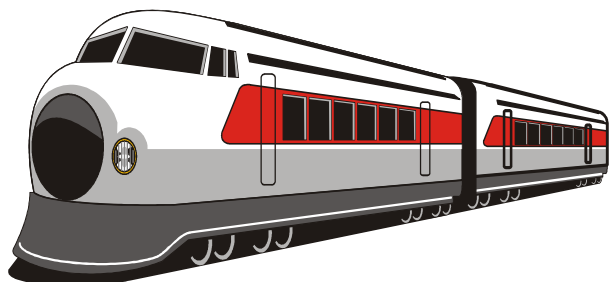


**ТОШКЕНТ ТЕМИР ЙЎЛ МУҲАНДИСЛАРИ ИНСТИТУТИ**



Кафедра Темир йўл транспортада ахборот тизимлари

РАЗРАБОТКА СИСТЕМЫ ИНФОРМАЦИОННОЙ ЗАЩИТЫ  
КОРПОРАТИВНОЙ СЕТИ ОТ ВИРУСНЫХ АТАК мавзусидаги

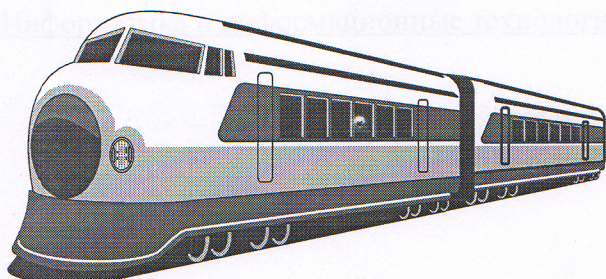
**БИТИРУВ МАЛАКАВИЙ ИШИ**

Муаллиф: Ишмурадова Ш.

Тошкент – 2019 й.



# Тошкент темир йўл муҳандислари институти



Ҳимоя қилишга  
руҳсат берилсин

Кафедра мудири

«27» 06 2019

Кафедра «Информационные системы на железнодорожном транспорте»

Разработка системы информационной защиты корпоративной сети от  
вирусных атак \_\_\_\_\_ мавзудаги

## БИТИРУВ МАЛАКАВИЙ ИШИ

Муаллиф \_\_\_\_\_ Ишмурадова Ш.

Асосий маслаҳатчи \_\_\_\_\_ Бабина В.Г.

Маслаҳатчилар \_\_\_\_\_ Батирова М.М.

Такризчи \_\_\_\_\_ Мирхамидов Ш.Ш.

Ташкент – 2019 й.



Ташкентский институт инженеров железнодорожного транспорта \_\_\_\_\_

Олий ўқув юрти

«Экономика» факультети «Информационные системы на ж.д. транспорте» кафедраси

«Информатика и информационные технологии (на ж.д. транспорте)» йўналиши АТ-26 гуруҳи

Тасдиқлайман \_\_\_\_\_

Каф. мудири \_\_\_\_\_

«10» 01 2019 йил

сана

**БИТИРУВ МАЛАКАВИЙ ИШИ БЎЙИЧА ТОПШИРИҚ**

Талаба \_\_\_\_\_ Ишмурадова Шахло Муродулло кизи

(фамилияси, исми, шарифи )

1. Битирув ишининг мавзуси «Разработка системы информационной защиты корпоративной сети от вирусных атак»

«19» декабр 2018 йил 5-сонли кафедра мажлисида маъқулланган ва институтнинг 07 январ 2019 йилги 4-Т буйруги билан тасдиқланган.

2. Битирув ишини топшириш муддати \_\_\_\_\_ 15.06.2019 \_\_\_\_\_

3. Битирув ишини бажаришга доир бошланғич маълумотлар Локальная вычислительная сеть (LAN) ТашИИТа, использует внешнюю (через WAN) и внутреннюю корпоративную почту, имеет несколько серверов баз данных (БД), почтовый и Proxy- сервера, FireWall. Разработать рекомендации и методики применения антивирусных систем в корпоративной сети, в т.ч.: защита серверов всех типов по всем информационным каналам

4. Ҳисоблаш-тушунтириш ёзувларининг таркиби (ишлаб чиқиладиган масалалар рўйхати) \_\_\_\_\_




1. Классификация вредоносных программ. Анализ угроз и рисков с точки зрения антивирусной защиты3. Разработка политики антивирусной защиты корпоративной сети4. Внедрение антивирусного программного обеспечения. Разработка рекомендаций и методик применения антивирусных средств5. Охрана труда. Антропометрические характеристики человека

5. Чизма ишлар рўйхати (чизмалар номи аниқ кўрсатилади)



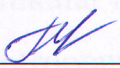
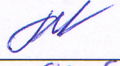
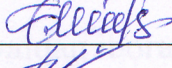
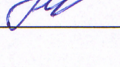
1. Схема корпоративной сети ТашИИТа и пути проникновения вирусов2. Внедрение антивирусного корпоративного программного обеспечения3. Политика антивирусной защиты сети ТашИИТ



6. Битирув бўйича маслаҳатчи (лар)

№	Бўлим мавзуси	Маслаҳатчи ўқитувчи Ф.И.Ш.	Имзо, сана	
			Топшириқ берилди	Топшириқ бажарилди
1	Аналитический обзор	Бабина В.Г.	01.02.2019	 19.02.2019
2	Техническая часть	Бабина В.Г.	20.02.2019	 01.06.2019
3	Охрана труда	Батирова М.М.	07.05.2019	06.06.2019
4	Оформление работы	Бабина В.Г.	28.05.2019	 15.06.2019

7. Битирув ишени бажариш режаси

№	Битирув иши босқичларининг номи	Бажариш муддати (сана)	Текширувдан ўтганлик Белгиси
1	Анализ угроз и рисков с точки зрения антивирусной защиты	7.02.2019	
2	Разработка политики антивирусной защиты	6.03.2019	
3	Внедрение антивирусного обеспечения	8.05.2019	
4	Разработка рекомендаций и методик	01.06.2019	
5	Охрана труда	06.06.2019	
6	Оформление выпускной работы	15.06.2019	

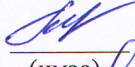
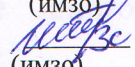
Битирув иши раҳбари \_\_\_\_\_ Бабина В.Г. \_\_\_\_\_

(Ф.И.Ш)

Топшириқни бажаришга олдим \_\_\_\_\_ Ишмурадова Ш.М \_\_\_\_\_

(Ф.И.Ш)

Топшириқ берилган сана « 10 » \_\_\_\_\_ 01 \_\_\_\_\_ 2019\_ йил

  
(имзо)  
  
(имзо)



АО «Узбекистон темир йуллари»

Ташкентский институт инженеров железнодорожного транспорта  
(ТашИИТ)

Факультет Экономика Кафедра Информатика и инфо. тех.

Направление образование: 5330200 Информатика и инфо. тех.

«Утверждаю»

Зав. Кафедрой [подпись]  
«10» 01 2019 год

**ЗАДАНИЕ**

Студенту Мухоморова Шахно Муррӯбо для выполнения раздела  
(фамилия, имя, отчество) жизн

«Безопасность жизнедеятельности» (БЖД) выпускной квалификационной работы.

1. Тема Разработка системы защиты  
корпоративной сети от вирусных атак

утверждена решением заседания кафедры протокол № \_\_\_\_\_ от «\_\_» \_\_\_\_\_ 20\_\_ г.

2. Срок сдачи завершённой выпускной работы (раздела) \_\_\_\_\_

3. Исходные данные для выполнения раздела «Безопасность жизнедеятельности» выпускной квалификационной работы \_\_\_\_\_

4. Содержание пояснительной записки (перечень вопросов, рассмотренных в данной работе)

Знакомство охраны труда и безопас-  
ности на железнодорожном транспорте  
с техникой зрения охраняемого объекта  
Антропометрические характеристики  
человека

5. Содержание графической части (перечень выполненных чертежей и плакатов)

Задание выдал

(дата, подпись руководителя раздела БЖД, должность, Ф.И.О.)

[подпись] ассистент Батирова М.М.

Задание принял

(дата, подпись, Ф.И.О. студента.)

[подпись] Мухоморова Ш.М.



## **Аннотация**

В выпускной работе выполнен обзор вредоносных программ и осуществлен анализ существующего антивирусного программного обеспечения, разработана политика антивирусной защиты корпоративной сети, описана технология внедрения антивирусного ПО. По результатам разработаны рекомендации и методики применения антивирусных средств для корпоративных сетей различной сложности.

В разделе охрана труда проведен анализ антропометрических характеристик человека.

В пояснительной записке содержится: 93 стр.; рисунков: 27; таблиц: 7.

## **Annotatsiya**

Bitiruv malakaviy ishda zararli dasturlarning umumiy ko'rinishi va antivirus dasturiy ta'minotining tahlillari o'tkazildi, korporativ tarmoq uchun antivirus siyosati ishlab chiqildi va antivirus dasturlarini joriy etish texnologiyasi tavsiflandi. Natijalar asosida korporativ tarmoqlar uchun turli murakkabliklarga qarshi antivirus vositalarini qo'llash bo'yicha tavsiyalar va texnikalar ishlab chiqildi.

Mehnatni muhofaza qilish bo'limida insonning antropometrik xususiyatlarini tahlil qilish amalga oshiriladi.

Quyidagi ko'rsatilgan ish 92 bet; 27 rasm; 7 jadvaldan iborat.

## **Annotation**

In the final work an overview of malicious programs was carried out and an analysis of existing antivirus software was carried out, an antivirus policy was developed for the corporate network, and the technology for introducing antivirus software was described. Based on the results recommendations and techniques for the use of anti-virus tools for corporate networks of varying complexity were developed.

In the labor protection section an analysis of the anthropometric characteristics of a person is carried out.

The explanatory note contains: 92 p .; figures: 27; tables: 7.



## РЕЦЕНЗИЯ

на выпускную квалификационную работу студента Ташкентского  
института инженеров железнодорожного транспорта  
по направлению -5330200 «Информатика и информационные  
технологии»

Ишмурадовой Шахло Муродулло кизи

(Ф.И.О. слушателя)

выполненную на тему: Разработка системы информационной защиты

(Название темы)

корпоративной сети от вирусных атак

1. Актуальность, новизна выбранная тема актуальна

2. Оценка содержания работы В целом квалификационная выпускная работа  
выполнена на высоком уровне, а автор заслуживает отличной оценки

3. Достоинства работы Выпускная работа студентки Ишмурадовой Ш.М.  
посвящена разработке системы защиты корпоративной сети от вирусных атак  
с акцентом на защиту серверов

4. Практическая значимость работы и рекомендации по внедрению Исходя из поставленной цели в выпускной работе приведена разработка  
системы защиты корпоративной сети от вирусных атак с акцентом на защиту  
серверов. Исходными данными явилась распределенная локальная  
вычислительная сеть (ЛВС) института. Также разработаны рекомендации и  
методики применения антивирусных средств для корпоративных сетей  
различной сложности

5. Недостатки и замечания по работе недостаточное использование литературных источников

6. Рекомендуемая оценка выполненной работы На основании представленных материалов считаю, что работа заслуживает  
оценки «отлично»

Рецензент Мирхамидов Ш.Ш

(Подпись)

(Ф.И.О.)

Заместитель начальника ИВЦ (ученая степень, знание, должность, место работы)

«  » июня 2019 г.  
(дата выдачи)





## ОТЗЫВ

руководителя на выпускную квалификационную работу студентки  
Ташкентского института инженеров железнодорожного транспорта  
по направлению -5330200 «Информатика и информационные  
технологии»

Ишмурадовой Шахло Муродулло кизи

(Ф.И.О. студента)

выполненную на тему: Разработка системы информационной защиты

(Название темы)

корпоративной сети от вирусных атак

### 1. Актуальность, новизна:

Актуальность темы, цель и задачи выпускной квалификационной работы обоснованы во введении.

Актуальность выбранной темы обусловлена тем, что использование высокоэффективных информационных систем является обязательным условием успешной деятельности современных организаций и предприятий. И в этом разрезе безопасность информации – это один из основных показателей качества информационной системы. Поэтому одной из важнейших и наиболее актуальных задач защиты информации является организация эффективной антивирусной защиты автономных рабочих станций, локальных и корпоративных компьютерных сетей, обрабатывающих информацию ограниченного доступа.

### 2. Достоинства работы:

Выпускная квалификационная работа Ишмурадовой Ш.М. представляет собой актуальное исследование технологии внедрения антивирусного программного обеспечения, разработки политики антивирусной защиты корпоративной сети.

Выпускная квалификационная работа имеет традиционное построение: обзор литературы, подготовленный по 17 источникам учебной и периодической литературы.

Выпускная квалификационная работа аккуратно оформлена на компьютере, иллюстрирована 27 рисунками и 7 таблицами.

### 3. Практическая значимость работы и рекомендации по внедрению:

Исходя из поставленной цели в выпускной работе проведен обзор вредоносных программ и осуществлен анализ существующего антивирусного программного обеспечения, разработана политика антивирусной защиты корпоративной сети, описана технология внедрения антивирусного ПО. По результатам разработаны рекомендации и методики применения антивирусных средств для корпоративных сетей различной сложности.



#### 4. Дополнительная информация для ГАК:

За время выполнения выпускной квалификационной работы Ишмурадова Ш.М. продемонстрировала способность не только самостоятельно решать поставленную задачу, но и творчески подходить к самой ее постановке и предлагать новые решения. По результатам работы был выполнен доклад на студенческую конференцию.

Задание на выпускную квалификационную работу выполнено полностью.

Выпускная квалификационная работа по своему содержанию и объему отвечает установленным требованиям, может быть допущена к защите и оценивается на «отлично».

Руководитель \_\_\_\_\_

(Подпись)

Бабина В.Г.

(Ф.И.О.)

старший преподаватель кафедры «Информационные системы  
на железнодорожном транспорте» Ташкентского института инженеров  
железнодорожного транспорта

(ученая степень, знание, должность, место работы)

«\_\_» июня 2019 г.

(дата выдачи)



## **Введение**

Государственные органы, юридические и физические лица обязаны обеспечить защиту информационных ресурсов и информационных систем, содержащих информацию о государственных секретах и конфиденциальную информацию. Включение информационных систем, содержащих информационные ресурсы ограниченного доступа, в международные информационные сети и во всемирную информационную сеть Интернет осуществляется только после принятия необходимых защитных мер. [1]

В целях коренного совершенствования качества образования в высших образовательных учреждениях, обеспечения их активного участия в осуществляемых в стране широкомасштабных реформах, а также последовательной реализации задач, определенных в Стратегии действий [3] по пяти приоритетным направлениям развития Республики Узбекистан в 2017 — 2021 годах разрабатывается комплекс мероприятий по укреплению и модернизации материально-технической базы высших образовательных учреждений, оснащение высших образовательных учреждений средствами современных информационно-коммуникационных технологий, расширение доступа студентов, преподавателей и молодых исследователей к мировым образовательным ресурсам, электронным каталогам передовой научной литературы и базам данных [4], который невозможен без осуществления мер безопасности локальных сетей.

3 апреля 2019 года Президент Шавкат Мирзиёев провел совещание, на котором были обсуждены методы практической реализации пяти инициатив, создания условий для воспитания и образования молодежи, повышения занятости женщин. Из пяти инициативах, третья инициатива – эффективное использование компьютерных технологий и интернета, для чего до 2020 года в республике будут созданы бесплатные учебные центры по цифровым технологиям и около 19 тысяч объектов социальной сферы будут обеспечены высокоскоростным доступом в интернет [2].



За последнее время было принято ряд постановлений, благодаря которым принимаются меры «по внедрению современных форм и методов обучения, компьютерных и информационно-коммуникационных технологий в образовательный процесс, обеспечению высших образовательных учреждений современным учебно-лабораторным оборудованием и учебно-методической литературой, поддержке и стимулированию научно-исследовательской и инновационной деятельности, организации и развитию современных научных лабораторий высших образовательных учреждений».[5]

А также по «оптимизации процессов управления в системе высшего образования на основе информационно-коммуникационных технологий, интеграции существующих информационных систем, внедрению эффективных систем подготовки аналитических данных».[6]

**Актуальность выпускной квалификационной работы.** В нынешнее время развития вирусной индустрии никто не станет отрицать важность системы антивирусной безопасности на предприятии – это в большинстве случаев наиболее актуальная система, из всего ряда развернутых систем обеспечения информационной безопасности. Сегодня уже невозможно представить себе серьезную компанию, не использующую в своей работе современные информационные технологии (ИТ) для ведения бизнеса. Одной из неперенных составляющих данных технологий является объединение вычислительных ресурсов компании в единую распределенную корпоративную сеть. И главным действующим лицом здесь является информация – она постоянно предъявляет все новые и новые, все более жесткие требования к тем, кто ее создает, кто ее передает, кто ею пользуется. Эти требования связаны, прежде всего, с защитой информации на всех стадиях ее существования, поскольку с развитием компьютерных и сетевых технологий и ростом зависимости всех сторон нашей жизни от качества и достоверности информации она становится самым ценным, самым важным и



поэтому самым желанным объектом посягательств со стороны различного рода злоумышленников.

Уничтожение, изменение, хищение информации всегда влечет за собой весьма серьезные отрицательные последствия, которые очень часто можно назвать катастрофическими. Одним из видов субъектов, которые чаще всего выступают в обезличенном виде, но которые при этом своими действиями могут нанести любой организации непоправимый ущерб, являются компьютерные вирусы.

Основными видами угроз антивирусной безопасности являются различные типы вредоносного программного обеспечения (ПО), способного нанести определённый ущерб автоматизированных систем (АС) или её пользователям. Вредоносный код может представлять собой компьютерные вирусы, а также программы типа «троянский конь», «adware» (рекламное ПО), «spyware» (шпионское ПО) и другие. Не менее значимой угрозой является спам, представляющий собой незапрошенные сообщения рекламного и иного характера, распространяемые посредством электронной почты.

Наличие спама в АС может привести к одному из следующих негативных последствий: нарушению работоспособности почтовой системы вследствие большого потока входящих сообщений; реализации фишинга («phishing») – это вид электронного мошенничества, нацеленный на кражу личных данных с целью получения, как прямой, так и косвенной, финансовой прибыли; снижению производительности труда персонала вследствие необходимости ежедневного просмотра и ручного удаления большого количества спама из своего почтового ящика.

Сегодня можно с уверенностью констатировать, что компьютерные вирусы вышли на первое место в перечне наиболее опасных угроз информационной безопасности (АС). По данным статистики наиболее успешными методами реализации угроз безопасности информации в автоматизированных системах являются вирусные атаки. На их долю



приходится около 57 % инцидентов с безопасностью информации и около 60 % реализованных угроз из числа зафиксированных и попавших в статистические обзоры.

Таким образом, использование высокоэффективных информационных систем является обязательным условием успешной деятельности современных организаций и предприятий. И в этом разрезе безопасность информации – это один из основных показателей качества информационной системы. Поэтому одной из важнейших и наиболее актуальных задач защиты информации является организация эффективной антивирусной защиты автономных рабочих станций, локальных и корпоративных компьютерных сетей, обрабатывающих информацию ограниченного доступа.

**Цель выпускной квалификационной работы.** Разработать систему антивирусной защиты типовой корпоративной сети, а также разработать рекомендации и методики применения антивирусных средств.

**Задачи выпускной квалификационной работы.** Для достижения поставленной цели необходимо решение следующих задач: выполнить обзор вредоносных программ и анализ существующего антивирусного программного обеспечения, разработать политику антивирусной защиты корпоративной сети и технологию внедрения антивирусного ПО.

**Структура работы.** Выпускная работа состоит из введения, четырех частей, заключения и содержит список использованной литературы.



# 1 Анализ состояния вопроса

## 1.1 Классификация вредоносных программ

Термин «компьютерный вирус» впервые был употреблен Фредериком Коэном в 1984 году на 7-й конференции по вопросам информационной безопасности проходившей в США. С тех пор появилось очень много определений компьютерного вируса, но до сих пор никто не сформулировал определения, которое бы однозначно характеризовало представителей данного класса вредоносных программ.

Классическое определение компьютерного вируса остается неизменным было дано Ф.Коэном в своей основополагающей работе: «компьютерный вирус – это программа, которая может заражать другие программы, изменяя их посредством добавления своей, возможно модифицированной, копии, которая сохраняет способность к дальнейшему размножению».

Наиболее удачным является следующее определение компьютерного вируса:

Компьютерный вирус – это сегмент программного кода, который может имплантировать себя в исполняемые файлы операционной системы, создавать программный код, выполняющий аналогичные функции, и внедрять его в файлы прикладных программ, системные области компьютера, вычислительные сети и т.д. Такие программы часто носят деструктивный характер, являются небольшими по размеру, и всеми возможными способами пытаются скрыть от пользователя свое присутствие в системе.

Вред, наносимый вирусами можно разделить на прямой и косвенный. Прямой вред – это целевая функция вируса, то, ради чего он создавался. Наиболее опасными являются вирусы, целевая функция которых – уничтожение или искажение информации на жестком диске. Реализация целевой функции обычно происходит при выполнении определенных условий. Например, вирус, может быть запрограммирован на активизацию



определенного числа конкретного месяца, а до этого момента вирус может быть абсолютно безвреден.

До выполнения своей целевой функции вирус только размножается. Размножение – и есть косвенный вред, причиняемый вирусом. Загрузка сетевого трафика, уменьшение свободной оперативной памяти и объема жесткого диска все это влияет на эффективность работы конечного пользователя или даже организации в целом. Порой ущерб от косвенного вреда вируса является более значительным, чем от реализации его целевой функции.

Вредоносные программы можно разделить на четыре большие группы: компьютерные вирусы, сетевые черви и троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети. Наглядная классификация вредоносных программ приведена на рис. 1.1.

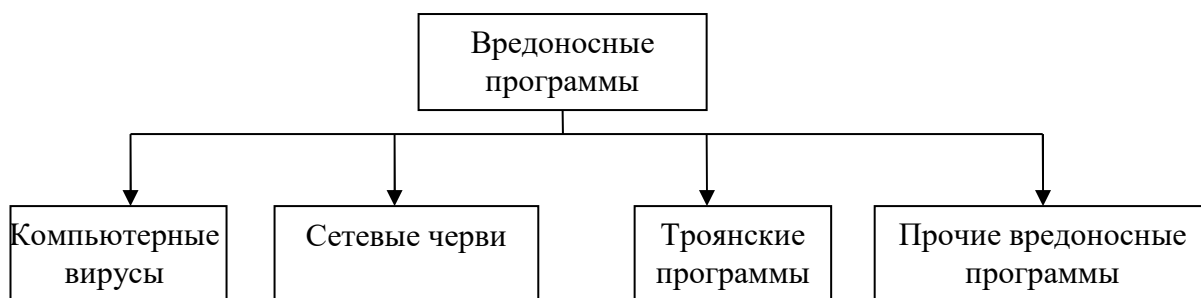


Рис. 1.1. Классификация вредоносных программ

Рассмотрим подробнее каждый тип вредоносных программ.

а) **Сетевые черви.** К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью проникновения на удаленные компьютеры, запуска своей копии на удаленном компьютере и дальнейшего распространения на другие компьютеры в сети. Для проникновения на удаленные компьютеры и запуска своей копии черви используют различные методы: социальный инжиниринг (например, текст электронного письма, призывающий открыть вложенный файл), недочеты в конфигурации сети (например, копирование на диск, открытый на полный доступ), ошибки в службах безопасности операционных



систем и приложений.

Основным признаком, по которому типы червей различаются между собой, является способ распространения червя – каким способом он передает свою копию на удаленные компьютеры. Другими признаками различия червей между собой являются способы запуска копии червя на заражаемом компьютере, методы внедрения в систему, а также полиморфизм, «стелс» и прочие характеристики, присущие и другим типам вредоносного программного обеспечения (вирусам и троянским программам). В табл. 1.1 приведена классификация сетевых червей по способу их распространения.

б) *Классические компьютерные вирусы*. К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью последующего запуска своего кода при каких-либо действиях пользователя и дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том случае, если зараженный объект по каким-либо, не зависящим от функционала вируса, причинам оказывается активизированным на другом компьютере.

