Министерство образования Белгородской области
Областное государственное автономное
профессиональное образовательное учреждение
«Белгородский индустриальный колледж»

Рассмотрено
предметно-цикловой комиссией
Протокол заседания № ____
От «____»_____ 2022
Председатель цикловой комиссии
_____/ Третьяк И.Ю.

Методические указания
по выполнению лабораторных работ по
МДК 04.02 «Обеспечение качества функционирования компьютерных систем»

по специальности

09.02.07 Информационные системы и программирование

Квалификация: Программист
(программа подготовки специалистов среднего звена)

Разработчик: Солдатенко М.Н.
преподаватель специальных дисциплин
ОГАПОУ «БИК»

Белгород 2022

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

МДК 04.02 Обеспечение качества функционирования компьютерных систем является специальным, формирующим базовые умения для получения выпускником профессиональных умений.

Методические указания по выполнению практических работ профессионального модуля ПМ.04 Сопровождение и обслуживание программного обеспечения компьютерных систем, основной профессиональной образовательной программы по специальности 09.02.07 Информационные системы и программирование квалификация «Программист» (приказ Минобрнауки России от 28.07.2014 № 804, зарегистрирован Минюстом России 21.08.2014 №33733) (программа подготовки специалистов среднего звена) соответствуют требованиям Федерального государственного образовательного стандарта по специальностям среднего профессионального образования.

Целью методических указаний по выполнению лабораторных работ является организация и управление работой студентов на практических занятиях при изучении данной дисциплины.

Методические указания по выполнению лабораторных работ содержат тематический план и общие положения и требования к оформлению отчетов. Методические указания к каждой лабораторной работе включают в себя следующие элементы: название темы, цель занятия, ход работы, теоретическую часть, практическую часть (указания по выполнению) и контрольные вопросы.

Методические указания содержат лабораторные работы, которые обеспечивают формирование базовых умений и навыков подбора и настраивания конфигурации программного обеспечения компьютерных систем; использования методов защиты программного обеспечения компьютерных систем; проведения инсталляции программного обеспечения компьютерных систем; настройки отдельных компонентов программного

обеспечения компьютерных систем; анализа рисков и характеристики качества программного обеспечения.

Выполнение лабораторных работ предназначено для получения умений и навыков работы с графическими операционными системами персонального компьютера, файловыми системами, программами управления файлами, прикладными программами.

В лабораторных работах, приведенных в данных методических указаниях, содержатся как задания с подробными указаниями к выполнению, так и задания без алгоритма работы.

Методические указания предназначены для студентов очной формы обучения специальности 09.02.07 «Информационные системы и программирование» квалификации - программист. По учебному плану по МДК 04.02 Обеспечение качества функционирования компьютерных систем на лабораторные работы студентов отводится 30 часов.

Методические указания направлены на повышение мотивации учащихся к изучению междисциплинарного курса Проектирование и разработка интерфейсов пользователя, развитие гибкого логического и пространственного мышления учащихся, развитие профессиональных компетенций учащейся молодежи.

ТЕМАТИЧЕСКИЙ ПЛАН ЛАБОРАТОРНЫХ РАБОТ

№ п/п	Наименование лабораторной работы	Кол-во часов
1.	Лабораторная работа №1 «Тестирование программных продуктов»	2
2.	Лабораторная работа №2 «Сравнение результатов тестирования с требованиями технического задания и/или спецификацией».	2
3.	Лабораторная работа №3«Анализ рисков»	2
4.	Лабораторная работа №4 «Выявление первичных и вторичных ошибок»	2
5.	Лабораторная работа №5 «Обнаружение вируса и устранение последствий его влияния»	4
6.	Лабораторная работа №6 «Установка и настройка антивируса. Настройка обновлений с помощью зеркала»	4
7.	Лабораторная работа №7 «Настройка политики безопасности»	4
8.	Лабораторная работа №8 «Настройка браузера»	2
9.	Лабораторная работа №9 «Работа с реестром»	4
10.	Лабораторная работа №10 «Работа с программой восстановления файлов и очистки дисков»	4
	Итого:	**30**

Лабораторная работа №1 «Тестирование программных продуктов»

Цель работы: провести функциональное тестирование разработанного программного средства в соответствии с заданным вариантом
Материально-техническое обеспечение: Компьютер, операционная система Windows 7

Краткие теоретические сведения:

Тестирование программ

Процесс тестирования состоит из трёх этапов:

1. Проектирование тестов.
2. Исполнение тестов.
3. Анализ полученных результатов.

На первом этапе решается вопрос о выборе некоторого подмножества множества тестов, которое сможет найти наибольшее количество ошибок за наименьший промежуток времени. На этапе исполнения тестов проводят, запуск тестов и отлавливают ошибки в тестируемом программном продукте.

Виды тестов

Функциональные тесты составляются на уровне спецификации, до решения задачи. Будущий алгоритм рассматривается как «черный ящик» - функция с неизвестной (или не рассматриваемой) структурой, преобразующая входы в выходы. Суть функциональных тестов: каким бы способом ни решалась задача, при заданных входных значениях должны получиться соответствующие выходные значения.

Структурные тесты составляются для проверки логики решения, или логики работы уже готового алгоритма. Логика определяется последовательностью операций, их условным выполнением или повторением (т.е. композицией базовых конструкций). Совокупность структурных тестов должна обеспечить проверку каждой из таких конструкций.

Чаще всего совокупность тщательно составленных функциональных тестов покрывает множество структурных тестов.

Приведенные понятия различаются тем, что первое рассматривает программу только с точки зрения входов и выходов, тогда как второе относится к ее структуре; но оба понятия не касаются процесса организации тестирования.

Общая последовательность разработки тестов

Наиболее рациональная процедура заключается в том, что сначала разрабатываются функциональные тесты, а затем – структурные.

Функциональное тестирование (тестирование «черного ящика»)

При функциональном тестировании выявляются следующие категории ошибок:

- некорректность или отсутствие функций;
- ошибки интерфейса;
- ошибки в структурах данных;
- ошибки машинных характеристик (нехватка памяти и др.);
- ошибки инициализации и завершения.

Техника тестирования ориентирована:

- на сокращение необходимого количества тестовых вариантов;
- на выявление классов ошибок, а не отдельных ошибок.

Способы функционального тестирования

Разбиение на классы эквивалентности

Это самый популярный способ. Его суть заключается в разделении области входных данных программы на классы эквивалентности и разработке для каждого класса одного тестового варианта.

Класс эквивалентности – набор данных с общими свойствами, в силу чего при обработке любого набора данных этого класса задействуется один и тот же набор операторов.

Классы эквивалентности определяются по спецификации программы. Тесты строятся в соответствии с классами эквивалентности, а именно: выбирается вариант исходных данных некоторого класса и определяются соответствующие выходные данные.

Самыми общими классами эквивалентности являются классы допустимых и недопустимых (аномальных) исходных данных. Описание класса строится как комбинация условий, описывающих каждое входное данное.

Условия допустимости или недопустимости данных задают возможные значения данных и могут описывать:

- некоторое конкретное значение; определяется один допустимый и два недопустимых класса эквивалентности: заданное значение, множество значений меньше заданного, множество значений больше заданного;
- диапазон значений; определяется один допустимый и два недопустимых класса эквивалентности: множество значений в границах диапазона; множество значений, выходящих за левую границу диапазона; множество значений, выходящих за правую границу диапазона;
- множество конкретных значений; определяется один допустимый и один недопустимый класс эквивалентности: заданное множество и множество значений, в него не входящих.

Такие классы можно описать языком логики, например, языком исчисления предикатов. Описания более сложных условий и соответствующих классов (например, элементы массива должны находиться в некотором диапазоне и при этом массив не должен содержать нулевых элементов) могут быть построены на основании приведенных выше условий.

В примере, приводимом в вопросе 2 темы 3, при построении тестов неформально использовался описанный метод. В методических целях были выделены только основные класс тестов. Кроме того, исходя из условия задачи, были выделены классы эквивалентности внутри класса правильных данных.

Анализ граничных значений

Этот способ построения тестов дополняет предыдущий и предполагает анализ значений, лежащих на границе допустимых и недопустимых данных. Построение таких тестов часто диктуется интуицией.

Основные правила построения тестов:

- если условие правильности данных задает диапазон, то строятся тесты для левой и правой границы диапазона; для значений чуть левее левой и чуть правее правой границы;
- если условие правильности данных задает дискретное множество значений, то строятся тесты для минимального и максимального значений; для значений чуть меньше минимума и чуть больше максимума;
- если используются структуры данных с переменными границами (массивы), то строятся тесты для минимального и максимального значения границ.

Диаграммы причин-следствий

Взаимосвязь классов эквивалентности и соответствующих им действий описывается формально в виде графа на основе автоматного подхода. Граф преобразуется в таблицу решений, столбцы которой в свою очередь преобразуются в тестовые варианты.

Порядок выполнения практической работы:

1. Изучить теоретический материал.
2. Выполнить предлагаемые задания.

3. Ответить на контрольные вопросы и предоставить в тетради в виде отчета. Отчет должен включать:
    - номер, наименование практической работы и тему;
    - ответы на контрольные вопросы;
    - выводы.
4. Выполненную работу и отчет по проделанной работе предъявить преподавателю.

