным средствам классов Б2, В2, Г2 и может использоваться для защиты информации, содержащей сведения, составляющие государственную тайну, при условии выполнения

требований формуляра 643.46856491.00068-03 30 01 и иной эксплуатационной документации.

2.2 Dr.Web Enterprise Security Suite 10.0

Dr. Web позиционируется как универсальное средство для защиты рабочих станций и файловых серверов Windows, а также почтовых серверов Unix (Linux, FreeBSD, Solaris). Наличие в списке устаревших версий ОС часто является решающим аргументом при выборе этой разработки в организациях, где таких систем много, а их замена нежелательна или невозможна. Соответственно, невысоки и системные требования, необходимые для работы агента Dr.Web на компьютерах пользователей.

Все компоненты (агент и сервер) разворачиваются с одного дистрибутива, что заметно упрощает процесс установки. Управление производится при помощи локализованных консоли управления и/или веб-интерфейса. Последний сделан с учетом возможной работы неподготовленного пользователя. В зависимости от вида лицензии, агент будет обеспечивать различную функциональность. Для лицензии "антивирус" пользователь получает антивирус, антируткит и антишпион, при наличии лицензии "комплексная защита" добавляются антиспам, веб-антивирус и офисный контроль (управление доступом к сетевым и локальным ресурсам). Дополнительно может устанавливаться NAP Validator, обеспечивающий проверку соответствия политикам NAP.

Dr.Web Enterprise Security Suite может использоваться даже в сетях сложной топологии, например, если антивирусные агенты не имеют прямого доступа к серверу ESS и между ними отсутствует маршрутизация пакетов (логически изолированная от Интернета внутренняя локальная сеть).

Для организации прямого доступа используется прокси-сервер. Прокси-сервер можно использовать также для значительного снижения сетевого трафика (оптимизация трафика) и уменьшения времени получения обновлений антивирусными агентами, поскольку он поддерживает кеширование обновлений и компонентов антивирусных агентов.

Использование технологии сжатия трафика (опция на сервере услуги) не является препятствием для использования прокси-сервера. Обработка пересылаемой информации осуществляется вне зависимости от того, сжимается трафик или нет.

Системные требования данного антивируса следующие:

- Intel Pentium 1 ГГц или выше;
- 512 Мб оперативной памяти;
- 750 Мб свободного места на диске.

Стоимость данного антивируса 20322 рубля для 10 узлов на 1 год.

Антивирус имеет сертификат ФСТЭК России № 3509 до 27.01.2019. Антивирус сертифицирован на соответствие требованиям САВЗ и САВЗ (ИТ.САВЗ.А2.ПЗ, ИТ.САВЗ.Б2.ПЗ, ИТ.САВЗ.В2.ПЗ, ИТ.САВЗ.Г2.ПЗ).

Так же данный антивирус имеет сертификат ФСБ России номер СФ/СЗИ-0051 до 30.06.2018. Согласно данному сертификату антивирус соответствует требованиям ФСБ России к антивирусным средствам классов А2, Б2, В2, Г2 и может использоваться для защиты информации, содержащей сведения, составляющие государственную тайну, при условии выполнения требований формуляра RU.72110450.00300 10 30 01 и иной эксплуатационной документации.

2.3 Symantec Endpoint Protection 12

Решение Symantec Endpoint Protection 12 предназначено для защиты рабочих станций и серверов, работающих под управлением ОС Windows, Mac OS X и Linux (как 32-битных редакций, так и 64-битных).

Symantec Endpoint Protection является корпоративным антивирусным решением, обеспечивающим администратора антивирусной сети предприятия необходимыми инструментами по развертыванию антивирусной сети предприятия, ее мониторингу, а также по управлению параметрами работы антивирусных клиентов на защищаемых объектах.

Система управления Symantec Endpoint Protection состоит из трех компонентов: Manager (сервер), Console и Database. В сети может работать

несколько серверов, обменивающихся политиками с родительским сервером. В качестве ОС для установки серверной части подходят XP/2003/2008/2012 (32/64-бит).

В комплекте с программой установки идет встроенная SQL база данных (на основе Sybase), которую рекомендуется использовать при подключении до 100 клиентов (она ставится автоматически при выборе режима инсталляции "Простой"). При наличии большого количества систем рекомендуется задействовать полнофункциональный SQL-сервер. Для работы серверной части потребуется наличие роли IIS, которую необходимо установить до развертывания Manager.

Все компоненты собраны в единый архив, который доступен на официальном сайте. Кроме этого, есть очень удобные мастера и инструменты. Так, мастер переноса и развертывания, который запускается сразу после инсталляции, помогает быстро установить антивирус на клиентских системах, перенести группы и политики с родительских серверов SEP.

В больших сетях вручную рассортировать клиентские системы весьма непросто — здесь на помощь приходят инструменты консоли Symantec. В критериях отбора систем можно задавать до 30 параметров: имя компьютера, IP-адрес, частота CPU, версия BIOS и так далее.

Системные требования данного антивируса следующие:

- Intel Pentium 1 ГГц или выше;
- 2 Гб оперативной памяти;
- 16 Гб свободного места на диске.

Стоимость данного антивируса 24350 рублей для 10 узлов на 1 год.

Антивирус имеет сертификат ФСТЭК России № 2586 до 13.03.2018. Антивирус сертифицирован на соответствие РД НДВ по 4 уровню контроля и ТУ.

Сертификата ФСБ России данный антивирус не имеет.

В таблице 1 приведено сравнение описанных выше антивирусных средств.

Таблица 1 – Сравнение антивирусных средств

	Kaspersky Endpoint Security 10	Dr.Web Enterprise Security Suite 10.0	Symantec Endpoint Protection 12
Процессор	1 ГГц	1 ГГц	1 ГГц
Оперативная память	1 ГБ	512 Мб	2 Гб
Жесткий диск	2ГБ	750 Мб	16 Гб
Поддерживаемые операционные системы	Windows, OS X, Linux		
Сертификат ФСТЭК России	№ 3025	№ 3509	№ 2586
Срок действия сертификата ФСТЭК России	До 25.11.2019	До 27.01.2019	До 13.03.2018
Сертификат ФСБ России	СФ/СЗИ-0100	СФ/СЗИ-0051	—
Срок действия сертификата ФСБ России	До 31.08.2019	До 30.06.2018	—
Стоимость лицензии на 10 узлов на 1 год	19210 рублей	20322 рублей	24350 рублей

3 Разработка типовой политики антивирусной безопасности

Политика антивирусной защиты – это документ «верхнего» уровня, разработка которого определяется степенью детализации основного документа предприятия в сфере информационной безопасности – политики или концепции информационной безопасности.

Политика антивирусной защиты определяет требования по защите информационно-телекоммуникационной инфраструктуры организации от угроз информационной безопасности, причина возникновения которых связана с распространением вредоносных программ. Данные требования минимизируют вероятность возникновения негативных последствий вследствие отсутствия защиты информационно-телекоммуникационной инфраструктуры. Негативные последствия могут включать в себя раскрытие или утрату чувствительной и конфиденциальной информации, кражу интеллектуальной собственности, репутационные последствия, а также влияние на важные внутренние системы организации.

В качестве основы для разработки политики антивирусной безопасности был взят раздел 10.4 ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» [6].

Содержание документа «верхнего» уровня определяет организационную часть вопроса и в нем должно быть указано:

- ответственные лица за его соблюдение;
- полномочия и ответственность отделов и служб в отношении реализации;
- объекты антивирусной защиты;
- средства антивирусной защиты;
- организационные мероприятия по антивирусной защите;
- мероприятия по профилактике вирусов;
- анализ ситуаций;
- применение средств антивирусной защиты.

Политика антивирусной защиты – это организационно-правовой и технический документ одновременно и при его составлении надо опираться на принцип разумной достаточности. Тщательность при подготовке документа не гарантирует его долговечности и требует регулярного пересмотра и приведения в соответствие с изменившимися условиями и требованиями бизнес-процессов и совершенствовании технической базы.

Разработанная типовая политика антивирусной безопасности в организации приведена в приложении Б.

4 Разработка методики управления антивирусной безопасностью в организации

Методика предназначена для развертывания и дистанционного управления системой антивирусной безопасности в организации с использованием сетевого центра управления.

Методика должна включать в себя:

- определение структурной схемы системы антивирусной безопасности
- руководство по развертыванию системы антивирусной безопасности;
- руководство по настройке базовых параметров функционирования антивирусных средств;
- рекомендации по обеспечению совместимости различных версий антивирусных средств;
- рекомендации по настройке параметров антивирусных средств для реагирования на инциденты информационной безопасности;
- рекомендации по настройке уведомлений о событиях антивирусной безопасности;
- рекомендации по формированию и рассылки отчетов о событиях антивирусной безопасности;
- рекомендации по масштабированию системы антивирусной безопасности;
- рекомендации по управлению пользователями системы антивирусной безопасности;
- рекомендации по контролю устройств и программного обеспечения на автоматизированных рабочих местах организации.

Полный текст разработанной методики приведен в приложении В.

5 Разработка лабораторного стенда для проверки методики

Лабораторный стенд предназначен для проверки разработанной методики управления антивирусной безопасностью в организации с использованием сетевого центра управления. В качестве антивирусного средства с сетевым центром управления был выбран Kaspersky Endpoint Security 10.

Лабораторный стенд построен на основе средства виртуализации Oracle VM VirtualBox и содержит три виртуальных машины. На первой установлена операционная система Windows Server 2008 R2 и программное обеспечение Kaspersky Security Center 10. Вторая виртуальная машина с операционной системой Windows 7 и с установленным антивирусным средством Kaspersky Endpoint Security 10 для Windows и агентом администрирования версии 10. На третьей виртуальной машине установлена операционная система Windows XP. Антивирусное средство Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 устанавливается на данную виртуальную машину в процессе проверки методики.

Диаграмма компонентов разработанного лабораторного стенда представлена на рисунке Г.1 в приложении Г.

Была проведена проверка разработанной методики управления антивирусной безопасностью в организации с помощью лабораторного стенда. Результаты проверки приведены в приложении Д.

6 Вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

6.1 Вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации

К опасных и вредных психофизиологических производственных факторов относятся физические (статические, динамические и гиподинамический) и нервно-психические перегрузки (умственное, зрительное, эмоциональное).

Среди физических перегрузок специалист по защите информации подвержен только статическим, так как он проводит большую часть времени в одном положении за компьютером

Среди нервно-психических перегрузок специалист по защите информации подвержен следующим:

- умственное перенапряжение, в том числе связанное с информационной нагрузкой;
- чрезмерное напряжение анализаторов, также вызванное информационной перегрузкой;
- монотонность труда, способствующая формированию монотонии, то есть снижению работоспособности в результате выполнения однообразной работы, связанной с частым повторением стереотипных действий;
- эмоциональные перегрузки [7].

Значительная нагрузка на все элементы зрительной системы при длительной работе за компьютером, умственные и нервно-эмоциональные нагрузки, продолжительная концентрация внимания, монотонность трудового процесса, большой объем информации, нерациональная организация рабочего места приводят к ухудшению психоэмоционального состояния специалиста.

Нервно-психические перегрузки в работе специалиста по защите информации определяются некачественными условиями передачи

изображения, несоответствием некоторых параметров информационных систем психофизиологическими особенностями человека, необходимостью внимательного наблюдения за информационными знаками, быстрого анализа постоянно изменяющейся информации, принятия продуктивных решений и выполнения определённых корректирующих действий.

Зачастую после длительной работы за компьютером возникают зрительное переутомление, головная боль, ноющие боли в мышцах шеи, плечевого пояса и спины, снижение способности к концентрации внимания.

Ухудшение самочувствия специалистами по защите информации при длительной работе связано также с повышением пульсации потоков света от источников искусственного освещения и монитора. Пульсации потоков света способствуют повышению общего и зрительного переутомления, ухудшению зрительной и общей работоспособности. При уменьшении частоты световых пульсаций вредное воздействие усиливается. К нервно-психическим факторам относится также низкочастотное мерцание экрана (до 200 Гц), то есть кажущееся изменение яркости свечения [8]. Оно возникает из-за взаимодействия пульсирующих потоков света экрана и источников света. Это объясняется тем, что у человека зрительная система по ходу эволюции приспособилась для восприятия изображения в отраженном свете (напечатанная информация, тексты, рисунки), а не для работы за монитором компьютера. Изображение на дисплее сильно отличается от привычного глазу объектов внешнего мира – оно светится, мерцает, состоит из дискретных точек, кроме этого цвета компьютерного изображения отличаются от естественных цветов. Однако зрительное переутомление вызывают не только особенности изображения на экране. Сильная нагрузка на глаза оказывается при введении информации, так как пользователю необходимо переводить часто взгляд с экрана на набираемый текст и клавиатуру, которые находятся на разном расстоянии от монитора и по-разному освещены.

Зрительное переутомление обычно проявляется при затуманивании зрения, сопровождается трудностями при переносе взгляда с близких

предметов на дальние и с дальних на близкие, кажущееся изменение цвета предметов, двоение предметов, чувством жжения, «песка» в глазах, болезненными ощущениями при движении глаз, покраснением век.

Специфическое воздействие электромагнитного поля выражается в биохимических изменениях, происходящие в клетках и тканях. Наиболее подвержены данным воздействиям центральная и сердечно-сосудистая системы. Могут наблюдаться отклонения в работе эндокринной системы. В начале воздействия отмечается повышение возбудимости нервной системы, проявляющееся повышением раздражительности, нарушением сна, эмоциональной неуравновешенностью. Затем развиваются астенические проявления, т.е. физическая и нервнопсихическая слабость. В целом хроническое воздействие ЭМП проявляется следующими симптомами: головная боль, повышенная утомляемость, ухудшение самочувствия, брадикардия (урежение пульса), а также гипотония (понижение артериального давления), боли в сердце. Данные негативные симптомы могут выражаться в разной степени [9].

6.2 Методы и средства физической культуры, снижающие воздействие вредных психофизиологических факторов

Существует большое количество методов для достижения расслабления глазного аппарата, в последнее время успешно зарекомендовал себя метод пальминга. Это упражнение, заключающееся в накладывании на закрытые глаза ладоней обеих рук (без давления). В таком положении следует находиться четыре-пять минут. Данную процедуру, направленную на естественное восстановление зрения, рекомендуется выполнять ежедневно.

Не менее эффективная профилактика для глаз - распределения слезной жидкости, обладающей увлажняющими и дезинфицирующими свойствами, по поверхности глазного яблока необходимо часто моргать. Моргание дает кратковременный отдых, укрепляет нервные волокна сетчатки, обеспечивает расслабление глазных мышц, улучшает центровку и способность глаза фокусировать изображение.

Упражнения для глаз за компьютером лучше выполнять в расслабленном состоянии. При наличии боли в области шеи или спины, необходимо сначала выполнить упражнения для этих зон. При выполнении упражнений для глаз надо глубоко дышать, так как при работе глазные мышцы должны активно насыщаться кислородом.

При умственном труде, который лежит в основе деятельности специалиста по защите информации, в коре головного мозга формируются замкнутые циклы возбуждения, которые характеризуются большой устойчивостью и инертностью. Поэтому, если после прекращения физической нагрузки человек практически сразу может переключиться на новый вид деятельности, то при умственном труде интенсивная работа мозга не заканчивается продолжительное время и после завершения интеллектуальной нагрузки [10].

В основе организации отдыха при умственных перегрузках лежит принцип активного отдыха, который предусматривает систему организованных движений до, в процессе и по окончании умственной деятельности, что оказывает благоприятный эффект не только в сохранении, но и повышении умственной работоспособности. Ежедневные и регулярные физические упражнения способствуют формированию в коре больших полушарий «доминанты движения», которая оказывает положительное воздействие на состояние дыхательной, мышечной, сердечно-сосудистой систем организма, активизирует зону сенсомоторной активности в коре головного мозга, способствует повышению тонуса всего организма.

Перед началом интенсивной умственной работы, для сокращения периода вработывания, рекомендуются в течение 5 минут произвольные движения умеренной или средней интенсивности, направленные на дополнительное напряжение мышц конечностей. При этом чем ниже исходное нервно-психическое и мышечное напряжение человека, и чем быстрее необходимо включиться в работу, тем интенсивнее должны быть упражнения на напряжение скелетных мышц. 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.).

Для повышения работоспособности мозга на фоне мышечного расслабления, улучшения функций дыхания и кровообращения, необходимо регулярно выполнять кратковременные физические упражнения. Например, раз в час при работе за компьютером проделать познотонические упражнения в течении нескольких минут. а через каждые 2 часа желательно проводить минутные динамические упражнения, такие как бег на месте, с ритмичным, глубоким дыханием [11].

Помимо всего этого для снижения воздействия вредных психофизиологических факторов, влияющие на психоэмоциональное состояние специалиста по защите информации важно правильно организовывать режим дня, соблюдая время отхода ко сну и ежедневного пробуждения, имея нормальную продолжительность сна.

Заключение

В результате выполнения выпускной квалификационной работы был проведен анализ процесса управления антивирусной безопасностью в организации при использовании сетевого центра управления. Для процесса была построена диаграмма по стандарту IDEF0. Были рассмотрены подпроцессы, для которых также были построены диаграммы.

Были рассмотрены три основных средства антивирусной защиты с сетевым центром управления: Kaspersky Endpoint Security 10, Dr.Web Enterprise Security Suite 10.0 и Symantec Endpoint Protection 12.

Была разработана типовая политика антивирусной безопасности организации, определяющая требования по защите информационно-телекоммуникационной инфраструктуры организации от угроз информационной безопасности, причина возникновения которых связана с распространением вредоносных программ.

На основании анализа процесса управления антивирусной безопасностью в организации и требований типовой политики антивирусной безопасности была разработана методика управления антивирусной безопасностью в организации с использованием сетевого центра управления.

Для проверки методики был разработан лабораторный стенд, в котором в качестве средства антивирусной защиты с сетевым центром управления был использован Kaspersky Endpoint Security 10.

Были рассмотрены вредные психофизиологические факторы, которые влияют на психоэмоциональное состояние специалиста по защите информации, а также методы и средства физической культуры, снижающие их воздействие.

Таким образом, все пункты технического задания на выпускную квалификационную работу выполнены полностью.

Список используемых 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-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00>, 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://haker.ru/2010/11/01/53650/>, свободный. – Загл. с экрана.
- 5 Антивирусное программное обеспечение | Symantec [Электронный ресурс]. – Режим доступа: <https://www.symantec.com/ru/ru/endpoint-protection/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/bezopasnost-zhiznedeyatelnosti/45.html>, свободный. – Загл. с экрана.

9 Вредные и опасные факторы при работе с компьютером [Электронный ресурс]. – Режим доступа: <http://www.grandars.ru/shkola/bezopasnost-zhiznedeyatelnosti/vrednye-factory-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.