Типы компьютерных вирусов различаются между собой по следующим основным признакам: среда обитания и способ заражения. Под «средой обитания» понимаются системные области компьютера, операционные системы или приложения, в компоненты (файлы) которых внедряется код вируса. Под «способом заражения» понимаются различные методы внедрения вирусного кода в заражаемые объекты. Классификация компьютерных вирусов приведена на рис.1.2.



## Классификация сетевых червей

Тип вредоносного ПО	Описание	Способ распространения
<b>Сетевые черви</b>		
1. Email-Worm (почтовые черви)	используют электронную почту	– червь отсылает свою копию в виде вложения в электронное письмо, код червя активизируется при открытии (запуске) зараженного вложения; - червь отсылает ссылку на свой файл, расположенный на каком-либо сетевом ресурсе, код червя активизируется при открытии ссылки на зараженный файл.
2. IM-Worm	используют интернет-пейджеры	– рассылка на обнаруженные контакты (из контактного листа) сообщений, содержащих URL на файл, расположенный на каком-либо веб-сервере.
3. IRC-Worm	используют IRC-каналы	– в отсылке URL-ссылки на копию червя; – отсылка зараженного файла какому-либо пользователю сети.
4. Net-Worm (прочие сетевые черви)		– копирование червя на сетевые ресурсы. Червь ищет удаленные компьютеры и копирует себя в каталоги, открытые на чтение и запись (если такие обнаружены); – проникновение червя на компьютер через уязвимости в операционных системах и приложениях Черви ищут в сети компьютеры, на которых используется программное обеспечение, содержащее критические уязвимости. Для заражения уязвимых компьютеров червь посылает специально оформленный сетевой пакет или запрос (эксплойт уязвимости), в результате чего код (или часть кода) червя проникает на компьютер-жертву; – проникновение в сетевые ресурсы публичного использования (веб- и FTP-сервера). Заражение происходит в два этапа. Сначала червь проникает в компьютер-сервер и необходимым образом модифицирует служебные файлы сервера. Затем червь «ждет» посетителей, которые запрашивают информацию с зараженного сервера, и таким образом проникает на другие компьютеры в сети. – паразитирование на других вредоносных программах. Для заражения удаленных компьютеров данные черви ищут другие компьютеры в сети и посылают на них команду скачивания и запуска своей копии.
5. P2P-Worm (черви для файлообменных сетей)	используют файлообменные сети	– для внедрения в P2P-сеть червь достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по распространению вируса P2P-сеть берет на себя – при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла.

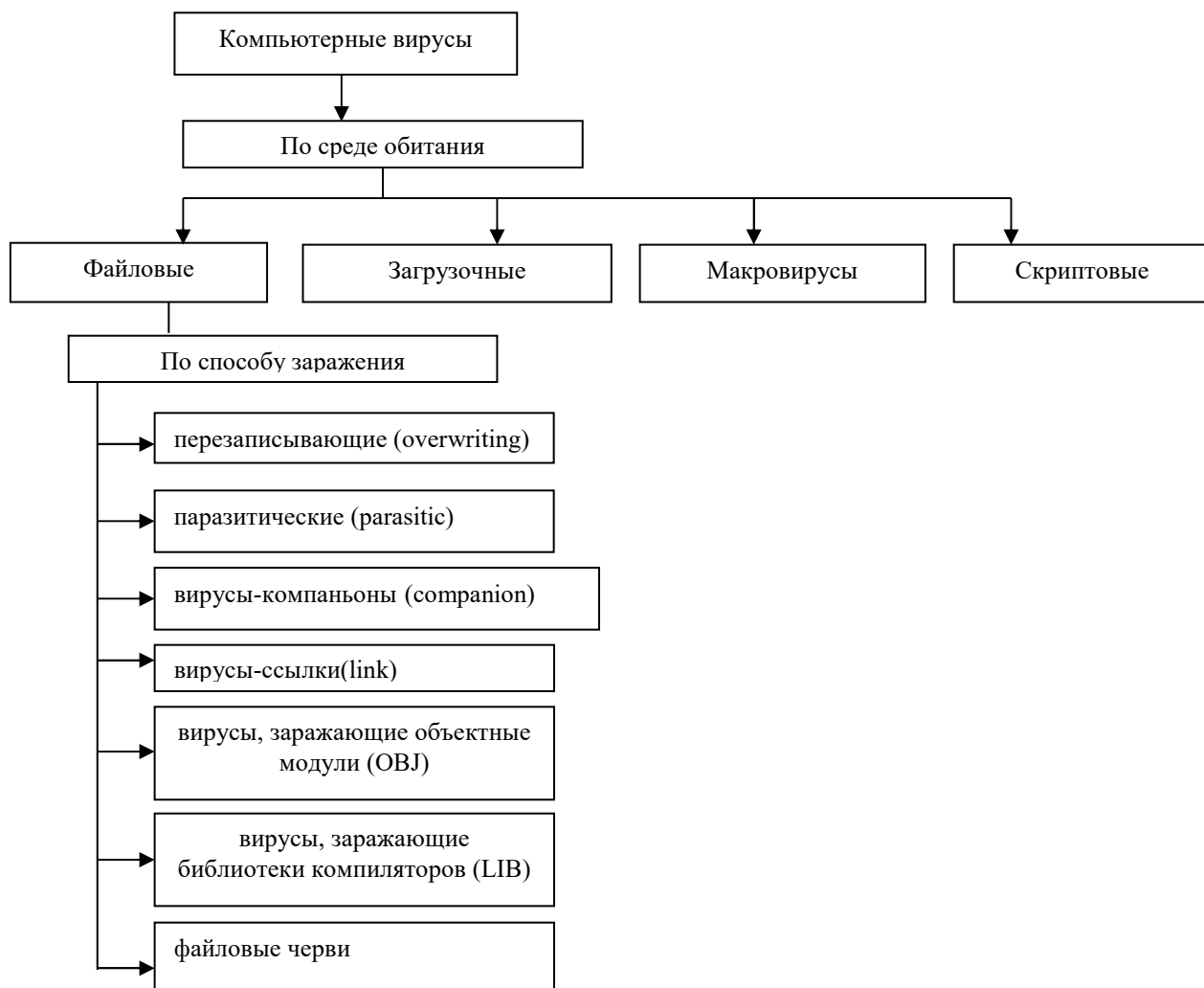


Рис.1.2 Классификация компьютерных вирусов

1. Файловые вирусы при своем размножении тем или иным способом используют файловую систему какой-либо (или каких-либо) ОС. Как видно из рис.1.2. файловые вирусы в свою очередь тоже подразделяются на классы:

- **Перезаписывающие (overwriting).** Данный метод заражения является наиболее простым: вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать;
- **Паразитические (parasitic).** К паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично



работоспособными. Основными типами таких вирусов являются вирусы, записывающиеся в начало файлов (prepending), в конец файлов (appending) и в середину файлов (inserting). В свою очередь, внедрение вирусов в середину файлов происходит различными методами – путем переноса части файла в его конец или копирования своего кода в заведомо неиспользуемые данные файла (cavity-вирусы);

- Вирусы-компаньоны (Companion). К этой категории относятся вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т. е. вирус. К вирусам данного типа относятся те из них, которые при заражении переименовывают файл в какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на диск под именем заражаемого файла. Например, файл NOTEPAD.EXE переименовывается в NOTEPAD.EXD, а вирус записывается под именем NOTEPAD.EXE. При запуске управление получает код вируса, который затем запускает оригинальный NOTEPAD;

- Файловые вирусы никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям «специальные» имена, чтобы подтолкнуть пользователя на запуск своей копии – например, INSTALL.EXE или WINSTART.BAT;

- Link-вирусы также не изменяют физического содержимого файлов, однако при запуске зараженного файла «заставляют» ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы;

- OBJ-, LIB-вирусы и вирусы в исходных текстах – это вирусы, заражающие библиотеки компиляторов, объектные модули и исходные тексты программ, достаточно экзотичны и практически не распространены.

Зараженный файл при этом не является выполняемым и не способен на распространение в текущем состоянии. Носителем же «живого» вируса становится COM- или EXE-файл, получаемый в процессе компоновки зараженного файла с другими объектными модулями и библиотеками.

2. Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор.

Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера – после необходимых тестов установленного оборудования (памяти, дисков и т.д.) программа системной загрузки считывает первый физический сектор загрузочного диска (A:, C: или CD-ROM в зависимости от параметров, установленных в BIOS Setup) и передает на него управление.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо какой-либо программы, получающей управление при загрузке системы. Принцип заражения, таким образом, одинаков во всех описанных выше способах: вирус «заставляет» систему при ее перезапуске считать в память и отдать управление не оригинальному коду загрузчика, но коду вируса.

Заражение сменных носителей производится единственным известным способом – вирус записывает свой код вместо оригинального кода boot-сектора дискеты. Винчестер заражается тремя возможными способами – вирус записывается либо вместо кода MBR, либо вместо кода boot-сектора загрузочного диска (обычно диска C:), либо модифицирует адрес активного boot-сектора в таблице разделов диска (Disk Partition Table), расположенной в MBR винчестера.

При инфицировании диска вирус в большинстве случаев переносит оригинальный boot-сектор (или MBR) в какой-либо другой сектор диска (например, в первый свободный). Если длина вируса больше длины сектора, то в заражаемый сектор помещается первая часть вируса, остальные части



размещаются в других секторах (например, в первых свободных).

3. Макровирусы. Многие табличные и графические редакторы, системы проектирования, текстовые процессоры имеют свои макроязыки для автоматизации выполнения повторяющихся действий. Эти макроязыки часто имеют сложную структуру и развитый набор команд. Макровирусы являются программами на макроязыках, встроенных в такие системы обработки данных. Для своего размножения вирусы этого класса используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Наибольшее распространение получили макровирусы для Microsoft Office (Word, Excel и PowerPoint), хранящих информацию в формате OLE2 (Object Linking and Embedding). Вирусы в прочих приложениях достаточно редки.

Физическое расположение вируса внутри файла MS Office зависит от его формата, который в случае продуктов Microsoft чрезвычайно сложен – каждый файл-документ Word, Office97 или таблица Excel представляют собой последовательность блоков данных (каждый из которых также имеет свой формат), объединенных между собой при помощи большого количества служебных данных. По причине такой сложности форматов файлов Word, Excel и Office97 представить расположение макровируса в файле можно лишь схематично, что показано на рис.1.3.

При работе с документами и таблицами MS Office выполняет различные действия: открывает документ, сохраняет, печатает, закрывает и т.д. При этом MS Word, например, ищет и выполняет соответствующие «встроенные макросы» – при сохранении файла по команде File/Save вызывается макрос FileSave, при сохранении по команде File/SaveAs – FileSaveAs, при печати документов – FilePrint и т.д., если, конечно, таковые макросы определены.

Существует также несколько «автомакросов», автоматически вызываемых при различных условиях. Например, при открытии документа MS Word проверяет его на наличие макроса AutoOpen. Если такой макрос

присутствует, то Word выполняет его. При закрытии документа Word выполняет макрос AutoClose, при запуске Word вызывается макрос AutoExec, при завершении работы – AutoExit, при создании нового документа – AutoNew. Автоматически (т.е. без участия пользователя) выполняются также макросы/функции, ассоциированные с какой-либо клавишей либо моментом времени или датой, т.е. MS Word/Excel вызывают макрос/функцию при нажатии на какую-либо конкретную клавишу (или комбинацию клавиш) либо при достижении какого-либо момента времени.

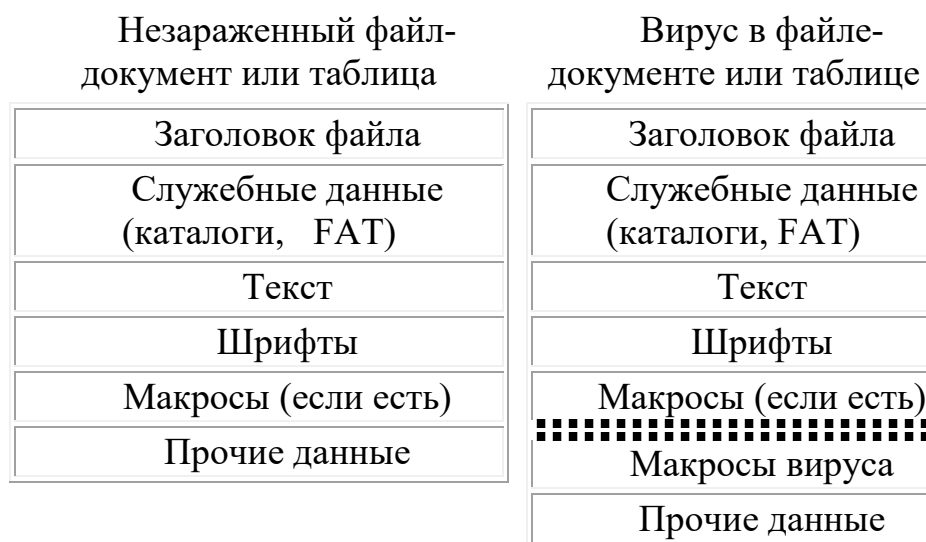


Рис.1.3. Схематичное расположение макровируса в файле

4. Скрипт-вирусы. Следует отметить также скрипт-вирусы, являющиеся подгруппой файловых вирусов. Данные вирусы, написаны на различных скрипт-языках (VBS, JS, BAT, PHP и т.д.). Они либо заражают другие скрипт-программы (командные и служебные файлы MS Windows или Linux), либо являются частями многокомпонентных вирусов. Также, данные вирусы могут заражать файлы других форматов (например, HTML), если в них возможно выполнение скриптов.

в) **Троянские программы.** Троянские программы (троянские кони или просто троянцы) – это программы, которые совершают деструктивные действия, но при этом не размножаются и не рассылаются сами. Своим названием эти программы обязаны троянскому коню из «Илиады» Гомера. Подобно троянскому коню программа-троянец выдает себя за что-либо



вполне безобидное, «подделываясь» под другие программы (игры, новые версии популярных утилит и пр.).

Главным отличием "троянов" от всех перечисленных выше вирусов является то, что троянские программы не размножаются сами. Они единоразово устанавливаются на компьютер и долгое время (как правило, либо до момента обнаружения, либо до переустановки операционной системы, по какой либо причине) выполняет свои функции. При этом троянский конь не может самостоятельно переместиться с одного компьютера в локальной сети на другой.

Троянские программы различаются между собой по тем действиям, которые они производят на зараженном компьютере.

г) *Прочие вредоносные программы.* К ним относятся разнообразные программы, которые не представляют угрозы непосредственно компьютеру, на котором исполняются, а разработаны для создания других вирусов или троянских программ, организации DoS-атак на удаленные сервера, взлома других компьютеров и т.п. Наглядная классификация этого типа вредоносных программ приведена в табл. 1.2.

Приведенная классификация не может считаться полной, так как прогресс не стоит на месте, появляются всё новые и новые интеллектуальные устройства и соответственно вирусы работающие на них, например уже появились вирусы поражающие мобильные телефоны.

## Классификация прочих вредоносных программ

Тип вредоносных программ	Описание
<b>Прочие вредоносные программы</b>	
1. Эмуляторы DoS, DDoS (Distributed Denial of Service) атак – сетевые атаки	Программы данного типа реализуют атаки на удаленные сервера, посылая на них многочисленные запросы, что приводит к отказу в обслуживании, если ресурсы атакуемого сервера недостаточны для обработки всех поступающих запросов (DoS = Denial of Service). DoS-программы реализуют атаку с одного компьютера с ведома пользователя. DDoS-программы реализуют распределенные атаки с разных компьютеров, причем без ведома пользователя зараженного компьютера.
2. Exploit, HackTool - взломщики удаленных компьютеров	Хакерские утилиты данного класса предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими (используя методы троянских программ типа backdoor) или для внедрения во взломанную систему других вредоносных программ.
3. Flooder - «замусоривание» сети	Данные хакерские утилиты используются для «забивания мусором» каналов интернета - IRC-каналов, компьютерных пейджинговых сетей, электронной почты и т. д.
4. Constructor - конструкторы вирусов и троянских программ	Конструкторы вирусов и троянских программ - это утилиты, предназначенные для изготовления новых компьютерных вирусов и «троянцев». Известны конструкторы вирусов для DOS, Windows и макро-вирусов. Они позволяют генерировать исходные тексты вирусов, объектные модули, и/или непосредственно зараженные файлы.
5. Nuker - фатальные сетевые атаки	Утилиты, отправляющие специально оформленные запросы на атакуемые компьютеры в сети, в результате чего атакуемая система прекращает работу. Используют уязвимости в программном обеспечении и операционных системах, в результате чего сетевой запрос специального вида вызывает критическую ошибку в атакуемом приложении.
6. Bad-Joke, Ноах - злые шутки, введение пользователя в заблуждение	К ним относятся программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности.
7. FileCryptor, PolyCryptor - скрывание от антивирусов	Хакерские утилиты, использующиеся для шифрования других вредоносных программ с целью скрывания их содержимого от антивирусной проверки.
8. PolyEngine – полиморфные генераторы	Полиморфные генераторы не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т.е. открытия, закрытия и записи в файлы, чтения и записи секторов и т.д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.
9. VirTool	Утилиты, предназначенные для облегчения написания компьютерных вирусов и для их изучения в хакерских целях.



## 1.2 Методы и средства обнаружения компьютерных вирусов

1. Сканирование – самый простой метод поиска вируса. Он основан на последовательном просмотре памяти компьютера, загрузочных секторов и проверяемых файлов в поиске так называемых сигнатур (масок) известных вирусов. Определение сигнатуры вируса очень сложная задача. Необходимо тщательно изучить принцип работы вируса и сравнить программы, зараженные данным вирусом, и незараженные. Кроме того, сигнатура не должна содержаться в других программах, иначе возможны ложные срабатывания. В разрезе данного метода существует тип антивирусных программ, которые называются программы-детекторы, или программы-сканеры. Они осуществляют поиск известных версий вирусов методом сканирования, т.е. поиском сигнатур вирусов. Поэтому программы-сканеры могут обнаружить только уже известные вирусы, которые были предварительно изучены, и для которых была определена сигнатура. Использование программ-сканеров не защищает компьютер от новых вирусов. Кроме того, такие программы не могут обнаружить большинство полиморфных вирусов, т.к. они не содержат сигнатур. Для эффективного использования программ-детекторов, реализующих метод простого сканирования, рекомендуется постоянно обновлять их, получая самые последние версии, так как в них уже будут включены новые типы вирусов.

Антивирусные программы-сканеры, которые могут удалить обнаруженный вирус, называются полифагами.

2. Обнаружение изменений, или контроль целостности, который основан на выполнении двух процедур: постановка на учет и контроль поставленного на учет. При внедрении вируса в компьютерную систему обязательно происходят изменения в системе (которые некоторые вирусы успешно маскируют). Это и изменение объема доступной оперативной памяти, и изменение загрузочных секторов дисков, и изменения самих файлов. Достаточно запомнить характеристики, которые подвергаются изменениям в результате внедрения вируса, а затем периодически сравнивать эти

эталонные характеристики с действующими.

Программы, реализующие этот метод, называются программы-ревизоры, которые первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, параметры всех контролируемых файлов (иногда только контрольную сумму файлов), информацию о структуре каталогов, номера плохих кластеров диска, иногда – объем установленной оперативной памяти, количество подключенных к компьютеру дисков и их параметры и многое другое. Для определения наличия вируса в системе программы-ревизоры проверяют созданные ими образы и производят сравнение с текущим состоянием. Если обнаружено изменение - вполне вероятно, что эти изменения произведены вирусом.

Ревизоры могут обнаружить любые вирусы, даже ранее неизвестные. Но для этого необходимо “поставить на учет” заведомо чистые от вирусов возможные объекты нападения. Кроме этого, ревизор не обнаружит вирус, который попал с новым зараженным уже файлом, так как он “не знает” параметров этого файла до заражения вирусом. Не сможет ревизор обнаружить вирус, заражающий файлы только при копировании, опять же не имея возможности сравнить параметры файлов. Ревизоры неэффективно использовать для обнаружения вирусов в файлах документов, так как эти файлы очень часто изменяются. Кроме того, следует учитывать, что ревизоры только обнаруживают изменения, но не все изменения связаны с внедрением вируса.

В этих случаях у ревизоров один общий недостаток с программами-мониторами: пользователь должен хорошо разбираться во всех таких случаях и сам принимать решения – является ли изменение результатом действия вируса или нет. То есть программы-ревизоры не предназначены для рядового пользователя.

Правда, в последнее время ревизоры дополняются базами сигнатур вирусов, и при подозрении на вирус ревизор тут же осуществляет сканирование в поисках вирусов. Такие ревизоры уже более пригодны для

использования рядовыми пользователями.

3. Метод резидентного сторожа. Этот метод направлен на выявление «подозрительных» действий пользовательских программ, например, таких, как запись на диск по абсолютному адресу, форматирование диска, изменение загрузочного сектора, изменение или переименование выполняемых программ, появление новых резидентных программ, изменение системных областей и других. При обнаружении «подозрительного» действия необходимо «спросить разрешение» у пользователя на выполнение такого действия.

Программы, реализующие этот метод, называются программы-мониторы, или резидентные сторожа. Это целый класс антивирусов, которые постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. С помощью монитора можно остановить распространение вируса на самой ранней стадии. Их цель – не пропустить вирус на компьютер. И поэтому они контролируют обращение к дискам. При обнаружении «подозрительного» действия программа-монитор либо блокирует выполнение такого действия до специального разрешения пользователя, либо просто выдаёт на экран предупреждающее сообщение, либо совершает другие специальные действия.

Невысокая популярность таких программ объясняется тем, что мониторы отнимают время на проверку программ во время их запуска, и процесс загрузки программы замедлится. Ещё одним недостатком программ-мониторов является то, что они уменьшают объём памяти, доступной программам пользователей, ведь он должен резидентно находиться в памяти.

Поэтому мониторы необходимо применять в следующих случаях:

- запуск новых программ неизвестного происхождения;
- во время подозрения на вирус;
- некоторое время после удаления вируса для исключения его появления вновь.



4. Вакцинирование программ. Этот метод заключается в дописывании к исполняемому файлу дополнительной подпрограммы, которая первой получает управление при запуске файла, выполняет проверку целостности программы. Проверяться могут любые изменения, например, контрольная сумма файла или другие характеристики.

5. Особого внимания заслуживают проактивные (превентивные) методы защиты методы, которые позволяют обнаруживать вредоносное ПО до обновления антивирусных баз, иначе говоря – обнаруживать угрозу до ее появления. При этом количество ложных срабатываний также должно быть минимальным (в идеале ложных срабатываний не должно быть вовсе).