Задания для выполнения практической работы:

1) Разработать тестовые наборы для функционального тестирования.
2) Провести тестирование программы и представить результаты в виде таблицы.
3) Выработать рекомендации для корректировки тестируемой программы.
4) Представить отчет по лабораторной работе для защиты.

Отчет состоять из следующих структурных элементов:

1. титульный лист;
2. текстовая часть;

Текстовая часть отчета должна включать пункты:

- условие задачи;
- порядок выполнения
- полученные результаты.

Защита отчета по практической работе заключается в предъявлении преподавателю полученных результатов, демонстрации полученных навыков в ответах на вопросы преподавателя.

Шаблон таблицы для представления результатов

Тест (значения для входных данных)	Ожидаемый результат (значения для выходных данных)	Фактический результат (полученные значения выходных данных)	Результат тестирования (успешно/неуспешно)

Контрольные вопросы:

1. Что такое тестирование ПС?
2. Чем тестирование отличается от отладки ПС?
3. Для чего проводится функциональное тестирование?
4. Что такое комплексное тестирование?
5. Каковы правила тестирования программы «как черного ящика»?
6. Как проводится тестирования программы по принципу «белого ящика»?
7. Что такое модульное тестирование?
8. Как осуществляется сборка программы при модульно тестировании?

Лабораторная работа №2 «Сравнение результатов тестирования с требованиями технического задания и/или спецификацией».

Цель работы: составить описание и выполнить анализ осуществимости разработки информационной системы, выполнить анализ рисков, ознакомиться с основными методами и средствами для реализации и документирования аналитического отчета по проектированию ИС

Материально-техническое обеспечение: Компьютер, операционная система Windows 7

Краткие теоретические сведения:

Техническое задание (также — **техзадание**, **ТЗ**) — технический документ (спецификация), оговаривающий набор требований к системе и утверждённый как заказчиком/пользователем, так и исполнителем/производителем системы. Такая спецификация может содержать также системные требования и требования к тестированию.

Техническое задание позволяет:

• исполнителю — понять суть задачи, показать заказчику «технический облик» будущего изделия, программного изделия или автоматизированной системы;

• заказчику — осознать, что именно ему нужно;

• обеим сторонам — представить готовый продукт;

• исполнителю — спланировать выполнение проекта и работать по намеченному плану;

• заказчику — требовать от исполнителя соответствия продукта всем условиям, оговорённым в ТЗ;

• исполнителю — отказаться от выполнения работ, не указанных в ТЗ;

• заказчику и исполнителю — выполнить попунктную проверку готового продукта (приёмочное тестирование — проведение *испытаний*);

• избежать ошибок, связанных с изменением требований (на всех стадиях и этапах создания, за исключением *испытаний*).

В зависимости от ожиданий заказчика существует три альтернативы для выбора шаблона Технического задания. Если заказчик требует оформления документации в соответствии с государственным стандартом, выбор делается в сторону стандарта ГОСТ 34.602-89. Подготовка Технического задания по ГОСТ 34.602-89 требует значительных временных затрат.

Если поставлены сжатые сроки подготовки ТЗ и заказчик не требует оформления документации в соответствии с государственным стандартом, то можно использовать шаблон технического задания по стандарту IEEE Std 830. Стандарт IEEE Std 830 предполагает, что детальные требования могут быть обширными и не существует оптимальной структуры для всех систем. По этой причине, стандартом рекомендуется обеспечивать такое структурирование детальных требований, которое делает их оптимальными для понимания. Стандартом рекомендуются различные способы структурирования детальных требований для различных классов систем.

Существует и третья альтернатива для выбора шаблона Технического задания, когда заказчик предлагает использовать принятый в компании Корпоративный шаблон для описания требований к информационным системам.

Порядок выполнения практической работы:

1. Изучить теоретический материал.
2. Выполнить предлагаемые задания.
3. Ответить на контрольные вопросы и предоставить в тетради в виде отчета. Отчет должен включать:

- номер, наименование практической работы и тему;
- ответы на контрольные вопросы;
- выводы.

4. Выполненную работу и отчет по проделанной работе предъявить преподавателю.

Задания для выполнения практической работы:

1. Составить подробное описание информационной системы.
2. На основании описания системы провести анализ осуществимости. В ходе анализа ответить на вопросы:

- *Что произойдет с организацией, если система не будет введена в эксплуатацию?*
- *Какие текущие проблемы существуют в организации и как новая система поможет их решить?*
- *Каким образом система будет способствовать целям бизнеса?*
- *Требует ли разработка системы технологии, которая до этого не использовалась в организации?*

Результатом анализа должно явиться заключение о возможности реализации проекта.

4. Заполнить разделы плана:

- *Введение*
- *Организация выполнения проекта*
- *Анализ рисков*

Разделы должны содержать рекомендации относительно разработки системы, базовые предложения по объёму требуемого бюджета, числу разработчиков, времени и требуемому программному обеспечению.

5. Составить отчет о проделанной работе.

Содержание отчета

Каждый студент составляет индивидуальный отчет по лабораторной работе.

В отчете следует указать:

1. Цель работы
2. Постановка задачи (в краткой форме)
3. Введение. Краткое описание целей проекта и проектных ограничений (бюджетных, временных и т.д.), которые важны для управления проектом
4. План проекта (ресурсы, необходимые для реализации проекта, разделение работ на этапы и временной график выполнения этих этапов)
5. Анализ рисков
6. Анализ осуществимости:

a) Характеристика основных элементов объекта проектирования.

1.1. Цели и задачи объекта

1.2. Организационная структура объекта (словесное и графическое описание)

1.3. Основные функции объекта (словесное и графическое описание)

1.4. Основные бизнес-процессы объекта (словесное описание)

b) Характеристика обеспечивающих элементов объекта проектирования.

2.1. Информационное обеспечение объекта

2.2. Документационное и методическое обеспечение объекта

2.3. Техническое обеспечение объекта

2.4. Кадровое обеспечение объекта

c) Технико-экономическое обоснование проекта

d) Книга бизнес-процессов предприятия (графическое представление)

7. Предварительный список актеров (на базе предыдущих отчетов)
8. Общая спецификация требований к информационной системе (на основе анализа деятельности предприятия)
9. Предварительный глоссарий
10. Заключение (выводы)

11. Список используемой литературы

Контрольные вопросы:

1. Что такое требования к системе. Способы сбора требований.
2. Основные методы описания требований к системе.
3. Основные инструменты визуализации требований.
4. Смысл и назначение технико-экономического обоснования
5. Определение бизнес-процесса.

Лабораторная работа №3 «Анализ рисков»

Цель работы: «Изучение методологии управления проектами. Получение навыков по применению данных методологий для планирования проекта»
Материально-техническое обеспечение: Компьютер, операционная система Windows 7

Краткие теоретические сведения:

Основные понятия

Проблемы управления программными проектами впервые проявились в 60-х — начале 70-х годов. Руководители программных проектов выполняют такую же работу, что и руководители технических проектов. Вместе с тем процесс разработки ПО существенно отличается от процессов реализации технических проектов, что порождает определенные сложности в управлении программными проектами. Ниже приведён краткий список этих отличий.

1. *Программный продукт нематериален.* Менеджер технического проекта видит результаты выполнения своего проекта. Если реализация проекта отстает от графика, это также видно воочию. В противоположность этому программное обеспечение нематериально. Его нельзя увидеть или потрогать. Менеджер программного проекта не видит процесс "роста" разрабатываемого ПО. Он может полагаться только на документацию, которая фиксирует процесс разработки программного продукта.
2. *Не существует стандартных процессов разработки ПО.* На сегодняшний день не существует четкой зависимости между процессом создания ПО и типом создаваемого программного продукта. Другие технические дисциплины имеют длительную историю, процессы разработки технических изделий многократно опробованы и проверены. Процессы создания большинства технических систем хорошо изучены. Изучением же процессов создания ПО специалисты занимаются только несколько последних лет. Поэтому пока нельзя точно предсказать, на каком этапе процесса разработки ПО могут возникнуть проблемы, угрожающие всему программному проекту.
3. *Большие программные проекты - это часто "одноразовые" проекты.* Большие программные проекты, как правило, значительно отличаются от проектов, реализованных ранее. Поэтому, чтобы уменьшить неопределенность в планировании проекта, руководители проектов должны обладать очень большим практическим опытом. Но постоянные технологические изменения в компьютерной технике и коммуникационном оборудовании обесценивают предыдущий опыт. Знания и навыки, накопленные опытом, могут не востребоваться в новом проекте.

Перечисленное выше может привести к тому, что реализация проекта выйдет из временного графика или превысит бюджетные ассигнования. Программные системы зачастую оказываются новинками как в "идеологическом", так и в техническом плане. Технические проекты, которые являются инновационными (например, новая транспортная система), также часто нарушают временные графики работ. Поэтому, предвидя возможные проблемы в реализации программного проекта, следует всегда помнить, что многим из них свойственно выходить за рамки временных и бюджетных ограничений.

Планирование проекта

Эффективное управление программным проектом напрямую зависит от правильного планирования работ, необходимых для его выполнения. План помогает менеджеру предвидеть проблемы, которые могут возникнуть на каких-либо этапах создания ПО, и разработать превентивные меры для их предупреждения или решения. План, разработанный на начальном этапе проекта, рассматривается всеми его участниками как руководящий документ, выполнение которого должно привести к успешному завершению проекта. Этот первоначальный план должен максимально подробно описывать все этапы реализации проекта.