ПРИЛОЖЕНИЕ А
(обязательное)
Диаграммы процессов

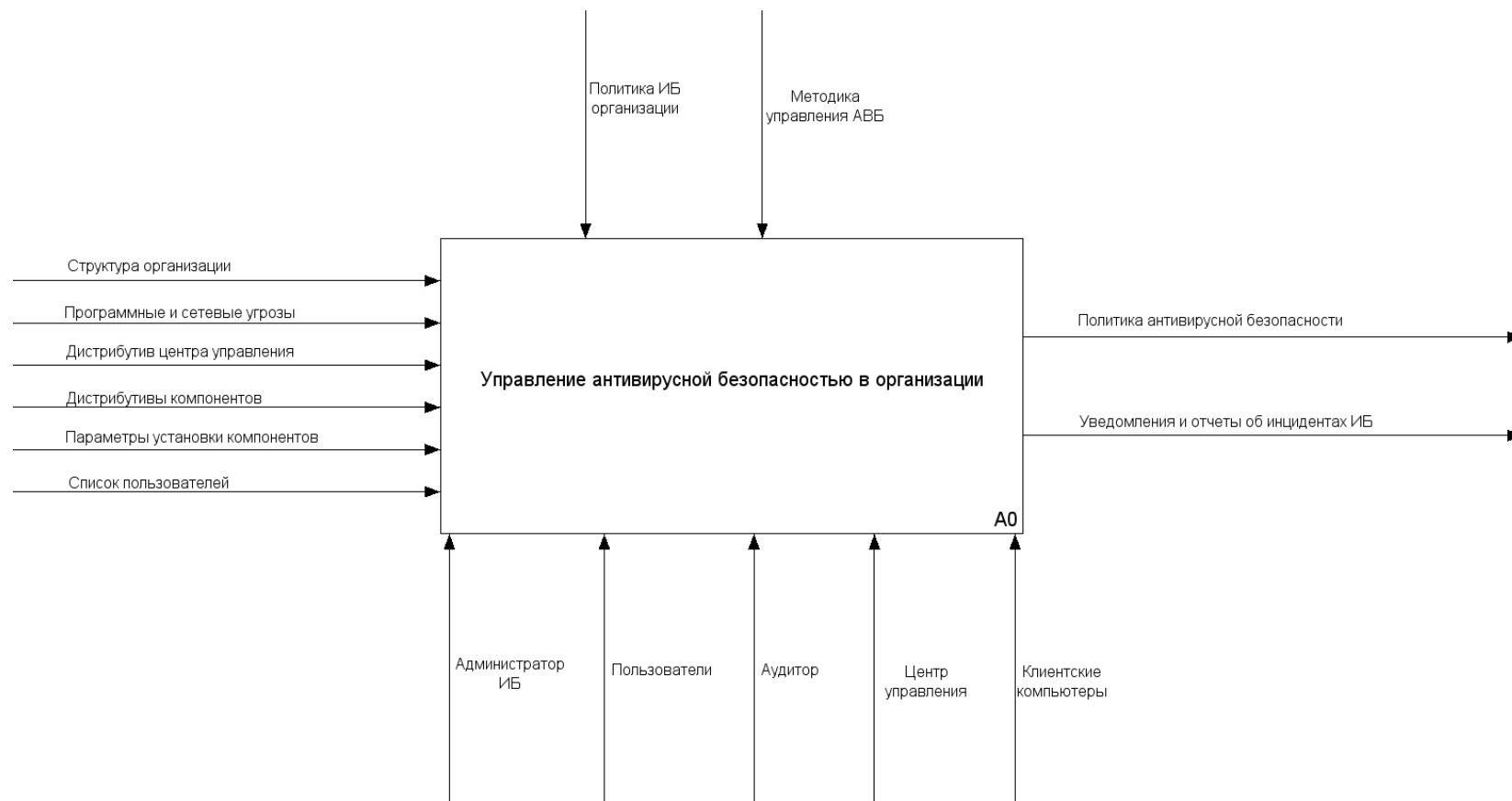


Рисунок А.1 – Процесс управления антивирусной безопасностью в организации

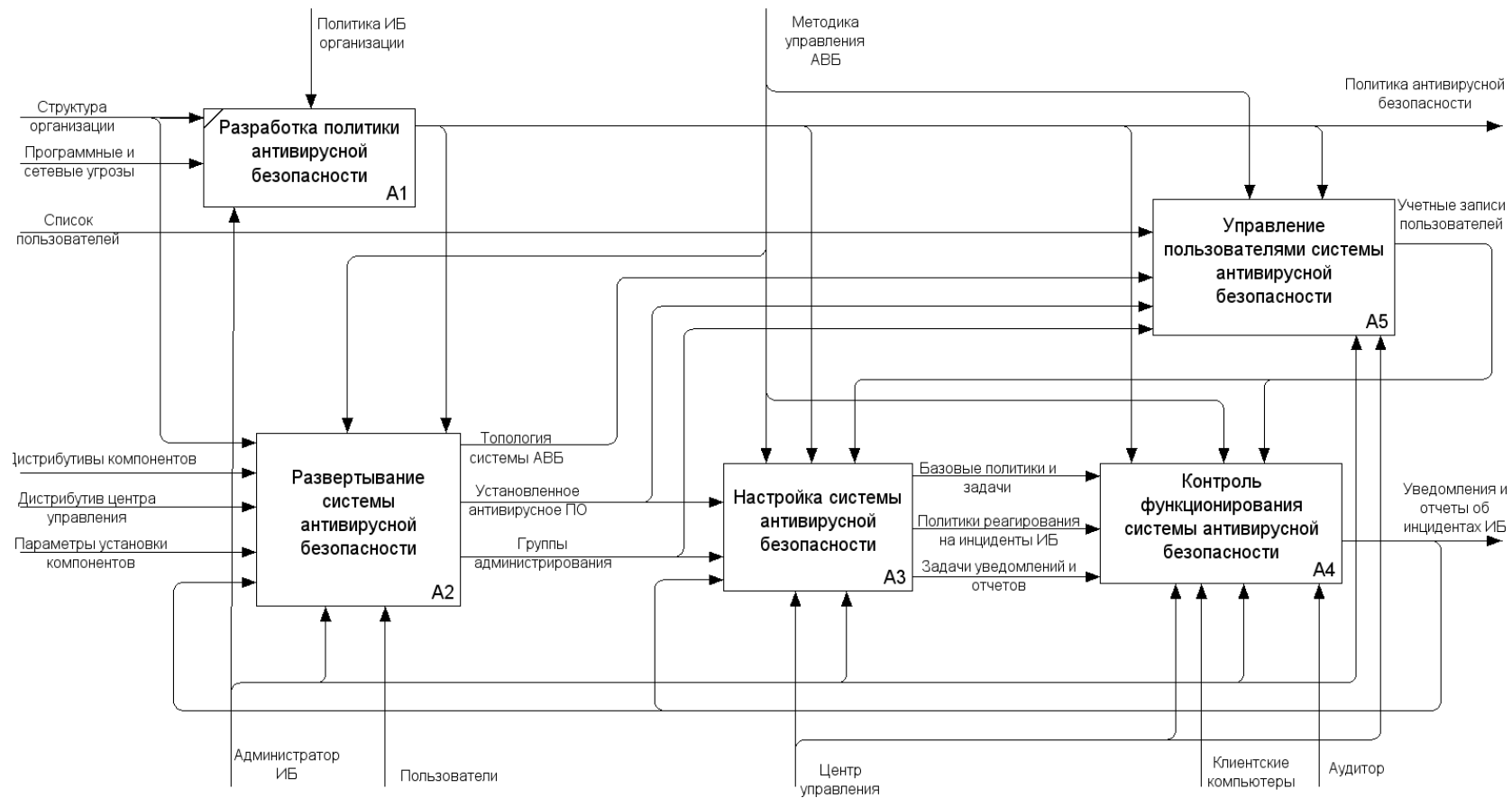


Рисунок А.2 – Декомпозиция процесса управления антивирусной безопасностью в организации

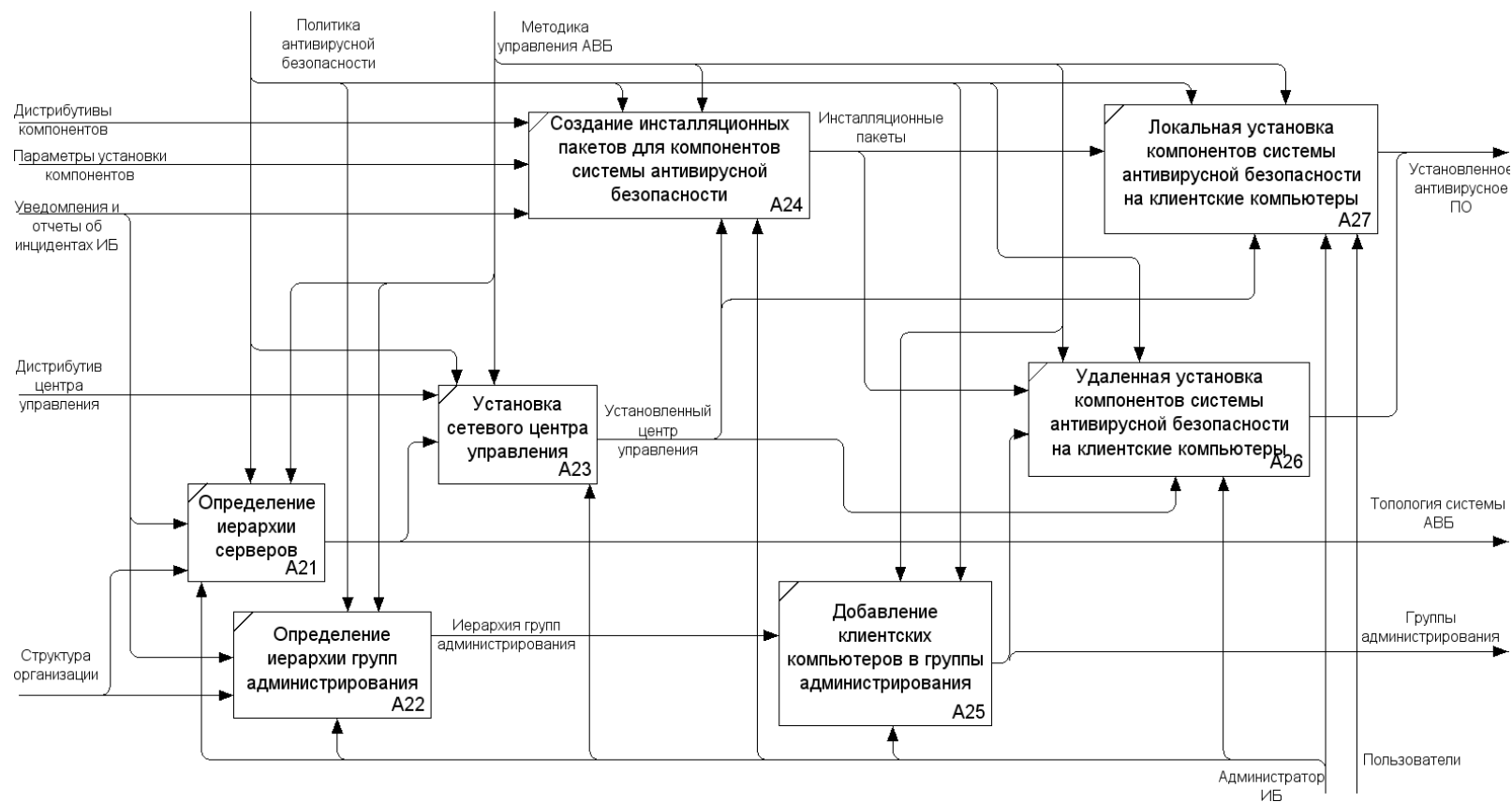


Рисунок А.3 – Декомпозиция процесса развертывания системы антивирусной безопасности в организации

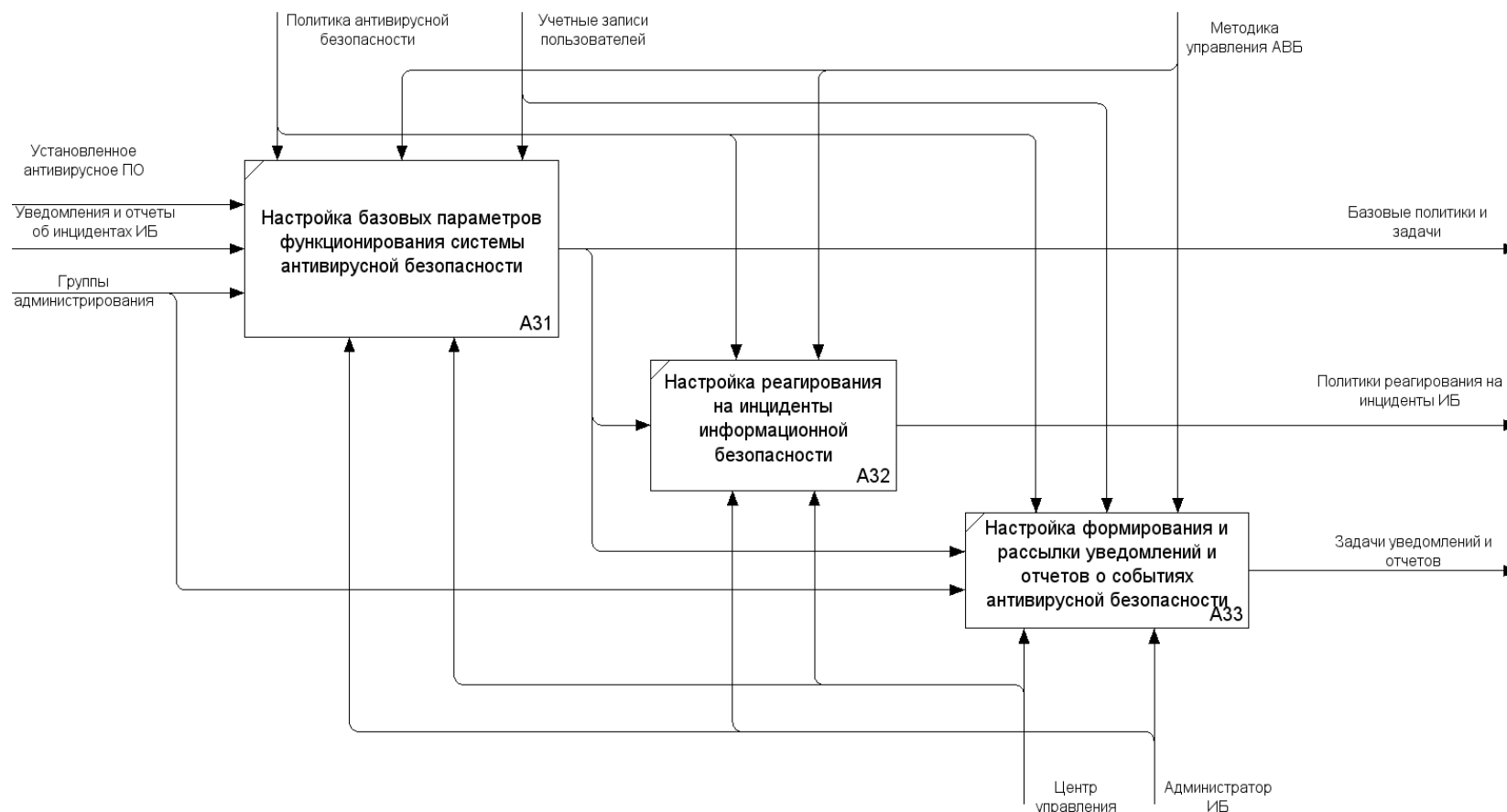


Рисунок А.4 – Декомпозиция процесса настройки системы антивирусной безопасности в организации

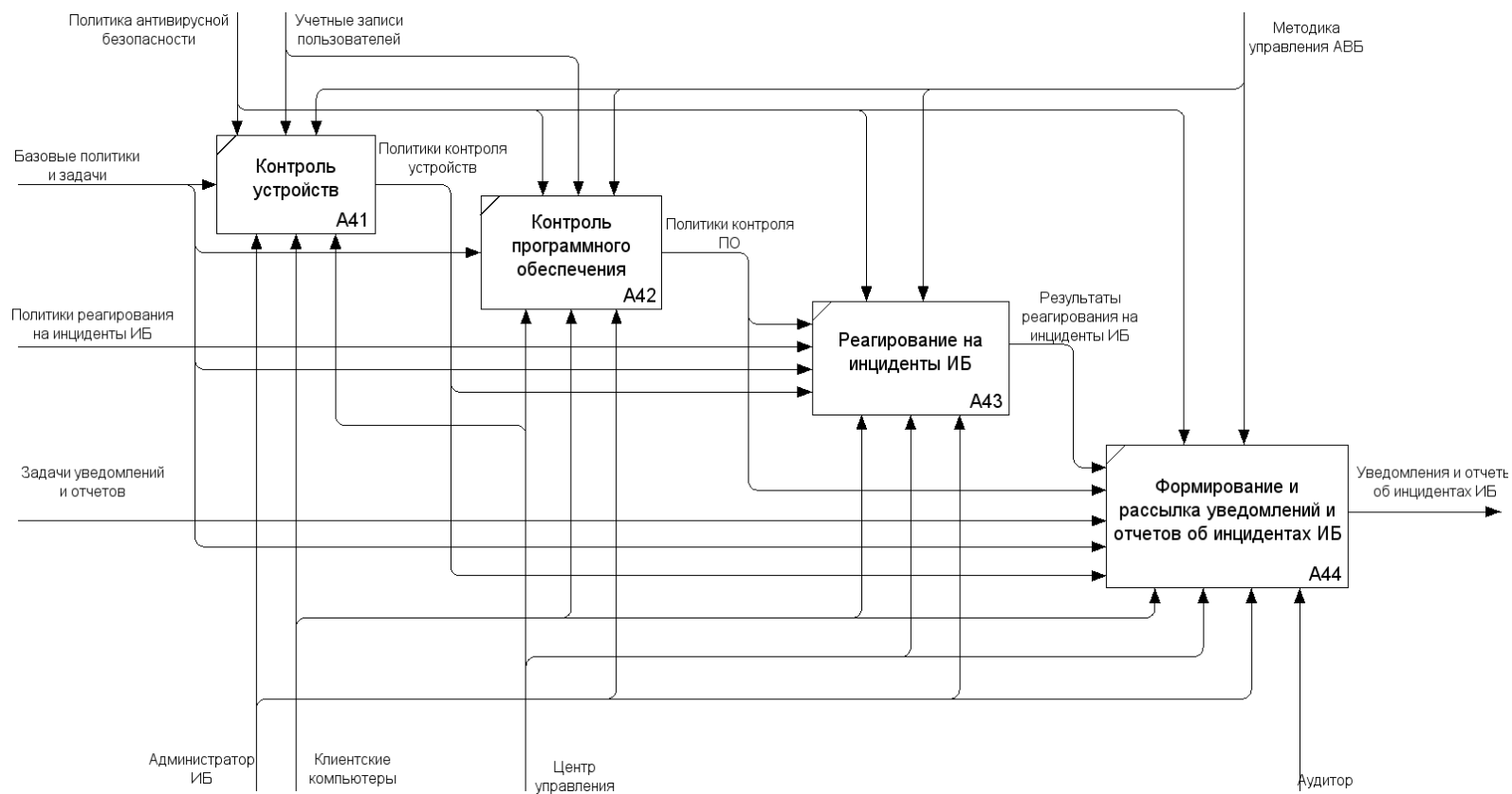


Рисунок А.5 – Декомпозиция процесса контроля функционирования системы антивирусной безопасности в организации