- Эвристический анализатор. Эвристическим анализатором называется набор программ, которые анализируют код исполняемых файлов, макросов, скриптов, памяти или загрузочных секторов для обнаружения в нем разных типов вредоносных компьютерных программ, не определяемых обычными (сигнатурными) методами. Другими словами – эвристические анализаторы предназначены для поиска неизвестного вредоносного ПО. Уровень детектирования у эвристических анализаторов не очень высок, так как существуют десятки различных методов их «обмана», которыми пользуются авторы вирусов. Кроме этого, для эвристических анализаторов с высоким уровнем обнаружения характерен высокий уровень ложных срабатываний, что делает их использование неприемлемым. Даже у самых лучших антивирусов уровень обнаружения новых вредоносных программ не превышает 25-30%. Несмотря на невысокий уровень обнаружения, эвристические методы остаются востребованными в современных антивирусах. Причина проста – комбинация различных методов превентивного обнаружения приводит к повышению качества обнаружения;

- Безопасность на основе политик. Политика безопасности является необходимым атрибутом любой продуманной стратегии защиты от ИТ-угроз. Продуманная политика позволяет в несколько раз уменьшить риск заражения вредоносной программой, атаки хакеров или утечки конфиденциальной

информации. Простой пример – запрет на открытие вложенных файлов из электронных писем снижает риск заражения почтовым червем практически до 0. Запрет на использование сменных носителей также снижает риск проникновения вредоносного кода. К разработке политики всегда нужно подходить очень взвешенно и учитывать потребности и бизнес-процессы всех подразделений и работников компании;

- Intrusion Prevention System (IPS). Системы предотвращения вторжений предусматривают возможность закрытия наиболее часто используемых вредоносными программами уязвимостей компьютера перед новой угрозой еще до выхода обновления антивирусных баз: блокировка портов, т.е. возможности попадания инфекции на компьютер и ее дальнейшего размножения; создание политик для ограничения доступа к директориям или отдельным файлам; обнаружение источника инфекции в сети и блокировка дальнейших коммуникаций с ним. Данная технология отлично работает против атак хакеров и бесфайловых червей и вирусов, но против почтовых червей, классических вирусов и троянских программ IPS не эффективна;

- Защита от переполнения буфера (Buffer Overrun). Идея технологии – не допустить переполнения буфера для наиболее распространенных программ, сервисов Windows, включая Word, Excel, Internet Explorer, Outlook и SQL Server. При большинстве современных атак задействуются различные уязвимости, использующие переполнение буфера. Предотвращение переполнения буфера также можно отнести к проактивной защите, т.к. эта технология просто исключает использование такой уязвимости любым вредоносным кодом или атакой;

- Поведенческие блокираторы. Основная идея блокиратора – анализ поведения программ и блокировка выполнения любых опасных действий. Теоретически блокиратор может предотвратить распространение любого, как известного, так и неизвестного (написанного после блокиратора) вируса. Именно в этом направлении и движется большинство разработчиков антивирусного ПО. Примеров реализации данной технологии довольно

много. В последнее время большинство систем предотвращения распространения почтовых червей по механизму являются поведенческими блокираторами;

- Другие методы. Для защиты почтового трафика могут использоваться особые методы, основанные на анализе писем, проходящих через почтовый сервер. С помощью такого анализа можно остановить эпидемию в самом ее начале. Статистика, дающая основания подозревать начало эпидемии, может быть следующей: массовая рассылка или прием одинаковых вложений; массовая рассылка или прием одинаковых писем с различными вложениями; наличие двойного расширения у вложений и т.д. Кроме этого, возможен лингвистический анализ тел писем.

Суммируя все вышесказанное, можно говорить о том, что под проактивными методами защиты, предлагаемыми на рынке, понимается:

- поведенческий анализатор процессов для анализа поведения запущенных в системе процессов и обнаружения подозрительных действий, т.е. неизвестных вредоносных программ;

- устранение возможностей попадания инфекции на компьютер, блокировка портов, которые используются уже известными вирусами, и могут использоваться их новыми модификациями (IPS/IDS-компонент);

- недопущение переполнения буфера для наиболее распространенных программ и сервисов Windows, чаще всего используемых злоумышленниками для осуществления атаки (IPS/IDS-компонент);

- минимизация ущерба, причиненного инфекцией, предотвращение дальнейшего ее размножения, ограничение доступа к файлам и директориям; обнаружение и блокировка источника инфекции в сети (IPS/IDS-компонент).

Достоинства и недостатки различных проактивных методов детектирования, а также сравнение проактивных и сигнатурным методов представлены в приложении Г.

Таким образом, можно сказать, что технологии проактивной защиты превращаются в инструмент, предназначенный для домашнего и



корпоративного пользователя, и являются приоритетным направлением работы для компаний-разработчиков антивирусного ПО.

### **1.3 Место серверов (LAN/WAN/E-mail/Proxy/FireWall) и их взаимодействия в корпоративной сети**

Для определения предмета защиты необходимо рассмотреть общие вопросы, касающиеся корпоративных информационных сетей.

Локальные (ЛВС) – охватывающие ограниченную территорию (обычно в пределах удаленности станций не более чем на несколько десятков или сотен метров друг от друга, реже на 1...2 км); локальные сети обозначают LAN (Local Area Network).

Глобальные сети – Wide Area Networks (WAN) – объединяют территориально рассредоточенные компьютеры, которые могут находиться в различных городах и странах.

Корпоративные (масштаба предприятия) сети – совокупность связанных между собой ЛВС, охватывающих территорию, на которой размещено одно предприятие или учреждение в одном или нескольких близко расположенных зданиях.

Типовая сеть предприятия с большим количеством офисов, умеренным использованием Web и числом пользователей не менее 1000 будет иметь примерно такую структуру, которая изображена на рис. 1.4.

Межсетевой экран (firewall) – это устройство, представляющее собой универсальный компьютер с установленным на нем специальным программным обеспечением, который размещается между защищаемой сетью и внешними сетями, потенциальными источниками опасности. Межсетевой экран контролирует все информационные потоки между внутренней и внешними сетями, пропуская данные, в соответствии с заранее установленными правилами. Эти правила являются формализованным выражением политики безопасности, принятой на данном предприятии.

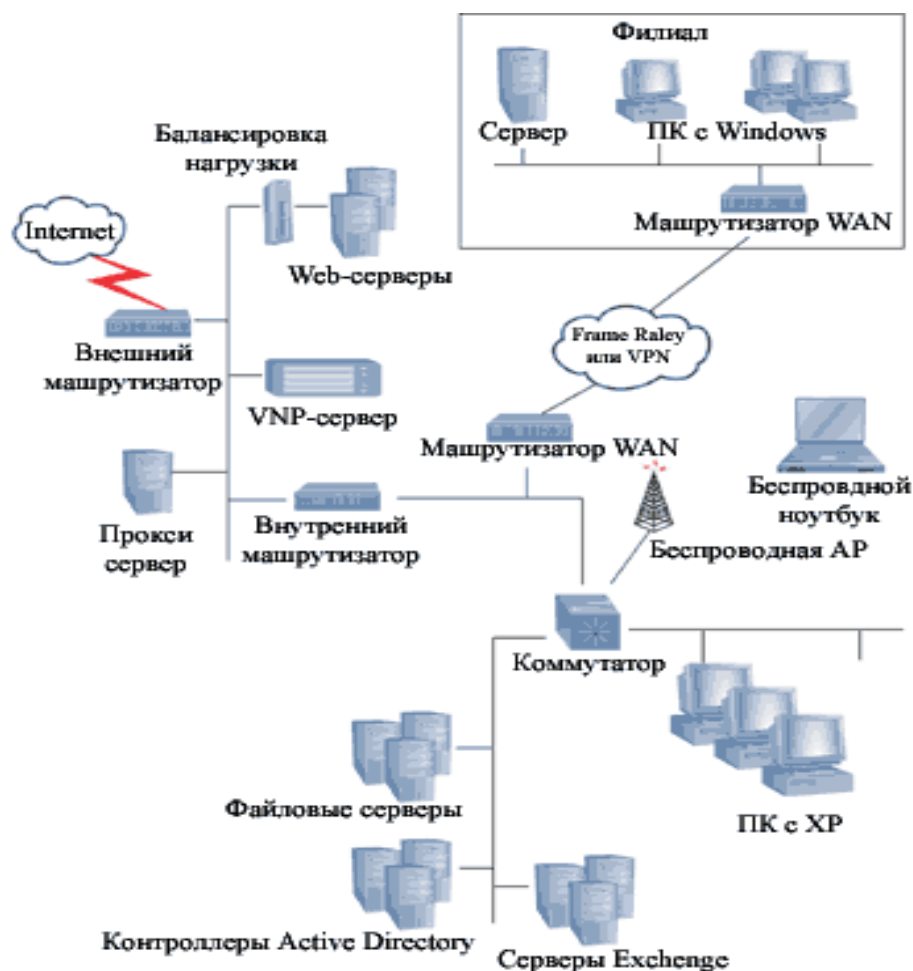


Рис. 1.4. Типичная сетевая топология предприятия.

Межсетевые экраны базируются на двух основных приемах защиты:

- пакетной фильтрации;
- сервисах-посредниках (proxyservices).

Эти две функции можно использовать как по отдельности, так и в комбинации.

Брандмауэр является защитным барьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра). Все входящие и исходящие пакеты должны проходить через брандмауэр, который пропускает только авторизованные пакеты.

При проектировании и построении брандмауэра можно использовать несколько вариантов. На рис.1.4 представлен один общий метод, когда внешний маршрутизатор подключается к Internet напрямую, а внутренний

маршрутизатор подключен к внутренней сети предприятия, а между ними располагается сетевой сегмент, содержащий несколько серверов, в том числе Web-серверы, устройства VirtualPrivateNetwork (VPN) и proxy-серверы для приложений. Этот промежуточный сетевой сегмент часто называется демилитаризованной зоной (Demilitarized Zone, DMZ). Предполагается, что серверы и устройства этого сегмента ненадежны, поскольку Internet-трафик непосредственно замыкается на устройствах DMZ. Таким образом, задача внутреннего маршрутизатора – защитить внутреннюю сеть предприятия от запрещенного трафика, который в действительности может исходить от злоумышленника, сумевшего скомпрометировать один из серверов DMZ и пытающегося проникнуть во внутреннюю сеть.

Брандмауэры не всегда реализуются с помощью маршрутизаторов или какой-либо иной аппаратуры. Программные маршрутизаторы могут играть ту же самую роль, что и аппаратные решения. Многие из них поддерживают интегрированный сервер VPN, который хостирует подключения VPN между внешними пользователями и внутренней сетью.

Технология защищенного канала (VPN) призвана обеспечивать безопасность передачи данных по открытой транспортной сети (Интернет). Защищенный канал включает в себя выполнение трех основных функций: взаимная аутентификация абонентов, защита передаваемых по каналу сообщений от несанкционированного доступа, подтверждение целостности поступающих по каналу сообщений.

Существует два способа образования VPN, которые представлены на рис. 1.5.

В первом случае (рис.1.5, а) программное обеспечение, установленное на компьютере удаленного клиента, устанавливает защищенный канал с сервером корпоративной сети, к ресурсам которого клиент обращается. Во втором случае (рис.1.5, б) клиенты и серверы не участвуют в создании защищенного канала - он прокладывается только внутри публичной сети с коммутацией пакетов, например внутри Интернет. Канал создается между



сервером удаленного доступа провайдера услуг публичной сети и пограничным маршрутизатором корпоративной сети.

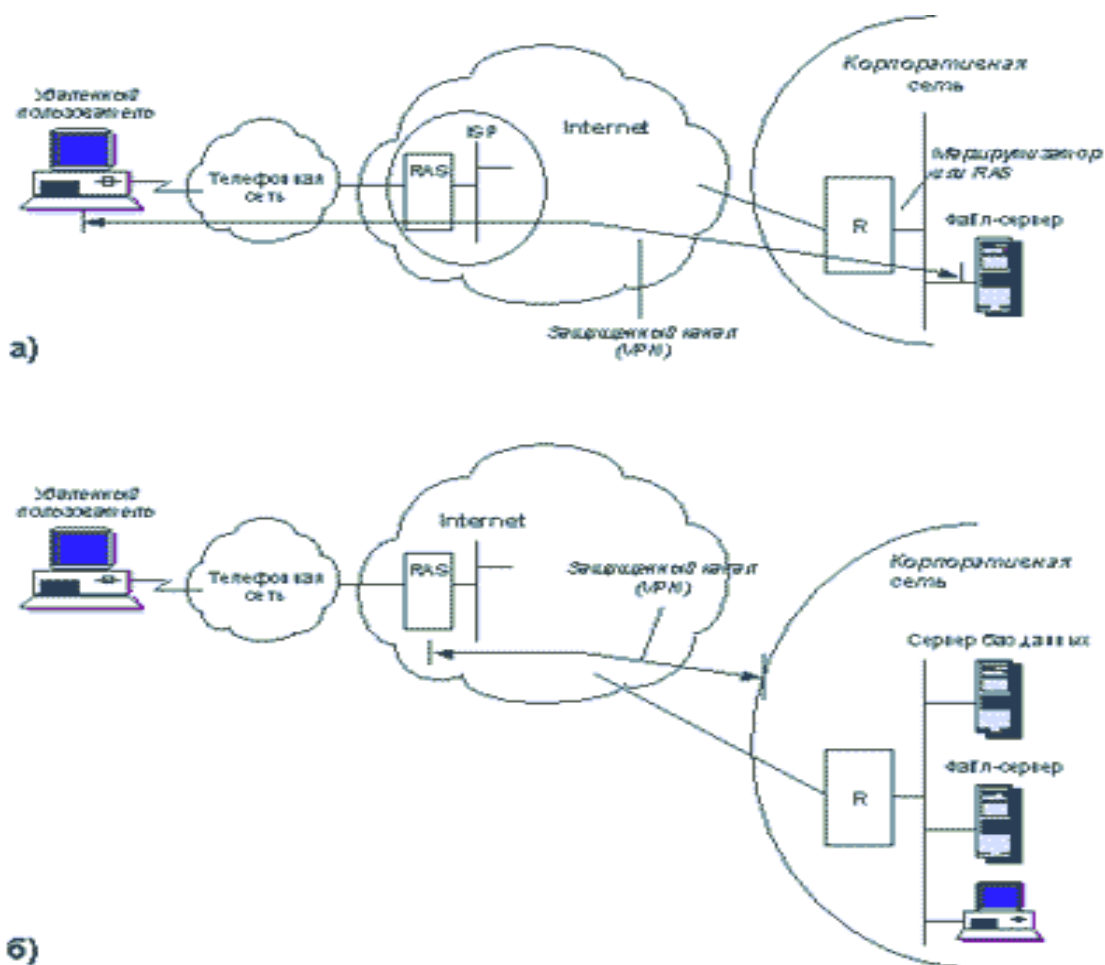


Рис.1.5 Схемы образования VPN: а) с помощью специального программного обеспечения конечных узлов; б) с помощью специального программного обеспечения шлюзов, стоящих на границе между частной и публичной сетями.

Прокси-серверы – общепринятый элемент сети предприятия. Прокси-сервер – это, как правило, программные решения (могут быть и аппаратные), которые обеспечивают информационные цепочки между хостами внутренней и внешней сети. Самый распространенный тип прокси-сервера – HTTP-прокси (известный также под названием Web-прокси), однако прокси-сервер можно использовать для самых разных типов прикладного трафика, включая FTP, Telnet, RPC-приложения и даже Internet Control Message Protocol (ICMP – Ping). Microsoft Internet Security and Acceleration (ISA) Server, работающий на базе Windows Server, – пример другого широко распространенного программного прокси-сервера. Прокси действуют как посредники между

внутренней и внешней сетью: запросы из внутренней сети во внешнюю замыкаются на них. Таким образом, между внутренней и внешней сетью (Интернет) непосредственное соединение отсутствует: проху-сервер выступает в роли связующего звена. Кроме того что тем самым достигается дополнительная безопасность сетевой работы, проху – удобное место для регистрации трафика между внутренней сетью и Интернет. Поскольку проху-серверы требуют доступа к внутренней и внешней сети, они обычно размещаются в DMZ или другом сегменте внутри сетевой топологии.

Теперь обратимся к использованию WAN во внутренней сети. Можно развернуть внутреннюю сеть WAN для подключения удаленных друг от друга территорий предприятия. В общем случае имеется всего два способа построения такой внутренней сети.

Первый (и наиболее распространенный) подход состоит в построении частной WAN с помощью собственной или внешней несущей сети. Второй подход к развертыванию WAN становится все более популярным и состоит в использовании VPN поверх Интернет для построения корпоративной сети. Применять VPN выгодно, поскольку Интернет в этом случае используется как магистральная сеть, доступная даже для самых удаленных офисов, о которой не приходится особенно беспокоиться. Недостатком развертывания VPN поверх Интернет (VPN-WAN) считается то обстоятельство, что гарантировать постоянную доступность Интернет (а следовательно, и VPN-WAN) нельзя. Аналогичное замечание касается и требуемой скорости доступа к Интернет. Если у организации имеется большое число офисов, необходимо развертывать и обслуживать устройства VPN на каждой площадке. И наконец, поскольку соединения VPN используют Интернет, злоумышленники теоретически могут взломать сеть и получить доступ к внутренним ресурсам корпорации. Таким образом, окончательный выбор, что развертывать на предприятии – частную WAN или решение на основе VPN, зависит от сложности проекта, затрат на его реализацию и требований к безопасности.

Наконец, использование беспроводных сетей (wireless networks) на предприятии (т. е. стандарты 802.11 или Wi-Fi и 802.11b). Беспроводные сети типичны для домашних пользователей и малого бизнеса, а развертывание беспроводной сети в крупных организациях сопряжено с рядом проблем, не последняя из которых – безопасность. Из трех стандартов Wi-Fi, используемых в настоящее время, 802.11b – наиболее популярный, и он был самым первым, обеспечившим полосу пропускания 11 Мбит/с. 802.11a и 802.11g – два конкурирующих стандарта высокоскоростных сетей Wi-Fi. Для развертывания беспроводных сетей требуется установка беспроводных точек доступа (Access Points, AP) для поддержки беспроводных пользователей. Беспроводные точки доступа, предназначенные для организаций, отличаются от своих домашних аналогов встроенным набором функций; тем не менее работают они примерно одинаково.

#### **1.4 Обзор антивирусных программных продуктов для корпоративных сетей**

Если сеть насчитывает сотни и тысячи компьютеров, то необходимо централизованное удаленное управление антивирусными программами и контроль их работы. Выполнять в "ручном" режиме такие операции, как отслеживание обновлений антивирусной базы данных и загрузочных модулей антивирусных программ, контроль эффективности обнаружения вирусов на рабочих станциях и серверах и т.п., затруднительно, если в сети много пользователей или если сеть состоит из территориально удаленных друг от друга сегментов.

Если же не обеспечить своевременное и эффективное выполнение перечисленных выше операций, технология антивирусной защиты корпоративной сети обязательно будет нарушена, что рано или поздно приведет к вирусному заражению.

В современных антивирусных системах реализованы следующие функции удаленного управления и контроля:



- установка и обновление антивирусных программ и антивирусных баз данных;
- централизованная дистанционная установка и настройка антивирусов;
- автоматическое обнаружение новых рабочих станций, подключенных к корпоративной сети, с последующей автоматической установкой на эти станции антивирусных программ;
- планирование заданий (таких, как обновление программ, обновление антивирусной базы данных, сканирование файлов и т. п.) для немедленного или отложенного запуска на любых компьютерах сети;
- отображение в реальном времени процесса работы антивирусов на рабочих станциях и серверах сети.

Сетевые центры управления позволяют управлять антивирусной защитой всей сети с одной рабочей станции системного администратора. Для ускорения установки антивирусов в удаленных сетях, подключенных к основной сети по медленным каналам связи, в этих сетях создаются собственные локальные дистрибутивные каталоги.

Все корпоративные программные комплексы имеют архитектуру «клиент-сервер», т.е. их компоненты устанавливаются на компьютеры локальной сети и обмениваются информацией через сетевые протоколы. К серверной части относится консоль управления, из которой выполняются все операции сканирования и мониторинга сети. Клиентская часть называется агентом рабочей станции. Совокупность компьютеров, на которых установлены взаимодействующие компоненты, называют антивирусной сетью.

При использовании клиент-серверной архитектуры, показанной на рис.1.6., основой сетевого центра управления служит антивирусный сервер, установленный на одном из серверов корпоративной сети. С ним взаимодействуют, с одной стороны, программы-агенты, установленные вместе с антивирусами на рабочих станциях сети, а с другой стороны – управляющая консоль администратора антивирусной защиты.

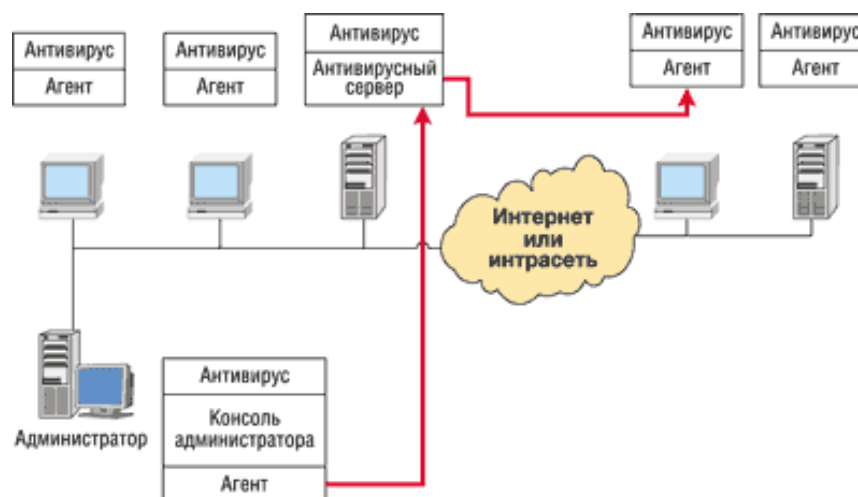


Рис.1.6. Взаимодействие консоли администратора, агентов и антивирусного сервера

Антивирусный сервер выполняет управляющие и координирующие функции. Он хранит общий журнал событий, имеющих отношение к антивирусной защите и возникающих на всех компьютерах сети, список заданий и расписание их выполнения. Антивирусный сервер отвечает за прием от агентов и передачу администратору антивирусной защиты сообщений о возникновении тех или иных событий в сети, периодически проверяет конфигурацию сети с целью обнаружения новых рабочих станций или рабочих станций с изменившейся конфигурацией антивирусных средств и т. д.

Помимо агентов, на каждой рабочей станции и сервере корпоративной сети устанавливается антивирус, выполняющий сканирование файлов и проверку файлов при их открытии. Результаты работы антивируса передаются через агентов антивирусному серверу, который их анализирует и протоколирует в журнале событий.

Управляющая консоль может представлять собой стандартное приложение Microsoft Windows с оконным интерфейсом или апплет (snap-in) управляющей консоли Control Panel ОС Microsoft Windows.

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

пользователей или доменов.

Существует также архитектура многоуровневой системы с Web-интерфейсом, проиллюстрированная на рис.1.7., которая предполагает использование Web-сервера в качестве ядра системы. В задачи этого ядра входит, с одной стороны, организация диалогового интерактивного взаимодействия с пользователем, а с другой - с программными модулями той или иной системы.



Рис.1.7. Антивирусная система с Web-интерфейсом

Преимущество такого подхода – унификация способов управления различными системами сети; кроме того, не требуется устанавливать на рабочую станцию администратора управляющие программы или консоли. Администрирование может выполняться с любого компьютера сети, а если она подключена к Интернету, то из любого места земного шара, где есть Интернет и компьютер с браузером. Для защиты управляющей информации при ее передаче по Интернету или корпоративной интрасети применяются протоколы SSH или аналогичные средства (например, собственные защищенные модификации протокола HTTP).

Эта схема аналогична той, что приведена была уже раньше. Различие между ними в том, что администратор антивирусной защиты управляет ее работой через браузер, а не через консольное приложение.

На рабочих станциях устанавливается антивирус, который управляется антивирусным сервером через агента.

На компьютере, играющем роль антивирусного сервера, устанавливается Web-сервер Microsoft IIS. Работающее на нем специальное Web-приложение управляет антивирусным сервером и предоставляет администратору пользовательский интерфейс для управления системой антивирусной защиты.

В рамках данной работы будем рассматривать антивирусный программный комплекс, предназначенный для предотвращения, проникновения и распространения вредоносного кода в корпоративную информационную сеть (КИС): Symantec – пакет Symantec Antivirus Corporate Edition сочетает постоянную эффективную защиту рабочих станций и сетевых серверов от вирусов и шпионских модулей с возможностями централизованного управления и администрирования. Symantec AntiVirus Corporate Edition автоматизирует защиту рабочих станций и сетевых серверов от вирусов и шпионских модулей, что позволяет максимально увеличить время бесперебойной работы систем в масштабах предприятия.



## **2 Разработка политики антивирусной защиты корпоративной сети**

### **2.1 Варианты построения схем корпоративных сетей**

К настоящему времени разработано значительное число разновидностей архитектурного построения сетей. Можно выделить несколько базовых вариантов построения корпоративных информационных сетей:

а) малая сеть с разделяемой средой передачи (коаксиальный кабель, витая пара, оптоволоконный кабель или в общем случае – совокупность кабельных сегментов, соединенных между собой повторителями). Этот вариант подходит для корпоративной сети, насчитывающей до 30 узлов.

б) сеть среднего размера (30-100 пользователей), имеющая выделенный сервер для выполнения прикладных задач (передача/прием почты, хранение баз данных и файлов, управление антивирусной защитой). В зависимости от масштаба сети конфигурация предусматривает выделение под каждую прикладную задачу отдельного сервера. Кроме того, для усиления защиты от несанкционированного доступа и обеспечения защиты данных при межсетевом взаимодействии используется Firewall.