Кроме разработки плана проекта, на менеджера ложится обязанность разработки других видов планов. Эти виды планов кратко описаны в табл. 1.

Таблица 1 - Виды планов

План	**Описание**
План качества	Описывает стандарты и мероприятия по поддержке качества разрабатываемого ПО
План аттестации	Описывает способы, ресурсы и перечень работ, необходимых для аттестации программной системы
План управления конфигурацией	Описывает структуру и процессы управления конфигурацией
План сопровождения ПО	Предлагает план мероприятий, требующихся для сопровождения ПО в процессе его эксплуатации, а также расчет стоимости сопровождения и необходимые для этого ресурсы
План по управлению персоналом	Описывает мероприятия, направленные на повышение квалификации членов команды разработчиков

В листинге 1 показан процесс планирования создания ПО в виде псевдокода. Здесь сделан акцент на том, что планирование — это итерационный процесс. Поскольку в процессе выполнения проекта постоянно поступает новая информация, план должен регулярно пересматриваться. Важными факторами, которые должны учитываться при разработке плана, являются финансовые и деловые обязательства организации. Если они изменяются, эти изменения также должны найти отражение в плане работ.

Листинг 1. Процесс планирования проекта

```
Определение проектных ограничений
Первоначальная оценка параметров проекта
Определение этапов выполнения проекта и контрольных отметок
while пока проект не завершится или не будет остановлен loop
Составление графика работ
Начало выполнения работ
Ожидание окончания очередного этапа работ
Отслеживание хода выполнения работ
Пересмотр оценок параметров проекта
Изменение графика работ
Пересмотр проектных ограничений
if (возникла проблема) then
Пересмотр технических или организационных параметров проекта
end if
end loop
```

Процесс планирования начинается с определения проектных ограничений (временные ограничения, возможности наличного персонала, бюджетные ограничения и т.д.). Эти ограничения должны определяться параллельно с оцениванием проектных параметров, таких как структура и размер проекта, а также распределением функций среди исполнителей. Затем определяются этапы разработки и то, какие результаты документация, прототипы, подсистемы или версии программного продукта) должны быть получены по окончании этих этапов. Далее начинается циклическая часть планирования. Сначала разрабатывается график работ по выполнению проекта или дается разрешение на продолжение использования ранее созданного графика. После этого (обычно через 2-3 недели) проводится контроль выполнения работ и отмечаются расхождения между реальным и плановым ходом работ.

Далее, по мере поступления новой информации о ходе выполнения проекта, возможен пересмотр первоначальных оценок параметров проекта. Это, в свою очередь, может привести к изменению графика работ. Если в результате этих изменений нарушаются

сроки завершения проекта, должны быть пересмотрены (и согласованы с заказчиком ПО) проектные ограничения.

Конечно, большинство менеджеров проектов не думают, что реализация их проектов пройдет гладко, без всяких проблем. Желательно описать возможные проблемы еще до того, как они проявят себя в ходе выполнения проекта. Поэтому лучше составлять "пессимистические" графики работ, чем "оптимистические". Но, конечно, невозможно построить план, учитывающий все, в том числе случайные, проблемы и задержки выполнения проекта, поэтому и возникает необходимость периодического пересмотра проектных ограничений и этапов создания программного продукта.

План проекта

План проекта должен четко показать ресурсы, необходимые для реализации проекта, разделение работ на этапы и временной график выполнения этих этапов. В некоторых организациях план проекта составляется как единый документ, содержащий все виды планов, описанных выше. В других случаях план проекта описывает только технологический процесс создания ПО. В таком плане обязательно присутствуют ссылки на планы других видов, но они разрабатываются отдельно от плана проекта.

План, представленны ниже, принадлежит именно к последнему типу планов. Детализация планов проектов очень разнится в зависимости от типа разрабатываемого программного продукта и организации-разработчика. Но в любом случае большинство планов содержат следующие разделы.

1. *Введение.* Краткое описание целей проекта и проектных ограничений (бюджетных, временных и т.д.), которые важны для управления проектом.
2. *Организация выполнения проекта.* Описание способа подбора команды разработчиков и распределение обязанностей между членами команды.
3. *Анализ рисков.* Описание возможных проектных рисков, вероятности их проявления и стратегий, направленных на их уменьшение. Тема управления рисками рассмотрена ниже.
4. *Аппаратные и программные ресурсы, необходимые для реализации проекта.* Перечень аппаратных средств и программного обеспечения, необходимого для разработки программного продукта. Если аппаратные средства требуется закупать, приводится их стоимость совместно с графиком закупки и поставки.
5. *Разбиение работ на этапы.* Процесс реализации проекта разбивается на отдельные процессы, определяются этапы выполнения проекта, приводится описание результатов ("выходов") каждого этапа и контрольные отметки. Эта тема представлена ниже.
6. *График работ.* В этом графике отображаются зависимости между отдельными процессами (этапами) разработки ПО, оценки времени их выполнения и распределение членов команды разработчиков по отдельным этапам.
7. *Механизмы мониторинга и контроля за ходом выполнения проекта.* Описываются предоставляемые менеджером отчеты о ходе выполнения работ, сроки их предоставления, а также механизмы мониторинга всего проекта.

План должен регулярно пересматриваться в процессе реализации проекта. Одни части плана, например график работ, изменяются часто, другие более стабильны. Для внесения изменений в план требуется специальная организация документопотока, позволяющая отслеживать эти изменения.

Контрольные отметки этапов работ

Менеджеру для организации процесса создания ПО и управления им необходима информация. Поскольку само программное обеспечение неосязаемо, эта управленческая информация может быть получена только в виде документов, отображающих выполнение очередного этапа разработки программного продукта. Без этой информации нельзя судить о степени готовности создаваемого продукта, невозможно оценить произведенные затраты или изменить график работ.

При планировании процесса определяются контрольные отметки— вехи, отмечающие окончание определенного этапа работ. Для каждой контрольной отметки создается отчет, который предоставляется руководству проекта. Эти отчеты не должны быть большими объемными документами; они должны подводить краткие итоги окончания отдельного логически завершенного этапа проекта. Этапом не может быть, например, "Написание 80% кода программ", поскольку невозможно проверить завершение такого "этапа"; кроме того, подобная информация практически бесполезна для управления, поскольку здесь не отображается связь этого "этапа" с другими этапами создания ПО.

Обычно по завершении основных больших этапов, таких как разработка спецификации, проектирование и т.п., заказчику ПО предоставляются результаты их выполнения, так называемые контрольные проектные элементы. Это может быть документация, прототип программного продукта, законченные подсистемы ПО и т.д. Контрольные проектные элементы, предоставляемые заказчику ПО, могут совпадать с контрольными отметками (точнее, с результатами выполнения какого-либо этапа). Но обратное утверждение неверно. Контрольные отметки — это внутренние проектные результаты, которые используются для контроля за ходом выполнения проекта, и они, как правило, не предоставляются заказчику ПО.

Для определения контрольных отметок весь процесс создания ПО должен быть разбит на отдельные этапы с указанным "выходом" (результатом) каждого этапа. Например, на рис. 1 показаны этапы разработки спецификации требований в случае, когда для ее проверки используется прототип системы, а также представлены выходные результаты (контрольные отметки) каждого этапа. Здесь контрольными проектными элементами являются требования и спецификация требований.

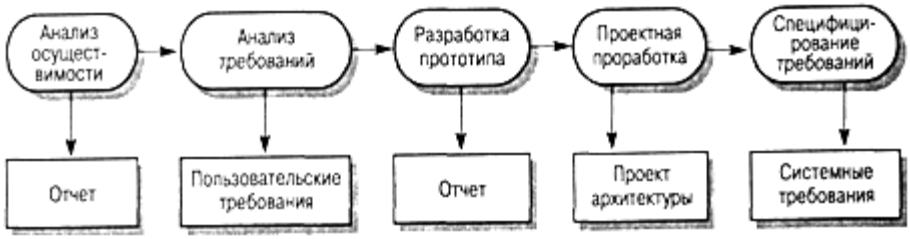


Рис. 1. Этапы процесса разработки спецификации

График работ

Составление графика - одна из самых ответственных работ, выполняемых менеджером проекта. Здесь менеджер оценивает длительность проекта, определяет ресурсы, необходимые для реализации отдельных этапов работ, и представляет их (этапы) в виде согласованной последовательности. Если данный проект подобен ранее реализованному, то график работ последнего проекта можно взять за основу для данного проекта. Но затем следует учесть, что на отдельных этапах нового проекта могут использоваться методы и подходы, отличные от использованных ранее.

Если проект является инновационным, первоначальные оценки длительности и требуемых ресурсов наверняка будут слишком оптимистичными, даже если менеджер попытается предусмотреть все возможные неожиданности. С этой точки зрения проекты создания ПО не отличаются от больших инновационных технических проектов. Новые аэропорты, мосты и даже новые автомобили, как правило, появляются позже первоначально объявленных сроков их сдачи или поступления на рынок, чему причиной являются неожиданно возникшие проблемы и трудности. Именно поэтому графики работ необходимо постоянно обновлять по мере поступления новой информации о ходе выполнения проекта.