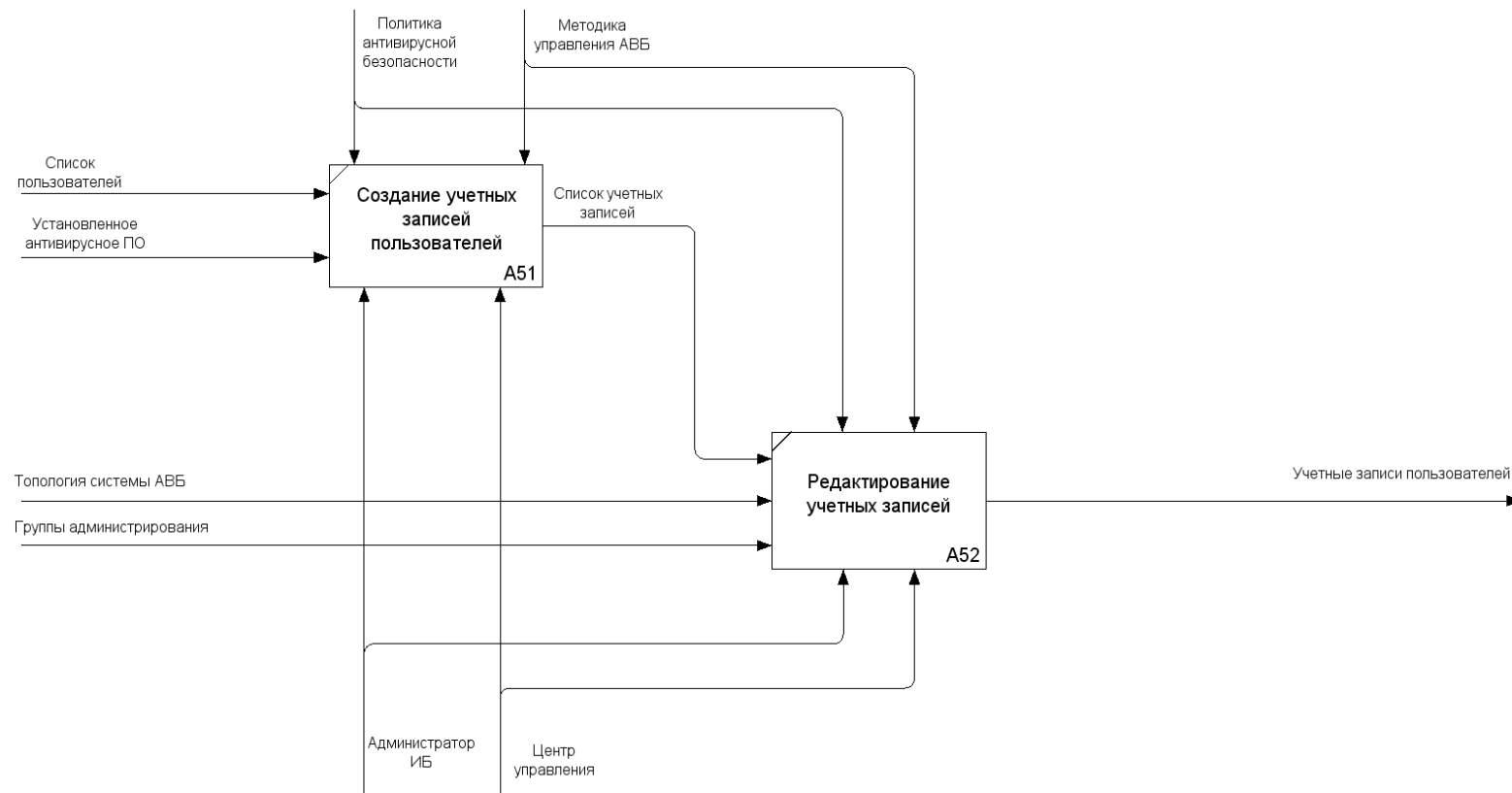


Рисунок А.6 – Декомпозиция процесса управления пользователями системы антивирусной безопасности в организации

ПРИЛОЖЕНИЕ Б

(обязательное)

Типовая политика антивирусной безопасности

Б.1 Общие положения

Настоящая типовая политика (далее – Политика) антивирусной защиты Организации разработана в соответствии с ГОСТ Р ИСО/МЭК 27002-2012, и определяет требования к обеспечению защиты программного обеспечения и информации от вредоносных программ, с целью предотвращения потери (искажения, перехвата) информации, заражения программного обеспечения.

Политика является руководящим документом, единым для всей Организации и обязательным для выполнения всеми работниками Организации

Б.2 Термины и определения

В настоящей Политике используются следующие термины с соответствующими определениями:

– вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы. К вредоносным программам относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в информационно-вычислительной сети;

– событие информационной безопасности – какое-либо событие информационной безопасности, идентифицируемое появлением определенного состояния системы, сервиса или сети, указывающее на возможное нарушение политики информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности;

– инцидент информационной безопасности – какой-либо инцидент информационной безопасности, являющийся следствием одного или нескольких нежелательных или неожиданных событий информационной

безопасности, которые имеют значительную вероятность компрометации операции бизнеса или создания угрозы информационной безопасности;

- администратор информационной безопасности — это субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации;

- пользователи средств антивирусной защиты — все пользователи информационно-вычислительной сети, а также пользователи компьютеров (ноутбуков), не включенных или периодически включаемых в информационно-вычислительной сети Организации, а также отдельных компьютеров (ноутбуков), на которых установлены антивирусные средства защиты.

Б.3 Объекты антивирусной защиты

К объектам антивирусной защиты относятся:

- серверы информационно-вычислительной сети;
- компьютеры (ноутбуки), принадлежащие Организации, подключенные или периодически подключаемые к информационно-вычислительной сети;

- компьютеры (ноутбуки), принадлежащие Организации, не подключенные к информационно-вычислительной сети Организации, но по специфике их использования предполагается копирование (перенос) информации, содержащейся в них, на ресурсы информационно-вычислительной сети или обратно;

- компьютеры (ноутбуки), принадлежащие третьим лицам и подключаемые к информационно-вычислительной сети Организации в рамках заключенных договоров на выполнение работ (оказания услуг);

- шлюз (шлюзы), соединяющий информационно-вычислительные сети Организации с сетью Интернет и другими сетями;

- корпоративная система электронной почты.

Обязательному антивирусному контролю подлежит любая информация, включая:

- исполняемые файлы;
- текстовые файлы любых форматов;
- файлы, поддерживающие макросы;
- веб-вложения (Java, ActiveX и др.);
- почтовые вложения;
- мультимедийные файлы.

Б.4 Средства антивирусной защиты

К средствам антивирусной защиты относятся утилиты, программы и программные комплексы, предназначенные для обнаружения и уничтожения вредоносных программ, а также ликвидации последствий, от их воздействий.

Все средства антивирусной защиты можно условно разделить на основные и вспомогательные.

Для постоянной защиты объектов, приведенных в пункте 3 настоящей Политики должны использоваться программные комплексы в корпоративном исполнении, состоящие из клиентских программ (модулей), устанавливаемых на каждом из объектов защиты, программ (модулей) централизованного администрирования, управления и обновления антивирусных баз и самих программ (модулей).

Основные антивирусные средства должны:

- быть официально приобретены, и использоваться согласно приобретенной лицензии (лицензиям);
- быть однородными по составу, то есть должны быть выпущены одним производителем, допускается использование средств антивирусной защиты других производителей на отдельных объектах защиты, таких, как шлюзы в Интернет (другие сети) и система корпоративной электронной почты;
- обеспечивать возможность управления (администрирования, конфигурирования, удаленной установки, контроля работы, запуска заданий и тому подобное) всеми клиентскими программами с единой консоли (панели) управления администратора;

- обеспечивать загрузку обновлений антивирусных баз и программного обеспечения через Интернет с серверов обновлений производителя и централизованную установку полученных обновлений с сервера информационно-вычислительной сети Организации клиентскими программами, без вмешательства пользователей, с периодичностью не реже одного раза в час;

- обеспечивать проверку в режиме реального времени Интернет-трафика, входящих и исходящих сообщений электронной почты, файлов, к которым обращается пользователь или операционная система;

- обеспечивать недоступность настроек клиентских программ, а также их отключения и деинсталляции для обычных пользователей информационно-вычислительной сети;

- иметь возможность оперативного оповещения пользователей и должностных лиц, отвечающих за антивирусную защиту, обо всех случаях срабатывания антивирусной защиты;

- иметь в составе средство формирования отчетов.

Вспомогательные антивирусные средства не предназначены для постоянной антивирусной защиты объектов, и используются периодически специалистами подразделений антивирусной защиты, как дополнительные инструментальные средства для погашения вирусных эпизодов, ликвидации последствий, профилактики заражений и тому подобного. В качестве вспомогательных средств могут использоваться как платные, так и бесплатные программные антивирусные средства.

Вспомогательные антивирусные средства:

- платные средства должны быть официально приобретены, и использоваться согласно приобретенной лицензии (лицензиям). Бесплатные средства должны использоваться согласно лицензии на их использование;

- должны иметь возможность обновления антивирусных баз и самих программ с серверов производителей перед их использованием;

– должны быть недоступными для обычных пользователей информационно-вычислительной сети.

Б.5 Организационные мероприятия по антивирусной защите

Председатель Правления Организации обеспечивает организацию работ по антивирусной защите.

В Организации планированием и проведением мероприятий по антивирусной защите занимаются выделенные для выполнения таких работ сотрудники Управления информационных технологий.

К использованию в Организации допускаются только лицензионные антивирусные средства, централизованно закупленные Управлением информационных технологий у разработчиков (поставщиков) указанных средств, рекомендованные к применению Отделом информационной безопасности.

В случае необходимости использования антивирусных средств, не вошедших в перечень рекомендованных, их применение необходимо согласовать с Отделом информационной безопасности Организации.

Установка средств антивирусной защиты на компьютерах в Организации осуществляется уполномоченными сотрудниками Управления информационных технологий. Настройка параметров средств антивирусной защиты осуществляется работниками Управления информационных технологий в соответствии руководствами по применению конкретных антивирусных средств.

Обновление антивирусных баз должно производиться не реже одного раза в сутки автоматически, согласно возможностям программного обеспечения. В случае сбоя автоматического обновления обновление баз производится вручную с той же периодичностью.

Мероприятия по антивирусной защите на компьютерах в Организации включают в себя:

- профилактику вирусов;
- анализ ситуаций;

- применение средств антивирусной защиты;
- проведение исследований инцидентов, связанных с вирусами.

Б.6 Профилактика вирусов

Регулярно проводимые профилактические работы по выявлению вирусов могут полностью исключить появление и распространение вирусов в компьютере. К основным профилактическим работам и мероприятиям относятся:

- ежедневная автоматическая проверка наличия вирусов при включении компьютера;
- регулярная (не реже одного раза в квартал) выборочная проверка компьютеров на наличие вирусов, даже при отсутствии внешних проявлений вирусов;
- изучение информации по сообщениям в компьютерных журналах, газетах и Интернете о новых вирусах;
- проверка наличия вирусов на компьютерах, вернувшихся с ремонта (в том числе гарантийного) в сторонних организациях;
- создание резервной копии программного продукта сразу же после приобретения;
- системные дискеты и дискеты с наиболее важными программами защищаются от записи на них информации путем установки переключателя на дискетах в положение только чтения;
- тщательная проверка всех поступающих и купленных программ и баз данных;
- ограничение доступа к компьютеру посторонних лиц.

Регулярную выборочную проверку наличия вирусов выполняет сотрудник Управления информационных технологий.

При обнаружении вирусов на компьютере, работающем в локальной сети, проверке подлежат все компьютеры, включенные в эту сеть и работающие с общими данными и программным обеспечением.

Создание резервной копии программного продукта выполняет сотрудник Управления информационных технологий, ответственный за внедрение этого программного продукта.

Проверку всех поступающих и купленных программ выполняет Управление информационных технологий.

Б.7 Анализ ситуаций

Если антивирусные программы выдают на экран дисплея сообщения о подозрении на наличие вирусов на компьютере, то прежде всего необходимо убедиться в действительном наличии вирусов. Возможны ситуации, при которых эти сообщения являются следствием неисправности компьютера.

При возникновении подобной ситуации необходимо приостановить работу и немедленно известить об этом руководителя подразделения, ответственного за информационную безопасность в подразделении, сотрудников Управления информационных технологий, а также смежные подразделения, использующие эти файлы в работе.

Анализ ситуации наличия вирусов или неисправности какого-либо устройства компьютера выполняет сотрудник Управления информационных технологий совместно с ответственным за информационную безопасность в подразделении. При анализе могут использоваться специальные программы проверки исправности компьютера. В результате анализа делается вывод либо об уничтожении вирусов, либо о необходимости дальнейшего восстановления работоспособности компьютера.

Основными источниками вирусов являются:

- съемный носитель (дискета, флеш-карта, CD-ROM, DVD-ROM, мобильное дисковое устройство) на котором находятся зараженные вирусом файлы;
- компьютерная сеть, в том числе система электронной почты и Интернет;
- жесткий диск, на который попал вирус в результате работы с зараженными программами.

Если вирус проник на компьютер со съемного носителя, то необходимо определить источник и, если источник информации на съемном носителе находится в Организации, то необходимо проверить на наличие вирусов компьютер – источник информации на съемном носителе. Если источник дискеты или съемного носителя – коммерческая или другая организация, то необходимо сообщить в эту организацию о факте выявления вирусов и в дальнейшем обратить особое внимание на носители информации, поступающие из этой организации.

В случае действительного наличия вирусов привлекаются специалисты Управления информационных технологий и Отдела информационной безопасности для проведения служебного расследования.

Б.8 Применение средств антивирусной защиты

Уничтожение вирусов выполняется сотрудником Управления информационных технологий.

Если вирус поразил какие-либо программы, то уничтожение вируса выполняется путем уничтожения программы на диске либо на дискете. После уничтожения зараженной программы необходимо восстановить программу, используя резервную копию программы.

Если вирус поразил файлы, то вирус уничтожается либо путем стирания этих файлов, либо путем использования специальных лечащих программ. Использование лечащих программ не дает полной гарантии восстановления файла. Поэтому после лечения необходима проверка восстановления данного файла. Лечащие программы используются лишь в тех случаях, когда отсутствует резервная копия зараженной программы либо файла с данными, либо восстановление уничтоженного файла с помощью резервной копии очень трудоемко.

В любом случае после уничтожения вирусов и восстановления зараженных программ и файлов с данными необходимо еще раз выполнить проверку наличия вирусов, используя антивирусные программы. Перед повторной проверкой необходимо перезагрузить компьютер через

выключение и последующее включение компьютера. Если повторная проверка не выявила вирусов, то можно быть уверенным в отсутствии вирусов.

Использование специализированного программного обеспечения для восстановления системных областей (FAT, загрузочной записи, и тому подобного) возможно лишь в тех случаях, когда отсутствует резервная копия диска компьютера, либо его восстановление с помощью резервной копии очень трудоемко.

Б.9 Ответственность за создание, использование и распространение вредоносных программ

Ответственность за создание, использование и распространение вредоносных программ согласно статье 273 Уголовного Кодекса Российской Федерации от 13.06.1996 года №63-ФЗ:

- создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев;

- деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы

на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового;

– деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, наказываются лишением свободы на срок до семи лет.

ПРИЛОЖЕНИЕ В

(обязательное)

Методика управления антивирусной безопасностью в организации

В.1 Определение структурной схемы системы антивирусной безопасности

Выбор структуры системы защиты организации определяют следующие факторы:

- топология сети организации;
- организационная структура;
- число работников, отвечающих за защиту сети, и распределение обязанностей между ними;
- аппаратные ресурсы, которые могут быть выделены для установки компонентов управления защитой;
- пропускная способность каналов связи, которые могут быть выделены для работы компонентов защиты в сети организации;
- допустимое время выполнения важных административных операций (например, распространение обновлений антивирусных баз и изменение политик для клиентских компьютеров) в сети организации.

При определении структуры защиты рекомендуется сначала определить имеющиеся сетевые и аппаратные ресурсы, которые могут использоваться для работы централизованной системы защиты.

Для анализа сетевой и аппаратной инфраструктуры рекомендуется следующий порядок действий:

а) определить следующие параметры сети, в которой будет развертываться защита:

- 1) число сегментов сети;
- 2) скорость каналов связи между отдельными сегментами сети;
- 3) число управляемых компьютеров в каждом из сегментов сети;
- 4) пропускную способность каждого канала связи, которая может быть выделена для функционирования защиты;

б) определить допустимое время выполнения ключевых операций администрирования для всех управляемых компьютеров;

в) провести нагрузочное тестирование системы администрирования;

г) проанализировать информацию из предыдущих пунктов. На основании проведенного анализа ответить на следующие вопросы:

1) возможно ли обслуживание всех клиентов одним Сервером администрирования или требуется иерархия Серверов администрирования;

2) какая аппаратная конфигурация Серверов администрирования требуется для обслуживания всех клиентов за время, определенное в пункте б;

3) требуется ли использование агентов обновлений для снижения нагрузки на каналы связи?

После ответа на перечисленные вопросы можно составить набор допустимых структур защиты организации.

В сети организации можно использовать одну из следующих типовых структур защиты:

- один Сервер администрирования. Все клиентские компьютеры подключены к одному Серверу администрирования. Роль агента обновлений выполняет Сервер администрирования;

- один Сервер администрирования с агентами обновлений. Все клиентские компьютеры подключены к одному Серверу администрирования. В сети выделены клиентские компьютеры, выполняющие роль агентов обновлений;

- иерархия Серверов администрирования. Для каждого сегмента сети выделен отдельный Сервер администрирования, включенный в общую иерархию Серверов администрирования. Роль агента обновлений выполняет главный Сервер администрирования;

- иерархия Серверов администрирования с агентами обновлений. Для каждого сегмента сети выделен отдельный Сервер администрирования, включенный в общую иерархию Серверов администрирования. В сети выделены клиентские компьютеры, выполняющие роль агентов обновлений.

В.2 Развертывание системы антивирусной безопасности

В.2.1 Установка сетевого центра управления

В первую очередь должны быть установлены такие компоненты сетевого центра управления, как Сервер администрирования и Консоль администрирования. Для этого нужно выбрать компьютер, на котором будут установлены Сервер и Консоль администрирования. Рекомендуется устанавливать эти компоненты на компьютер, входящий в домен, обладая при этом правами администратора домена. Это позволит предоставить необходимые права учетной записи, под которой будет работать Сервер администрирования.