в) территориально-распределенная сеть крупного масштаба (свыше 100 пользователей) с выделенными серверами, в доступе к которым нуждаются работники сети, мобильные пользователи и, возможно, сотрудники сторонних организаций и другие внешние пользователи. Для управления антивирусной защитой выделен отдельный сервер. Для усиления защиты от несанкционированного доступа и обеспечения защиты данных при межсетевом взаимодействии используется Firewall.

г) виртуальная локальная сеть – по сути, домен ширококвещательных кадров. Позволяет повысить полезную пропускную способность за счет локализации ширококвещательного трафика, формирования виртуальных рабочих групп из некомпактно (в плане подключения) расположенных узлов, а также обеспечивает безопасность.

д) сеть с разграничением доступа в Интернет на уровне IP-адресов – к примеру, все пользователи, за исключением пользователей с IP-адресами

рабочих станций 194.87.23.10... 194.87.23.17, имеют выход в Интернет.

Определившись с предметом защиты, необходимо рассмотреть цели, функции и задачи защиты информации в корпоративных сетях, а в частности антивирусной защиты информации.

## **2.2 Цели и задачи создания системы антивирусной защиты.**

### **Основные функции**

Во многом функционирование корпоративной сети зависит от правильной организации антивирусной защиты.

Цель антивирусной защиты – блокировать все возможные точки проникновения вирусов, такие как:

– проникновение вирусов на рабочие станции при использовании на рабочей станции инфицированных файлов с переносимых источников (флоппи-диски, компакт-диски, Zip, Jazz, Floptical и т. д.);

– заражение вирусами с помощью бесплатного инфицированного программного обеспечения, полученного из Интернета через web или FTP и сохраненного на локальной рабочей станции;

– проникновение вирусов при подключении к корпоративной сети инфицированных рабочих станций удаленных или мобильных пользователей;

– заражение вирусами с удаленного сервера, подсоединенного к корпоративной сети и обменивающегося инфицированными данными с корпоративными серверами файл-приложений и баз данных;

– распространение электронной почты, содержащей в приложениях файлы Excel и Word, инфицированные макровирусами.

Основными рубежами антивирусной защиты типовой корпоративной сети (ТКС) являются:

- защита внешнего сетевого периметра;
- защита корпоративных файловых серверов;
- защита серверов коллективной работы;

- защита рабочих мест пользователей;
- управление корпоративной политикой антивирусной защиты.

Для защиты ТКС от вирусов необходимо решить следующие основные задачи:

1. Прежде всего, должны быть перекрыты все возможные каналы распространения вирусов. Основными каналами распространения вирусов в настоящее время являются:

- электронная почта;
- HTTP/FTP сервисы, используемые для получения доступа к ресурсам ЛВС и сети Интернет;
- съемные носители информации (дискеты, CD-ROM и т. п.);
- файловые серверы ЛВС (UNiX/Windows/NetWare);
- системы коллективной работы (MS Exchange, Lotus Notes и т. п.).

2. На следующем этапе должна быть обеспечена антивирусная защита серверов ЛВС и рабочих мест пользователей.

Подобная многоуровневая распределенная система должна быть положена в основу разработки технологии защиты от вирусов, поскольку только так можно обеспечить максимальную защиту. При этом вирус лишается возможности найти в сети нишу, в которой его существованию ничто не угрожает.

Для решения поставленных задач система антивирусной защиты должна выполнять следующие основные функции:

- непрерывный антивирусный мониторинг внешнего и внутреннего SMTP/HTTP/FTP трафика;
- централизованный антивирусный мониторинг и регулярное сканирование файловых систем на рабочих местах пользователей, серверах ЛВС и серверах коллективной работы;
- регистрацию и оповещение о событиях, связанных с вирусными атаками;
- централизованное управление всеми компонентами антивирусной

защиты;

– помещение подозрительных файлов и неизвестных вирусов, выявленных с использованием эвристических алгоритмов, на карантинный сервер для их последующего анализа.

В общем случае, антивирусная защита информационной системы должна строиться по иерархическому принципу, проиллюстрированному на рис.2.1.



Рис.2.1. Модульность системы антивирусной защиты

Службы всех уровней объединяются в единую вычислительную сеть (образуют единую инфраструктуру) посредством локальной вычислительной сети. При этом службы общекорпоративного уровня должны функционировать в непрерывном режиме.

Антивирусная система должна предоставлять следующие виды сервисов:

- получение обновления программного обеспечения и антивирусных баз;
- управление распространением антивирусного программного обеспечения;
- управление обновлением антивирусных баз;
- контроль за работой системы в целом (получение предупреждений об обнаружении вируса, регулярное получение комплексных отчетов о работе системы в целом);

на уровне подразделений:

- обновление антивирусных баз конечных пользователей;
- обновление антивирусного программного обеспечения конечных пользователей, управление локальными группами пользователей;



на уровне конечных пользователей:

– автоматическая антивирусная защита данных пользователя.

Основные функции современных механизмов антивирусной защиты:

- поиск и удаление вирусов из всех типов файлов, оперативной памяти и загрузочных секторов сканером, контроль памяти резидентным монитором;
- контроль изменения файлов;
- фоновый перехват скрипт-вирусов, защита от макро-вирусов поведенческим блокиратором;
- удаление вирусов из архивов распространенных форматов (ZIP, ARJ, RAR и др.);
- эвристический анализ для поиска неизвестных, зашифрованных и "невидимых" (stealth) вирусов;
- обновление антивирусных баз;
- возможность настройки для интеграции в различные программные среды.

Антивирусные средства защиты компьютерных сетей обеспечивают дополнительные функциональные возможности:

- управление одним или несколькими серверными антивирусами с удаленного рабочего места по локальной или глобальной сети;
- управление антивирусами по SNMP-протоколу;
- автоматическую проверку файлов при доступе по сети (scan on access);
- отключение от сети зараженных станций (карантин);
- инициирование запуска персональных антивирусных средств на рабочих станциях;
- централизованное обновление антивирусных баз с удаленного узла;
- автоматическое сканирование входящей и исходящей почты почтового сервера;
- периодическое сканирование всех файлов;
- централизованное ведение отчетов и рассылка предупреждений по

электронной почте о вирусной активности в сети;

- разграничение прав по управлению и конфигурированию средств антивирусной защиты;
- автоматическое сканирование информации, проходящей через межсетевые экраны, в том числе автоматическую проверку проходящего через экран трафика.

### **2.3 Сбор информации о системе. Инвентаризация информационных задач**

Во время выполнения этого этапа выпускной работы необходимо было собрать и систематизировать информацию о структурной схеме ТКС с указанием мест подключения ее к внешним сетям передачи данных, а также подключенных к системе рабочих станциях и серверах (определение так называемой программно-аппаратной конфигурации рабочих мест и серверов). Важным явился и этап инвентаризации информационных задач. Наличие данной информации позволяет существенно облегчить работу на следующих этапах, а зачастую позволяет дать рекомендации по оптимизации системы и повышению уровня защиты информации в целом.

Рассмотренные базовые варианты построения корпоративных информационных сетей сводятся к типовой схеме корпоративной сети, изображенной на рис.2.2, поскольку алгоритмы антивирусной защиты не зависят от масштабов сети, а VPN-технология имеет отношение к шифрованию, что опять же никак не связано с антивирусной защитой. А значит, идеология защиты от вирусов во всех приведенных случаях следует одинакова.

Итак, возьмем за основу ТКС, которая использует внешнюю (через сети общего пользования WAN) и внутреннюю корпоративную почту, состоит из нескольких серверов баз данных, почтовых серверов и Proxy-сервера на платформах Microsoft, Novell, Linux (к примеру, трех файл-серверов на Windows Server 2003, E-mail сервера на Novell NetWare 6.0 и Proxy-сервера

на Linux RedHat 9.0) и 50 рабочих станций.

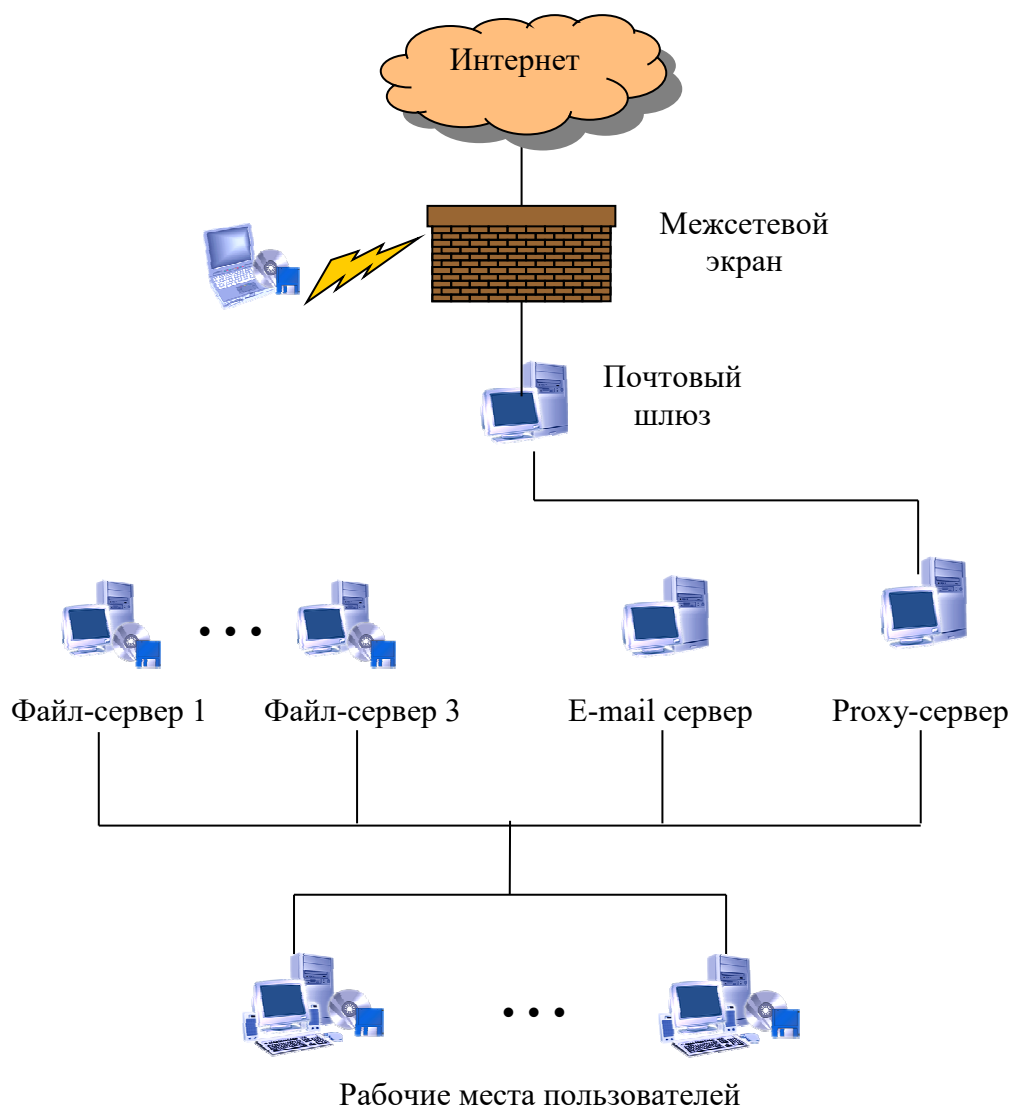


Рис.2.2. Типовая схема корпоративной сети

На файл-серверах хранятся базы данных, к которым идет постоянное обращение с рабочих станций. Выход в Интернет имеют только mail-сервер и половина рабочих станций (доступ через проху-сервер). Таким образом, наиболее важным для сети является бесперебойная связь рабочих станций с серверами. Значит нужно предупредить в первую очередь появление в сети вирусов, увеличивающих сетевой трафик.

Инвентаризация информационных задач приведена в таблице 2.1.

## Инвентаризация информационных задач

Наименование	Назначение	Используемое ПО		Разграничение доступа пользователей	Узлы обработки	Узлы хранения
		-Клиент	-Сервер			
Корпоративная почта	Обеспечение всех сотрудников компании почтовыми ящиками и рассылка почты	Wise Group клиент	Wise Group сервер	Администратор Оператор Бухгалтер	Рабочие места пользователей	E-mail сервер
Административная деятельность	Информационное обеспечение административной деятельности в компании	Клиентская часть ALFA	ALFA	Администратор	Рабочие места пользователей, сервера	Сервера
Внешний и внутренний документооборот	Обеспечение внешнего и внутреннего электронного обмена бухгалтерскими документами	Клиентская часть 1С	Серверная часть 1С	Администратор Бухгалтер	Рабочие места пользователей	Файл - сервер 1 и 2

## 2.4 Категорирование информационных ресурсов

Для формулировки требований к системе безопасности информационной системы, необходимо определить – что нужно защищать.

Вся информация делится на открытую и информацию ограниченного распространения, которая в свою очередь делится на конфиденциальную и информацию, составляющую государственную тайну.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Республики Узбекистан.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Республики



Узбекистан.

В соответствии с представленной классификацией категорирование обрабатываемой в ТКС информации представим в виде таблицы 2.2.

Таблица 2.2.

### Категорирование информации

Вид информации	Категория	Степень доступности
Информация отдела продаж	Конфиденциально	В рабочее время
Информация отдела поставок	Конфиденциально	В рабочее время
Бухгалтерская информация	Строго конфиденциально	В рабочее время
Информация о клиентах, прочая административная информация	Конфиденциально	В рабочее время
Корпоративная почта	Конфиденциально	Круглосуточно

## 2.5 Анализ угроз и рисков с точки зрения антивирусной защиты

### 2.5.1 Угрозы и риски в информационных системах

Для построения эффективной системы информационной безопасности, необходимо определить, откуда могут исходить угрозы, перечень рисков и вероятность их наступления по каждой из возможных угроз. Для примера рассмотрим сеть ТашИИТ.

Потенциальные угрозы принято условно разделять на четыре основных типа: внешние, внутренние, непреодолимые и прочие.

Масштаб внешних угроз значительно вырос с массовым распространением Интернет и систем электронной коммерции. Основными источниками внешних угроз являются:

- хакеры, которые находятся на нижней ступени иерархии внешних угроз (но будучи объединенными в ассоциации и союзы, предоставляющие возможность обмена опытом, могут составить серьезную угрозу);

- мошенники и информационные брокеры. Информационные брокеры собирают информацию из различных источников и (или) продают ее заинтересованным лицам, или используют ее в личных целях. Мошенники работают в сферах, способных принести быстрый доход с помощью использования ложной или искаженной информации.

- кибервоины. Находятся на вершине иерархии внешних угроз.

Представлены, как правило, профессионалами информационных технологий. Знают каждую лазейку в системах защиты и способны ей воспользоваться. Имеют доступ к сети телекоммуникаций.

Внутренние угрозы имеют самое различное происхождение. Некоторые из них являются преднамеренными, другие носят случайный характер. По некоторым данным нарушения распределяются в пропорции, приведенной на рис 2.3.



Рис. 2.3. Внутренние угрозы

Некомпетентность, беспечность, отсутствие или слабость системы защиты информации составляют типичный набор атрибутов случайных нарушений системы информационной безопасности. Проблема внутренней безопасности заключается в основном в организации и управлении системой безопасности внутри самого предприятия.

Что касается преднамеренных нарушений системы безопасности, то здесь проблема касается, в основном, сотрудников предприятия, имеющих доступ к конфиденциальной информации. Эти проблемы гораздо шире проблем безопасности информации в компьютерных системах и относятся в первую очередь к задачам подбора и управления персоналом.

Оборудование и программы также могут содержать ошибки проектирования и конфигурирования, что может привести к сбоям в работе ТКС и потере данных.

Непреодолимые угрозы включают катастрофы природного характера, такие как ураганы, наводнения, поражения молнией, а также террористические акты и войны. От таких угроз трудно защититься, но наличие плана действий на случай возникновения такого рода воздействий позволит не только уменьшить риски, но и сократить время на

восстановление работоспособности системы после катастрофы.

В категорию прочие угрозы попадают все прочие угрозы, не вошедшие в предыдущие. Например, компьютерные вирусы вначале представляют собой внешнюю угрозу и предполагают средства защиты от внешнего проникновения. После того, как вирус проник в информационную систему, он становится источником внутренней угрозы.

На основании представления о вероятных угрозах строят матрицу рисков с учетом текущего состояния информационной системы.

Риск – стоимостная оценка вероятностного события, ведущего к потерям (ущербу). Риск позволяет оценить вероятность того, что некоторая величина финансового ущерба будет находиться в определенных количественных пределах.

### **2.5.2 Угрозы и риски с точки зрения антивирусной защиты**

Оценим угрозы безопасности для сети ТашИИТ с точки зрения антивирусной защиты. Основные из них:

1. Недисциплинированность пользователей (отключение систем антивирусной защиты; не соблюдение правил работы в компьютерной сети, принятых в организации; установка программ, загруженных из Интернета, без разрешения администраторов сети и соответствующей проверки службой безопасности).

2. Нерегулярное обновление средств защиты информации (в том числе антивирусных баз данных).

3. Ограниченный состав информационной службы, следящей не только за состоянием программно-аппаратного комплекса, но и решающей целый комплекс дополнительных вопросов (от обучения пользователей до закупок расходных материалов).

4. Отсутствие специализированных систем централизованного контроля за работой информационной системы и действиями пользователей.

На рис. 2.4. стрелками показаны наиболее вероятные пути проникновения вирусов в сеть ТашИИТ:

1. Попадание вирусов через рабочие станции пользователей с переносных носителей, содержащих электронные документы от клиентов и партнеров по бизнесу (наиболее вероятно проникновение макро-вирусов).

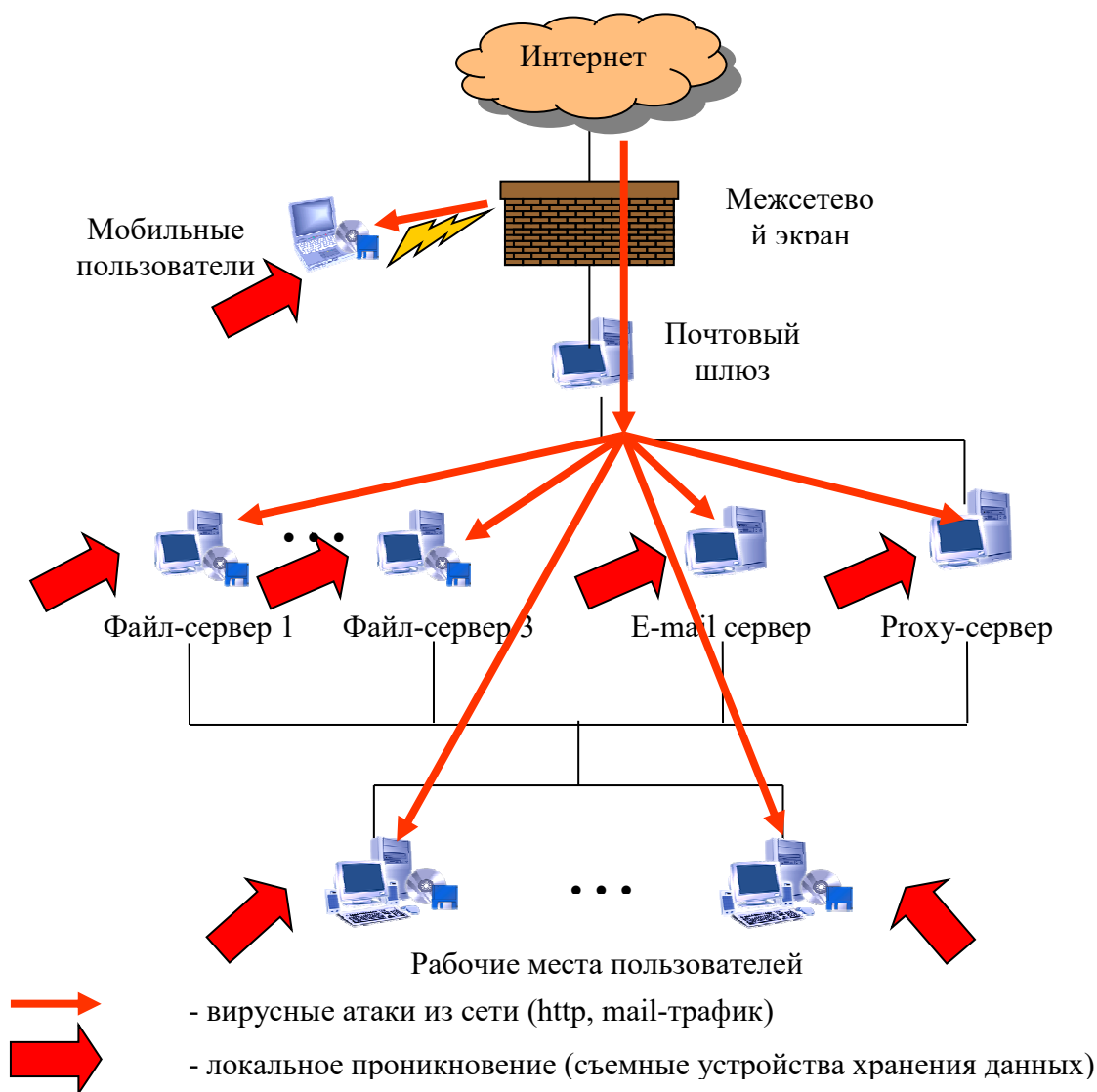


Рис.2.4. Наиболее вероятные пути проникновения вирусов в сеть ТашИИТ

2. Попадание вирусов через рабочие станции пользователей из зараженных программ, полученных из Интернет (потенциально – достаточно разнообразный набор вирусов, начиная со «стареньких» бутовых и заканчивая новейшими Интернет-червями).

3. Проникновение из Интернет и внутреннее распространение через систему электронной почты.

4. Распространение вирусов, полученных из различных источников, на все информационные устройства, подключенные к сети, через файл-сервер.

5. Проникновение вирусов через серверы, установленные в сети, в результате халатности сотрудников информационной службы (например, установка прикладного серверного ПО, полученного из сомнительных источников, без надлежащей проверки).

На основании этих данных построена матрица рисков угрозы вирусного вторжения, представленная в табл.2.3.

Таблица 2.3.

Матрица рисков угрозы вирусного вторжения

№	Событие	Описание рисков	Вероятность наступления	Оценка риска для бизнеса
1	Несанкционированная передача информации, просмотр баз данных и передаваемой информации (нарушение конфиденциальности)	Получение информации о входных ценах продукции, получаемой от поставщиков. Утечка информации о суммах ежедневного денежного оборота организации	Низкая	Низкий
2	Несанкционированная модификация передаваемых данных (нарушение целостности и достоверности)	Неправильное оформление документации на поступивший/проданный товар. Задержка оформления приема/продажи продукции. Получение недостоверных данных об оплате продукции. Несвоевременное оформление платежных переводов. Формирование недостоверной статистики покупки/продажи продукции.	Средняя	Высокий
3	Несанкционированная модификация баз данных (нарушение целостности и достоверности)	Формирование неверной информации о стоимости/наличии продукции. Формирование недостоверной информации о состоянии оплаты счетов, ежедневного денежного оборота в организации.	Средняя	Высокий
4	Сбои в работе программного обеспечения	Материальные потери на восстановление информации и штрафы за несвоевременную сдачу отчетностей	Высокая	Средний
5	Загрузка сетевого трафика	Замедление работы, нарушение нормального режима функционирования оборудования (атаки DoS)	Высокая	Средний



## **2.6 Оценка возможных реализаций антивирусной защиты серверов и выбор варианта защиты**

Наибольшую эффективность в противодействии вирусным атакам будет представлять комплексный подход. Комплексность предполагает согласованное применение правовых, организационных и программно-технических мер, перекрывающих в совокупности все основные каналы реализации вирусных угроз. В соответствии с этим подходом в организации должен быть реализован следующий комплекс мероприятий:

- меры по выявлению и устранению уязвимостей, на основе которых реализуются вирусные угрозы. Это позволит исключить причины возможного возникновения вирусных атак;

- меры, направленные на своевременное обнаружение и блокирование вирусных атак и спама;

- меры, обеспечивающие выявление и ликвидацию последствий вирусных угроз. Данный класс мер защиты направлен на минимизацию ущерба, нанесённого в результате реализации вирусных угроз.