В процессе составления графика (рис. 2) весь массив работ, необходимых для реализации проекта, разбивается на отдельные этапы и оценивается время, требующееся для выполнения каждого этапа. Обычно многие этапы выполняются параллельно. График работ должен предусматривать это и распределять производственные ресурсы между ними

наиболее оптимальным образом. Нехватка ресурсов для выполнения какого-либо критического этапа - частая причина задержки выполнения всего проекта.

Длительность этапов обычно должна быть не меньше недели. Если она будет меньше, то окажется ниже точности временных оценок этапов, что может привести к частому пересмотру графика работ. Также целесообразно (в аспекте управления проектом) установить максимальную длительность этапов, не превышающую 8 или 10 недель. Если есть этапы, имеющие большую длительность, их следует разбить на этапы меньшей длительности.

При расчете длительности этапов менеджер должен учитывать, что выполнение любого этапа не обойдется без больших или маленьких проблем и задержек. Разработчики могут допускать ошибки или задерживать свою работу, техника может выйти из строя либо аппаратные или программные средства поддержки процесса разработки могут поступить с опозданием. Если проект инновационный и технически сложный, это становится дополнительным фактором появления непредвиденных проблем и увеличения длительности реализации проекта по сравнению с первоначальными оценками.

Требования к ПО

Диаграммы процессов и временные диаграммы

Рис. 2.- Процесс составления графика работ

Кроме временных затрат, менеджер должен рассчитать другие ресурсы, необходимые для успешного выполнения каждого этапа. Особый вид ресурсов — это команда разработчиков, привлеченная к выполнению проекта. Другими видами ресурсов могут быть необходимое свободное дисковое пространство на сервере, время использования какого-либо специального оборудования и бюджетные средства на командировочные расходы персонала, работающего над проектом.

Существует хорошее эмпирическое правило: оценивать временные затраты так, как будто ничего непредвиденного и "плохого" не может случиться, затем увеличить эти оценки для учета возможных проблем. Возможные, но трудно прогнозируемые проблемы существенно зависят от типа и параметров проекта, а также от квалификации и опыта членов команды разработчиков. К исходным расчетным оценкам рекомендуется добавлять 30% на возможные проблемы и затем еще 20%, чтобы быть готовым к тому, что невозможно предвидеть.

График работ по проекту обычно представляется в виде набора диаграмм и графиков, показывающих разбиение проектных работ на этапы, зависимости между этапами и распределение разработчиков по этапам.

Временны*е* и сетевые диаграммы

Временные и сетевые диаграммы полезны для представления графика работ. Временная диаграмма показывает время начала и окончания каждого этапа и его длительность. Сетевая диаграмма отображает зависимости между различными этапами проекта. Эти диаграммы можно создать автоматически с помощью программных средств поддержки управления на основе информации, заложенной в базе данных проекта.

Рассмотрим этапы некоего проекта, представленные в табл. 2, из которой, в частности, видно, что этап Т3 зависит от этапа Т1. Это значит, что этап Т1 должен завершиться прежде, чем начнется этап Т3. Например, на этапе Т1 проводится компонентный анализ создаваемого программного продукта, а на этапе Т3 — проектирование системы.

На основе приведенных значений длительности этапов и зависимости между ними строится сетевой график последовательности этапов (рис. 3). На этом графике видно, какие работы могут выполняться параллельно, а какие должны выполняться

последовательно друг за другом. Этапы обозначены прямоугольниками. Контрольные отметки и контрольные проектные элементы показаны в виде овалов и обозначены (как и в табл. 2) буквой М с соответствующим номером. Даты на данной диаграмме соответствуют началу выполнения этапов. Сетевую диаграмму следует читать слева направо и сверху вниз.

Таблица 2 - Этапы проекта

Этап	Длительность (дни)	Зависимость
Т1	8	
Т2	15	
Т3	15	Т1 (М1)
Т4	10	
Т5	10	Т2, Т4 (М2)
Т6	5	Т1, Т2 (М3)
Т7	20	Т1 (М1)
Т8	25	Т4 (М5)
Т9	15	Т3, Т6 (М4)
Т10	15	Т5, Т7 (М7)
Т11	7	Т9 (М6)
Т12	10	Т11 (М8)

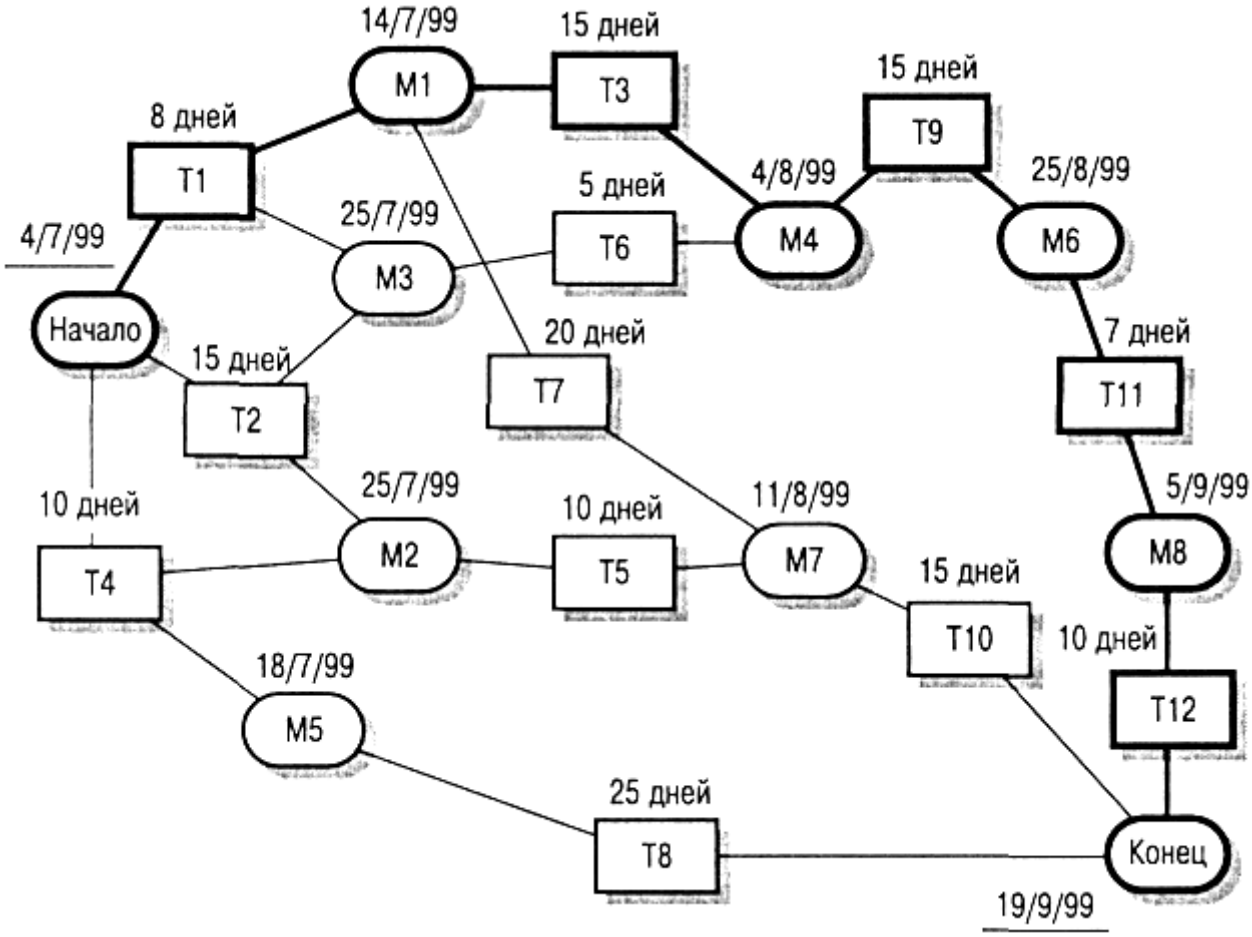


Рис. 3. Сетевая диаграмма этапов

Если для создания сетевой диаграммы используются программные средства поддержки управления проектом, каждый этап должен заканчиваться контрольной отметкой. Очередной этап может начаться только тогда, когда будет получена контрольная отметка

(которая может зависеть от нескольких предшествующих этапов). Поэтому в третьем столбце табл. 2 приведены контрольные отметки; они будут достигнуты только тогда, когда будет завершен этап, в строке которого помещена соответствующая контрольная отметка.

Любой этап не может начаться, пока не выполнены все этапы на всех путях, ведущих от начала проекта к данному этапу. Например, этап Т9 не может начаться, пока не будут завершены этапы Т3 и Т6. Отметим, что в данном случае достижение контрольной отметки М4 говорит о том, что эти этапы завершены.

Минимальное время выполнения всего проекта можно рассчитать, просуммировав в сетевой диаграмме длительности этапов на самом длинном пути (длина пути здесь измеряется не количеством этапов на пути, а суммарной длительностью этих этапов) от начала проекта до его окончания (это так называемый критический путь). В нашем случае продолжительность проекта составляет 11 недель или 55 рабочих дней. На рис. 3 критический путь показан более толстыми линиями, чем остальные пути. Таким образом, общая продолжительность реализации проекта зависит от этапов работ, находящихся на критическом пути. Любая задержка в завершении любого этапа на критическом пути приведет к задержке всего проекта.