Запустить исполняемый файл `setup.exe` и следовать указаниям мастера установки. Выбрать стандартный тип установки. Большинство параметров в этом случае задается автоматически. После этого на компьютер будут установлены необходимые для работы программы, если они не были установлены ранее.

На следующем этапе работы мастера начнется копирование файлов установки, и будет создана база данных, в которой Сервер администрирования централизованно хранит информацию об антивирусной защите сети.

По завершении работы мастера установки можно сразу запустить Консоль администрирования и выполнить первоначальную настройку параметров программы с помощью мастера первоначальной настройки.

В.2.2 Создание групп администрирования

Каждая созданная группа, сначала содержит только пустую папку для работы с подчиненными Серверами администрирования этой группы. Информация о политиках, задачах этой группы, а также о входящих в ее состав устройствах отображается на соответствующих закладках в рабочей области этой группы.

Чтобы создать группу администрирования, необходимо выполнить следующие действия:

а) в сетевом центре управления открыть папку Управляемые компьютеры;

б) если нужно создать подгруппу существующей группы администрирования, в папке Управляемые компьютеры выбрать вложенную папку, соответствующую группе, в состав которой должна входить новая группа администрирования. Если создается новая группа администрирования верхнего уровня иерархии, этот шаг можно пропустить;

в) запустить процесс создания группы администрирования одним из следующих способов:

1) с помощью команды контекстного меню Создать – Группу;

2) по ссылке Создать подгруппу, расположенной в рабочей области главного окна программы на закладке Группы;

г) в открывшемся окне Имя группы ввести имя группы и нажать на кнопку ОК.

В результате в дереве консоли появится новая папка группы администрирования с заданным именем.

В.2.3 Перемещение компьютеров в группы администрирования

Если компьютер не подключен к Серверу администрирования, то при обнаружении его в сети он окажется в папке Нераспределенные компьютеры. Чтобы вновь обнаруженные в сети компьютеры автоматически переносились в группы по определенному правилу необходимо выполнить следующие действия:

а) в свойствах папки Нераспределенные компьютеры выбрать пункт Добавить новое правило;

б) ввести имя для нового правила;

в) выбрать группу администрирования, в которую следует перемещать компьютеры;

г) выбрать условие, в соответствии с которым компьютеры будут перемещаться в группу администрирования. Такими условиями могут быть,

например, версия операционной системы, диапазон IP-адресов, наличие Агента администрирования и так далее;

д) включить созданное правило.

В.2.4 Создание инсталляционного пакета компонентов системы антивирусной безопасности

Перед установкой программ на клиентские компьютеры требуется создание инсталляционного пакета, который будет использоваться для удаленной или локальной установки.

Чтобы создать инсталляционный пакет для установки на клиентские компьютеры, необходимо выполнить следующие действия:

а) в дереве консоли выбрать виртуальный Сервер администрирования, под управлением которого находятся клиентские компьютеры;

б) в папке Удаленная установка виртуального Сервера администрирования выбрать вложенную папку Инсталляционные пакеты;

в) в рабочей области выбрать пункт Создать инсталляционный пакет;

г) указать название инсталляционного пакета;

д) выбрать необходимый дистрибутив программы и дождаться окончания распаковки архива. После этого начнется загрузка файлов на Сервер администрирования. По окончании загрузки инсталляционный пакет появится в общем списке пакетов, после чего его можно использовать для удаленной или локальной установки на клиентские компьютеры.

В.2.5 Удаленная установка компонентов системы антивирусной безопасности

Чтобы провести удаленную установку программы на клиентские компьютеры, необходимо выполнить следующие действия:

а) в дереве консоли перейти в узел Сервера администрирования, под управлением которого находятся клиентские устройства;

б) в дереве консоли в папке Удаленная установка запустить мастер удаленной установки;

в) в окне мастера Выбор инсталляционного пакета указать инсталляционный пакет программы, которую требуется установить;

г) следовать указаниям мастера.

В результате работы мастера создается задача удаленной установки программы на клиентских устройствах. Мастер удаленной установки создает и запускает задачу удаленной установки выбранной программы. В зависимости от выбранного набора устройств или группы администрирования созданная задача размещается в папке Задачи для наборов компьютеров или в рабочей области выбранной группы администрирования, на закладке Задачи.

После завершения работы созданной задачи программа будет установлена на выбранные клиентские устройства.

В.2.6 Локальная установка компонентов системы антивирусной безопасности

Некоторые программы, управление которыми доступно через сетевой центр управления, могут быть установлены на клиентские компьютеры только локально.

Чтобы провести локальную установку программы на клиентские компьютеры, необходимо выполнить следующие действия:

а) в сетевом центре управления на основе инсталляционных пакетов создать автономные пакеты установки для выбранных программ;

б) передать на клиентские компьютеры автономные пакеты установки, например, публикуя ссылку на автономные пакеты, через электронную почту или при помощи съемного носителя или другим способом;

в) пользователи клиентских компьютеров запускают установку программ с помощью полученных автономных пакетов установки.

В.3 Настройка базовых параметров функционирования антивирусного средства

В.3.1 Создание политик

Чтобы создать политику необходимо выполнить следующие действия:

а) перейти в группу администрирования, для которой требуется создать политику;

б) в рабочей области выбрать Создать политику, после чего запустится Мастер создания политик. Ввести название новой политики;

в) указать программу для создания групповой политики;

г) параметры политики можно импортировать из уже существующей или настроить при создании политики вручную;

д) активировать созданную политику или определить для нее автоматическую активацию при наступлении определенного события, например, в случае вирусной атаки.

После создания политика будет применена на компьютерах группы администрирования.

В.3.2 Создание задач

Задачи могут быть следующих типов:

– групповые задачи, выполняемые на клиентских компьютерах выбранной группы администрирования;

– задачи Сервера администрирования, выполняемые на Сервере администрирования;

– локальные задачи, выполняемые на конкретном клиентском компьютере.

Базовый набор задач включает:

– задачу поиска вирусов;

– задачу установки обновлений.

Для выполнения требований типовой политики антивирусной безопасности необходимо для данных типов задач необходимо установить ежедневный автоматический запуск по расписанию.

Чтобы создать задачу необходимо выполнить следующие действия:

а) перейти в группу администрирования, для которой требуется создать задачу;

б) в рабочей области выбрать Создать задачу, после чего запустится Мастер создания задач. Далее следовать его указаниям.

В.4 Обеспечение совместимости различных версий антивирусных средств

На клиентских компьютерах в сети могут быть установлены различные версии антивирусных программ. Для их совместимости используется конвертация задач и политик. С помощью сетевого центра управления можно конвертировать задачи и политики предыдущих версий программ с задачи и политики текущих версий программ.

Чтобы конвертировать задачи и политики необходимо выполнить следующие действия:

- а) в сетевом центре управления выбрать Сервер администрирования, для которого требуется выполнить конвертацию;
- б) для выбранного Сервера администрирования запустить мастер конвертации политик и задач. Далее следовать его указаниям.

В результате работы мастера будут сформированы новые задачи и политики, которые используют параметры задач предыдущих версий программ.

В.5 Настройка параметров антивирусных средств для реагирования на инциденты информационной безопасности

На случай возникновения в системе каких-либо инцидентов информационной безопасности необходимо создать политики реагирования на них. Данные политики должны быть неактивными и запускаться только после обнаружения инцидента, например, при вирусной атаке. В настройках данных политик должно быть следующее:

- все компоненты антивирусного средства включены;
- заблокирована возможность менять настройки антивирусного средства пользователями;
- установлен высокий уровень безопасности.

При возникновении инцидента должна быть выполнена проверка компьютера на вирусы. Для этого создать задачу поиска вирусов, которая будет запускаться автоматически в случае возникновения инцидента.

В.6 Настройка уведомлений о событиях антивирусной безопасности

Уведомления администратора о событиях на клиентских компьютерах могут происходить несколькими способами:

- электронная почта;
- NET SEND (служба сообщений);
- SMS;
- исполняемый файл.

Чтобы настроить параметры уведомлений о событиях на клиентских компьютерах необходимо выполнить следующие действия:

а) в сетевой центре управления открыть окно свойств папки Отчеты и уведомления;

б) в разделе Уведомления выбрать подходящий способ уведомления о событиях и настроить параметры уведомления.

В результате настроенные параметры уведомления будут распространяться на все события антивирусной безопасности, происходящих на клиентских компьютерах.

В.7 Формирование и рассылка отчетов о событиях антивирусной безопасности

Отчеты формируются на основе информации, хранящейся на Сервере администрирования и могут быть созданы для следующих объектов:

- для выборки клиентских компьютеров;
- для компьютеров, входящих в определенную группу администрирования;
- для набора клиентских компьютеров из различных групп администрирования;
- для всех компьютеров в сети.

Создание отчетов происходит в соответствии с шаблонами отчетов. Для создания шаблона отчета в сетевом центре управления в рабочей области папки Отчеты и уведомления выбрать Создать шаблон отчета. В результате запустится мастер создания шаблона отчета. Далее следовать его указаниям.

Рассылка отчетов осуществляется с помощью задачи рассылки отчета. Отчеты могут быть отправлены по электронной почте или сохраняться в выбранной папке.

Чтобы создать задачу рассылки одного отчета необходимо выполнить следующие действия:

- а) в сетевом центре управления открыть папку Отчеты и уведомления, где представлен перечень шаблонов отчетов;
- б) выбрать нужный шаблон отчета;
- в) в контекстном меню шаблона или в его свойствах выбрать пункт Рассылка отчетов;
- г) в запущившемся мастере создания задачи рассылки отчета указать способ рассылки, а также другие необходимые параметры.

Чтобы создать задачу рассылки нескольких отчетов необходимо выполнить следующие действия:

- а) в сетевом центре управления выбрать папку Задачи Сервера администрирования;
- б) запустить процесс создания задачи;
- в) в запущившемся мастере создания задачи Сервера администрирования выбрать тип задачи Рассылка отчета.

В.8 Масштабирование системы антивирусной безопасности

В.8.1 Добавление виртуального Сервера администрирования

Чтобы добавить виртуальный Сервер администрирования в состав выбранной группы администрирования необходимо выполнить следующие действия:

- а) в сетевом центре управления в папке группы администрирования выбрать узел Серверы администрирования;

б) запустить процесс создания виртуального сервера администрирования. В результате запустится мастер создания виртуального Сервера администрирования;

в) ввести имя виртуального сервера;

г) выбрать существующую или создать новую учетную запись администратора виртуального Сервера администрирования;

д) выбрать требуемые инсталляционные пакеты.

В.8.2 Добавление компьютера в группу виртуального Сервера администрирования

Перемещать компьютеры в разных группах можно только в пределах одного сервера. Для подчинения компьютера другому серверу необходимо создать задачу переноса. Для переноса компьютера на другой Сервер администрирования необходимо выполнить следующие действия:

а) в сетевом центре управления запустить процесс создания задачи;

б) в качестве типа задачи выбрать Смена Сервера администрирования;

в) указать адрес сервера администрирования;

г) выбрать компьютер для переноса на другой Сервер администрирования;

д) запустить задачу после создания.

В результате выполнения задачи выбранный компьютер будет перенесен на другой Сервер администрирования.

В.9 Управление пользователями системы антивирусной безопасности

В.9.1 Добавление учетной записи пользователя

Чтобы добавить новую учетную запись пользователя необходимо выполнить следующие действия:

а) в сетевом центре управления открыть папку Учетные записи пользователей;

б) в рабочей области выбрать Добавить нового пользователя;

в) указать параметры учетной записи и пароль для подключения к сетевому центру управления.

Учетные записи пользователей должны быть объединены в группы, в зависимости от типовых задач и обязанностей пользователей.

В.9.2 Настройка прав. Роли пользователей

Предоставлять права доступа к функциям программы можно:

- настраивая права каждого пользователя или группы пользователей индивидуально;
- создавая типовые роли пользователей с заранее настроенным набором прав.

Роли можно предоставлять пользователю или группе пользователей. Права доступа в роли должны быть настроены в соответствии с типовыми задачами и служебными обязанностями пользователей.

Должны быть созданы следующие группы пользователей:

- группа администраторов, наделяющая входящих в нее пользователей правами по настройке системы. Добавлять учетные записи пользователей в данную группу должен иметь право только главный администратор системы;
- группа аудиторов, наделяющая входящих в нее пользователей только правами по формированию и просмотру отчетов;
- другие группы, наделяющая входящих в нее пользователей минимально необходимым набором прав в зависимости от их служебных обязанностей. Все остальные действия для данных пользователей должны быть запрещены.

Чтобы добавить роль пользователя необходимо выполнить следующие действия:

- а) в сетевом центре управления выбрать узел с нужным Сервером администрирования;
- б) в свойствах Сервера администрирования в разделе Роли пользователей выбрать пункт Добавить;
- в) указать имя новой роли, настроить набор прав, установив флажки Разрешить и Запретить напротив функций программы.

Чтобы назначить роль пользователю или группе пользователей необходимо выполнить следующие действия:

- а) в сетевом центре управления выбрать нужный Сервер администрирования и открыть окно его свойств;
- б) в окне свойств выбрать раздел Безопасность;
- в) выбрать пользователя или группу пользователей, которой требуется присвоить роль;
- г) в окне Роли пользователя выбрать роль для пользователя или группы пользователей.

В.10 Контроль устройств и программного обеспечения на автоматизированных рабочих местах организации

В.10.1 Контроль устройств

Контроль устройств позволяет обеспечить безопасность конфиденциальной информации путем ограничения доступа пользователей к устройствам, установленным или подключенным к компьютеру. Такими устройствами могут быть:

- устройства памяти (жесткие диски, съемные носители информации, CD/DVD-приводы);
- инструменты передачи информации (внешние сетевые карты, модемы);
- шины подключения (USB, FireWire).

Ограничение доступа пользователей к устройствам обеспечивается с помощью политик. Чтобы создать политику контроля устройств необходимо выполнить следующие действия:

- а) в сетевом центре управления выбрать группу администрирования, для которой требуется создать политику;
- б) для выбранной группы администрирования запустить мастер создания политики;
- в) при настройке политики в качестве параметра контроля указать Контроль устройств;

г) указать учетные записи пользователей, входящие в выбранную группу администрирования, для которых требуется настроить контроль устройств;

д) разрешить или запретить доступ, в зависимости от типа устройства и прав, которые необходимы для выбранных учетных записей пользователей;

е) при необходимости установить расписание доступа к устройствам.

В.10.2 Контроль запуска программ

Контроль запуска программ позволяет установить ограничения на запуск программ на клиентских компьютерах. При запуске программ проверяются такие условия, как:

- категория программы (браузер, мессенджер и так далее);
- учетная запись пользователя, от имени которой выполняется запуск программы;
- политики, регулирующие запуск программ данной категории для данной учетной записи.

Чтобы создать политику контроля запуска программ необходимо выполнить следующие действия:

а) в сетевом центре управления выбрать группу администрирования, для которой требуется создать политику;

б) для выбранной группы администрирования запустить мастер создания политики;

в) при настройке политики в качестве параметра контроля указать Контроль запуска программ;

г) указать учетные записи пользователей, входящие в выбранную группу администрирования, для которых требуется настроить контроль запуска программ;

д) добавить правило, которое будет запрещать или разрешать запуск программ, в зависимости от категории программ или других условий. В случае, если правило разрешает запуск программ по выбранным условиям, то запуск всех остальных программ, которые не удовлетворяют этим условиям, будет запрещен.

В.10.3 Контроль активности программ

Контроль активности программ предназначен для регулирования действий уже запущенных программ, таких как доступ к файловой системе, системному реестру и взаимодействие с другими программами. Ограничения для программ задаются с помощью политик.

Чтобы создать политику контроля активности программ необходимо выполнить следующие действия:

а) в сетевом центре управления выбрать группу администрирования, для которой требуется создать политику;

б) для выбранной группы администрирования запустить мастер создания политики;

в) при настройке политики в качестве параметра контроля указать Контроль активности программ;

г) указать учетные записи пользователей, входящие в выбранную группу администрирования, для которых требуется настроить контроль активности программ;

д) задать для требуемых программ защищаемые ресурсы и права доступа к этим ресурсам для четырех типов операций:

- 1) чтение;
- 2) запись;
- 3) удаление;
- 4) создание.

ПРИЛОЖЕНИЕ Г

(обязательное)

Диаграмма компонентов лабораторного стенда

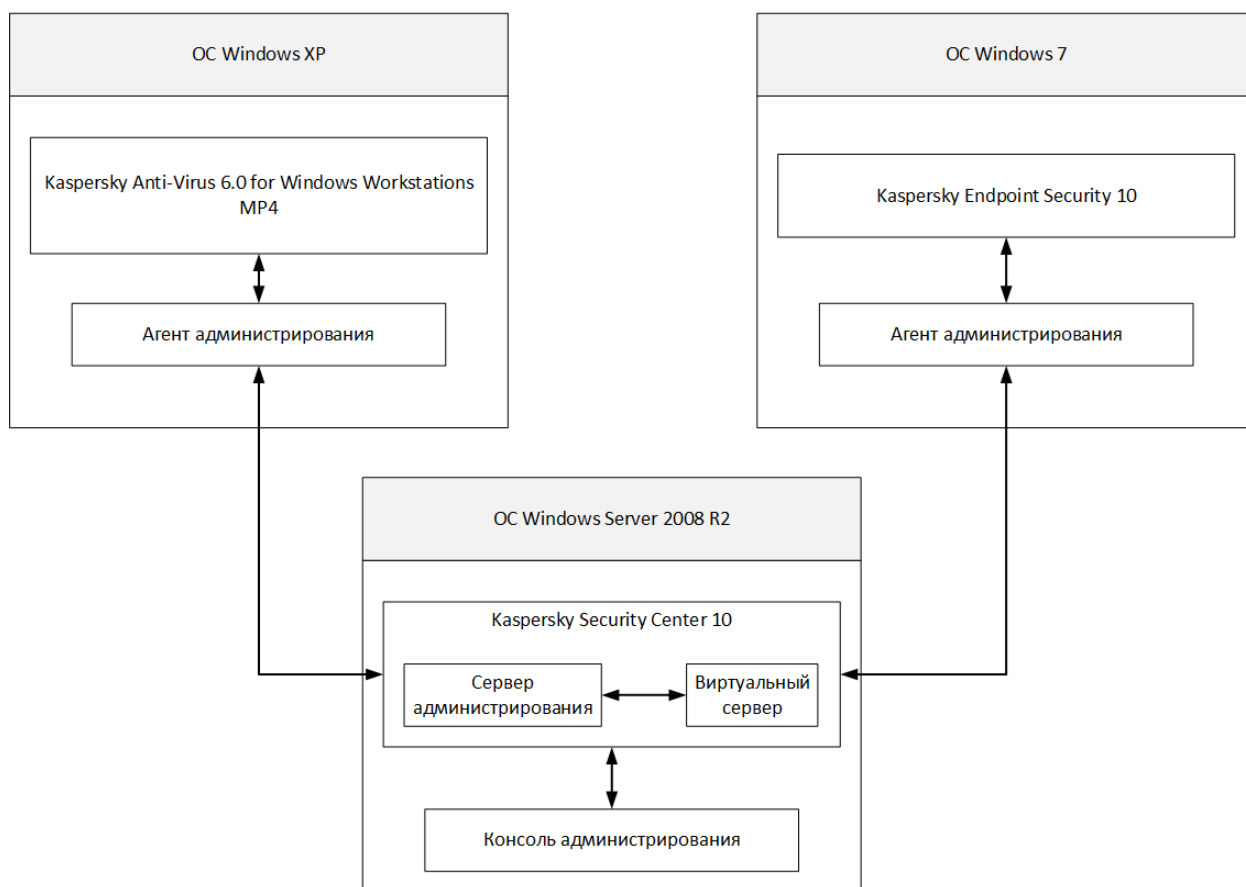


Рисунок Г.1

ПРИЛОЖЕНИЕ Д

(обязательное)

Проверка методики управления антивирусной безопасностью в организации

Д.1 Развертывание системы

Д.1.1 Установка сетевого центра управления

На виртуальной машине с операционной системой Windows Server 2008 R2 был установлен Kaspersky Security Center 10, содержащий в себе Консоль администрирования и Сервер администрирования. Для этого был запущен исполняемый файл setup.exe. В запустившемся окне можно выбрать установку как отдельных компонентов, так и всех сразу. Был выбран пункт «Установить Kaspersky Security Center 10». Тип установки выбран «Стандартный». Размер сети выбран «Менее 100 компьютеров в сети». Выбрана учетная запись администратор для запуска службы Сервера администрирования. Тип сервера базы данных выбран «Microsoft SQL Server (SQL Express)». В настройках параметров подключения к Microsoft SQL Server выбрано «Установить Microsoft SQL Server R2 Express SP2». Режим аутентификации выбран «Режим аутентификации Microsoft Windows». Создана папка общего доступа. Все остальные параметры оставлены без изменений. В результате был установлен Kaspersky Security Center 10.