Важно представлять, что эффективная реализация вышеперечисленных мер на предприятии возможна только при условии наличия нормативно-методического, технологического и кадрового обеспечения антивирусной безопасности.

Нормативно-методическое обеспечение антивирусной безопасности предполагает создание сбалансированной правовой базы в области защиты от вирусных угроз. Для этого в компании должен быть разработан комплекс внутренних нормативных документов и процедур, обеспечивающих процесс эксплуатации системы антивирусной безопасности. Состав таких документов во многом зависит от размеров самой организации, уровня сложности АС, количества объектов защиты и т.д. Так, например, для крупных организаций основополагающим нормативным документом в области защиты от вредоносного кода должна быть концепция или политика антивирусной безопасности. Для небольших компаний достаточно разработать

соответствующие инструкции и регламенты работы пользователей, а также включить требования к обеспечению антивирусной защиты в состав политики информационной безопасности организации.

В рамках кадрового обеспечения антивирусной безопасности в компании должен быть организован процесс обучения сотрудников по вопросам противодействия вирусным угрозам. Программа обучения должна быть направлена на минимизацию рисков, связанных с ошибочными действиями пользователей, приводящих к реализации вирусных атак. Примерами таких действий являются: запуск приложений с непроверенных внешних носителей, использование нестойких к угадыванию паролей доступа, загрузка ActiveX-объектов с недоверенных Web-сайтов и др. В процессе обучения должны рассматриваться как теоретические, так и практические аспекты антивирусной защиты.

Процесс повышения уровня компетенции сотрудников компании должен включать в себя как теоретические, так и практические аспекты проблемы антивирусной защиты. При этом программа обучения должна состояться в зависимости от должностных обязанностей сотрудника, а также от того к каким информационным ресурсам он имеет доступ.

Технологическое обеспечение должно быть направлено на создание комплексной системы антивирусной защиты (КСАЗ), которая помимо антивирусов дополнительно должна включать в себя подсистемы защиты от спама, обнаружения и предотвращения атак, выявления уязвимостей, сетевого экранирования, резервного копирования и подсистемы управления.

Комплексность предполагает замкнутый жизненный цикл системы антивирусной защиты, представленный на рис. 2.5.

В любом случае, комплексное решение в области антивирусной защиты предполагает:

- защиту максимально возможного числа путей проникновения и распространения вирусов внутри предприятия;
- построение централизованной и структурированной системы

управления антивирусным ПО;

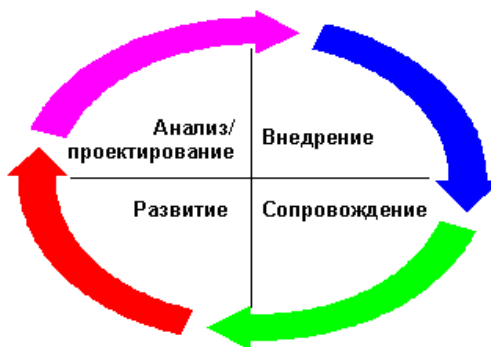


Рис. 2.5. Жизненный цикл системы антивирусной защиты

- обеспечение регулярного обновления антивирусных баз и антивирусного ПО;
- интеграцию процессов поддержания работоспособности системы антивирусной защиты с имеющимися процессами обеспечения безопасности информации;
- обучение и поддержание уровня знаний администраторов;
- разработка и внедрение правил элементарной антивирусной безопасности среди обычных пользователей;
- разработку и внедрение процессов развития системы антивирусной защиты в условиях постоянного изменения количественных и качественных характеристик вычислительной системы, ее развития и реорганизации.

## 2.7 Защита серверов всех типов по всем информационным каналам

Структура обычной сети включает такие элементы, как рабочие станции (мобильные и стационарные), файловые серверы и серверы приложений (физические и логические), почтовые шлюзы и web-серверы. Вместе с тем продуманная система антивирусной защиты сети – это не просто установка специализированного антивирусного ПО. Более того, такой подход к проблеме может привести к неправильному или неэффективному функционированию вычислительных мощностей предприятия. В результате может снизиться производительность сети в целом и антивирус пропустит вирусную атаку, последствия чего трудно предсказать.

При построении антивирусной защиты (АВЗ) необходим комплексный подход, при котором защита от вирусов сегментов сети работала бы как совокупность взаимосвязанных и взаимодополняющих элементов. Схема вирусной атаки представлена на рис. 2.6. В связи с этим необходим контроль мест хранения данных и каналов их передачи, а также равномерное распределение нагрузки на элементы корпоративной сети.

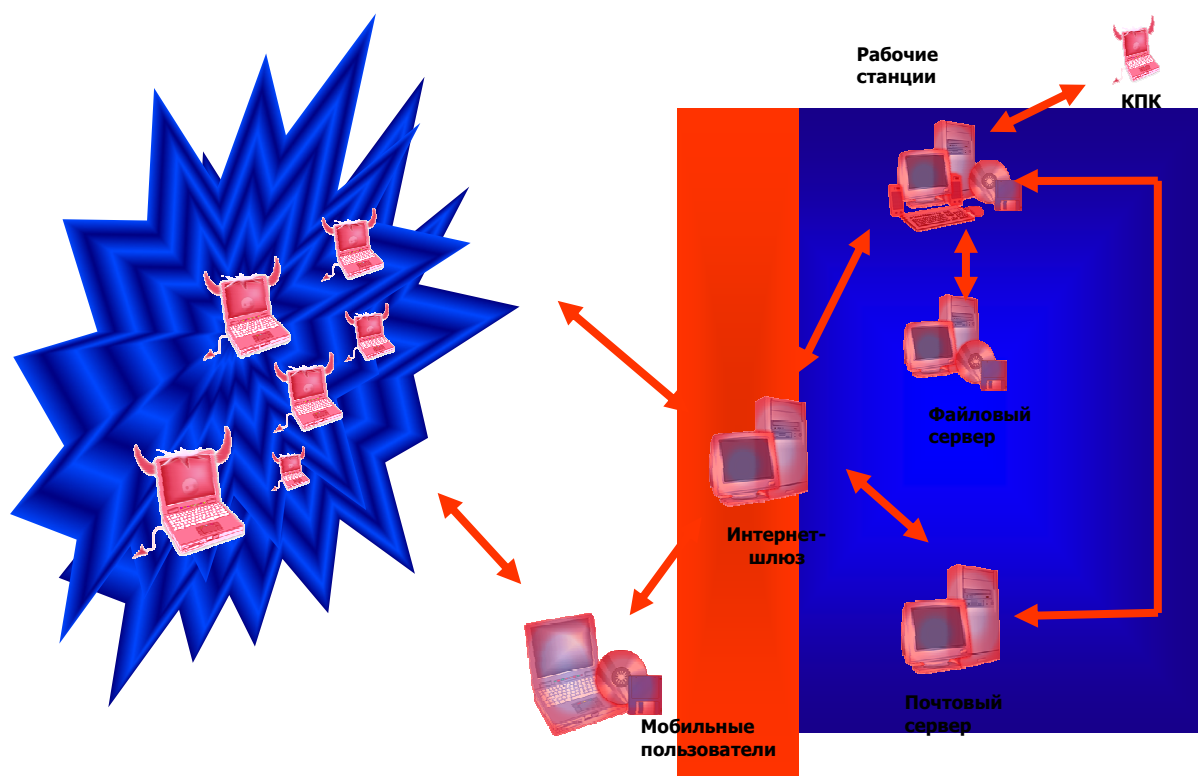


Рис. 2.6. Схема вирусной атаки

Рабочие станции являются наиболее уязвимым местом в защите корпоративной сети, поскольку управляются наименее опытными в плане "вирусоустойчивости" пользователями. Сквозь них проникает до 95% всех вредоносных программ. В этой связи важно максимально исключить человеческий фактор и установить соответствующее антивирусное ПО. "Соответствующее" означает, во-первых, антивирусный монитор, проверяющий все используемые на компьютере объекты в масштабе реального времени, т.е. в момент попытки их запуска. В случае попытки выполнения зараженного файла монитор автоматически сообщит об инциденте пользователю и системному администратору, которые смогут

своевременно принять необходимые меры. Во-вторых, ежедневно все локальные диски рабочих станций должны проходить всеобъемлющую проверку антивирусным сканером с максимальной глубиной поиска. Максимальная глубина поиска подразумевает применение эвристического анализатора кода и избыточного сканирования. Обе технологии требуют больших затрат вычислительных ресурсов компьютера, однако вряд ли это будет принципиально, если сканирование проводится уже, например, по окончании рабочего дня.

Также необходимо исключить возможность изменения параметров и отключения антивирусов локальными пользователями.

Все эти действия проводятся удаленно и в полностью автоматическом режиме с помощью интегрированных технологий, в антивирусные продукты.

Другим уязвимым элементом корпоративной сети является почтовый шлюз, через который проходит электронная корреспонденция предприятия. По некоторым данным более 80% всех зарегистрированных вирусных инцидентов происходит именно через электронную почту, т.к. электронная почта – это идеальный транспорт для компьютерных вирусов.

Основным правилом является защита всех узлов и установка многоуровневой системы фильтрации всей почтовой корреспонденции. Наиболее распространенной структурой размещения опорных пунктов антивирусной защиты является так называемая схема 2+1. Схема подразумевает установку антивирусного модуля на корпоративный почтовый сервер, который осуществляет первичную проверку поступающих сообщений. В связи с нагрузкой, которая ложится на почтовый сервер, рекомендуется настраивать антивирусный модуль на минимальное потребление системных ресурсов, т.е. отключать такие функции, как избыточное сканирование, эвристический анализ, проверка архивированных и сжатых файлов.

Второй уровень защиты составляет специальное антивирусное ПО, устанавливаемое на рабочих станциях, подключенных к службе электронной



почты. Оптимальным вариантом является использование антивирусных модулей, интегрированных в локальные почтовые клиенты. Здесь рекомендуется включить все имеющиеся инструменты защиты от вирусов: это будет несколько замедлять работу компьютера, однако никак не скажется на функционировании сети в целом. Существует альтернатива интегрированным антивирусным модулям – антивирусные мониторы, которые в масштабе реального времени проверяют все используемые объекты. Однако первый вариант все же является более предпочтительным, потому как проверяет все входящие и исходящие сообщения сразу же после их получения или отправления, в то время как мониторы способны распознать вредоносный код, только когда пользователь попытается его запустить. Кроме того, антивирусный модуль способен не только обнаруживать, но и успешно лечить зараженные сообщения.

В-третьих, необходимо использовать и классический антивирусный сканер, способный проверять сетевые и локальные диски. Это необходимо для проведения регулярных (не менее 1 раза в день) проверок почтовых баз, хранящихся на сервере и рабочих станциях. Данное обстоятельство накладывает определенные требования на используемый антивирус, а именно поддержку различных форматов почтовых баз.

Опасным рассадником вирусов могут также стать файловые серверы и серверы приложений, совместно используемые сразу многими сотрудниками предприятия. На серверы, как и на рабочие станции, необходимо устанавливать антивирусные мониторы, проверяющие файлы "на лету", и регулярно проводить полномасштабную проверку антивирусным сканером. Как и в случае с почтовыми шлюзами, для оптимизации работы сервера рекомендуется отключать некоторые инструменты борьбы с вирусами (эвристический анализатор и пр.) на уровне сервера и возлагать эту задачу на клиентские антивирусные программы.

В качестве дополнительного барьера на пути вирусов в сеть предприятия рекомендуется установить специальный антивирусный модуль на

корпоративный межсетевой экран, который сможет проводить антивирусную фильтрацию всех входящих и исходящих потоков данных.

Наконец, корпоративный web-сервер, который является предметом открытого доступа, к которому могут обращаться не только сотрудники компании, но и любой желающий. Источниками вирусов могут быть внутренние сетевые ресурсы и внешний взлом. Первая проблема решается реализацией описанной выше структуры антивирусной защиты. Причинами взлома могут быть недавно обнаруженные "дыры" в системах безопасности, перехват или простой подбор паролей доступа к web-серверу. Для исключения такой возможности можно использовать специализированные ревизоры изменений. В случае нарушения целостности информации ревизор мгновенно оповестит о произошедшем инциденте системного администратора и восстановит первоначальное содержимое сервера.

С учетом вышеизложенного схему защищенной компьютерной сети можно представить, как показано на рис. 2.7.

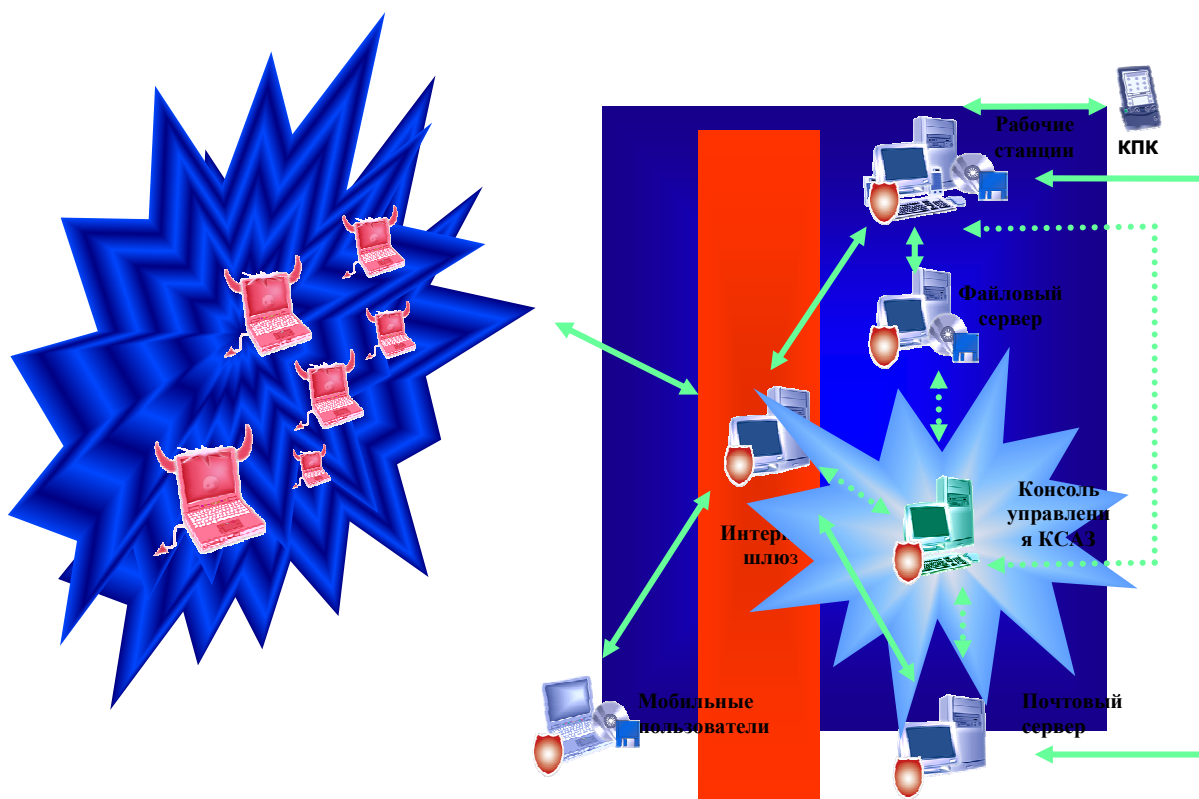


Рис.2.7. Защищенная компьютерная сеть

### **3. Внедрение антивирусного программного обеспечения. Разработка рекомендаций и методик применения антивирусных средств**

#### **3.1 Технология внедрения антивирусного ПО**

Методические рекомендации по построению и технологии внедрения системы АВЗ для сети ТашИИТ предлагается реализовать в виде блок-схемы алгоритма на рис.3.1. Разрабатываемые рекомендации предназначены для защиты корпоративных сетей любых масштабов. Построение системы АВЗ информации предлагается реализовать в виде последовательности этапов, следующих друг за другом.

1 этап. Проведение анализа объекта защиты и определение основных угроз:

- аудит состояния компьютерной системы и средств обеспечения АЗ;
- анализ возможных сценариев реализации потенциальных угроз, связанных с проникновением вирусов.

2 этап. Разработка политики антивирусной защиты:

- классификация, составление перечня и определение необходимого уровня защиты информационных ресурсов организации от вирусных атак;
- определение структуры и состава подразделений, обеспечивающих антивирусную защиту, с разделением полномочий и обязанностей;
- организация административно-правовой поддержки антивирусной защиты, разработка документов, определяющих обязанности и ответственность различных групп пользователей за соблюдение правил антивирусной защиты;
- определение требований к системе и средствам антивирусной защиты;
- расчет затрат на обеспечение антивирусной безопасности.

3 этап. Разработка плана антивирусной защиты:

- разработка требований и выбор средств антивирусной защиты локальных и удаленных серверов и рабочих станций, приложений, электронной почты, шлюзов Интернет, межсетевых экранов и других элементов сети;
- разработка организационных мероприятий для обеспечения политики антивирусной защиты с учетом результатов анализа рисков: периодический

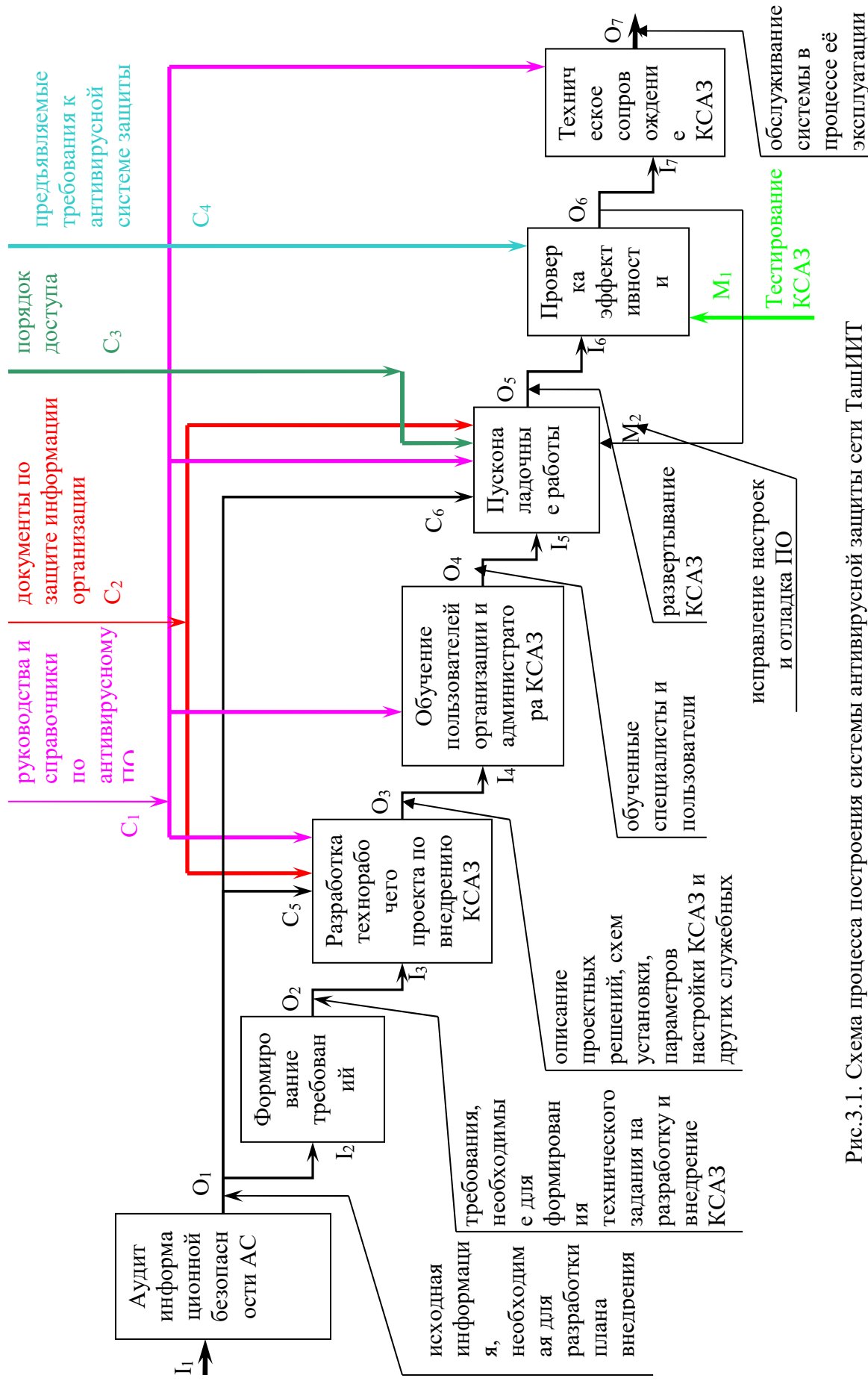


Рис.3.1. Схема процесса построения системы антивирусной защиты сети ТашИИТ

- анализ состояния антивирусной защиты; план и порядок обновления антивирусных средств; контроль за соблюдением персоналом инструкций по обеспечению антивирусной безопасности; план обучения пользователей.

4 этап. Реализация плана антивирусной безопасности:

- поставка средств антивирусной защиты;
- интеграция антивирусных и других защитных технологий в единую систему сетевой безопасности корпоративной сети;
- организация технической поддержки.

### **3.2 Порядок и схема инсталляции антивирусного ПО для сети ТашИИТ**

Необходимо отметить, что сам процесс развертывания КСАЗ представляет собой сложный многоступенчатый процесс, который включает в себя следующие основные этапы:

- инсталляция антивирусного программного обеспечения на файловые серверы и рабочие станции: установлен корпоративный продукт Symantec AntiVirus Corporate Edition версии 10.0;

- инсталляция антивирусного программного обеспечения на почтовый сервер: установлено программное обеспечение Symantec Mail Security, которое предназначено для защиты корпоративных систем обмена сообщениями и групповой работы на основе Microsoft Exchange Server или IBM Lotus Domino;

- инсталляция программно-аппаратного комплекса для контроля входящих информационных потоков: установлен аппаратно-программный комплекс Symantec Gateway Security, который защищает от угроз, связанных с работой в Интернете. Аппаратно-программный комплекс Symantec Gateway Security обеспечивает защиту в масштабах предприятия и располагается на шлюзе между Интернетом и корпоративной сетью или между сегментами сети. Комплекс объединяет: межсетевой экран с анализом трафика; модули обнаружения и предупреждения вторжений, основанные на выявлении аномалий протоколов и на анализе сигнатур; лучшие в своей области технологии защиты от вирусов; средства фильтрации web-ресурсов; средства



подавления спама; совместимую с протоколом IPsec технологию виртуальных частных сетей (VPN); быстродействующие аппаратные системы шифрования;

- установка системы централизованного управления и интеграция всех компонент антивирусного программного обеспечения в комплексную систему антивирусной защиты: централизованное управление, система распространения обновлений, система извещений.

Схема установки антивирусных средств защиты компании Symantec в сети ТашиИИТ приведена на рис.3.2.