Задержка в завершении этапов, не входящих в критический путь, не влияет на продолжительность всего проекта до тех пор, пока суммарная длительность этих этапов (с учтом задержек) на каком-нибудь пути не превысит продолжительности работ на критическом пути. Например, задержка этапа Т8 на срок, меньший 20 дней, никак не влияет на общую продолжительность проекта. На рис. 4 представлена временная диаграмма, на которой показаны возможные задержки на каждом этапе.

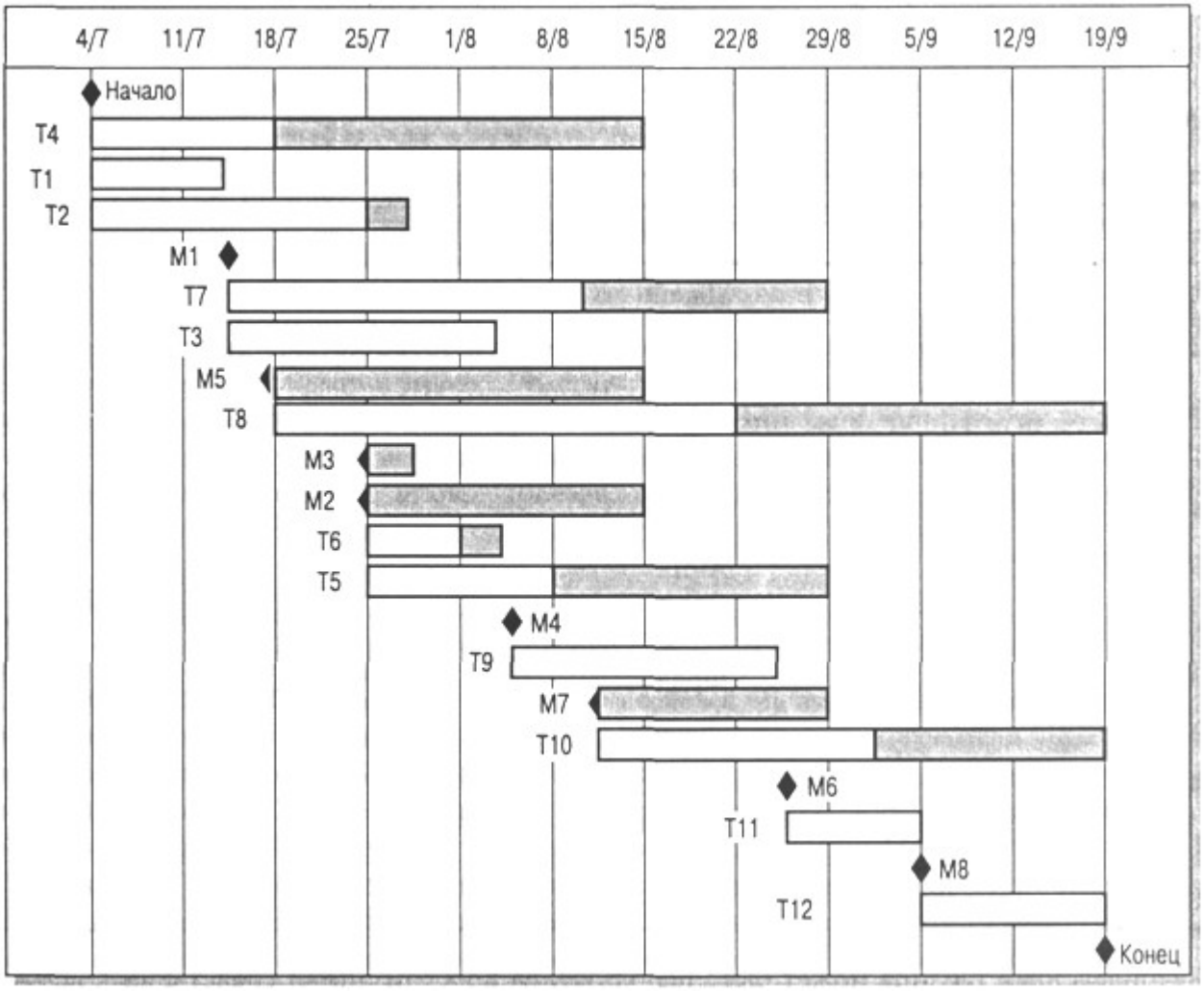


Рис. 4. Временная диаграмма длительности этапов

Сетевая диаграмма позволяет увидеть в зависимости этапов значимость того или иного этапа для реализации всего проекта. Внимание к этапам критического пути часто позволяет найти способы их изменения с тем, чтобы сократить длительность всего проекта. Менеджеры используют сетевую диаграмму для распределения работ.

На рис. 4 показано другое представление графика работ. Это временная диаграмма (иногда называемая по имени ее изобретателя диаграммой Гантта) может быть построена программными средствами поддержки процесса управления. Она показывает длительность выполнения каждого этапа и возможные их задержки (показаны затененными прямоугольниками), а также даты начала и окончания каждого этапа. Этапы критического пути не имеют затененных прямоугольников; это означает, что задержка с завершением данных этапов приведет к увеличению длительности всего проекта.

Подобно распределению времени выполнения этапов, менеджер должен рассчитать распределение ресурсов по этапам, в частности назначить исполнителей на каждый этап. В табл. 3 приведено распределение разработчиков на каждый этап, представленный на рис. 4.

Таблица 3 - Распределение исполнителей по этапам

Этап	**Исполнитель**
T1	Джейн
T2	Анна
T3	Джейн
T4	Фред
T5	Мэри
T6	Анна
T7	Джим
T8	Фред
T9	Джейн
T10	Анна
T11	Фред
T12	Фред

Приведенная таблица может быть использована программными средствами поддержки процесса управления для построения временной диаграммы занятости сотрудников на определенных этапах работ (рис. 5). Персонал не занят в работе над проектом все время его реализации. В течение периода незанятости сотрудники могут быть в отпуске, работать над другими проектами, проходить обучение и т.д.

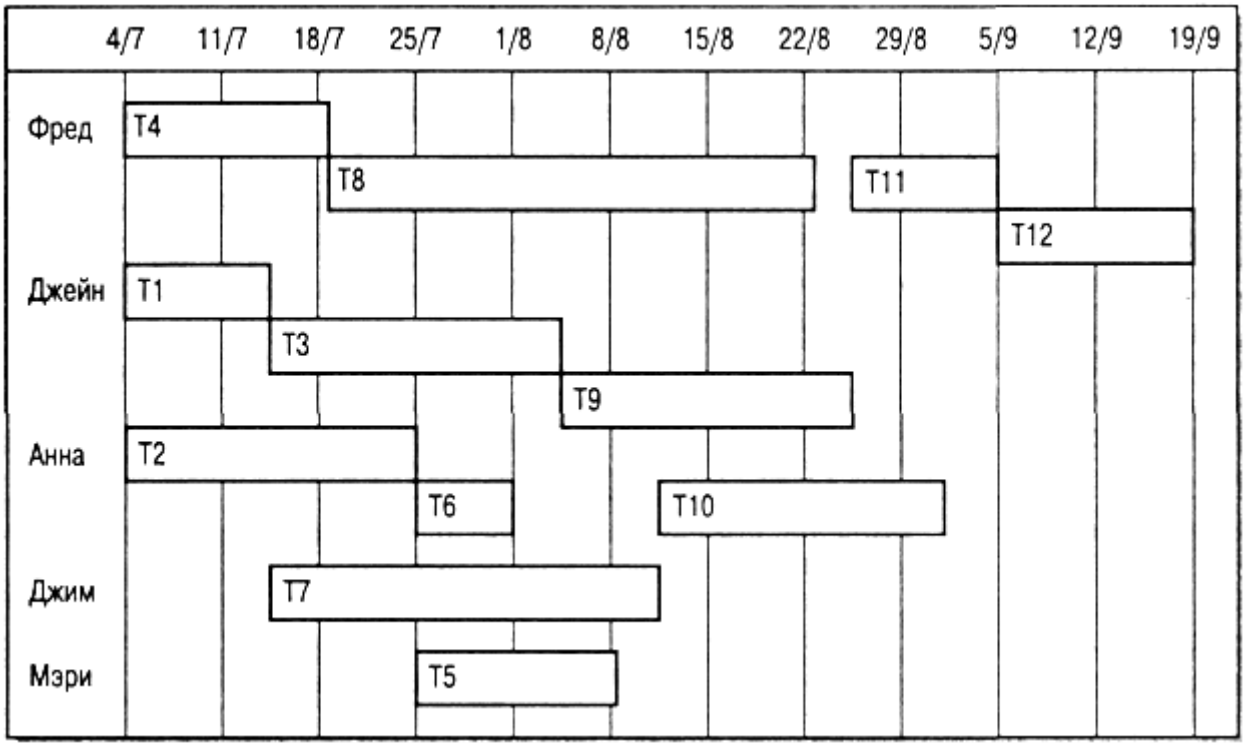


Рис. 5. Временная диаграмма распределения работников по этапам

В больших организациях обычно работает много специалистов, которые задействуются в проекте по мере необходимости. Конечно, такой подход может создать определенные проблемы для менеджеров проектов. Например, если специалист занят в проекте, который задерживается, это может создать прямые сложности для других проектов, где он также должен участвовать.