При первом запуске Kaspersky Security Center 10 запустился мастер первоначальной настройки. На странице мастера «Выбор способа добавления ключа» было выбрано «Указать файл ключа». В открывшейся странице нажата кнопка «Выбрать» и указан путь к файлу ключа. Все остальные настройки оставлены без изменения.

Д.1.2 Создание групп администрирования

Компьютеры будут разделяться по группам администрирования по версиям установленного на них антивирусного средства. Структура групп была создана на основе содержимого текстового файла. Для этого на рабочем столе был создан текстовый файл и в него записаны названия создаваемых групп. Имя каждой группы начинается с новой строки, разделительный символ – перевод строки, пустые строки игнорируются. Содержимое текстового файла выглядит, как показано на рисунке Д.1.

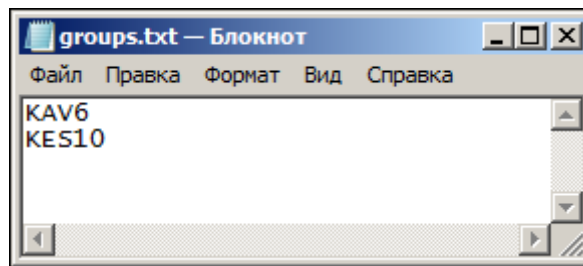


Рисунок Д.1 – Текстовый файл с названиями групп

Чтобы запустить автоматическое создание структуры групп администрирования, были выполнены следующие действия:

- в дереве консоли выбрана папка «Управляемые компьютеры»;
- в контекстном меню папки «Управляемые компьютеры» выбран пункт «Все задачи» – «Создать структуру групп», как показано на рисунке Д.2.

В результате запустился мастер создания структуры групп администрирования.

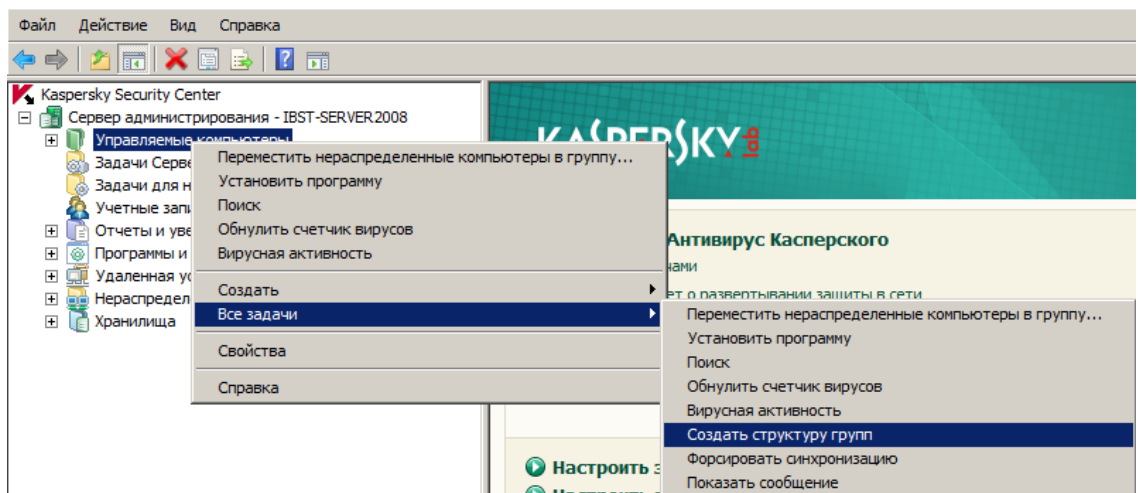


Рисунок Д.2 – Создание структуры групп

В поле «Создать структуру групп на основе» выбран пункт «Содержимого текстового файла». В качестве группы назначения выбрана «Управляемые компьютеры», и указан созданный текстовый файл с названиями групп, как показано на рисунке Д.3.

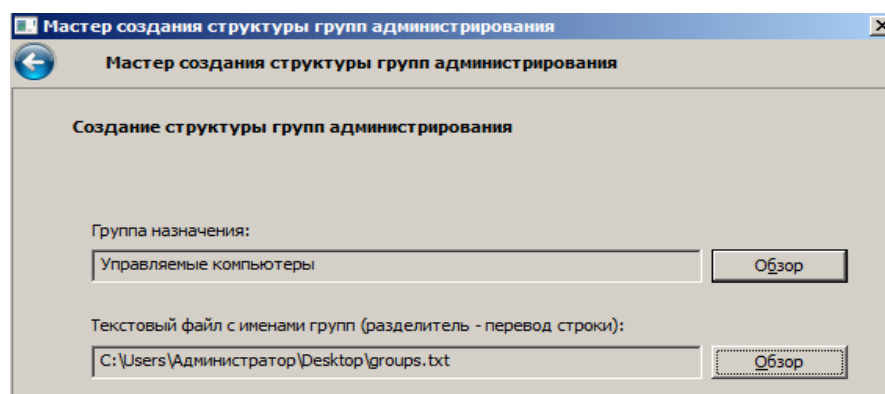


Рисунок Д.3 – Мастер создания структуры групп

В результате работы мастера в группе «Управляемые компьютеры» была создана структура групп, показанная на рисунке Д.4.

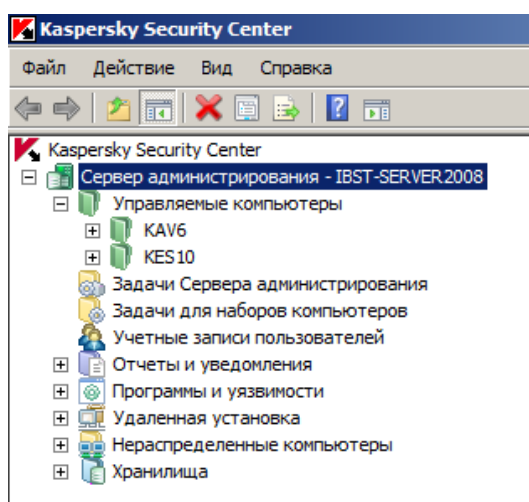


Рисунок Д.4 – Дерево консоли с созданной структурой групп

Д.1.3 Создание инсталляционного пакета

Скопирован дистрибутив программы «Антивирус Касперского 6.0 для Windows Workstations MP4» на рабочий стол виртуальной машины Сервера администрирования. Для этого было выполнено «Пуск» – «Компьютер», в адресной строке введено «\\VBOXSRV\share» и скопирован файл «kav6.0.4.1611_winwksru».

В дереве консоли администрирования выбран узел «Удаленная установка» – «Инсталляционные пакеты». В рабочей области нажато «Создать инсталляционный пакет».

Запустился мастер создания инсталляционного пакета. Выбрано «Создать инсталляционный пакет для программы «Лаборатории Касперского». На следующей вкладке указать название создаваемого пакета

KAV6. На вкладке выбора дистрибутива программы нажата кнопка «Выбрать». В открывшемся окне указан тип файлов «Самораспаковывающиеся архивы», выбран «kav6.0.4.1611_winwksru».

После распаковки снят флажок «Скопировать обновления из хранилища в инсталляционный пакет». Это позволяет ускорить процесс установки и уменьшить размер инсталляционного пакета.

После нажатия «Далее» начинается загрузка файлов на Сервер администрирования. После окончания загрузки нажата кнопка «Готово». Созданный инсталляционный пакет появился в общем списке пакетов, что показано на рисунке Д.5.

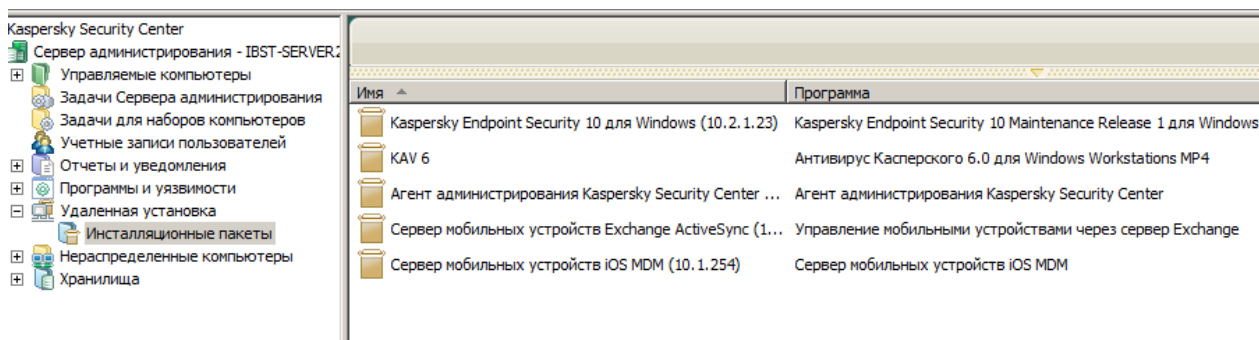


Рисунок Д.5 – Список инсталляционных пакетов

Д.1.4 Перемещение компьютеров в группы администрирования

Д.1.4.1 Настройка правил переноса вновь обнаруженных компьютеров в группу

Не подключенные к серверу администрирования компьютеры при обнаружении их в сети оказываются в папке «Нераспределенные компьютеры», откуда их можно вручную переместить в нужную группу. Однако в Kaspersky Security Center 10 существует возможность автоматического переноса вновь обнаруженных в сети компьютеров по определенному правилу.

Было создано правило перемещения обнаруженных компьютеров в группу KAV6 в том случае, если на них установлена операционная система Windows XP. Ниже описан порядок создания такого правила.

В дереве консоли выбран пункт «Нераспределенные компьютеры». В рабочей области в поле «Действия» выбрано «Настроить правила перемещения компьютеров в группы администрирования».

В открывшемся окне свойств папки «Нераспределенные компьютеры» нажата кнопка «Добавить». Появилось окно «Новое правило». В разделе «Общие» введено название нового правила «Перемещение XP», в поле «Группа, в которую следует перемещать» выбрана группа «KAV6». В поле «Выполнение правила» установлен переключатель «Правило работает постоянно» и установлен переключатель «Включить правило», как показано на рисунке Д.6.

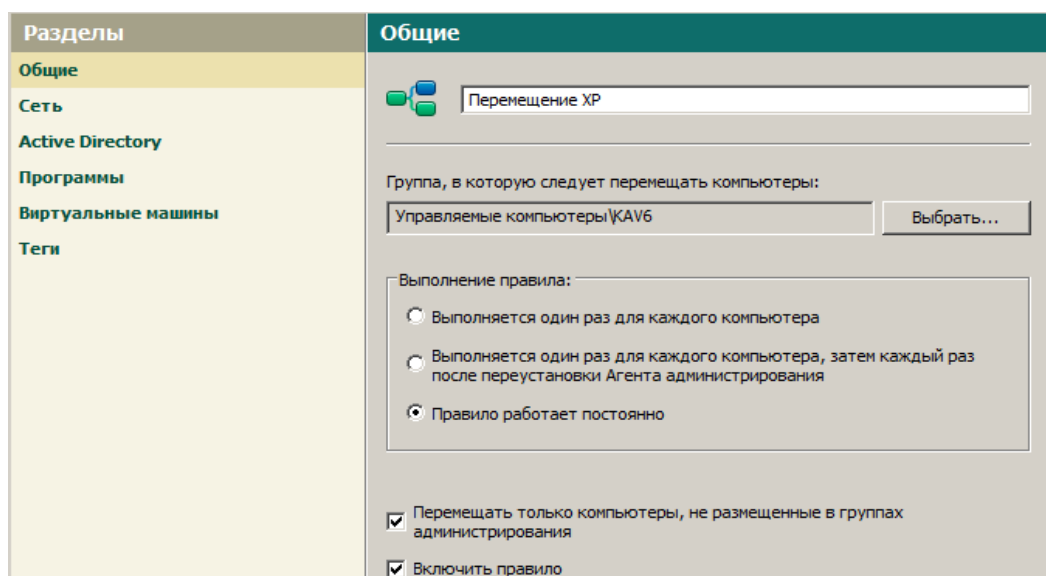


Рисунок Д.6 – Правило перемещения компьютеров

Затем в раздел «Программы», установлен флажок «Версия операционной системы» и выбрано «Microsoft Windows XP», как показано на рисунке Д.7.

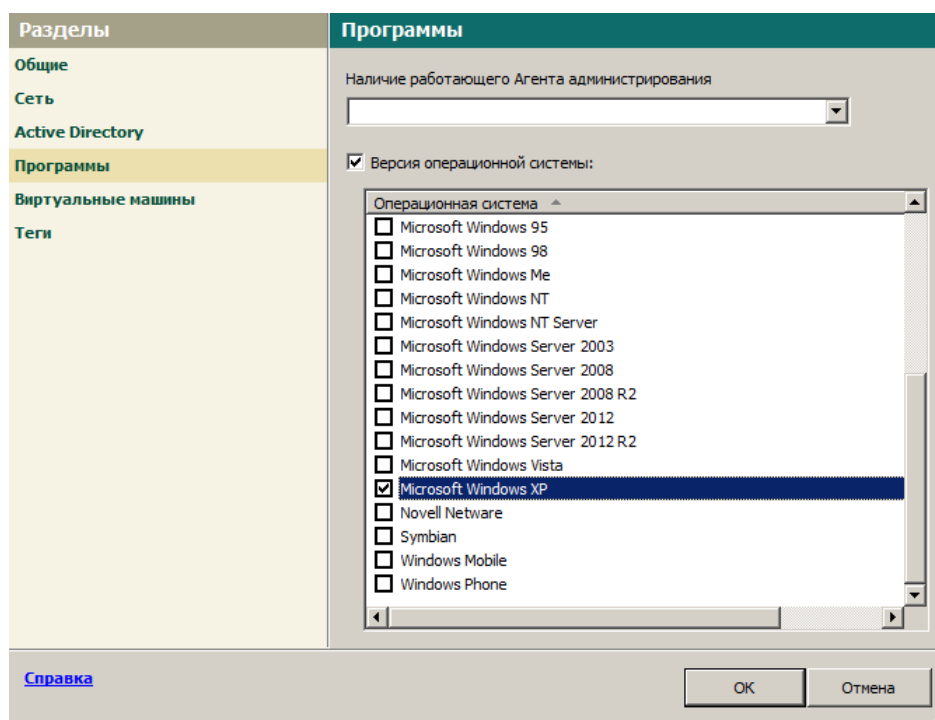


Рисунок Д.7 – Выбор версии операционной системы

В списке правил перемещения добавилось новое правило, которое сработает при обнаружении в сети сервером администрирования компьютера с ОС Microsoft Windows XP, как показано на рисунке Д.8.

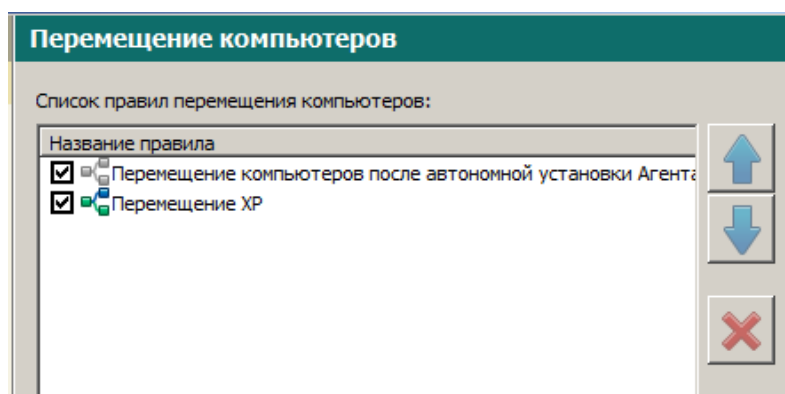


Рисунок Д.8 – Список правил перемещения компьютеров

В результате работы правила компьютер не виртуальной машине с операционной системой Windows XP был перемещен в группу KAV6.

Д.1.4.2 Поиск компьютеров в сети и перемещение их в группы вручную

Если компьютер не определяется автоматически, то можно выполнить его поиск. Для этого в дереве консоли вызвано контекстное меню пункта «Нераспределенные компьютеры», в нем выбрано «Поиск». Открылось окно поиска.

Виртуальные машины лабораторного стенда имеют следующие IP-адреса:

- виртуальная машина с Windows XP – 10.0.2.4;
- виртуальная машина с Windows 7 – 10.0.2.5.

Поэтому в окне поиска поставлен флажок на «IP-интервал», указан интервал IP-адресов от 10.0.2.2 до 10.0.2.7 и нажата кнопка «Найти».

В списке найденных компьютеров был выбран компьютер с операционной системой Windows 7 и его контекстном меню выбрано «Все задачи» – «Переместить в группу». В открывшемся окне, показанном на рисунке Д.9 выбрана группа KES10.