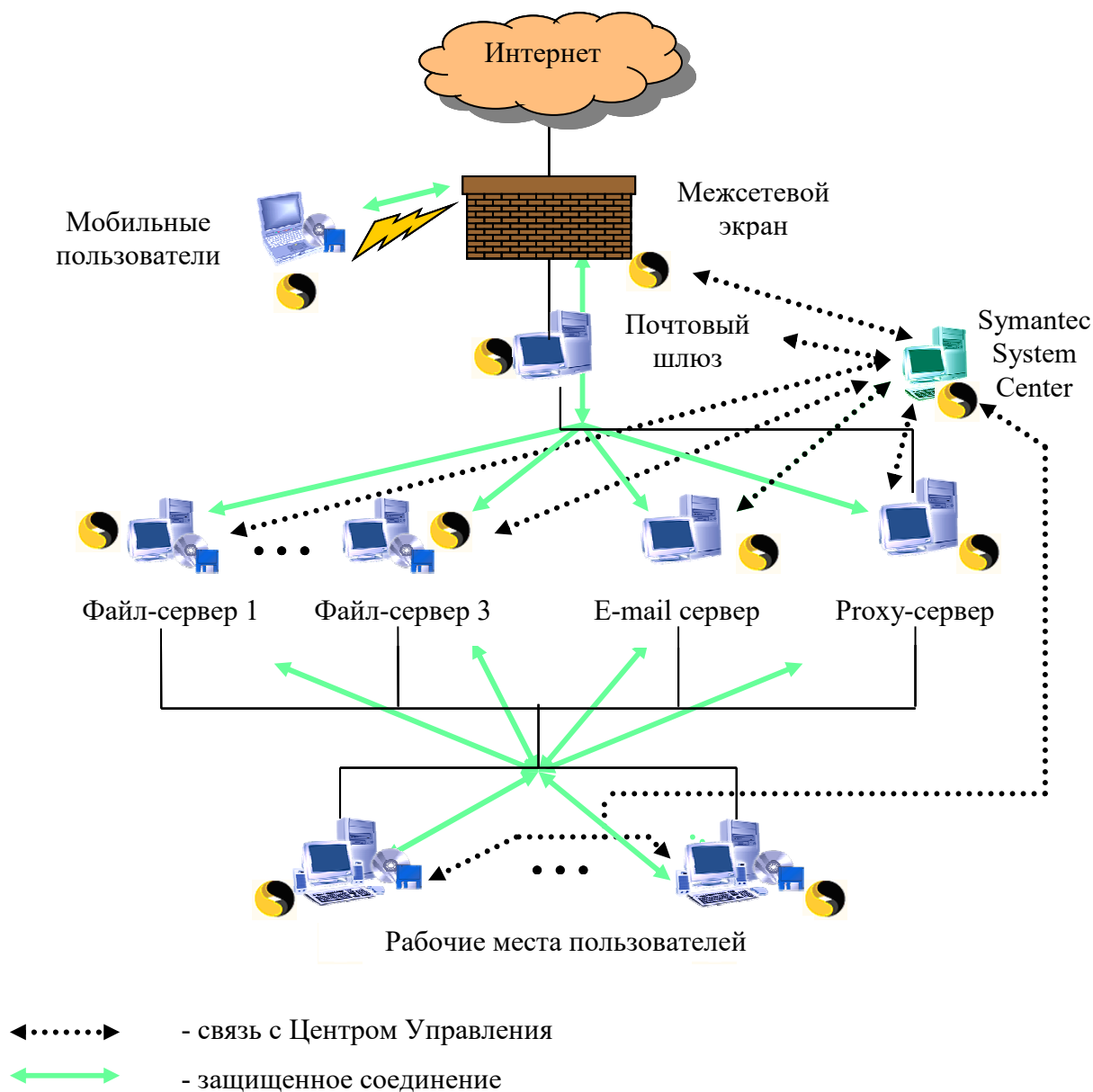


Рис.3.2. Схема защищенной сети ТашиИИТ с использованием продуктов компании Symantec

### 3.3 Порядок и схема обновления баз данных и антивирусных систем

Существует несколько способов загрузки файлов описаний и их рассылки серверам и клиентам.

Способы обновления описаний Symantec AntiVirus Corporate Edition описаны в приложении в табл.3.1.

Таблица 3.1

Способы обновления описаний

Способ	Описание	Рекомендации по использованию
Метод передачи описаний вирусов	После получения первичным сервером управления новых описаний вирусов и угроз с FTP-узла Symantec или с сервера LiveUpdate запускается операция установки. Первичный сервер управления передает пакет описаний на все вторичные серверы управления в группе серверов. Вторичные серверы управления извлекают описания и сохраняют их в соответствующем каталоге. Клиенты получают пакет описаний от своих родительских серверов управления. Клиенты извлекают описания и помещают их в соответствующий каталог.	Рекомендуется применять в том случае, когда управлять обновлением описаний вирусов и угроз необходимо из Symantec System Center. Кроме того, этот метод может применяться во время эпидемии вирусов для немедленной установки файлов описаний на компьютеры сети.
LiveUpdate	При запросе новых описаний вирусов и угроз клиентом или сервером, запускается плановая операция загрузки. Функцию LiveUpdate можно настроить на каждом компьютере таким образом, чтобы она запрашивала обновления со специализированного внутреннего сервера LiveUpdate или непосредственно с сервера.	Рекомендуется применять тогда, когда защищаемые компьютеры должны загружать обновления описаний вирусов и угроз с внутреннего сервера LiveUpdate или непосредственно с сервера Symantec.
Intelligent Updater	Intelligent Updater – это самораспаковывающийся исполняемый файл, содержащий файлы описаний вирусов и угроз.	Рекомендуется применять в тех случаях, когда необходимо разослать обновления описаний вирусов и угроз пользователям, не имеющим активного соединения с сетью.
Опрос Центрального изолятора	Сервер центрального изолятора периодически опрашивает шлюз Digital Immune System на предмет наличия новых файлов описаний вирусов и угроз. При наличии новых описаний сервер центрального изолятора может автоматически установить эти описания на те компьютеры, которым они необходимы.	Можно автоматизировать рассылку обновлений файлов описаний по сети.

Рекомендуемый способ: совместное использование метода передачи описаний вирусов и функции LiveUpdate. Можно одновременно применять метод передачи описаний вирусов и функцию LiveUpdate. Применение метода передачи описаний вирусов позволяет планировать и устанавливать обновления описаний вирусов и угроз из Symantec System Center. Кроме того, метод передачи описаний вирусов может применяться в качестве аварийного метода для быстрой рассылки новых описаний вирусов при появлении угрозы заражения сети новым вирусом. Хотя метод передачи описаний вирусов используется чаще, некоторые крупные сети полагаются на использование функции LiveUpdate. В таких системах не следует разрешать прямой доступ к узлу компании Symantec большому числу серверов и клиентов. Один или несколько серверов выступают в качестве внутренних серверов LiveUpdate для всех остальных серверов сети и, в некоторых случаях, для всех клиентов.

На рис.3.3 показан пример настройки обновления файлов описаний вирусов и угроз в небольшой сети, состоящей из шести файловых серверов, разделенных на две группы.

Первичный сервер управления 1 настроен таким образом, чтобы он получал обновления файлов описаний вирусов и угроз с сервера HTTP, FTP или с другого компьютера (первый уровень). Первичный сервер управления 2 настроен для получения последних обновлений с первичного сервера управления 1 (второй уровень). Таким образом, первичный сервер управления 1 будет главным первичным сервером, он будет рассылать файлы обновлений на серверы Symantec AntiVirus из группы серверов А (второй уровень). Серверы Symantec AntiVirus из группы серверов В будут получать обновления от своего первичного сервера управления (второй уровень). Клиенты будут автоматически получать обновления со своих родительских серверов Symantec AntiVirus (третий уровень).

На рис.3.4 показано, как можно организовать обновление файла описаний, если в организации имеется несколько локальных сетей, связанных между собой через глобальную сеть (WAN).

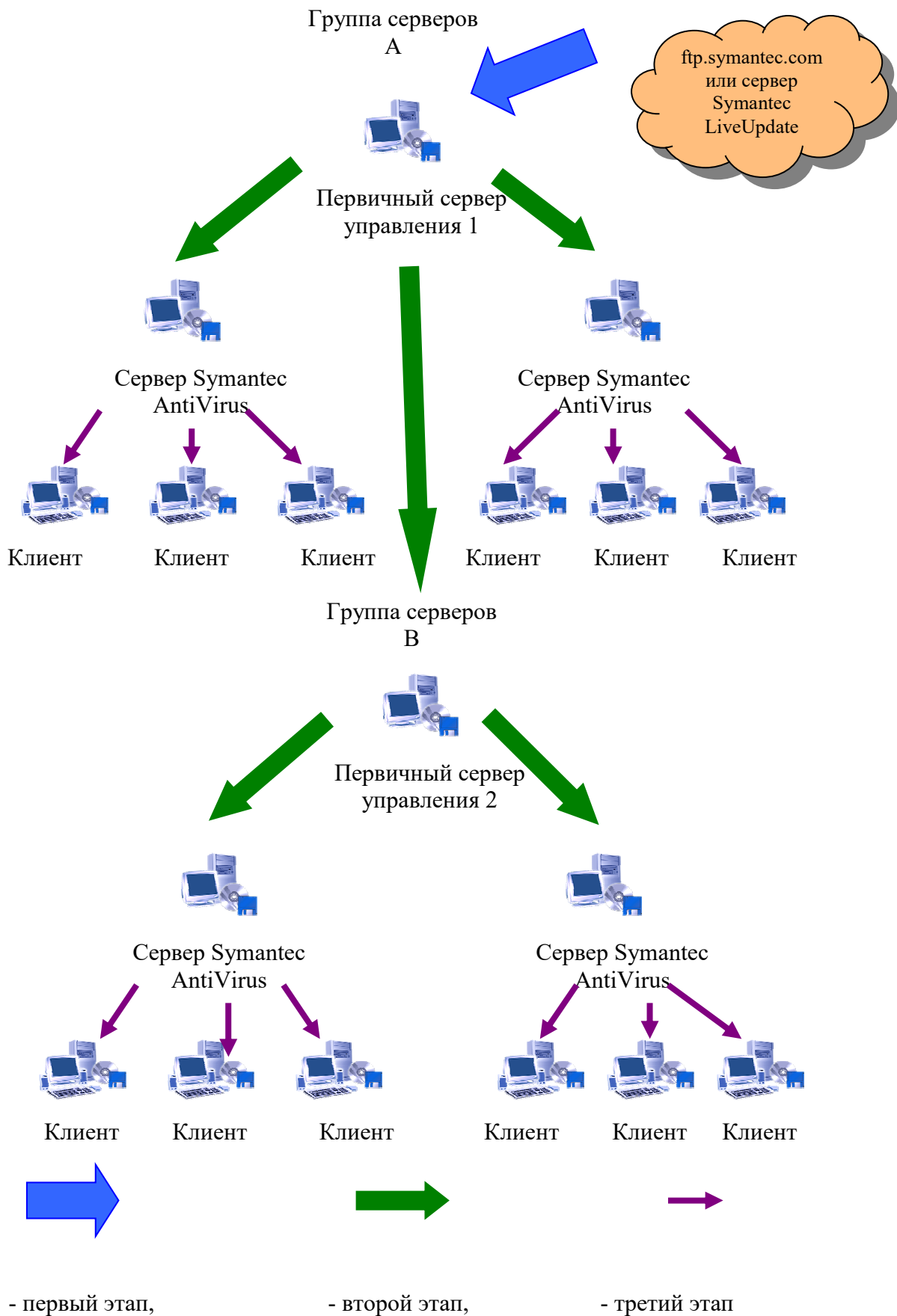


Рис.3.3. Обновление файлов описаний с использованием метода передачи описаний вирусов

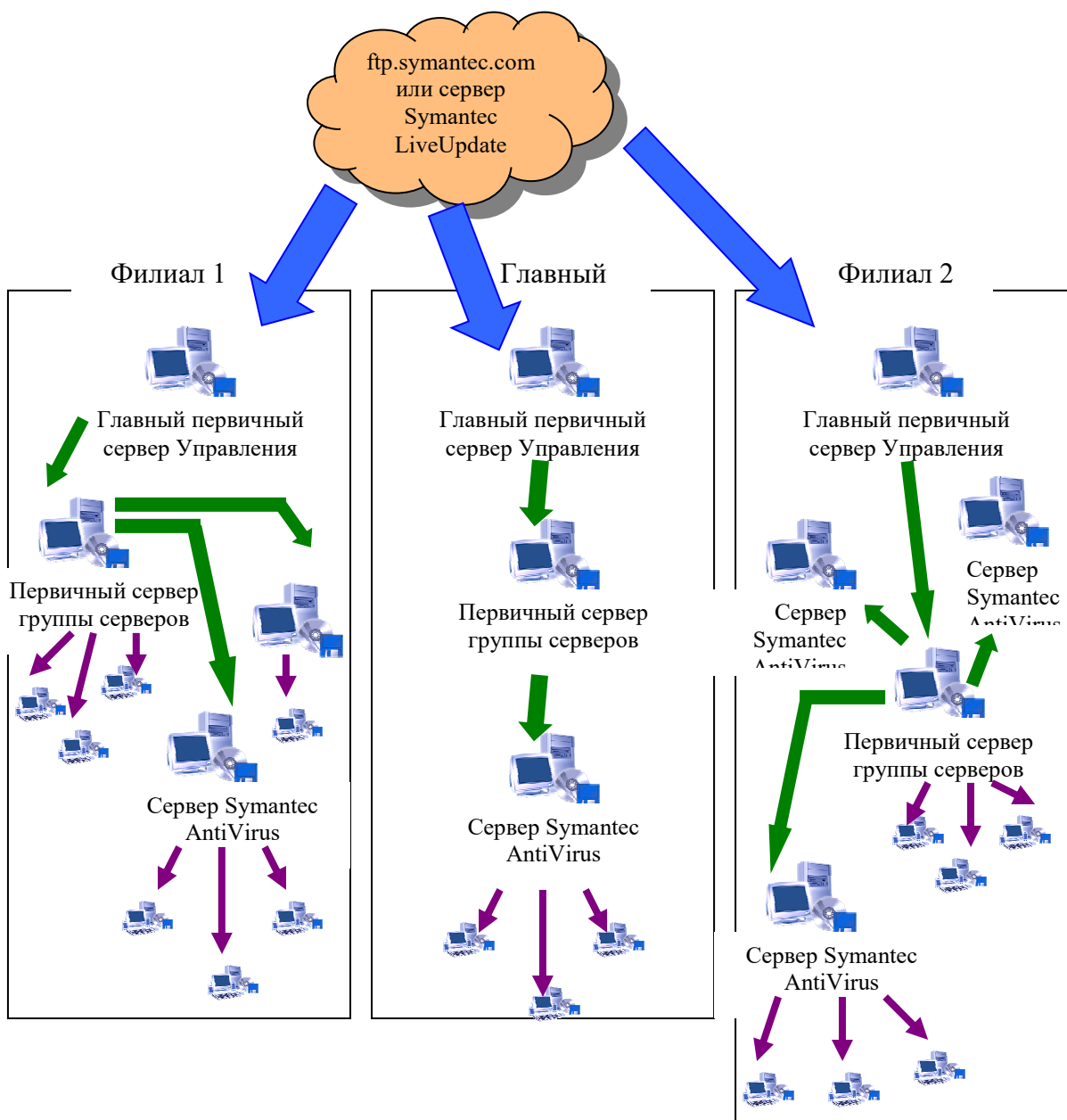


Рис.3.4. Обновление файла описаний в нескольких сетях, связанных через WAN

Главные первичные серверы управления из групп серверов в отдельных сетях получают обновления с FTP-сервера Symantec или с сервера LiveUpdate. Эти первичные серверы управления рассылают обновления на первичные серверы управления остальных групп серверов в своей локальной сети. Первичные серверы управления рассылают обновления другим защищенным серверам и клиентам в своей группе серверов.

Обновление серверов с помощью LiveUpdate реализуется в зависимости от размеров сети следующими способами:

- В небольших сетях (менее 1000 узлов) рекомендуется настроить



управляемые серверы для непосредственной загрузки обновлений с FTP-узла Symantec, с сервера Symantec LiveUpdate или с внутреннего сервера LiveUpdate.

- В больших сетях (более 1000 узлов) рекомендуется настроить внутренний сервер LiveUpdate, загрузить обновления на этот сервер и разрешить управляемым серверам загрузку обновлений с внутреннего сервера LiveUpdate.

### **3.4. Разработка рекомендаций и методик применения антивирусных средств для корпоративных сетей**

Перед выбором антивирусной программы следует выполнить несколько подготовительных этапов:

1. Разработать структурную схему корпоративной сети, на которой должны быть указаны места подключения ее к внешним сетям передачи данных. Составить подробную таблицу программно-аппаратной конфигурации рабочих мест и серверов.

2. Проанализировать информационные потоки, используемое ПО, решаемые задачи, а также функции, выполняемые пользователями в данной сети. На основе полученных данных произвести инвентаризацию информационных задач в виде таблицы.

3. Произвести категорирование обрабатываемой в КС информации и оценить при этом степень ее доступности.

4. Выявить потенциальные угрозы и риски. Составить схему корпоративной сети с указанием вероятных путей проникновения вирусов.

5. Сделать стоимостную оценку вероятностного события, ведущего к потерям (ущербу), т.е. оценить риски. Составить подробную матрицу рисков угрозы вирусного заражения, в которой должны быть описание самого риска, оценка вероятности наступления риска и последствий для бизнеса.

6. Составить классификационную таблицу эффективности каждого из программных продуктов.

7. На основе полученной информации выделить два ведущих по указанным критериям продукта и сравнить их такие потребительские характеристики как простота и удобство интерфейса, при этом страна-производитель антивирусов в

большинстве случаев не имеет значения, поскольку на сегодняшний день процесс эмиграции вируса в другие страны и иммиграции антивирусных программ ограничивается только скоростью Интернет, поэтому для вирусов, как и для антивирусов не существует границ.

#### 8. Осуществить окончательный выбор антивирусного средства защиты.

Методика применения антивирусных средств выглядит следующим образом:

- следить за тем, чтобы антивирусные программы, используемые для проверки, были самых последних версий (при этом в Symantec AntiVirus предусмотрено обновление самого продукта);

- если произошло заражение макровирусом на период лечения убедиться в том, что соответствующий редактор (Word или Excel) неактивен на всех компьютерах;

- в случае загрузочного вируса проверить все сменные носители, загрузочные ли они или нет;

- вирус может проникнуть и в резервные копии ПО при обновлении этих копий. Причем архивы и резервные копии являются основными поставщиками давно известных вирусов. Вирус может годами находиться в дистрибутивной копии какого-либо программного продукта и неожиданно проявиться при установке программ на новом компьютере;

- для исключения или уменьшения риска заражения вирусами при использовании документов MS Word, можно порекомендовать следующее: если нет необходимости применять макросы в документах, рекомендуется сохранять файлы в формате .rtf, который исключает использование макросов, а значит, безопасен в смысле заражения вирусами. Если же такая необходимость существует, рекомендуется установить режим среднего уровня безопасности (Сервис/Макрос/Безопасность). В этом режиме при открытии файла с макросами будет выдано предупреждение. Если установить высокий уровень безопасности, то все макросы "из ненадежных источников" будут отключены без предупреждения, но при этом будут сохраняться в документе. Таким

образом, компьютер не будет заражен, но о том, что, возможно, заражен файл, так и не будет известно, а это представляет потенциальную опасность.

• при работе с документами в формате RTF и PDF соблюдать следующие правила:

1) своевременно устанавливать "заплатки" к используемым текстовым редакторам, особенно, если они касаются работы с RTF- и PDF-документами;

2) обязательно проверять RTF- и PDF-документы антивирусными программами с последними обновлениями антивирусных баз данных;

3) ни в коем случае не запускать содержащиеся в RTF- и PDF-документах прямые ссылки на какие бы то ни было файлы.

### **3.5 Разработка методических рекомендаций для должностных лиц, ответственных за АВЗ сети ТашИИТ**

#### **3.5.1 Методические рекомендации для ответственного за АВЗ на объектах информатизации, выделенных ЛВС и локальных персональных электронно-вычислительных машин (ПЭВМ)**

Ответственного за обеспечение АВЗ на объектах информатизации рекомендуется назначать из числа подготовленных сотрудников структурных подразделений, эксплуатирующих данные средства вычислительной техники, либо сотрудников информационно-технических отделов.

Рекомендуемые функции ответственного за АВЗ:

• обеспечение своевременного (не реже двух раз в неделю) обновления базы данных антивирусной программы, установленной на выделенных компьютерах или ЛВС;

• осуществление периодического контроля функциональности антивирусной программы;

• формирование, обеспечение хранения и регулярного (в зависимости от важности и скорости изменения информации) обновления резервных копий информационных массивов и дистрибутивов программного обеспечения на случай ликвидации последствий внедрения программных вирусов.

### 3.5.2 Методические рекомендации для администратора АВЗ

Администратора АВЗ рекомендуется назначать из числа сотрудников подразделения защиты информации. В случае временного отсутствия (по причине отпуска, командировки или болезни) администратора АВЗ его обязанности следует возлагать на сотрудников ИТ-подразделения. В работе рекомендуется придерживаться следующих правил:

- для уменьшения риска заражения файлов на сервере локальной сети активно использовать стандартные возможности защиты сети: ограничение прав пользователей, установку атрибутов «только на чтение» или даже «только на запуск» для всех выполняемых файлов и т.д.;

- ограничить круг лиц, допущенных к работе на конкретном компьютере, поскольку, как правило, наиболее подвержены заражению многопользовательские компьютеры;

- использовать бездисковые рабочие станции, что значительно уменьшает риск заражения компьютерной сети;

- перед запуском нового ПО пробовать его на тестовом компьютере, не подключенном к общей сети;

- покупать дистрибутивные копии ПО у официальных продавцов;

- хранить дистрибутивные копии ПО (в том числе операционной системы);

- при наличии стримера или какого-либо внешнего носителя большого объема копировать все содержимое винчестера;

- использовать специализированные антивирусы, проверяющие на лету файлы, к которым идет обращение. Если это по какой-либо причине невозможно, регулярно проверять сервер обычными антивирусными программами.

Рекомендуемые функции администратора АВЗ:

- формирование эталонного экземпляра дистрибутива антивирусной программы и обеспечение его хранения;

- при поступлении обновлений дистрибутивов антивирусных программ в

недельный срок осуществление их рассылки в подчиненные организации;

- обеспечение регулярного (не реже двух раз в неделю) обновления базы данных антивирусной программы;

- осуществление периодического контроля функциональности системы антивирусной защиты;

- проведение внеплановых проверок магнитных носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса в организации;

- периодический контроль выполнения требований положения о системе антивирусной защиты информации в организации.

### **3.5.3 Разработка методических рекомендаций для пользователей ЛВС и локальных компьютеров**

В работе рекомендуется придерживаться следующих правил:

- осторожно относиться к программам и документам Word/Excel, приходящим из глобальных сетей. Перед тем как запустить файл на выполнение или открыть документ / таблицу, проверить их на наличие вирусов. Использовать специализированные антивирусы – для проверки на лету всех файлов, приходящих по электронной почте и по Интернет в целом;

- пользоваться хорошо зарекомендовавшими себя источниками программ и прочих файлов;

- не запускать непроверенные файлы, в том числе полученные из компьютерной сети. Перед запуском новых программ обязательно проверить их одним или несколькими антивирусами;

- желательно также, чтобы при работе с новым ПО в памяти резидентно находился какой-либо антивирусный монитор. Если запускаемая программа заражена вирусом, то такой монитор поможет обнаружить вирус и остановить его распространение;

- использовать утилиты проверки целостности информации. Такие утилиты сохраняют в специальных базах данных информацию о системных областях

дисков (или целиком системные области) и информацию о файлах (контрольные суммы, размеры, атрибуты, даты последней модификации файлов и т.д.). Периодически необходимо сравнивать информацию, хранящуюся в подобной базе данных, с реальным содержимым винчестера, так как практически любое несоответствие может служить сигналом о появлении вируса или «троянской» программы;

- не ограничиваться встроенной в BIOS защитой от вирусов, она достаточно просто обходится многими вирусами. То же верно для систем антивирусной защиты, встроенных в Word и Office: они могут быть отключены вирусом (или самим пользователем, поскольку эти системы могут сильно мешать в работе);

- не работать на компьютере (открывать файлы, запускать программы) при выключенной либо не инсталлированной антивирусной программе;

- не распространять полученные средства антивирусной защиты в сторонние организации.

### **3.6 Разработка политики регулярного антивирусного сканирования, лечения, удаления и оповещения**

Можно дать следующие рекомендации по настройке политики регулярного антивирусного сканирования или осмотра с помощью консоли Symantec System Center:

- Осмотры автоматической защиты должны быть постоянно включены, т.к. при каждом обращении, копировании, перемещении и открытии файла они осматривают его на наличие вирусов и угроз безопасности. Осмотры автоматической защиты включают в себя:

- Осмотры файловой системы в рамках автоматической защиты;
- Осмотр вложений в сообщениях электронной почты Lotus Notes, Microsoft Exchange и Outlook (MAPI и Интернет) в рамках автоматической защиты (выполняется только на клиентах);
- Функция автоматической защиты осматривает почтовые сообщения и



вложения, использующие протоколы связи POP3 и SMTP. При этом также выполняется эвристический осмотр отправляемых сообщений.