Первоначальный график работ неизбежно содержит какие-нибудь ошибки или недоработки. По мере реализации проекта рассчитанные оценки длительности выполнения этапов работ должны сравниваться с реальными сроками выполнения этих этапов. Результаты сравнения должны использоваться в качестве основы для пересмотра графика работ еще не реализованных этапов проекта, в частности для того, чтобы попытаться уменьшить длительность этапов критического пути.

Управление рисками

Важной частью работы менеджера проекта является оценка рисков, которые могут повлиять на график работ или на качество создаваемого программного продукта, и разработка мероприятий по предотвращению рисков. Результаты анализа рисков должны быть отражены в плане проекта. Определение рисков и разработка мероприятий по уменьшению их влияния на ход выполнения проекта называется управлением рисками.

Упрощенно риск можно понимать как вероятность проявления каких-либо неблагоприятных обстоятельств, негативно влияющих на реализацию проекта. Риски могут угрожать проекту в целом, создаваемому программному продукту или организации-разработчику. Можно выделить три типа рисков.

1. *Риски для проекта,* которые влияют на график работ или ресурсы, необходимые для выполнения проекта.
2. *Риски для разрабатываемого продукта,* влияющие на качество или производительность разрабатываемого программного продукта.
3. *Бизнес-риски,* относящиеся к организации-разработчику или поставщикам.

Конечно, эти типы рисков могут пересекаться. Например, если опытный программист покидает проект, это будет риском для проекта (поскольку задерживается срок сдачи готового продукта), риском для продукта (так как новый программист, заменивший ушедшего, может оказаться не слишком опытным и сделать ошибки в программе) и

бизнес-риском (поскольку задержка данного проекта может негативно повлиять на будущие деловые контакты между заказчиком и организацией-разработчиком).

Конкретные типы рисков, которые могут оказать влияние на данный проект, зависят от вида создаваемого программного продукта и от организационного окружения, где реализуется программный проект. Вместе с тем многие типы рисков способны повлиять на любые программные проекты, эти риски приведены в табл. 4.

Таблица 4 - Возможные риски программных проектов

Риск	**Типы риска**	**Описание риска**
Текучесть разработчиков	Риск для проекта	Опытные разработчики покидают проект до его завершения
Изменение в управлении организацией	Риск для проекта	Организация меняет свои приоритеты в управлении проектом
Неготовность аппаратных средств	Риск для проекта	Аппаратные средства, которые необходимы для проекта, не поступили вовремя или не готовы к эксплуатации
Изменение требований	Риск для проекта и для разрабатываемого продукта	Появление большого количества непредвиденных изменений в требованиях, предъявляемых к разрабатываемому ПО
Задержка в разработке спецификации	Риск для проекта и для разрабатываемого продукта	Спецификации основных интерфейсов подсистем не поступили к разработчикам в соответствии с графиком работ
Недооценка размера разрабатываемой системы	Риск для проекта и для разрабатываемого продукта	Размер системы значительно превысил первоначальную оценку
Недостаточная эффективность CASE -средств	Риск для разрабатываемого продукта	CASE-средства, предназначенные для поддержки проекта, оказались менее эффективными, чем ожидалось
Изменения в технологии разработки ПО	Бизнес-риск	Основные технологии построения программной системы заменяются новыми
Появление конкурирующего программного продукта	Бизнес-риск	На рынке программных продуктов до окончания проекта появилась конкурирующая программная система

Схема процесса управления рисками показана на рис. 6. Этот процесс состоит из четырех стадий.

1. *Определение рисков.* Определяются возможные риски для проекта, для разрабатываемого продукта и бизнес-риски.
2. *Анализ рисков.* Оценивается вероятность и последовательность появления рисковых ситуаций.
3. *Планирование рисков.* Планируются мероприятия по предотвращению рисков или минимизации их воздействия на проект.
4. *Мониторинг рисков.* Постоянное оценивание вероятностей рисков и выполнение мероприятий по смягчению последствий проявления рисковых ситуаций.

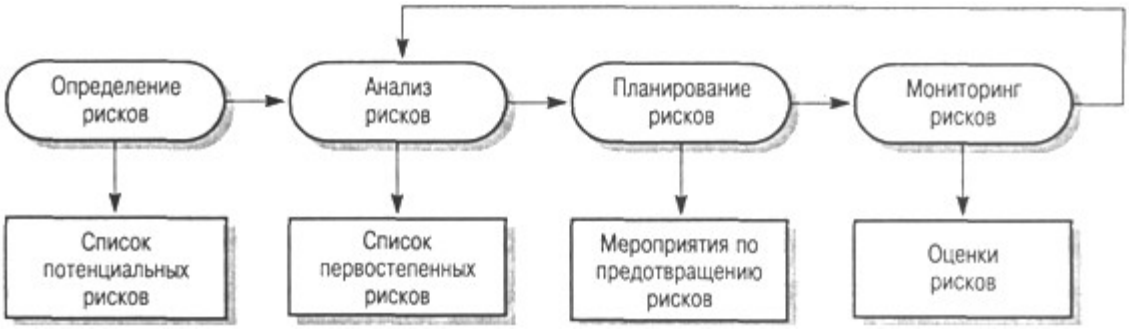


Рис. 6. Процесс управления рисками

Процесс управления рисками, как и другие процессы планирования, является итерационным, выполняемым в течение всего срока реализации проекта. Сначала разрабатываются планы управления рисками, затем постоянно отслеживается ситуация вокруг реализации проекта. При поступлении новой информации о возможных рисках заново проводится анализ рисков и первостепенное внимание уделяется новым рискам. По мере поступления новой информации также изменяются планы мероприятий по предотвращению и смягчению рисков.

Результаты процесса управления рисками документируются в виде планов управления рисками. Они должны включать описание возможных проектных рисков, их анализ и перечень мероприятий, необходимых для управления рисками.

Определение рисков

Определение рисков — первая стадия процесса управления рисками. На этой стадии описываются риски, которые могут проявиться при реализации проекта. В принципе на этой стадии не должна оцениваться вероятность и значимость рисков, но на практике маловероятные риски с незначительными последствиями обычно отбрасываются сразу.

Определение рисков может выполняться в режиме командной работы с использованием подхода "мозговой штурм" либо основываться на опыте менеджера. При определении рисков может помочь приведенный ниже список возможных категорий рисков.

1. *Технологические риски.* Проистекают из программных и аппаратных технологий, на основе которых разрабатывается система.
2. *Риски, связанные с персоналом.* Связаны с членами команды разработчиков.
3. *Организационные риски.* Проистекают из организационного окружения, в котором выполняется проект.
4. *Инструментальные риски.* Связаны с используемыми CASE-средствами и другими средствами поддержки процесса создания ПО.
5. *Риски, связанные с системными требованиями.* Проявляются при изменении требований, предъявляемых к разрабатываемой системе.
6. *Риски оценивания.* Связаны с оцениванием характеристик программной системы и ресурсов, необходимых для реализации проекта.

В табл. 5 представлены некоторые примеры, относящиеся к каждой из описанных категорий рисков. Результатом этапа определения рисков будет длинный список возможных рисков, которые могут повлиять на разрабатываемый программный продукт, проект или организацию-разработчика.

Таблица 5 - Категории рисков

Категория рисков	**Примеры рисков**
Технологические риски	База данных, которая используется в программной системе, не обеспечивает обработку ожидаемого объема транзакций. Программные компоненты, которые используются повторно, имеют дефекты, ограничивающие их функциональные возможности
Риски, связанные с персоналом	Невозможно подобрать работников с требуемым профессиональным уровнем. Ведущий разработчик заболел в самое критическое время.

	Невозможно организовать необходимое обучение персонала
Организационные риски	В организации, выполняющей разработку ПО, произошла реорганизация, в результате чего изменились приоритеты в управлении проектом. Финансовые затруднения в организации привели к уменьшению бюджета проекта
Инструментальные риски	Программный код, генерируемый CASE-средствами, не эффективен. CASE-средства невозможно интегрировать с другими средствами поддержки проекта
Риски, связанные с системными требованиями	Изменения требований приводят к значительным повторным темными требованиями работам по проектированию системы. Первоначальная нечеткая формулировка пользовательских требований привела к значительным изменениям системных требований, проявившихся на поздних стадиях разработки проекта
Риски оценивания	Недооценки времени выполнения проекта. Скорость выявления дефектов в системе ниже ранее запланированной. Размер системы значительно превышает первоначально рассчитанный

Анализ рисков

При анализе для каждого определенного риска подсчитывается вероятность его проявления и ущерб, который он может нанести. Не существует простых методов выполнения анализа рисков — в значительной мере он основан на мнении и опыте менеджера. Можно привести следующую шкалу вероятностей рисков и их последствий.

1. Вероятность риска считается очень низкой, если она имеет значение менее 10%; низкой, если ее значение от 10 до 25 %; средней при значениях от 25 до 50%; высокой, если значение колеблется от 50 до 75%; очень высокой при значениях более 75%.
2. Возможный ущерб от рисковых ситуаций можно подразделить на катастрофический, серьезный, терпимый и незначительный.