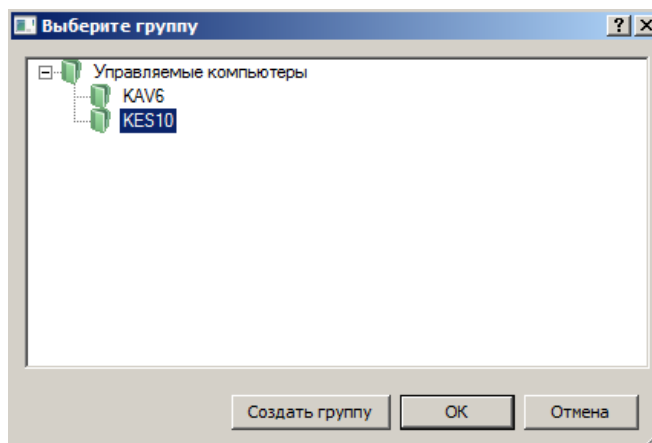


Рисунок Д.9 – Выбор группы

После нажатия кнопки «ОК» выбранный компьютер появился в группе «KES10».

Д.1.5 Установка компонентов системы антивирусной безопасности

Д.1.5.1 Подготовка компьютера к удаленной установке

Если на компьютере не установлен Агент администрирования, при удаленной установке программы могут возникнуть следующие проблемы:

- на клиентском компьютере включен параметр «Простой общий доступ к файлам»;
- не работает служба Server;
- закрыты необходимые порты;
- у учетной записи, под которой выполняется задача, недостаточно прав.

Для решения этих проблем есть утилита `iprerp.exe` для подготовки компьютера к удаленной установке.

В окне виртуальной машины с операционной системой Windows XP (далее – WinXP) на рабочем столе запущена утилита `iprerp.exe`. Установлены флажки, как показано на рисунке Д.10. Нажата кнопка «Запустить». После окончания работы утилиты закрыто окно утилиты. На компьютере отключен Брандмауэр Windows.

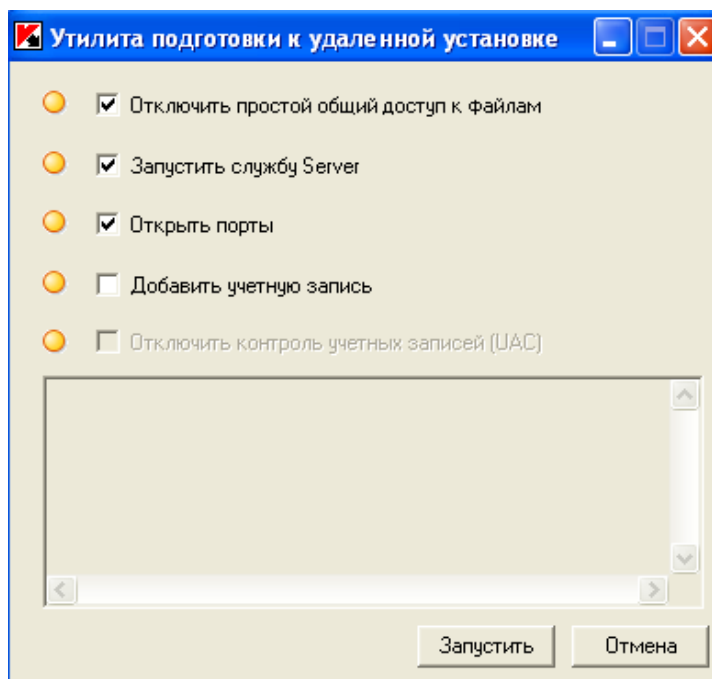


Рисунок Д.10 – Утилита `iprerp`

Д.1.5.2 Удаленная установка инсталляционного пакета

В окне виртуальной машины Сервера администрирования в дереве консоли администрирования выбран узел «Удаленная установка». В рабочей области узла выбрано «Запустить мастер удаленной установки». Указан созданный ранее инсталляционный пакет KAV6 для установки.

На следующей вкладке выбрано «Установить на группу управляемых компьютеров». Далее нажато «Обзор» и выбрана группа «KAV6».

Значения на вкладке «Определение параметров задачи удаленной установки» оставлено без изменения. На вкладке «Выбор ключа» выбран ключ, у которого не истек срок действия. На следующей вкладке указан «Перезагрузить компьютер». На вкладке «Выбор учетных записей для

доступа к компьютерам» нажата кнопка «Добавить» и введено имя учетной записи «Администратор», пароль «xp1-admin» (учетная запись локального администратора компьютера с операционной системой Windows XP). Нажато «Далее» и запущена установка.

После запуска в Консоли администрирования отобразилась вкладка «Задачи» группы «KAV6». Процесс выполнения задачи можно контролировать в блоке работы с задачей. После завершения задачи осуществлен переход к окну виртуальной машины WinXP. На экран выведено информационное сообщение, показанное на рисунке Д.11.

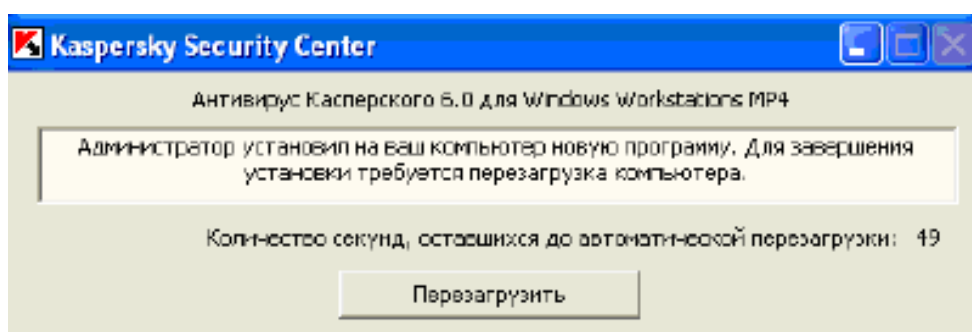


Рисунок Д.11 – Информационное сообщение

Д.1.5.3 Локальная установка компонентов системы антивирусной безопасности

Была выполнена локальная установка Kaspersky Endpoint Security 10 на виртуальную машину с операционной системой Windows 7 (далее – Win7). Для этого в дереве консоли администрирования выбран узел «Удаленная установка». В рабочей области узла выбрано «Запустить мастер удаленной установки» и в списке инсталляционных пакетов для «Kaspersky Endpoint Security 10 для Windows» в контекстном меню выбран пункт «Создать автономный пакет установки». В запущившемся мастере создания автономного пакета установки все параметры оставлены без изменений. После окончания работы мастера созданный автономный пакет был размещен в папке общего доступа, откуда была выполнена ручная установка с виртуальной машины Win7.

Д.2 Настройка базовых параметров функционирования антивирусного средства

Д.2.1 Создание политик

Перейдя в группу KAV6 на вкладку «Политики» в рабочей области выбрано «Создать политику». Запустился мастер создания политик.

Введено название новой политики. На следующей вкладке указана программа для создания групповой политики – «Антивирус Касперского 6.0 для Windows Workstations MP4». На вкладке «Импорт параметров» нажато «Далее», ничего не изменяя. На вкладке «Защита» отключен компонент «Анти-Хакер», сняв флажок, как показано на рисунке Д.12.

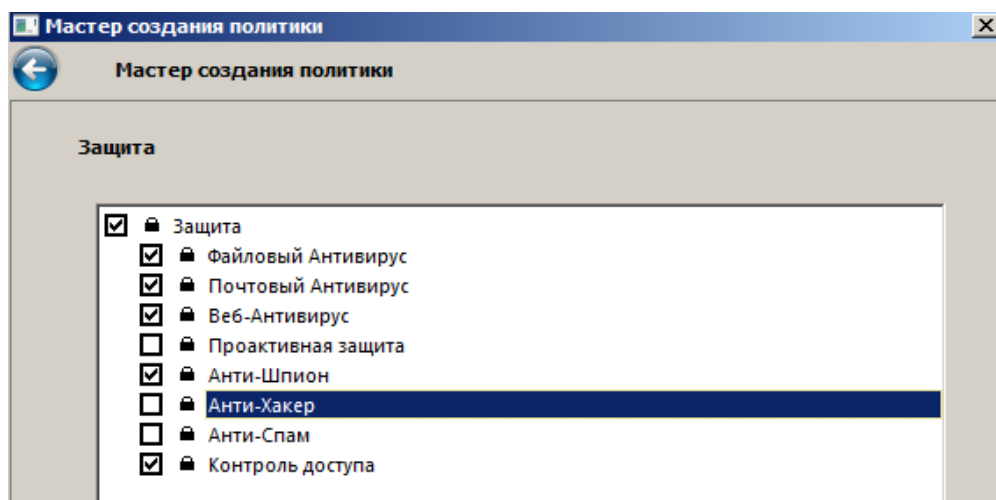


Рисунок Д.12 – Выбор компонентов

Остальные параметры оставлены по умолчанию. Созданная политика отобразилась в списке политик. Выделив ее в списке, справа отобразится ее состояние – «Применена на 1 компьютерах». Нажав «Подробнее», можно посмотреть на каком компьютере применена политика.

Д.2.2 Создание задачи

В группе KAV6 осуществлен переход на вкладку «Задачи». Установлен флажок отображения унаследованных задач. В списке задач отображаются 3 унаследованные задачи:

- поиск вирусов;
- поиск уязвимостей и обновлений программ;
- установка обновлений.

В списке задач выбрана задача «Поиск вирусов». Для запуска этой задачи в контекстном меню задачи можно выбрать пункт «Запустить», либо нажать соответствующую кнопку в блоке работы с выбранной задачей. Цвет статуса задачи после ее запуска с серого изменился на бежевый, справа от индикатора появится надпись: «Распространяется на 1 компьютеров», как показано на рисунке Д.13.

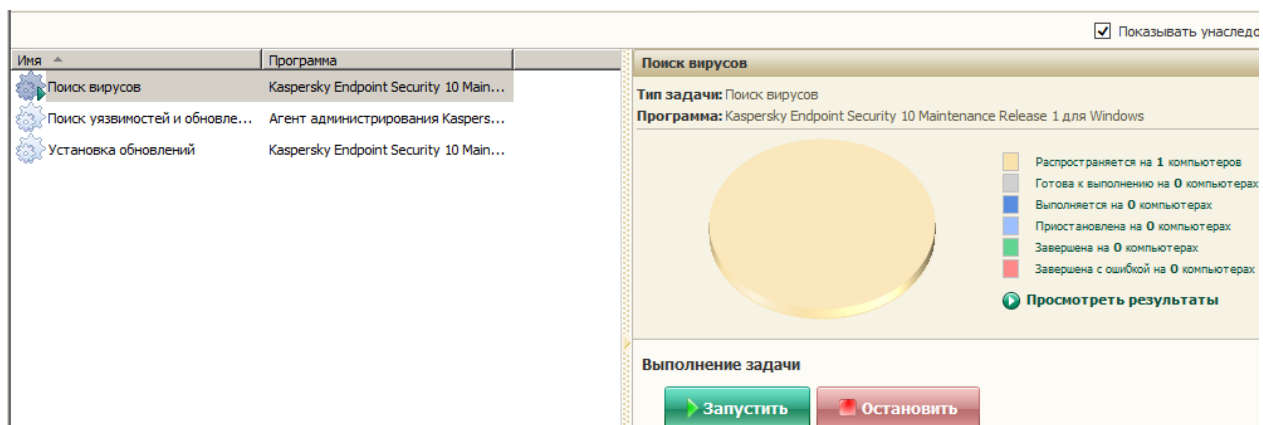


Рисунок Д.13 – Статус задачи

Нажав на кнопку «Просмотреть результаты» можно увидеть на какой компьютер какой группы распространяется эта задача.

Закрывается окно результатов и останавливается выполнение задачи.

Осуществлен переход в группу «Управляемые компьютеры» на вкладку «Задачи» и выбрана задача «Поиск вирусов». В контекстном меню задачи выбран пункт «Свойства». В открывшемся окне выбран раздел «Исключения из области действия задачи», нажата кнопка «Добавить» и выбрана группа KAV6. Аналогичные действия выполнены для задачи «Установка обновлений».

Осуществлен переход в группу KAV6. На вкладке «Задачи» нажата кнопка «Создать задачу». Открылось окно мастера создания задачи. Введено название задачи «Поиск вирусов KAV6». В окне «Выбор типа задачи» выбрано «Поиск вирусов» для «Антивирус Касперского 6.0 для Windows Workstation MP4», как показано на рисунке Д.14.

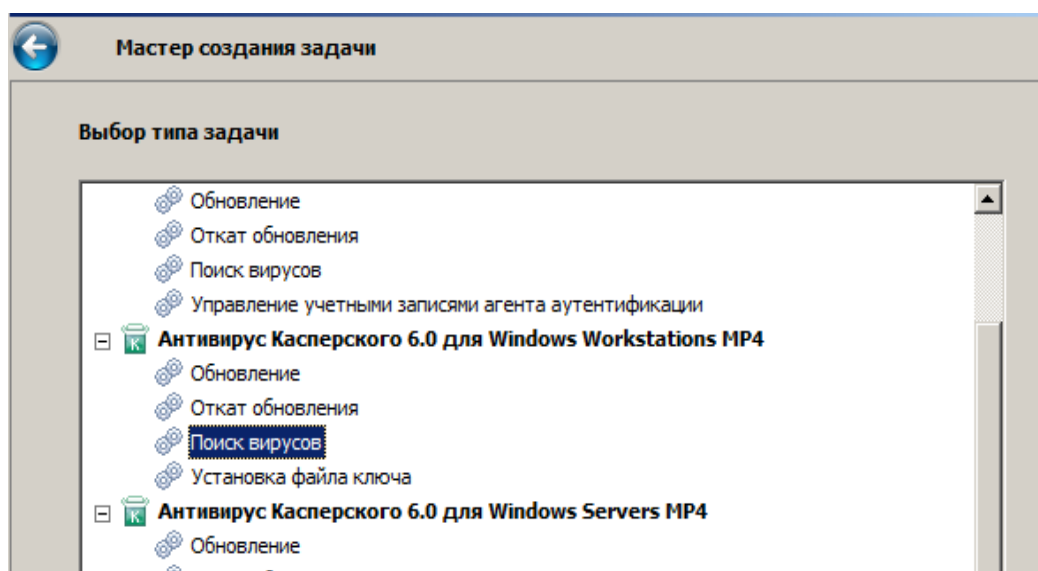


Рисунок Д.14 – Мастер создания задачи

Остальные параметры оставлены без изменений. Созданная задача появилась в списке задач. После запуска данная задача выполняется на одном компьютере.

Перейдя к окну виртуальной машины WinXP, открыто контекстное меню антивируса на панели задач. В контекстном меню указано выполнение задачи, как показано на рисунке Д.15.

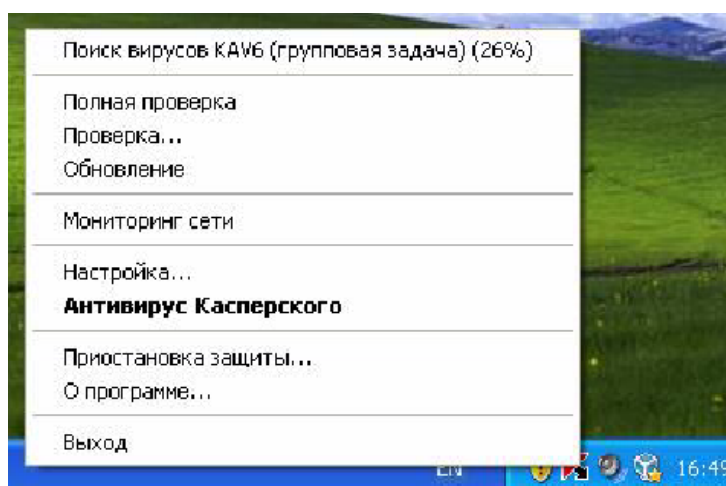


Рисунок Д.15 – Выполнение задачи

Д.3 Обеспечение совместимости различных версий антивирусных средств

Д.3.1 Экспорт и импорт политики

Осуществлен переход на вкладку «Политики» группы «KAV6». В списке политик выделена ранее созданная политика. В контекстном меню

политики выбран пункт «Экспортировать». Введено имя файла экспортированной политики и нажата кнопка «Сохранить».

Осуществлен переход в группу KES10 на вкладку «Политики». Выбрано в рабочей области «Импортировать политику из файла». Выбрана ранее экспортированная политика (файл с расширением klp). В списке политик появилась импортированная политика. Выбран в контекстном меню этой политики пункт «Активная политика». В статусе политики в блоке работы с выбранной политикой указано, что политика не применяется.

Д.3.2 Экспорт и импорт задач

Осуществлен переход на вкладку «Задачи» группы «KAV6». В списке задач выбрана задача «Поиск вирусов KAV6». В контекстном меню задачи выбран пункт «Все задачи» – «Экспортировать». Введено имя файла экспортируемой политики и нажато «Сохранить».

Осуществлен переход в группу «KES10» на вкладку «Задачи». В рабочей области выбран пункт «Импортировать задачу из файла». Выбрана ранее экспортированная задача. Осуществлен запуск задачи.

Д.3.3 Конвертация политик и задач

В дереве консоли выбран «Сервер администрирования», далее в контекстном меню Сервера администрирования выбран пункт «Все задачи» – «Мастер конвертации политик и задач».

В окне выбора программы указано «Kaspersky Endpoint Security 10», в окне выбора политик и задач сняты флажки у политик и задач, находящихся в группе KAV6. Остальные параметры оставлены без изменений.

В списке политик группы «KES10» появилась конвертированная импортированная политика.

Конвертированная политика сделана активной. Открыто окно свойств конвертированной политики. В разделе «Антивирусная защита» некоторые компоненты KES10 отключены в конвертированной политике, поскольку при создании политики для Антивируса Касперского 6.0 был отключен компонент Анти-Хакер.

Удалена импортированная политика для KAV6 из списка политик группы KES10.

На вкладке «Задачи» группы KES10 запущена конвертированная задача.

Удалена импортированная задача из списка задач группы KES10.

Д.4 Настройка параметров антивирусных средств для реагирования на инциденты информационной безопасности

Были настроены политики и задачи для случая вирусной атаки.

Для имитации инцидента используется тестовый файл eicar.com, который не является вирусом, но на него реагируют антивирусы.

Осуществлен переход на вкладку «Политики» группы «KAV6». В списке политик выбрана ранее созданная политика. В контекстном меню политики выбран пункт «Копировать». Затем «Вставить». В списке политик появилась неактивная копия политики. Открыто окно свойств политики.

В разделе «Общие» введено название «Новая политика KAV6 вирусная атака».

Осуществлен переход в раздел «Защита» и в выпадающем списке выбран «Файловый антивирус». В поле «Уровень безопасности» установлен уровень в положение «Высокий».

Включено выключенные компоненты антивирусного средства и заблокирована возможность менять настройки антивирусного средства пользователям.

На вкладке «Задачи» группы KAV6 скопирована задача «Поиск вирусов KAV6» и открыто окно свойств скопированной задачи.