При настройке автоматической защиты для клиентов и серверов рекомендуется выбрать следующие параметры:

- типы файлов: все типы;
- параметры: поиск угроз безопасности;
- типы накопителей: для клиента – сетевые, гибкие диски и компакт – диски, для сервера - сетевые, гибкие диски (при необходимости компакт-диски).

Причем в ходе настройки автоматической защиты следует заблокировать все параметры на клиентах для применения политики безопасности компании, действующей в отношении вирусов и угроз безопасности.

- Осмотры вручную (осмотр по требованию) проверяют выбранные файлы и папки на определенных компьютерах на наличие вирусов и угроз безопасности, таких как программы-шпионы и программы показа рекламы. Осмотр вручную оптимален для быстрой проверки отдельных областей сети или локального жесткого диска.

- Осмотры в рамках сплошных проверок осматривают структуру системы, группу серверов или отдельный сервер. В ходе сплошной проверки выполняется осмотр на наличие вирусов и угроз безопасности. Проведение сплошной проверки следует осуществлять в случае обнаружения нескольких подозрительных файлов и когда непонятно, связана ли возникшая проблема только с тем компьютером или сервером, на котором эти вирусы были обнаружены, или заражение могло распространиться на другие области сети. Если клиент Symantec AntiVirus будет недоступен во время сплошной проверки, то он будет проверен сразу после включения. Для этого компьютеру не обязательно входить в сеть.

В зависимости от объекта, выбранного в окне консоли Symantec System Center, можно запустить сплошную проверку всей сети, группы серверов или отдельного сервера.

- Плановые осмотры. На консоли Symantec System Center следует запланировать выполнение осмотров на клиентах и серверах Symantec AntiVirus на определенное время. Пользователи могут настраивать плановые осмотры на клиентах Symantec AntiVirus, но они не могут изменять или отключать осмотры, запланированные администратором. Рекомендуется настроить запуск планового осмотра не реже одного раза в неделю (день и час выбираются на усмотрение администратора).

При этом возможны следующие способы осмотра: осмотр одного или нескольких серверов и клиентов Symantec AntiVirus и осмотр групп серверов и клиентов Symantec AntiVirus с помощью групп серверов.

Можно в дополнение к плановым осмотрам применять осмотр при запуске системы. Часто такие осмотры ограничиваются наиболее важными папками, такими как папка Windows и папки с шаблонами Microsoft Word и Microsoft Excel.

Для неуправляемых клиентов в Symantec AntiVirus следует настроить осмотр при запуске, который называется автоматически созданным быстрым осмотром. Этот тип осмотра проверяет на наличие вирусов и угроз файлы, загруженные в оперативную память, и другие стандартные для заражения расположения при каждом входе пользователя в систему. Такой осмотр следует настроить так же, как и осмотры вручную, за исключением того, что в его параметрах нельзя отключить осмотр загруженных в память файлов и других стандартных для заражения расположений компьютера.

- Пользовательские осмотры рекомендуется настраивать для часто осматриваемых наборов файлов и папок. Этот тип осмотра позволяет быстро проверить заданные объекты на наличие вирусов и других угроз. Рекомендации по настройке осмотров сведены в схему, представленную на рис.3.5.

Одной из важнейших составляющих осмотра являются действия, выполняемые программой Symantec AntiVirus при обнаружении вируса или угрозы безопасности. Следует настроить первое действие и второе действие, выполняемое в случае сбоя первого действия (рис.3.6).

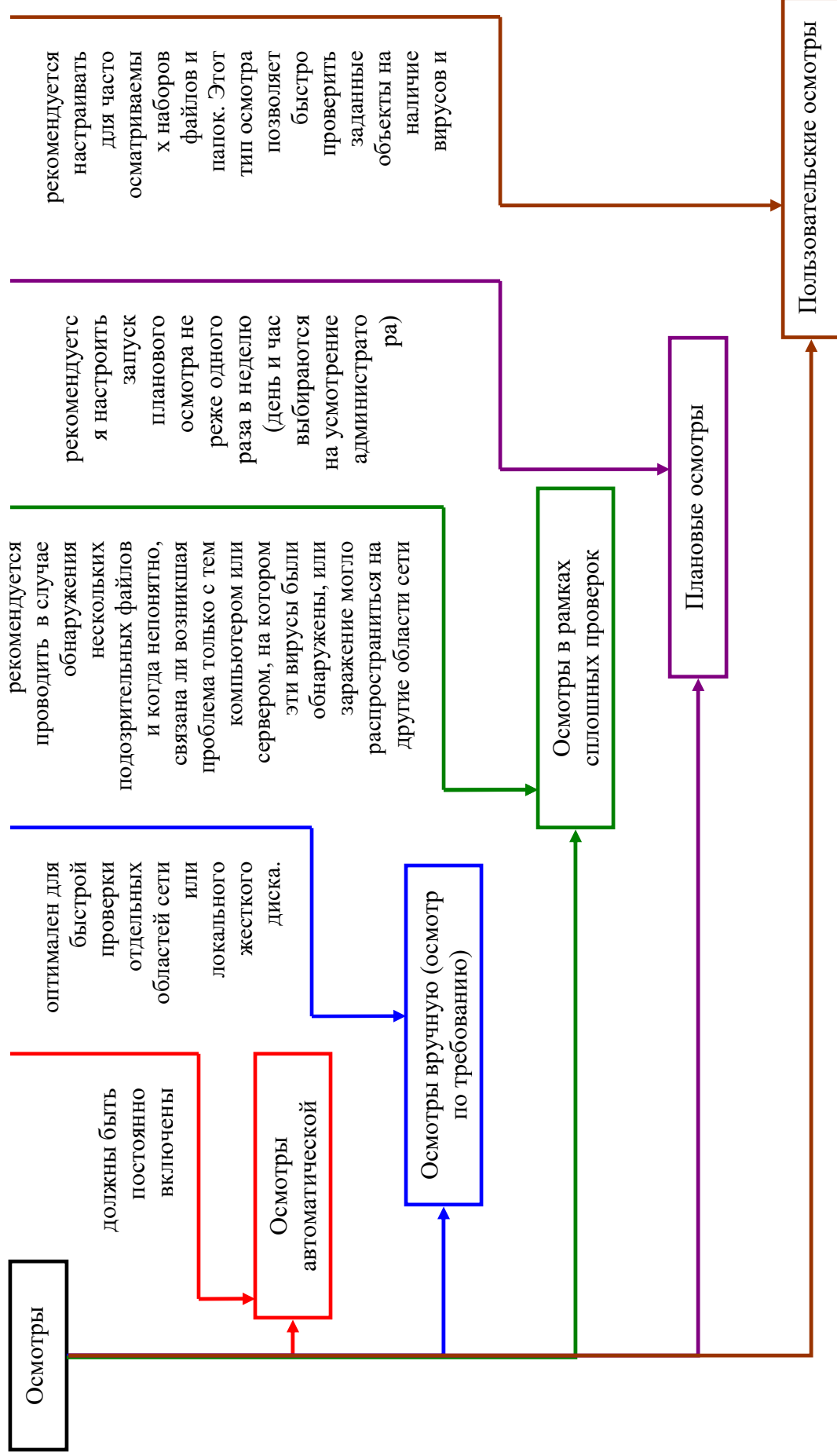


Рис. 3.5. Рекомендации по настройке осмотров, поддерживаемых Symantec AntiVirus

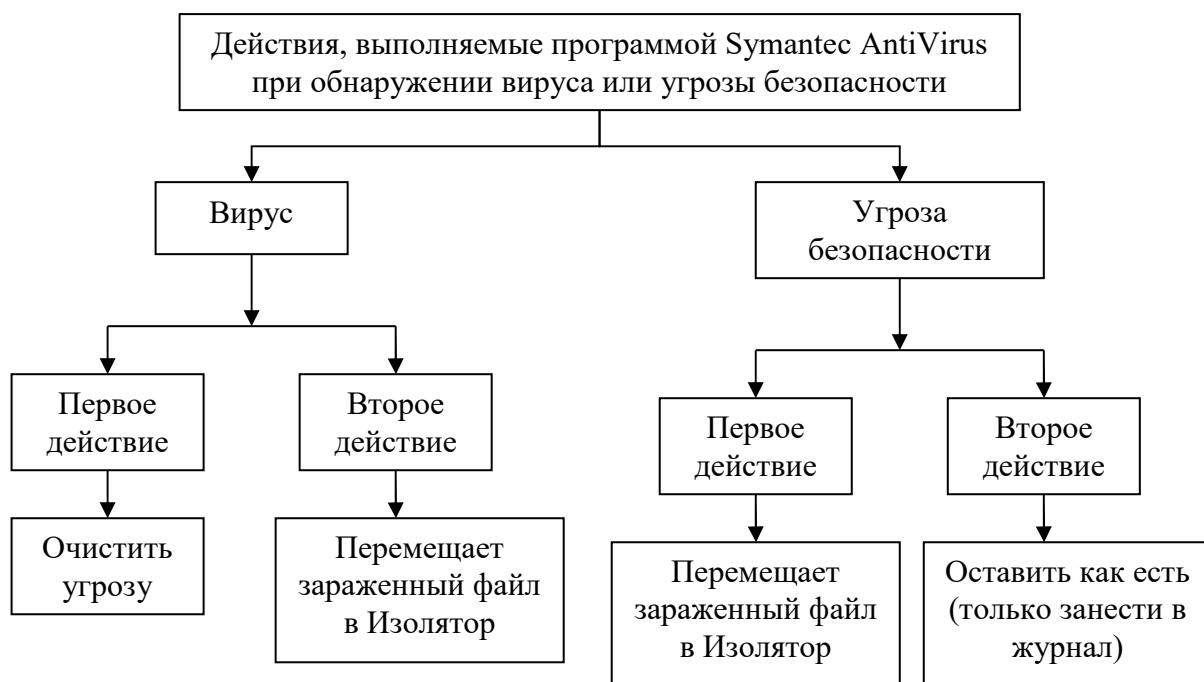


Рис.3.6. Рекомендации по выбору первого и второго действия для вирусов и угроз безопасности

1. Очистить угрозу – удаляет вирус из зараженного файла. Очистку всегда следует выбирать в качестве основного действия для вирусов при всех типах осмотра, а для угроз безопасности это действие недоступно. Если Symantec AntiVirus успешно удалит вирус из зараженного файла, то другие действия предпринимать не потребуется. Вирус будет удален с компьютера и его распространение на другие элементы системы станет невозможным.

2. Изолировать угрозу. Выполняет одно из следующих действий:

- В случае вируса перемещает зараженный файл в Изолятор, а в журнал событий заносится соответствующее сообщение. Вирусы из помещенных в Изолятор зараженных файлов теряют способность к распространению. Для вирусов это действие следует настраивать в качестве второго действия.

- В случае угрозы безопасности перемещает зараженные файлы в Изолятор и пытается устранить побочные эффекты. Для угроз безопасности это действие настроить в качестве первого действия.

В Изоляторе по умолчанию сохраняется информация обо всех выполненных действиях, для того чтобы можно было восстановить то состояние компьютера,

которое было до устранения угрозы.

3. Устранить угрозу – удаляет зараженный файл с жесткого диска компьютера. Если Symantec AntiVirus не может удалить файл, дополнительная информация о действии, выполняемом Symantec AntiVirus, появляется в окне уведомления, а также заносится в журнал событий.

Применять это действие следует только в том случае, если имеется возможность заменить удаляемый файл незараженной резервной копией, поскольку файл удаляется без возможности восстановления с помощью Корзины.

Следует соблюдать осторожность при выборе этого действия для угроз безопасности, так как в некоторых случаях удаление угрозы может привести к прекращению работы некоторых функций приложения.

4. Оставить как есть (только занести в журнал). Выполняет одно из следующих действий:

- В случае вируса обработка файла не выполняется. Вирус остается в файле, сохраняя способность к распространению. В журнал угроз добавляется запись с информацией о зараженном файле.

Действие «Оставить как есть (только занести в журнал)» можно выбрать в качестве второго действия для макровирусов и вирусов других типов. Не выбирайте это действие для масштабных, автоматизированных осмотров, в том числе плановых осмотров, если только вы не хотите получить результаты осмотра и выполнить необходимые действия позднее (например, изолировать файл).

- В случае угрозы безопасности зараженные файлы не обрабатываются, а в журнал угроз добавляется запись об угрозе. Выберите эту опцию, если вы хотите вручную управлять тем, каким образом Symantec AntiVirus обрабатывает угрозы. Для угроз безопасности это действие следует настроить в качестве второго действия.

Системный администратор может настроить сообщение с инструкциями по противодействию угрозам, отправляемое при обнаружении вируса или угрозы,

отправляемое зараженному компьютеру.

Перемещенный в Изолятор файл можно попытаться исправить (вылечить), удалить или восстановить в исходной папке. После обновления файла описаний вирусов можно повторно проверить находящиеся в Изоляторе файлы, зараженные вирусами.

При удалении файла в Изоляторе Symantec AntiVirus удаляет этот файл с жесткого диска компьютера без возможности его восстановления.

Поскольку вирусы могут частично повредить файл, в некоторых случаях вместо исправления зараженного файла целесообразно удалить его, а затем восстановить из резервной копии. Это действие можно выполнить и вручную после перемещения зараженного файла в Изолятор. Удаление зараженного файла из Изолятора является эффективным способом удаления вируса, находящегося в файле, который не удалось исправить. Использовать это действие следует только при наличии незараженных резервных копий файлов, выбранных для осмотра.

После помещения файла в Изолятор следует обновить описания. В зависимости от заданной администратором конфигурации Изолятора, при обновлении описаний изолированные файлы могут автоматически осматриваться, исправляться и восстанавливаться, либо может запускаться Мастер лечения, позволяющий вручную повторно осмотреть изолированные файлы.

Если после повторного осмотра изолированного файла Symantec AntiVirus не удастся удалить вирус, то зараженный файл можно передать для дальнейшего анализа в службу Symantec Security Response.

Для получения уведомлений об обнаруженном вирусе или угрозе безопасности, следует установить систему Alert Management System (AMS) на все первичные серверы, которая обеспечит возможность управления критическими ситуациями.

Например, можно настроить отправку электронной почты в случае обнаружения вируса или угрозы безопасности на защищенном сервере



администратору сети, или настроить любые другие способы уведомления. Своевременное уведомление часто помогает предотвратить вирусную эпидемию, распространяющуюся в сети.

### **3.7 Разработка плана действий при эпидемии вирусов в сети ТашИИТ**

Реакция на эпидемию требует заблаговременной подготовки и наличия стратегии, позволяющей адекватно отреагировать на это событие. Схема реакции на эпидемию приведена на рис.3.7.

Помимо установки Symantec AntiVirus на серверы и рабочие станции сети, подготовка к эпидемии включает также следующие задачи:

1) План реакции на эпидемию. Заблаговременно создать план реакции на эпидемию, и определить в нем действия по обработке вирусов.

Для завершения создания стратегии обработки вирусов следует выполнить следующие дополнительные действия:

- Определить различные действия по восстановлению для разных типов вирусов. Например, программу Symantec AntiVirus можно настроить таким образом, чтобы она автоматически удаляла макровирусы, а при обнаружении вируса в программном файле предлагала пользователю выбрать действие.

- Выбрать резервное действие для файлов, которые Symantec AntiVirus не может исправить, например удаление зараженного файла.

- Получать предупреждения о вирусах, например с помощью пейджера или электронной почты, при использовании системы AMS.

- Настроить локальный изолятор для пересылки зараженных файлов в центральный изолятор. Центральный изолятор можно настроить таким образом, чтобы он пытался исправить зараженные файлы с помощью своих файлов описаний (которые могут быть более новыми, чем описания на локальном компьютере), либо чтобы он автоматически пересылал образцы зараженных файлов в центр Symantec Security Response для анализа.

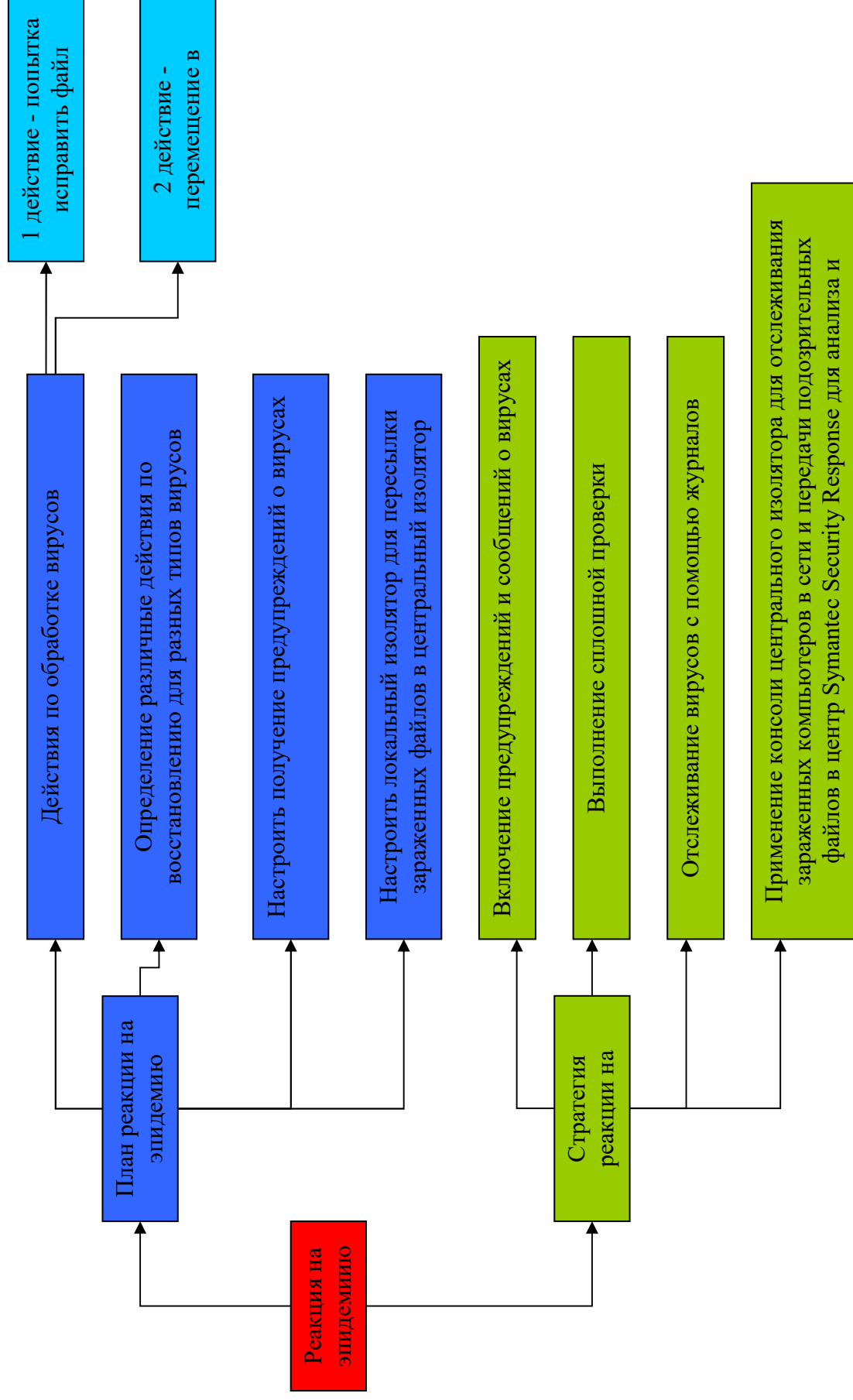


Рис.3.7. План действий при эпидемии вирусов в сети ТашИИТ

2) Стратегия реакции на эпидемию включает следующие компоненты:

- Включение предупреждений и сообщений о вирусах – отправка встроенных предупреждений (с помощью консоли Symantec System Center можно настроить пользовательское сообщение, которое должно появляться на клиентах Symantec AntiVirus при обнаружении подозрительного файла) и предупреждений AMS.

- Выполнение сплошной проверки сети.

- Отслеживание вирусов с помощью журналов. Позволяет отслеживать вирусы и операции отправки файлов в центральный изолятор на уровне группы серверов, отдельного сервера или клиента.

- Применение консоли центрального изолятора для отслеживания зараженных компьютеров в сети и передачи подозрительных файлов в центр Symantec Security Response для анализа и исправления. Консоль Symantec System Center заносит в журнал событий информацию обо всех операциях передачи подозрительных файлов в центр Symantec Security Response с клиента Symantec AntiVirus

## **4. Охрана труда**

### **4.1 Значения охраны труда и безопасности на железнодорожном транспорте**

Охрана труда – это система законодательных социально-экономических, организационных, технических, санитарно-гигиенических мероприятий, обеспечивающих безопасность, здоровье и работоспособность человека в процессе труда. Безопасность труда – система организационных и технических мероприятий и средств, предотвращающих воздействие на работающих опасных производственных факторов, которые в определенных условиях приводят к травме или другому ухудшению здоровья.

Условия труда на железнодорожном транспорте связаны с воздействием на работников опасных и вредных производственных факторов, основными из которых являются:

- повышенная или пониженная температура, влажность и подвижность воздуха рабочей зоны;
- повышенный уровень шума (давления) на рабочих местах;
- недостаточная освещенность рабочих зон;
- повышенная яркость света прожекторов, пониженная контрастность, прямая блесккость;
- острые кромки, заусеницы на поверхности оборудования, в том числе вагонах, локомотивах, стрелочных переводах и др.;
- химические факторы, источниками которых являются главным образом перевозимые грузы;
- психофизиологические факторы – физические перегрузки, нервно психические перегрузки дежурного персонала;
- воздействие электромагнитных полей.

Для снижения воздействия опасных и вредных производственных факторов при проектировании и эксплуатации железнодорожных объектов проводят всесторонний анализ условий труда – производственного оборудования, технологического процесса, трудовых операций и санитарно-

гигиенической производственной обстановки. При анализе оборудования исследуются прочность сооружений и надежность оборудования, наличие опасных зон, соответствие оградительных устройств требованиям техники безопасности, эффективность и надежность действия предохранительных, блокировочных и специальных устройств, устройств сигнализации, герметичность оборудования, возможные источники шума, вибрации, излучения и др.

Безопасность технологических процессов подразумевает гарантию безопасности работающих при нормальной эксплуатации оборудования и организации работ, а также при возможных нарушениях. Для обеспечения безаварийной и надежной работы оборудования правила и нормы охраны труда предусматривают проведение приемосдаточных и периодических испытаний, осмотров, расчетов на прочность и устойчивость сооружений и устройств. Исходя из анализа условий труда вырабатываются рекомендации по рациональной планировке территории, зданий предприятий и цехов, конструкции оборудования, организации труда, технологических процессов, обучению персонала, контролю на рабочих местах.

Работа железнодорожного транспорта сопряжена с повышенной опасностью, поэтому к персоналу, связанному с движением поездов, предъявляются особые требования и проводятся специальные организационные мероприятия по обеспечению безопасности движения поездов. При приеме на работу, связанную с движением поездов, каждый работник должен пройти медицинский (ведомственный) профессиональный отбор в железнодорожных поликлиниках. При этом предъявляются жесткие требования к органам зрения, слуха, нервно-физиологическому состоянию и др. В процессе работы лица, связанные с движением поездов, периодически подвергаются медицинскому переосвидетельствованию. Несовершеннолетние к самостоятельным работам, связанным с движением поездов, не допускаются. После положительных результатов медицинского

освидетельствования каждый вновь принятый перед изданием приказа о зачислении должен изучить вводную инструкцию.

Каждый работник, связанный с движением поездов, должен хорошо знать и уметь применять на практике ПТЭ, инструкцию по сигнализации и по движению поездов, должностную инструкцию и другие документы, устанавливающие его обязанности, а также правила и инструкции по технике безопасности и производственной санитарии.

Решающее значение в организации безопасности движения поездов имеет технологическая и трудовая дисциплина работников железнодорожного транспорта: порядок приема и сдачи дежурств, допуск и отстранение от работы с оформлением соответствующих документов, регламент телефонных переговоров, проверки исполнения распоряжений, приказов и др.