Результаты анализа рисков должны быть представлены в виде таблицы рисков, упорядоченных по степени возможного ущерба. В табл. 6 приведен упорядоченный список рисков, описанных в табл. 5; там же указаны вероятности этих рисков. Здесь вероятности рисков и степень ущерба от них указаны произвольно. На практике для их определения необходима подробная информация о проекте, технологии создания ПО, команде разработчиков и о самой организации.

Таблица 6 - Список рисков после проведения их анализа

Риск	**Вероятность**	**Степень ущерба**
Финансовые затруднения в организации привели к уменьшению бюджета проекта	Низкая	Катастрофическая
Невозможно подобрать работников с требующимся профессиональным уровнем	Высокая	Катастрофическая
Ведущий разработчик заболел в самое критическое время	Средняя	Серьезная
Программные компоненты, используемые повторно, имеют дефекты, ограничивающие их функциональные возможности	Средняя	Серьезная
Изменения требований приводят к значительным повторным работам по проектированию системы	Средняя	Серьезная
В организации, выполняющей разработку ПО, произошла реорганизация, в результате чего	Высокая	Серьезная

изменились приоритеты в управлении проектом		
База данных, которая используется в программной системе, не обеспечивает обработку ожидаемого объема транзакций	Средняя	Серьезная
Недооценки времени выполнения проекта	Высокая	Серьезная
CASE-средства невозможно интегрировать с другими средствами поддержки проекта	Высокая	Терпимая
Первоначальная нечеткая формулировка пользовательских требований привела к значительным изменениям системных требований, проявившихся на поздних стадиях разработки проекта	Средняя	Терпимая
Невозможно организовать необходимое обучение персонала	Средняя	Терпимая
Скорость выявления дефектов в системе ниже ранее спланированной	Средняя	Терпимая
Размер системы значительно превышает первоначально рассчитанный	Высокая	Терпимая
Программный код, генерируемый CASE-средствами, неэффективен	Средняя	Незначительная

Конечно, как вероятность рисков, так и возможный ущерб от них должны пересматриваться при поступлении дополнительной информации об этих рисках и по мере реализации мероприятий по управлению ими. Поэтому подобные таблицы рисков должны переделываться на каждой итерации процесса управления рисками.

После проведения анализа рисков определяются наиболее значимые риски, которые затем отслеживаются на протяжении всего срока выполнения проекта. Определение этих значимых рисков зависит от их вероятностей и возможного ущерба. В общем случае всегда отслеживаются риски с катастрофическими последствиями, а также риски с серьезным ущербом, значение вероятности которых выше среднего.

В некоторых статьях рекомендуется определить и отслеживать "10 верхних" рисков, но это не всегда обоснованная рекомендация. Количество рисков, которые необходимо отслеживать, зависит от конкретного проекта. Это может быть пять рисков, а может — пятнадцать. Но, конечно, количество рисков, по которым проводится мониторинг, должно быть обозримым. Большое количество отслеживаемых рисков потребует огромного количества собираемой информации. Из списка рисков, представленных в табл. 6, для мониторинга следует отобрать те риски, которые могут привести к катастрофическим и серьезным последствиям для вашего проекта.

Планирование рисков

Планирование заключается в определении стратегии управления каждым значимым риском, отобранным для мониторинга после анализа рисков. Здесь также не существует общепринятых подходов для разработки таких стратегий — многое основывается на "чутье" и опыте менеджера проекта. В табл. 7 показаны возможные стратегии управления основными рисками, приведенными в табл. 6.

Таблица 7 - Стратегии управления рисками

Риск	**Стратегия**
Финансовые проблемы организации	Подготовить краткий документ для руководства организации, показывающий важность данного проекта для достижения финансовых целей организации
Проблемы неквалифицированного персонала	Предупредить заказчика о потенциальных трудностях и возможной задержке проекта, рассмотреть вопрос о покупке компонентов системы

Болезни персонала	Реорганизовать работу команды разработчиков таким образом, чтобы обязанности и работа членов команды перекрывали друг друга, вследствие этого разработчики будут знать и понимать задачи, выполняемые другими сотрудниками
Дефектные системные компоненты	Заменить потенциально дефектные системные компоненты покупными компонентами, гарантирующими качество работы
Изменения требований	Попытаться определить требования, наиболее вероятно подверженные изменениям; в структуре системы не отображать детальную информацию
Реорганизация компании-разработчика	Подготовить краткий документ для руководства компании, показывающий важность данного проекта для достижения финансовых целей компании
Недостаточная производительность базы данных	Рассмотреть возможность покупки более производительной базы данных
Недооценки времени выполнения проекта	Рассмотреть вопрос о покупке системных компонентов, исследовать возможность использования генератора программного кода

Существует три категории стратегий управления рисками.

1. *Стратегии предотвращения рисков.* Согласно этим стратегиям следует проводить мероприятия, снижающие вероятность проявления рисков. Примером может служить стратегия исключения потенциально дефектных компонентов, описанная в табл. 7.
2. *Минимизационные стратегии.* Направлены на уменьшение возможного ущерба от рисков. Примером служит стратегия уменьшения ущерба от болезни членов команды разработчиков (см. табл. 7).
3. *Планирование "аварийных" ситуаций.* Согласно этим стратегиям необходимо иметь план мероприятий, которые следует выполнить в случае проявления рисковой ситуации. В табл. 7 это стратегия поведения при возникновении финансовых проблем у организации-разработчика.

Мониторинг рисков

Мониторинг рисков заключается в регулярном пересчете вероятностей рисков и ущерба, который они могут нанести. Для этого необходимо постоянно отслеживать факторы, которые влияют на вероятность рисков и возможный ущерб. Эти факторы зависят от типов риска. В табл. 8 приведены признаки, которые помогают определить тип риска.

Таблица 8 - Признаки рисков

Тип риска	**Признаки**
Технологические риски	Задержки в поставке оборудования или программных средств поддержки процесса создания ПО, многочисленные документированные технологические проблемы
Риски, связанные с персоналом	Низкое моральное состояние персонала, натянутые отношения между членами команды разработчиков, низкое качество выполненной работы
Организационные риски	Разговоры среди персонала о пассивности и недостаточной компетентности высшего руководства организации
Инструментальные риски	Нежелание разработчиков использовать программные средства поддержки, неодобрительные отзывы о CASE-средствах, запросы на более мощные инструментальные средства
Риски, связанные с системными требованиями	Необходимость пересмотра многих системных требований, недовольство заказчика ПО
Риски оценивания	Изменения графика работ, многочисленные отчеты о нарушении

	графика работ

Мониторинг рисков должен быть непрерывным процессом, отслеживающим ход выполнения мероприятий по управлению рисками, при этом каждый основной риск должен рассматриваться отдельно.

Порядок выполнения практической работы:

1. Изучить теоретический материал.
2. Выполнить предлагаемые задания.
3. Ответить на контрольные вопросы и предоставить в тетради в виде отчета. Отчет должен включать:
   - номер, наименование практической работы и тему;
   - ответы на контрольные вопросы;
   - выводы.
4. Выполненную работу и отчет по проделанной работе предъявить преподавателю.

Задания для выполнения практической работы:

Требования к результатам выполнения практикума:

- Построить модель управления проектом, включающую:
  - определение всех этапов проекта, зависимых этапов, определение длительности этапов;
  - построение на основе полученных данных сетевой и временной диаграмм;
  - построение диаграммы распределения работников по этапам;
- при определении этапа указывается его название – отражающее суть этапа (например, определение пользовательских требований, проектирование интерфейса и т.д.);
- этапов должно быть не менее 7, срок реализации проекта – с 1.09 по 31.12;
- в проекте задействовано 3 человек персонала (группа разработчиков).

1. Построить временную и сетевую диаграммы для выбранного проекта.
2. Построить диаграмму распределения участников группы по этапам.
3. Построить список возможных рисков с указанием названия риска, его описание и типа.
4. Провести анализ рисков.
5. Описать стратегию планирования рисков.
6. Построить отчёт, включающий все полученные диаграммы и описание стратегии планирования рисков.

Содержание отчета

В отчете следует указать:

1. Цель работы
2. Введение
3. Программно-аппаратные средства, используемые при выполнении работы.
4. Основную часть (описание самой работы), выполненную согласно требованиям к результатам выполнения лабораторного практикума (п.2).
5. Заключение (выводы)
6. Список используемой литературы

Контрольные вопросы:

1. В чем заключается понятие риска в программном обеспечении?
1. Какие виды рисков существуют?

Лабораторная работа №4 «Выявление первичных и вторичных ошибок»

Цель работы: провести тестирование и отладку программного продукта
Материально-техническое обеспечение: Компьютер, операционная система Windows 7

Краткие теоретические сведения:

Одной из наиболее трудоемких задач, решаемых на этапе разработки, является тестирование и отладка программ. Под отладкой следует понимать процесс, позволяющий получить программу функционирующую с заданными характеристиками в заданной области входных данных.

Основным методом отладки является тестирование. Тест – это последовательность исходных данных, подаваемых на вход изделия и соответствующие им наборы эталонных результирующих данных.

Процесс отладки включает:

1. создание совокупности тестовых эталонных заданий и значений, которым должна соответствовать программа.
2. статическую проверку текстов разрабатываемых программ,
3. тестирование и выполнение программ с различным уровнем детализации,
4. комплексную динамическую отладку, при необходимости, в режиме реального времени
5. диагностику и локализацию причин отклонения результатов тестов от эталонных,
6. изменение программы с целью исключения причин отклонений.