В разделе «Общие» изменено название задачи, дописав «...вирусная атака».

В разделе «Расписание» в выпадающем списке «Запуск по расписанию» выбрано «При обнаружении вирусной атаки».

В разделе «Объекты» выбрано «Компьютер», «Системная память» и «Объекты автозапуска».

В разделе «Параметры» установлен высокий уровень безопасности.

В дереве консоли выбран в контекстном меню Сервера администрирования пункт «Свойства». Затем выбран раздел «Вирусная атака». Указатель установлен в поле «Антивирусы для рабочих станций и файловых серверов» и поставлено значение 1 вирус. Затем нажата ссылка «Настроить активацию политик по событию «Вирусная атака» в правом нижнем углу окна.

В окне «Активация политик» нажата кнопка «Добавить». Выбрана политика «Новая политика KAV6 вирусная атака».

В окне виртуальной машины WinXP на рабочем столе распакован архив eiscar.zip. Открыта папка с распакованным файлом и вирус был обнаружен.

Осуществлен переход к окну виртуальной машины сервера администрирования. Определено, что активной в текущий момент является созданная политика. На вкладке «Задачи» группы «KAV6» определено, что выполняется созданная задача поиска вирусов.

Д.5 Настройка уведомлений о событиях антивирусной безопасности

В рабочей области папки «Отчеты и уведомления» на вкладке «Уведомления» открыто окно по ссылке «Изменить параметры доставки уведомлений». В разделе «Уведомление» выбрано «Электронная почта». Указан произвольный адрес электронной почты и адрес SMTP-сервера 10.0.2.4.

На вкладке «Задачи» группы «KAV6» выбрана задача поиска вирусов и открыты ее свойства. В свойствах задачи в разделе «Уведомление» в поле «Уведомлять о результатах» установлен указатель «Уведомлением по электронной почте», снят указатель «Уведомлять только об ошибках» и нажата ссылка «Параметры». По умолчанию настройки уведомлений заблокированы, однако можно изменить их для каждой задачи снятием указателя «Использовать параметры Сервера администрирования».

На сервере запущен диспетчер служб IIS6.0 «Пуск» – «Администрирование» – «Диспетчер служб IIS6.0». В окне диспетчера

раскрыт узел «IBST-SERVER2008». В контекстном меню узла «SMTP Virtual Server #1» выбран пункт «Запустить».

В окне виртуальной машины WinXP на рабочем столе распакован архив «eicar.zip» в папку «Мои рисунки».

В окне виртуальной машины сервера и запущена задача поиска вирусов. После окончания выполнения задачи просмотрено отправленное уведомление в папке C:\inetpub\mailroot\Queue.

Д.6 Формирование и рассылка отчетов о событиях антивирусной безопасности

В дереве консоли открыта папка «Отчеты и уведомления», в которой представлен перечень шаблонов отчетов. В контекстном меню шаблона отчета «Отчет о вирусах» выбран пункт «Рассылка отчетов». В результате запустился мастер создания задачи рассылки выбранного отчета. В окне «Параметры» отмечены отчеты, которые необходимо рассылать, установлены указатели «Посылать отчет по электронной почте» и «Сохранять отчет в папке», как показано на рисунке Д.16. Остальные параметры оставьте без изменений.

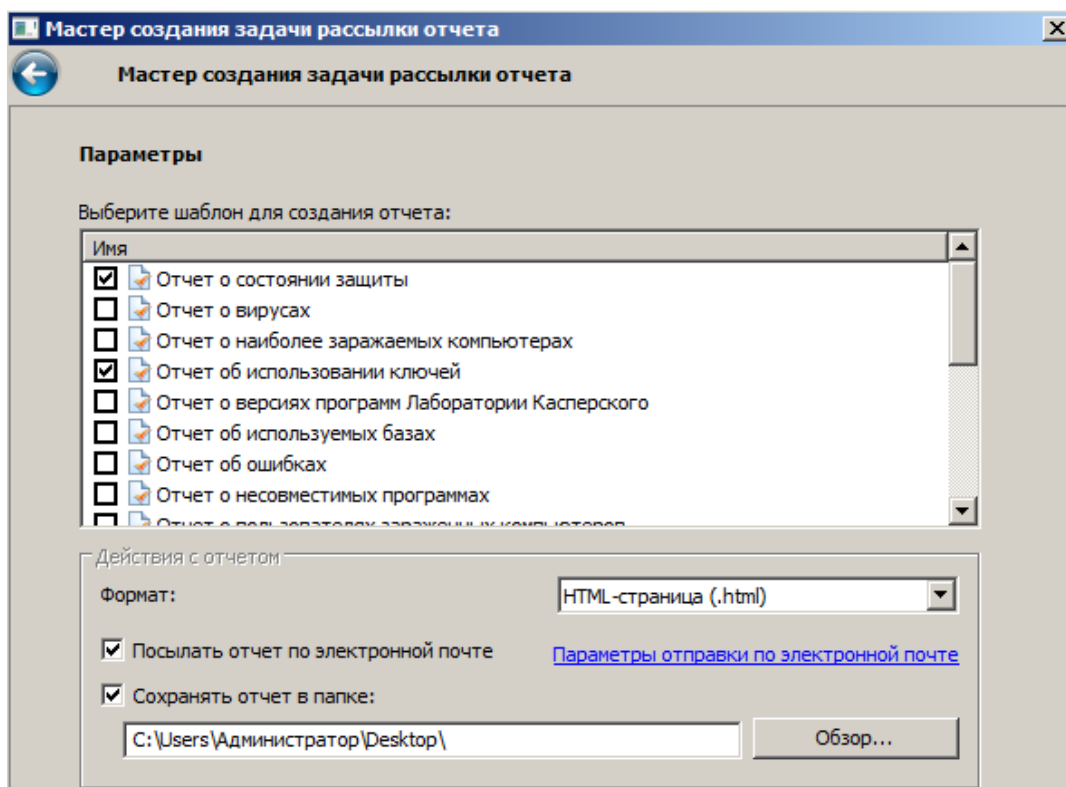


Рисунок Д.16 – Мастер создания задачи рассылки отчета

Созданная задача рассылки отчета отобразилась в папке дерева консоли «Задачи Сервера администрирования».

Запущена задача, в результате чего были сформирован отчет не рабочем столе.

Д.7 Масштабирование системы антивирусной безопасности

Д.7.1 Создание виртуального Сервера администрирования

В дереве консоли был выбран узел «Сервер администрирования». В меню консоли администрирования выбрано «Вид» – «Настройка интерфейса» и установлен флажок «Отображать подчиненные Серверы администрирования», как показано на рисунке Д.17. После этого перезапущена Консоль администрирования.

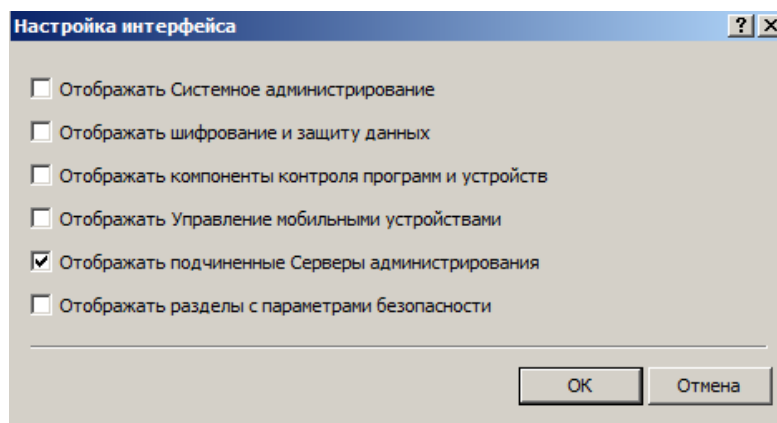


Рисунок Д.17 – Настройка интерфейса

В дереве консоли выбрано «Управляемые компьютеры» – «Серверы администрирования» и в рабочей области выбрано «Добавить виртуальный Сервер администрирования».

В открывшемся окне введено имя виртуального сервера «V_Server».

На вкладке «Создание учетной записи администратора виртуального Сервера» нажата кнопка «Создать» и в открывшемся окне введено имя новой учетной записи «V_admin» и пароль. В результате была создана новая учетная запись внутреннего пользователя Kaspersky Security Center.

После нажатия «Далее» запустился мастер добавления нового виртуального Сервера администрирования. На странице выбора способа добавления ключа выбран пункт «Добавить ключ позже». В окне выбора

инсталляционных пакетов сняты указатели со всех пакетов, начинающихся с «Сервер мобильных устройств...», как показано на рисунке Д.18.

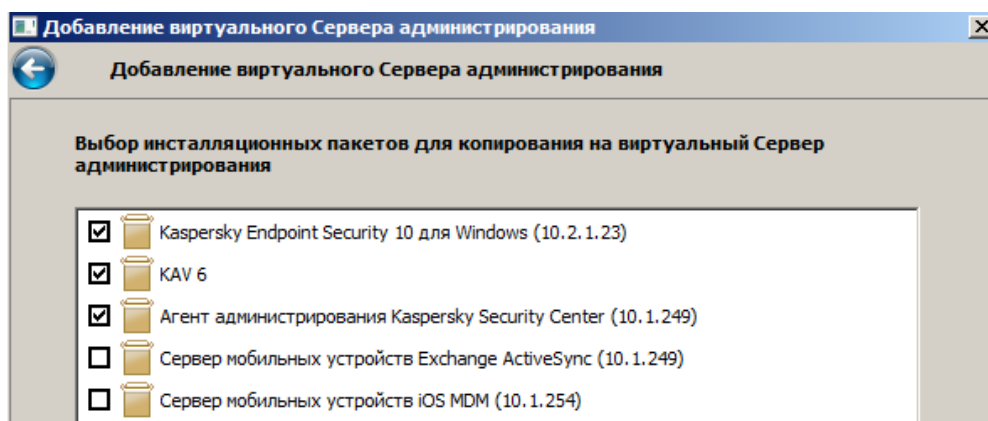


Рисунок Д.18 – Выбор инсталляционных пакетов

После завершения работы мастера в дереве консоли открыт узел «Сервер администрирования» – «V_Server». Структура дерева виртуального сервера показана на рисунке Д.19.

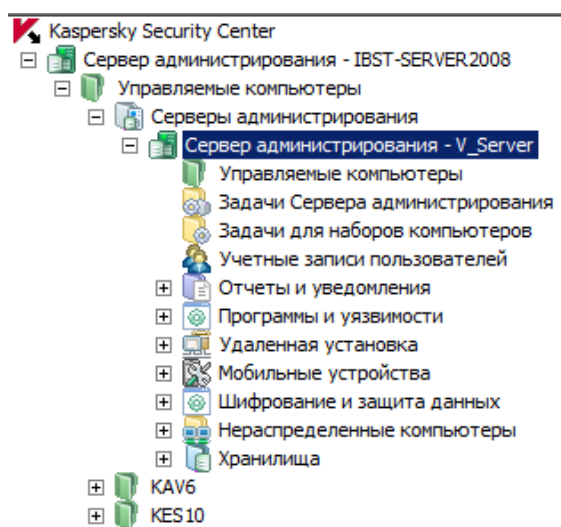


Рисунок Д.19 – Структура дерева виртуального сервера

Д.7.2 Добавление компьютеров в группу виртуального сервера

Перемещать компьютеры в разных группах можно только в пределах одного сервера. Для подчинения компьютера другому серверу необходимо либо создать задачу переноса, либо перенести компьютер вручную с помощью утилиты klmover.exe.

В окне виртуальной машины WinXP запущена командная строка. Запущена утилиту, с помощью набора в командной строке: C:\Program Files\Kaspersky Lab\NetworkAgent>klmover.exe – address 10.0.2.4/V_Server, где

10.0.2.4 – IP-адрес основного сервера администрирования, V_Server – имя виртуального сервера.

В окне Сервера администрирования проверен результат переноса компьютера.

На виртуальном сервере в узел «Задачи для наборов компьютеров» нажато «Создать задачу». Введено название задачи, а на следующей вкладке «Тип задачи» выбрана в папке «Дополнительно» задача «Смена Сервера администрирования», как показано на рисунке Д.20.

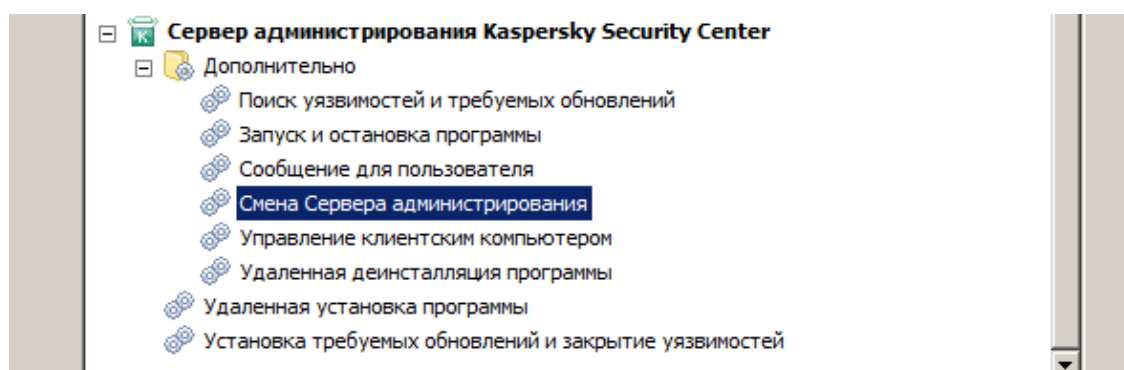


Рисунок Д.20 – Выбор типа задачи

На следующей вкладке указан адрес сервера: «IBST-SERVER2008», как показано на рисунке Д.21.

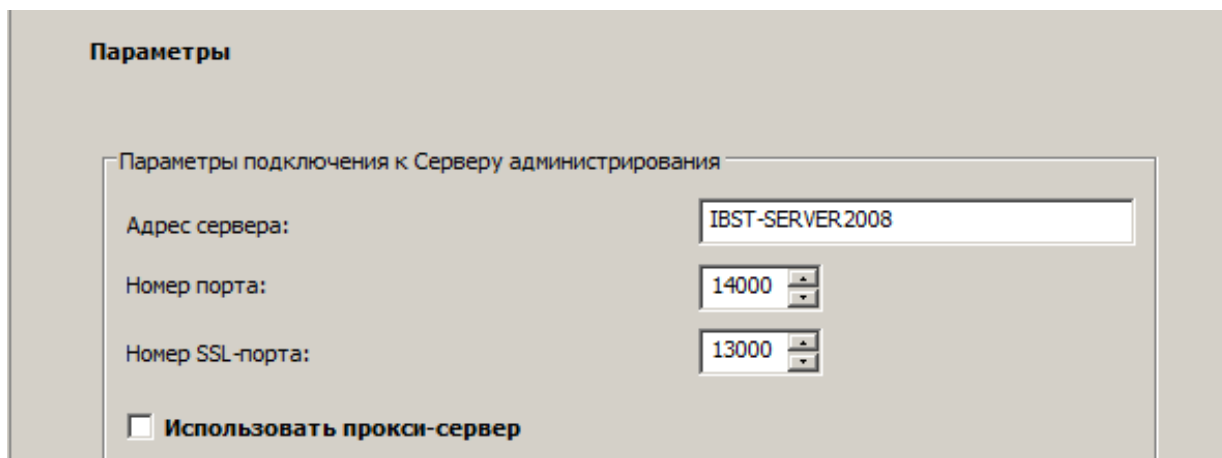


Рисунок Д.21 – Параметры подключения

Нажато «Выбрать компьютеры, обнаруженные в сети Сервера администрирования» и выбран компьютер ХР-1 для переноса на другой Сервер администрирования. Запущена задача после создания. В результате применения задачи компьютер ХР-1 перемещен в группу виртуального сервера.

Д.8 Управление пользователями системы антивирусной безопасности
Компьютер ХР-1 перемещен на виртуальный сервер администрирования.

На вкладке «Учетные записи пользователей» виртуального сервера в рабочей области выбрано «Добавить нового пользователя». Открылось окно свойств пользователя. Введено имя пользователя и задан для него пароль.

Осуществлен переход в дереве консоли главного сервера к узлу «Учетные записи пользователей», как показано на рисунке Д.22.

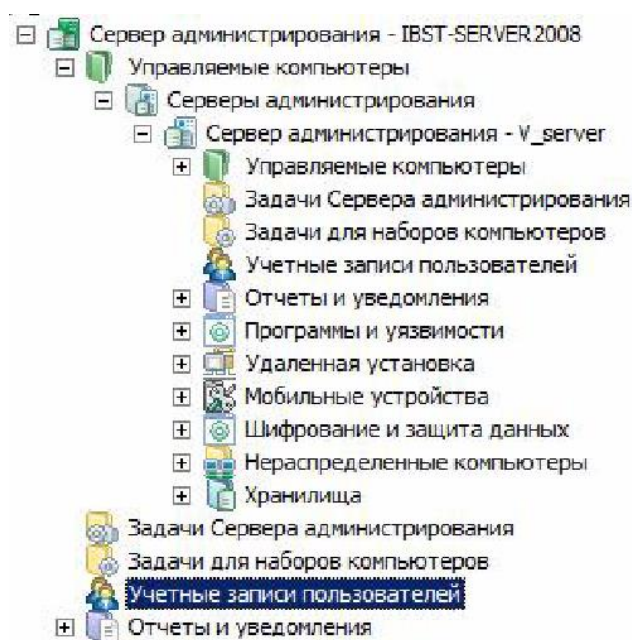


Рисунок Д.22 – Учетные записи пользователей

Создан пользователя, по аналогии с предыдущими действиями. Добавленная учетная запись появилась в списке пользователей.

Осуществлен переход к виртуальному серверу. Открыто контекстное меню виртуального сервера и выбран пункт «Свойства». В окне свойств выбран раздел «Безопасность».

Раскрыт выпадающий список у кнопки «Добавить» и выбрана строка «Аутентификация Kaspersky Security Center ...», как показано на рисунке Д.23.

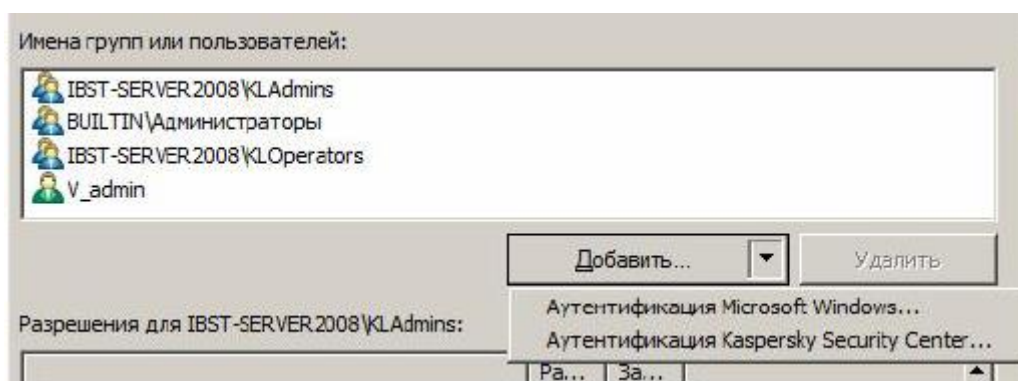


Рисунок Д.23 – Добавление учетных записей

В открывшемся окне для выбора доступны только учетные записи, созданные Kaspersky Security Center:

- учетная запись администратора виртуального сервера, добавленная при создании сервера;
- учетная запись пользователя, добавленная ранее.