Обеспечение безопасности в практических условиях осуществляется по двум направлениям:

- предотвращением выхода систем (объектов, процессов) в аварийные (нерасчетные) режимы, что достигается обеспечением надежности, долговечности, безотказности;
- предотвращением перерастания аварийной ситуации в аварию и катастрофу, что достигается проведением технического диагностирования, обеспечением средств защиты.

Человеческий фактор играет важную роль в обеспечении безопасности движения поездов и безаварийной работы объектов железнодорожного транспорта. Более 50 % аварий происходит вследствие ошибочных решений или действий людей, т.е. человеческий фактор может существенным образом воздействовать на увеличение степени риска и соответственно на снижение безопасности технической системы. Ошибки человека в ходе выполнения своих служебных обязанностей зачастую в условиях возникновения непредвиденной обстановки и дефицита времени становятся практически неизбежным. Поэтому в технических средствах предусматривают такую



защиту, которая позволила бы исключить результаты ошибочных действий людей, демпфировала бы неверные действия человека и его поведение в системе человек-машина.

#### **4.2 Характеристика проектируемого объекта с точки зрения охраны труда**

Технический прогресс способствует все более широкой механизации и автоматизации деятельности, централизации управления техникой, внедрению в производство электронно-вычислительных машин и автоматизированных систем управления.

Все это существенно изменяет специфику и структуру трудовой деятельности, предъявляет повышенные требования к оптимизации взаимодействия работника с современной техникой. В связи с этим возникает большой круг теоретических и прикладных проблем, связанных с изучением и совершенствованием систем "человек-машина" (СЧМ), с деятельностью оператора и его местом в системе управления.

Деятельность оператора – целенаправленная активность, совокупность действий и поступков человека, направленных на достижение сознательно поставленных целей при работе с информационными моделями реальных объектов.

Операторская деятельность представляет собой специфический вид трудовой деятельности человека, возникший на определенной ступени развития техники и производства в целом. Как особый вид деятельности операторская деятельность сформировалась в связи с достижениями научно-технического прогресса, с развитием сложной техники. Развитие техники привело к тому, что человек постепенно освободился от энергетических, транспортных и технологических функций; его основными функциями стали: программирование работы машин, управление ими и контроль за их работой.

Специфика деятельности оператора состоит в том, что он, как правило, удален от реальных объектов труда (например, на атомной электростанции) и работает с их информационными моделями.

На рис. 4.1 приведен схематичный план нашего помещения, в котором работают 4 оператора.

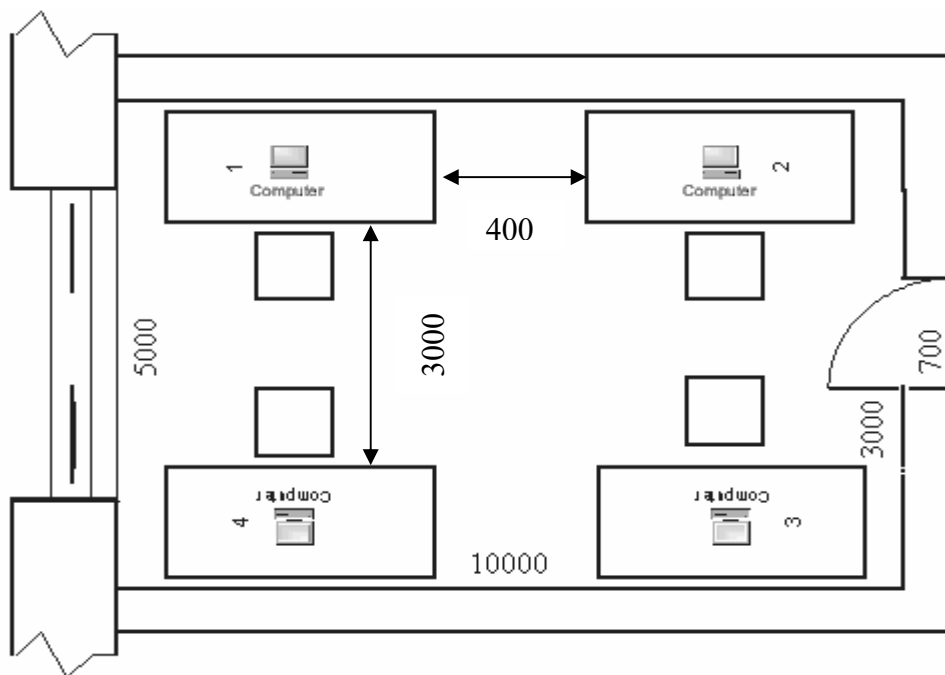


Рис.4.1 Схема помещения

План представляет собой комнату со следующими размерами: длина 10 метров, ширина 5 метров и высота 4 метра. По краям комнаты располагаются четыре рабочих места, естественный свет падает на них сбоку. Расстояния между рабочими столами с видеомониторами указаны на рисунке. Оконные проемы в помещении оборудованы жалюзи.

В нашем рабочем помещении, как и в любом помещении с видеодисплейными терминалами (ВДТ) и ПЭВМ, из опасных и вредных производственных факторов присутствуют физические и психофизиологические. Физические (статические и динамические) и нервно-психические перегрузки (умственное перенапряжение, перенапряжение анализаторов (органов слуха, зрения), монотонность труда, эмоциональные стрессы).

Основными физическими факторами являются электростатическое поле, переменные низкочастотные электрические и магнитные поля. Потенциально возможными вредными физическими факторами могут быть рентгеновское и ультрафиолетовое излучение электронно-лучевой трубки дисплея ПЭВМ,

электромагнитное излучение радиочастотного диапазона, электромагнитный фон, создаваемый сторонними источниками на рабочем месте с компьютерной техникой.

Несмотря на то, что деятельность оператора в любой системе “человек – машина” имеет ряд общих свойств, существуют ее разновидности, каждая из которых имеет свои специфические черты.

### 4.3. Антропометрические характеристики человека

Антропометрические характеристики определяются размерами тела человека и его отдельных частей и используются для проектирования наиболее рациональных, а значит и безопасных условий труда, так как они позволяют рассчитывать пространственную организацию рабочего места, устанавливать зоны досягаемости и видимости, размеры конструктивных параметров рабочего места и приспособлений (высота, ширина, длина, глубина и т. п.).

Антропометрические характеристики (АХ) подразделяют на динамические и статические. Их состав показан на рис. 4.2.

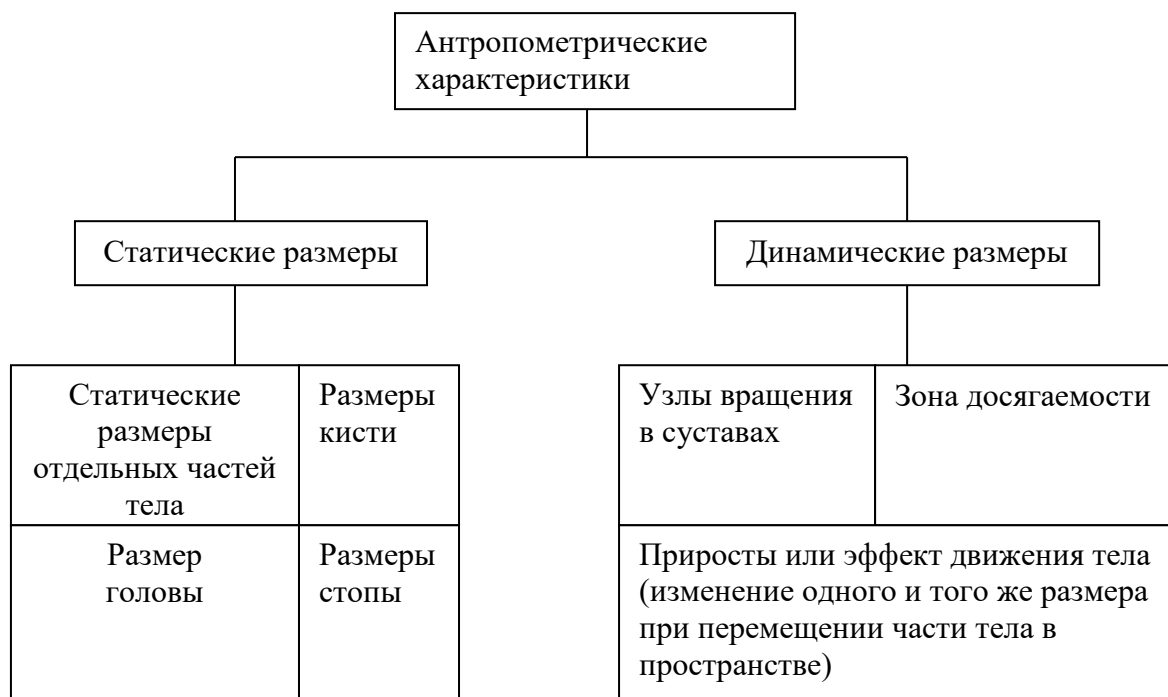


Рис. 4.2. Классификация антропометрических характеристик

Динамические АХ используются для определения объема рабочих движений, зон досягаемости (табл. 4.1, рис. 4.3) и видимости, по ним рассчитывают пространственную организацию рабочего места.

Статические АХ могут быть линейными и дуговыми. В зависимости от ориентации тела в пространстве линейные размеры делятся на продольные (высота различных точек над полом или сиденьем), поперечные (ширина плеч, таза и т. п.), переднезадние (передняя досягаемость руки и др.). Последние две группы линейных АХ иначе называются диаметрами.

Минимальные и максимальные значения антропометрических характеристик используются с учетом характера выполняемой рабочей операции или выбора параметра приспособления; в тех случаях, когда оператор что-то должен доставать, до чего-то дотянуться, выбирают минимальные значения, а при определении размеров сиденья, высоты ниши для ног и т.п. – максимальные.

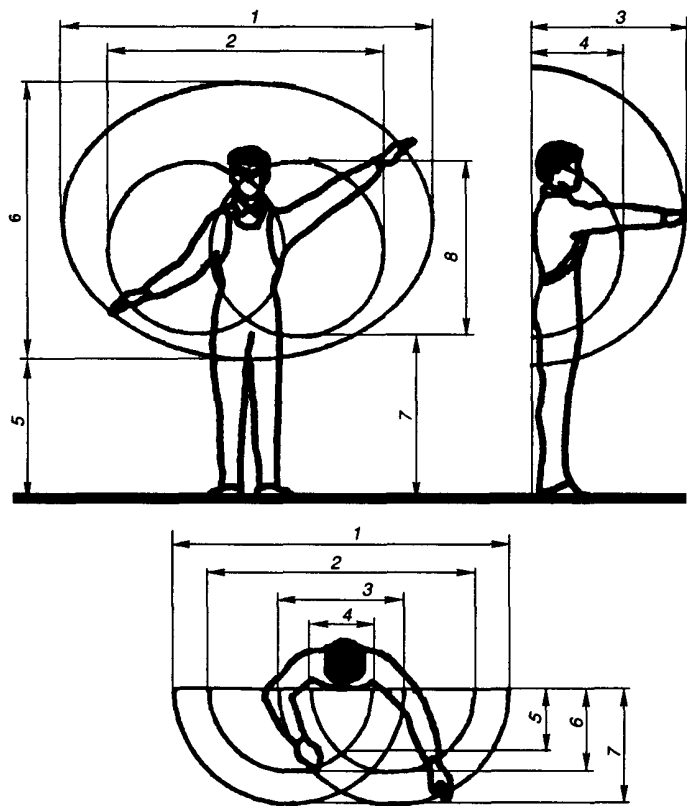


Рис. 4.3. Зоны досягаемости (1 – 8) рук человека в вертикальной плоскости

Таблица 4.1.

## Размеры зоны досягаемости рук человека, мм

Номер позиции на рис. 4.2	В вертикальной плоскости		В горизонтальной плоскости	
	для женщин	для мужчин	для женщин	для мужчин
1	1400	1550	1370	1550
2	1100	1350	1100	1350
3	730	800	660	720
4	430	500	200	240
5	630	700	200	240
6	1260	1400	300	335
7	680	770	480	550
8	720	800	—	—

Следует отметить, что (рис. 4.4, а, в) поза «стоя» требует больших энергетических затрат и менее устойчива из-за поднятого центра тяжести. Для этой позы характерно более быстрое утомление.

Рабочая поза «сидя» (рис. 4.4, б – г) является менее утомительной, так как резко уменьшается высота центра тяжести над точкой опоры, благодаря чему возрастает устойчивость тела. Кроме того, резко сокращаются энергетические затраты.

Рабочая поза выбрана правильно, если проекция общего центра тяжести лежит в пределах площади опоры. Если в процессе работы действует небольшая группа мышц, то предпочтительнее поза «сидя», при работе большой группы мышц – поза «стоя».

Всякая поза, проекция центра тяжести которой выходит за границы площади опоры, будет вызывать значительные мышечные усилия, т.е. статические напряжения (рис. 4.4, в и г). Длительные статические напряжения мышцы могут вызвать быстрое утомление, снижение работоспособности, профзаболевания (искривление позвоночника, расширение вен, плоскостопие) и травматизм. При проектировании рабочего места необходимо учитывать следующее: если при прямой позе «сидя» мышечную работу принять равной единице, то при прямой позе «стоя» мышечная работа

составляет 1,6; при наклонной позе «сидя» – 4, а при наклонной позе «стоя» – 10. Статичная поза утомительнее, чем динамическая.

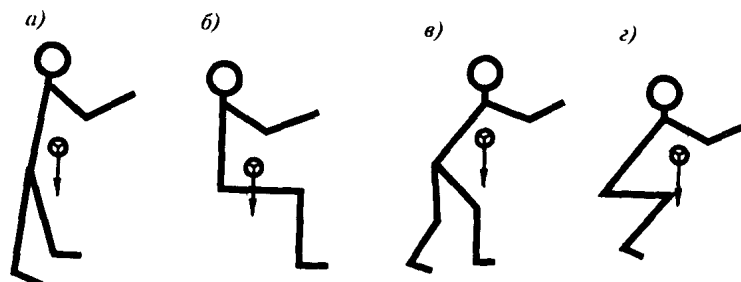


Рис. 4.4. Схема биомеханического анализа рабочей позы при устойчивой (а и б) и неустойчивой (в и г) позах; а, в – стоя; б, г – сидя

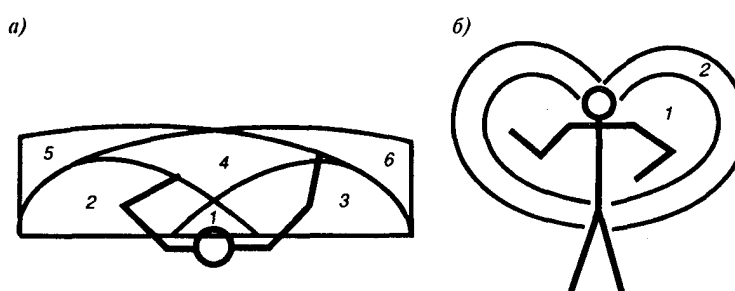


Рис. 4.5. Структурная схема рабочих зон

Наиболее важными моментами, определяющими выбор рабочей позы, являются: а) применяемое усилие в процессе работы; б) степень подвижности рабочего, обусловленная характером и конкретным содержанием технологического процесса; в) величина рабочей зоны и соотношение между антропометрическими характеристиками человека и пространственной организацией рабочих мест.

В тех случаях, когда в процессе работы происходит смена поз, учитывают следующие требования: сохранять одинаковое положение рабочего по отношению к рабочей поверхности как при работе стоя, так и при работе сидя; создавать необходимые условия свободного перехода от одной позы к другой и прежде всего за счет выбора наиболее рациональных геометрических размеров рабочей поверхности и средств подманивания.

Пространство рабочего места, в котором осуществляются трудовые процессы, может быть разделено на рабочие зоны. Рабочая поза будет

наименее утомительна только при условии, если рабочая зона сконструирована правильно.

Правильное конструирование рабочих зон определяется соответствием их с оптимальным полем зрения рабочего и определяется дугами, которые может описать рука, поворачивающаяся в плече или в локте на уровне рабочей поверхности (т.е. учитывая динамические АХ), а движением рук управляет мозг человека в соответствии с коррекцией глаз. Поэтому рабочую зону, удобную для действия обеих рук, нужно обязательно совмещать с зоной, удобной для охвата человеческим взором. На рис. 4.5 представлены структурные схемы рабочих зон: а – при позе «сидя» в горизонтальной плоскости; б – при позе «стоя» в вертикальной плоскости.

При производственном процессе для позы «сидя» (так же, как и для позы «стоя») каждая зона может быть оценена следующим образом:

Зона 1 является самой благоприятной, поскольку она наиболее применима для точных и мелких сборочных работ, так как в ней работают обе руки и хорошо осуществляется зрительный контроль. В случае оперативной работы в этой зоне следует разместить органы управления и индикаторы, которыми оператору придется пользоваться наиболее часто, интенсивно и быстро.

Зоны 2 и 3 хорошо доступны для одной и мало доступны для другой руки; зрительный контроль осложнен. В этих зонах удобно размещать инструменты и материалы, которые рабочий часто берет правой (левой) рукой, или органы управления, зрительный контроль за которыми не требуется постоянно.

Зона 4 (запасная) – труднодоступная зона; в ней могут быть размещены инструменты и материалы, которые не поместились в зонах 2 и 3.

Зона 5 (зона 6) доступна только для правой (левой) руки; здесь можно разместить инструменты и материалы, которые употребляются изредка (например, измерительные инструменты), или органы управления, которыми пользуются «не глядя».



В соответствии с рабочими зонами и антропометрическими данными проектируются рабочие места в любом производственном процессе и любые машины и механизмы, обслуживаемые человеком.

Органы управления могут быть ручными и ножными. Предпочтительнее управление ручное, причем выгоднее использовать регуляторы, которые приводятся в движение рукой к себе или от себя. Следует иметь в виду, что движения руки к себе более быстрые, но менее точные, тогда как от себя – более точные, но менее быстрые. Если органы управления не требуют усилий, то оператор «не чувствует» рукоятки и действует очень неточно. Для предотвращения дрожания руки и повышения точности движений требуется определенный момент сопротивления рукоятки в пределах 3...16,7 Н·м. Для ножных педалей при полном их нажатии момент сопротивления должен составлять 20...80 Н·м. Ножные органы управления используют тогда, когда требуются большие усилия и небольшая точность: включение – выключение, грубая регулировка напряжения или тока и т.п. При ручном управлении максимальные усилия прилагаются к рычагам, которые захватываются стоящим оператором на уровне плеча, а сидящим — на уровне локтя (рис. 4.6), поэтому органы управления, которые используются наиболее часто, следует располагать на высоте между локтем и плечом.

В процессе управления человек обязательно должен прилагать некоторые усилия, так как отсутствие их дезориентирует человека, лишает его уверенности в правильности своих действий, а излишние усилия приводят к биомеханической перегрузке.

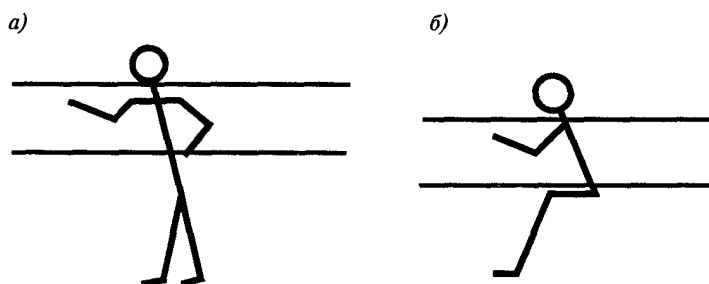


Рис. 4.6. Зона размещения органов управления: а – поза «стоя»; б – поза «сидя»

Форма и размеры органов управления должны быть согласованы с размерами и биомеханическими особенностями руки оператора. Чтобы исключить биомеханическую перегруженность, следует придерживаться соответствия управляющего воздействия на оборудование биомеханическим возможностям человека. Ниже приведены показатели силы (в Н) различных мышечных групп для мужчин (числитель) и женщин (знаменатель). Кисть (сжатие динамометра):

Кисть (сжатие динамометра):

правая рука..... 38,6/22,5

левая рука ..... 36,2/20,4

Бицепс:

правая рука..... 27,9/13,6

левая рука ..... 26,8/13,0

Кисть (сгибание):

правая рука..... 27,9/21,7

левая рука..... 26,6/20,7

Кисть (разгибание):

правая рука..... 11,9/9,0

левая рука..... 10,9/8,3

Стан (мышцы, выпрямляющие согнутое туловище)..... 123,1/71,0

## **Заключение**

В ходе выполнения выпускной квалификационной работы были получены следующие результаты:

1. Разработана система антивирусной защиты типовой корпоративной сети с акцентом на защиту серверов, предложения по построению антивирусной защиты, в том числе, один вариант, реализованный на практике в ТашИИТ.

2. Разработана концепция антивирусной защиты для сети ТашИИТ.

3. Разработаны рекомендации по конфигурированию систем АВЗ для базовых конфигураций сетей на примере сети ТашИИТ, план действий при эпидемии вирусов, методические рекомендации для должностных лиц и пользователей, методика выбора антивирусных средств, а также методика регулярного сканирования, лечения, удаления и оповещения.

4. Проведен анализ исследований антивирусных средств Kaspersky Corporate Suite, Symantec Antivirus Corporate Edition, Dr.Web Enterprise Suite, Eset Enterprise Edition, NeatSuite Enterprise Edition и сформирован их сравнительный анализ. На его основе осуществлен выбор антивирусного продукта для ТКС. Выполнен анализ рынка антивирусных средств, по итогам которого составлен справочный материал по антивирусному ПО.

6. Проведен анализ антропометрических характеристик человека.

### Список использованных источников

1. Закон Республики Узбекистан «Об информатизации» № 560-II от 11.12.2003
2. Указ Президента Республики Узбекистан «Важные задачи по пяти инициативам повышению духовности молодежи», № ПП-4235 от 07.03.2019
3. Указ Президента Республики Узбекистан «О стратегии действий по дальнейшему развитию Республики Узбекистан», № УП-4947 от 7 февраля 2017 г.
4. Постановление Президента Республики Узбекистан «О мерах по дальнейшему развитию системы высшего образования», № ПП-2909 от 20.04.2017
5. Постановление Президента Республики Узбекистан «О мерах по дальнейшему расширению участия отраслей и сфер экономики в повышении качества подготовки специалистов с высшим образованием», № ПП-3151 от 27.07.2017
6. Постановление Президента Республики Узбекистан «О дополнительных мерах по повышению качества образования в высших образовательных учреждениях и обеспечению их активного участия в осуществляемых в стране широкомасштабных реформах», № ПП-3775 от 05.06.2018
7. Касперский Е.В. Построение и администрирование систем антивирусной защиты. Часть 1. – М.: 2003, 189 с.
8. Касперский Е.В. Построение и администрирование систем антивирусной защиты. Часть 2. – М.: 2003, 188 с.
9. Кирко И. Н., Сомова М. В. Антивирусные средства /<http://www.fivt.krgtu.ru/>
10. Матаков В. Технические вопросы обеспечения безопасности информационных систем предприятия /<http://www.bezpeka.mk.ua/>статьи
11. Барсуков В.С. Безопасность: технологии, средства, услуги. – М.: КУДИУ-ОБРАЗ, 2001 - 496 с.

12. Никитина В.Н. Гигиенические аспекты безопасности труда пользователей персональных ЭВМ // КомпьюЛог, №2 / 98

13. Фомин А. А. Организация охраны труда на предприятии в современных условиях: Справочно-методическое пособие для руководителей и специалистов предприятий, организаций и учреждений. – Новосибирск: Изд. «Модус», 1997. – 300 с.: ил.

14. <http://www.viruslist.com/> // Безруков Н.Н. «Классификация компьютерных вирусов и методы защиты от них»

15. <http://www.academ.org> // Мостовой Д.Ю. «Современные технологии борьбы с вирусами»

16. <http://journal-shkolniku.ru> // Моисеенков И. «Безопасность компьютерных систем»

17. <http://prontocom.ru> // А.В.Михайлов «Компьютерные вирусы и борьба с ними»