В текущем окне также можно создать новую учетную запись или удалить ранее созданную. Выбрана учетную запись ранее созданного пользователя и нажато «ОК». По умолчанию ему разрешены все права на действия с сервером.

Убрано право на чтение у добавленного пользователя.

В дереве консоли вызвано контекстное меню виртуального сервера. Выбран пункт «Отключиться от Сервера администрирования».

Затем в контекстном меню выбран пункт «Подключиться к Серверу администрирования». Если выбрать кнопку «Подключиться к Серверу администрирования» в рабочей области Консоли администрирования, то подключение будет осуществляться с параметрами предыдущей сессии, то есть с параметрами администратора виртуального сервера. В появившемся окне введены параметры учетной записи пользователя, как показано на рисунке Д.24.

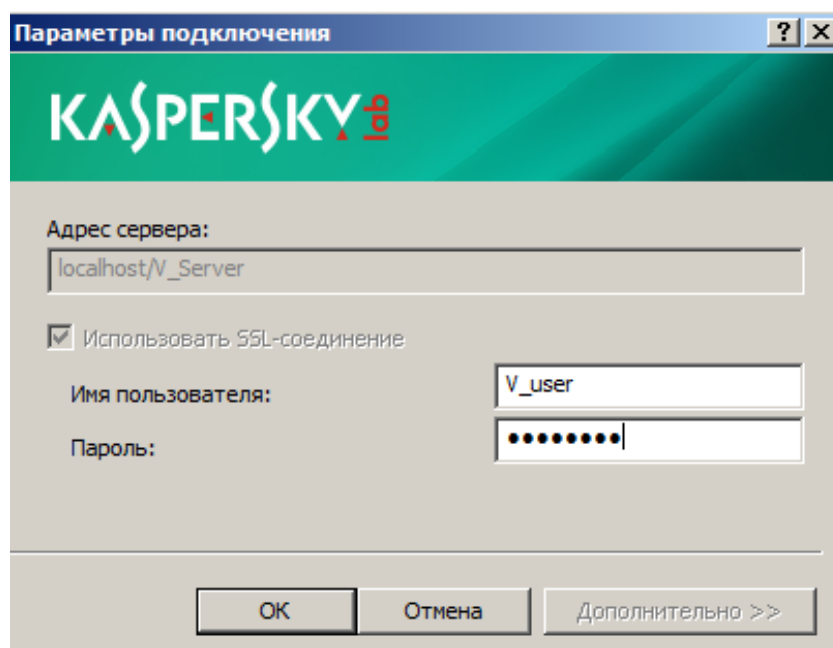


Рисунок Д.24 – Параметры подключения

При подключении к Серверу администрирования пользователя, у которого отсутствуют права на чтение, было выдано сообщение об ошибке, как показано на рисунке Д.25.

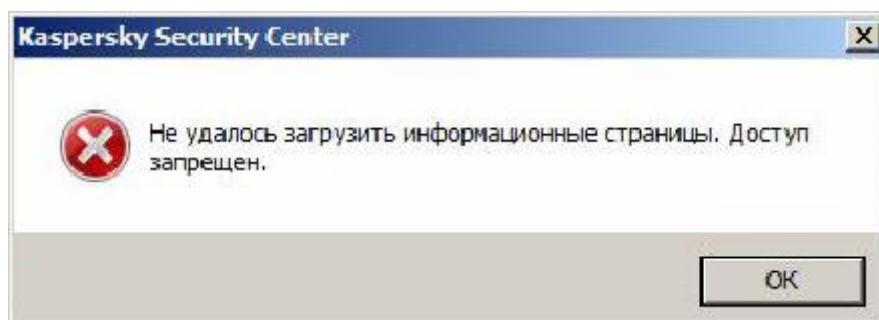


Рисунок Д.25 – Сообщение об ошибке

Аналогичные сообщения будут выдаваться при попытке обращения к любому узлу в дереве консоли виртуального сервера. Подобных ошибок не будет, если обращаться к узлам дерева консоли основного сервера, поскольку для него текущей является сессия администратора.

Д.9 Контроль устройств и программного обеспечения

Д.9.1 Контроль устройств

Для контроля устройств на виртуальной машине Win7 была создана политика контроля устройств, запрещающая использовать съемные носители информации.

Выбрана группа KES10 и на вкладке «Политики» выбрано «Создать политику». Запустился мастер создания политики. Имя политики введено «Контроль устройств».

На странице выбора программы для создания групповой политики выбрано «Kaspersky Endpoint Security 10 Maintenance Release 1 для Windows». На странице настройки параметров контроля выбрано «Контроль устройств», как показано на рисунке Д.26.

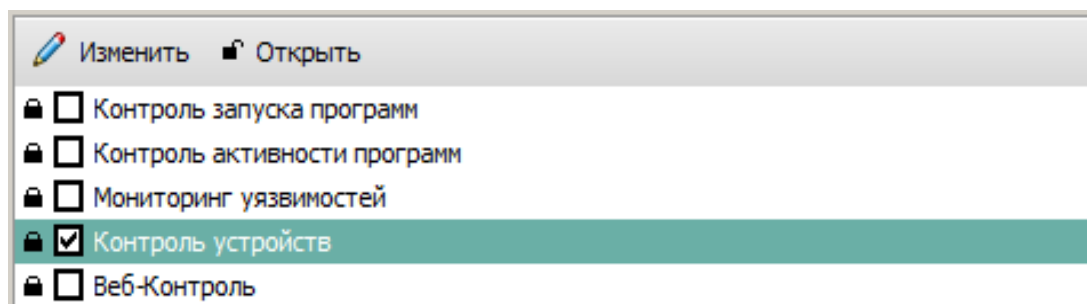


Рисунок Д.26 – Настройка параметров контроля

Выделив «Контроль устройств» нажато «Изменить». В открывшемся окне для устройства «Съемные диски» установлен доступ «Запретить», как показано на рисунке Д.27.

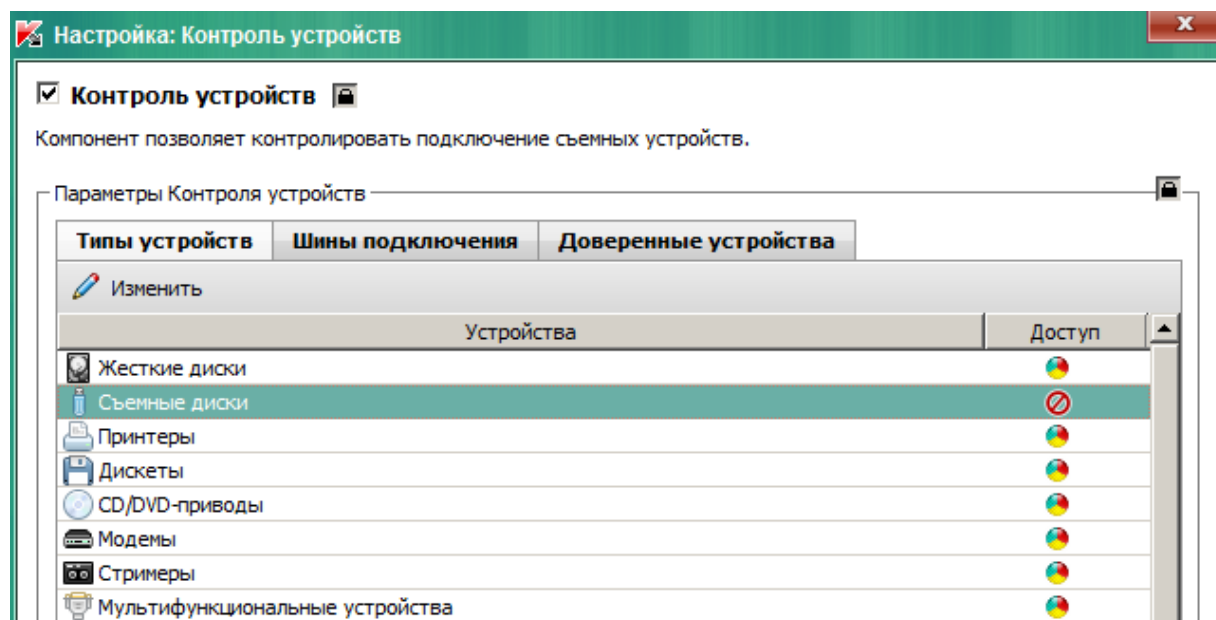


Рисунок Д.27 – Выбор прав доступа для устройств

Все остальные параметры создаваемой политики оставлены по умолчанию.

При попытке открыть съемный носитель появились сообщения, показанные на рисунке Д.28.

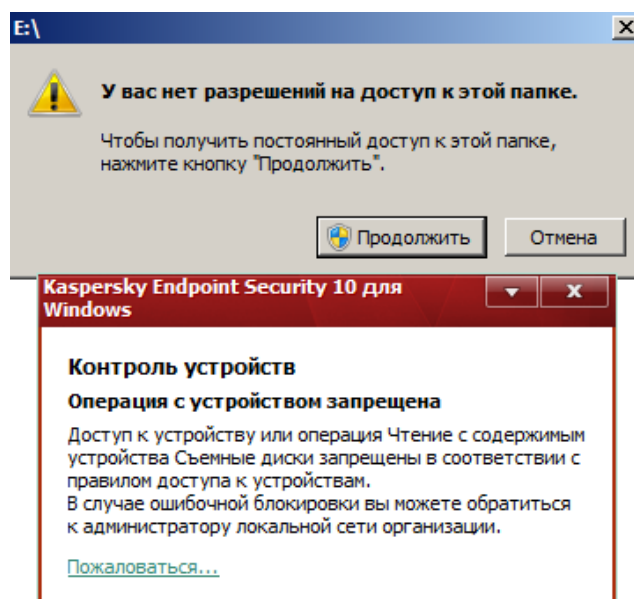


Рисунок Д.28 – Сообщения при попытке открыть съемный носитель
Д.9.2 Контроль запуска программ

Выбрана группа KES10 и на вкладке «Политики» выбрано «Создать политику». Запустился мастер создания политики. Введено название новой политики «Контроль запуска программ». На странице настройки параметров контроля оставлен флажок только на «Контроль запуска программ», как показано на рисунке Д.29.

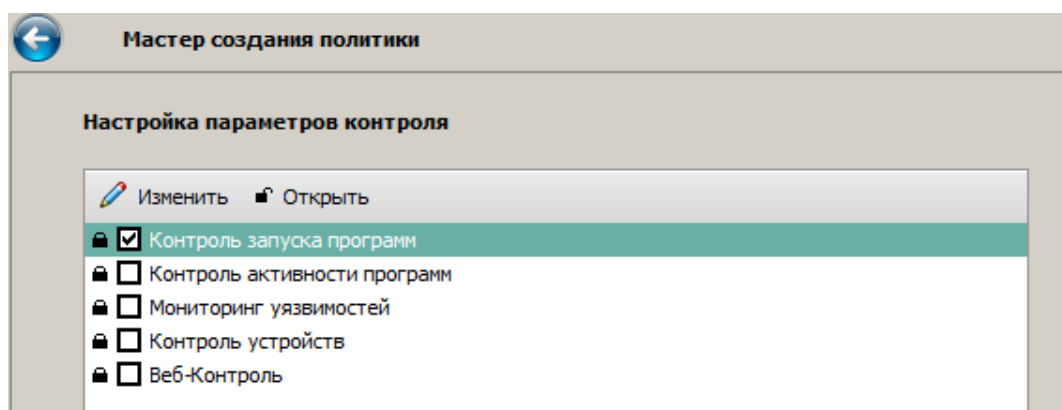


Рисунок Д.29 – Мастер создания политики

Остальные параметры оставлены по умолчанию.

В контекстном меню созданной политики выбрано «Свойства». В разделе «Контроль рабочего стола» – «Контроль запуска программ» добавлено правило, блокирующее запуск браузеров. Для этого нажато «Добавить» и

введено название правила. Нажато «Добавить» для типа условия срабатывания правила «Включающие условия» и выбрано «Условие(я) «КЛ-категория», как показано на рисунке Д.30.

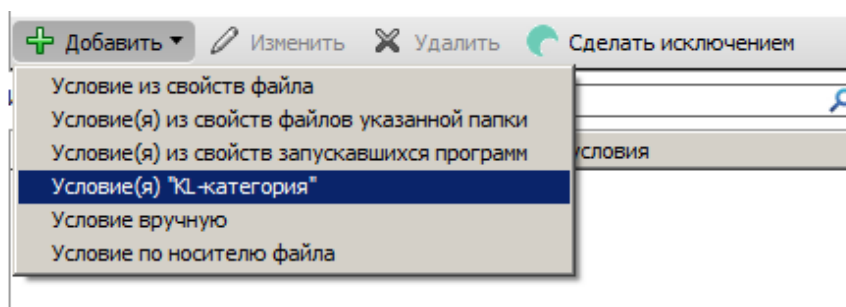


Рисунок Д.30 – Добавление условия

В открывшемся окне указатель поставлен на «Браузеры».

В пункте «Пользователи и / или группы, получающие разрешение» нажато «Удалить». Для «Пользователи и / или группы, получающие разрешение» нажато «Выбрать...». В окне «Выбор: «Пользователи» или «Группы» нажато «Дополнительно» – «Поиск» и выбрано «Все».

В столбце «Статус» для созданного правила выбрано «Вкл». Сохранены изменения в политике.

На виртуальной машине Win7 осуществлен вход под учетной записью «ИБСТ». Запущен браузер Internet Explorer. Было выведено системное сообщение об отказе в доступе, а также сообщение от Kaspersky Endpoint Security 10 for Windows о запрете запуска программы, показанные на рисунке Д.31.

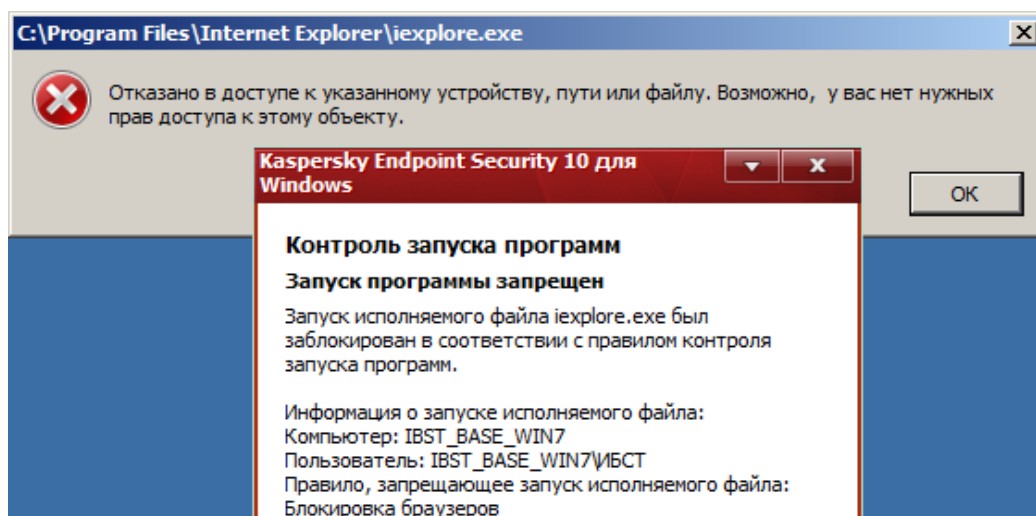


Рисунок Д.31 – Сообщения об отказе в доступе

ПРИЛОЖЕНИЕ Е

(обязательное)

Протокол проверки ВКР в системе Антиплагиат

Ректору Пензенского
государственного университета
А.Д. Гулякову
студента 6 курса ФПИТЭ
очной формы обучения
Анучина Романа Александровича

ЗАЯВЛЕНИЕ

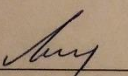
Я, Анучин Роман Александрович, студент 6 курса очной формы обучения специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», прошу провести проверку с использованием системы «Антиплагиат» дипломного проекта на тему «Методика управления антивирусной безопасностью в организации», выполненного мной самостоятельно, на содержание элементов плагиата.

Все прямые заимствования из печатных и электронных источников, а также из защищенных ранее выпускных квалификационных работ, кандидатских и докторских диссертаций имеют соответствующие ссылки.

Я ознакомлен с действующим Стандартом университета «Выпускная квалификационная работа обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры», согласно которому обнаружение плагиата является основанием для недопуска ВКР к защите и отчисления из университета.

 /Р.А. Анучин/
22.01.18

ВКР представлена на проверку 22.01.18

Руководитель ВКР  /О.В. Липилин/

Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Методика управления антивирусной безопасностью в организации» студента 6 курса Р.А. Анучина специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем».

Руководитель ВКР к.т.н., доцент О.В. Липилин.

Отчет о проверке на заимствования

Автор: Анучин Роман Александрович anuchin.roman@yandex.ru / ID: 655

Проверяющий: Фатеев Алексей Григорьевич (ibst@pnzgu.ru / ID: 393)

Организация: Пензенский гос. Университет

Отчет предоставлен сервисом «Антиплагиат» - <http://pnzgu.antiplagiat.ru>

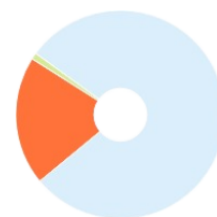
ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 42
Начало загрузки: 22.01.2018 23:02:17
Длительность загрузки: 00:00:06
Имя исходного файла: Анучин Роман Александрович ВКР_12ПТ1_Анучин.docx
Размер текста: 1440 кБ
Символов в тексте: 115226
Слов в тексте: 13543
Число предложений: 757

ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Последний готовый отчет (ред.)
Начало проверки: 22.01.2018 23:13:01
Длительность проверки: 00:00:20
Комментарии: не указано
Модули поиска: Модуль поиска ЭБС "БиблиоРоссика", Модуль поиска ЭБС "BOOK.ru", Коллекция РГБ, Цитирование, Модуль поиска ЭБС "Университетская библиотека онлайн", Коллекция eLIBRARY.RU, Модуль поиска ЭБС "Айбукс", Модуль поиска Интернет, Модуль поиска ЭБС "Лань", Модуль поиска "ПГУ", Кольцо вузов

ЗАИМСТВОВАНИЯ	ЦИТИРОВАНИЯ	ОРИГИНАЛЬНОСТЬ
19,57%	0,19%	80,24%



22.01.2018

_____ О.В. Липилин