Можно выделить три основных стадии тестирования:

1. стадия обнаружения ошибок в программе (на этой стадии выявляются все отклонения результатов функционирования от эталонных)
2. стадия диагностики и локализации причин (на этой стадии необходимо точно определить место в котором произошло искажение программы или данных и установить причину)
3. стадия контроля выполнения корректировок (после локализации и устранения ошибок выполняется контрольное тестирование, подтверждающее правильность выполненной корректировки и подтверждающее, что в результате корректировки не возникли вторичные ошибки).

Эффективность тестирования определяет стоимость и длительность разработки.

Характеристики ошибок в процессе проектирования ПО помогают:

- оценить реальное состояние проекта, планировать трудоемкость, стоимость, и длительность разработки,
- разрабатывать эффективные средства оперативной защиты от невыявленных первичных ошибок,
- оценивать требуемые ресурсы с учетом затрат на устранение ошибок,

и т.д.

Анализ первичных ошибок проводится на двух уровнях детализации:

Во-первых, **дифференциированно**– с учетом типов ошибок, сложности и степени автоматизации их выявления, затрат на корректировку и этапов наиболее вероятного устранения.

Во-вторых, **обобщенно** – по суммарным характеристикам их обнаружения в зависимости от продолжительности разработки, эксплуатации и сопровождения ПО.

Существует несколько основных типов ошибок:

1. **Технические ошибки**документации и фиксирования программы в памяти машины (составляют 5-10% от общего объема ошибок, большинство выявляется автоматизированными формализованными методами).
2. **Программные ошибки**, (по количеству и типу определяются: степенью квалификации разработчика, степенью автоматизации разработки, глубиной

формализованного контроля текстов программ, объемом и сложностью разрабатываемого ПО, глубиной логического и информационного взаимодействия модулей и др. факторами).

3. **Алгоритмические ошибки**– обнаружение таких ошибок методами формализованного контроля практически невозможно. Как правило, эти ошибки выявляются только на этапе эксплуатации. К ним можно отнести ошибки, вызванные некорректной постановкой задачи или ее неверной интерпретации разработчиком.

4. **Системные** – такие ошибки определяются неполной информацией о реальных процессах происходящих в источниках и потребителях информации, причем эти процессы не зависят от алгоритмов и не могут быть заранее определены и описаны они выявляются при исследовании функционирования ПО и при обработке результатов его взаимодействия с внешней средой.

Порядок выполнения практической работы:

1. Изучить теоретический материал.
2. Выполнить предлагаемые задания.
3. Ответить на контрольные вопросы и предоставить в тетради в виде отчета. Отчет должен включать:
    - номер, наименование практической работы и тему;
    - ответы на контрольные вопросы;
    - выводы.
4. Выполненную работу и отчет по проделанной работе предъявить преподавателю.

Задания для выполнения практической работы:

1. Провести тестирование разработанного программного продукта и выявить ошибки.
2. Используя теоретический материал, проанализировать, классифицировать имеющиеся ошибки.
3. Осуществить корректировку выявленных ошибок.
4. Проверить программу на наличие вторичных ошибок.

Содержание отчета:

Программа без ошибок, готовая к эксплуатации, представленная на электронном носителе

Контрольные вопросы:

1. Для чего необходимо проводить тестирование ПО?
1. Перечислите основные типы ошибок при тестировании?

Лабораторная работа №5 «Обнаружение вируса и устранение последствий его влияния»

Цель работы: изучение методов обнаружения вирусов и методов удаления последствий заражения вирусами с использованием антивирусной утилиты AVZ
Материально-техническое обеспечение: Компьютер, операционная система Windows 7

Краткие теоретические сведения:

Массовое распространение вирусов, серьезность последствий их воздействия на ресурсы КС вызвали необходимость разработки и использования специальных антивирусных средств и методов их применения. Антивирусные средства применяются для решения следующих задач:

- обнаружение вирусов в КС;
- блокирование работы программ-вирусов;
- устранение последствий воздействия вирусов.

Обнаружение вирусов желательно осуществлять на стадии их внедрения или, по крайней мере, до начала осуществления деструктивных действий вирусов. Не существует антивирусных средств, гарантирующих обнаружение всех возможных вирусов.

При обнаружении вируса необходимо сразу же прекратить работу программы-вируса, чтобы минимизировать ущерб от его воздействия на систему.

Устранение последствий воздействия вирусов ведется в двух направлениях:

- удаление вирусов;
- восстановление (при необходимости) файлов, областей памяти.

Восстановление системы зависит от типа вируса, а также от момента времени обнаружения вируса по отношению к началу деструктивных действий. Восстановление информации без использования дублирующей информации может быть невыполнимым, если вирусы при внедрении не сохраняют информацию, на место которой они помещаются в память, а также, если деструктивные действия уже начались, и они предусматривают изменения информации.

Для борьбы с вирусами используются программные и аппаратно-программные средства, которые применяются в определенной последовательности и комбинации, образуя методы борьбы с вирусами, подразделяемые на:

- методы обнаружения вирусов;
- методы удаления вирусов.

Методы обнаружения вирусов

- ***сканирование*** (осуществляется программой-сканером, которая просматривает файлы в поисках опознавательной части вируса – сигнатуры. Программа фиксирует наличие уже известных вирусов, за исключением полиморфных вирусов, которые применяют шифрование тела вируса, изменяя при этом каждый раз и сигнатуру. Программы-сканеры могут хранить не сигнатуры известных вирусов, а их контрольные суммы. Программы-сканеры часто могут удалять обнаруженные вирусы. Такие программы называют полифагами). Пример – Aidstest Дмитрия Лозинского;

- ***обнаружение изменений*** (базируется на использовании программ-ревизоров, которые определяют и запоминают характеристики всех областей на дисках, в которых обычно размещаются вирусы. При периодическом выполнении программ-ревизоров сравниваются хранящиеся характеристики и характеристики, получаемые при контроле областей дисков, по результата которых программа выдает сообщение о предположительном наличии вирусов. Недостатки метода – с помощью программ-ревизоров невозможно определить вирус в файлах, которые поступают в систему уже зараженными; вирусы будут обнаружены только после размножения в системе);

- ***эвристический анализ*** (позволяет определить неизвестные вирусы, но не требует предварительного сбора, обработки и хранения информации о файловой системе.

Сущность метода – проверка возможных сред обитания вирусов и выявление в них команд (групп команд), характерных для вирусов (команды создания резидентных модулей в ОП, команды прямого обращения к дискам, минуя ОС);

- ***использование резидентных сторожей*** (основан на применении программ, которые постоянно находятся в ОП ЭВМ и отслеживают все действия остальных программ: при выполнении каких-либо подозрительных действий (обращение для записи в загрузочные сектора, помещение в ОП резидентных модулей, попытки перехвата прерываний и т.п.) резидентный сторож выдает сообщение пользователю. Недостаток – значительный процент ложных тревог, что мешает работе и вызывает раздражение пользователя);

- ***вакцинирование программ*** (создание специального модуля для контроля ее целостности. В качестве характеристики целостности файла обычно используется контрольная сумма. При заражении вакцинированного файла, модуль контроля обнаруживает изменение контрольной суммы и сообщает об этом пользователю. Метод позволяет обнаруживать все вирусы, в т.ч. и незнакомые, за исключением «стелс»-вирусов);

- ***аппаратно-программная защита от вирусов*** (самый надежный метод защиты. В настоящее время используются специальные контроллеры и их программное обеспечение. Контроллер устанавливается в разъем расширения и имеет доступ к общей шине, что позволяет ему контролировать все обращения к дисковой системе. В программном обеспечении контроллера запоминаются области на дисках, изменение которых в обычных режимах работы не допускается. Можно устанавливать защиту на изменение главной загрузочной записи, загрузочных секторов, файлов конфигурации, исполняемых файлов и др.).

Методы удаления последствий заражения вирусами

Существует два метода удаления последствий воздействия вирусов антивирусными программами:

первый – предполагает восстановление системы после воздействия известных вирусов (разработчики программы-фага, удаляющей вирус, должен знать структуру вируса и его характеристики размещения в среде обитания);

второй – позволяет восстанавливать файлы и загрузочные сектора, зараженные неизвестными вирусами (для восстановления файлов программа восстановления должна заблаговременно создать и хранить информацию о файлах, полученную в условиях отсутствия вирусов. Имея информацию о незараженном файле и используя сведения об общих принципах работы вирусов, осуществляется восстановление файлов. Если вирус подверг файл необратимым изменениям, то восстановление возможно только с использованием резервной копии или с дистрибутива. При их отсутствии существует только один выход – уничтожить файл и восстановить его вручную).

Антивирусная утилита AVZ

Антивирусная утилита AVZ предназначена для обнаружения и удаления:

- SpyWare и AdWare модулей - это основное назначение утилиты;
- Dialer (Trojan.Dialer);
- Троянских программ;
- BackDoor модулей;
- Сетевых и почтовых червей;
- TrojanSpy, TrojanDownloader, TrojanDropper.

Утилита является прямым аналогом программ TrojanHunter и LavaSoft Ad-aware 6. Первичной задачей программы является удаление SpyWare и троянских программ. Интерфейс программы представлен на рисунке 1.

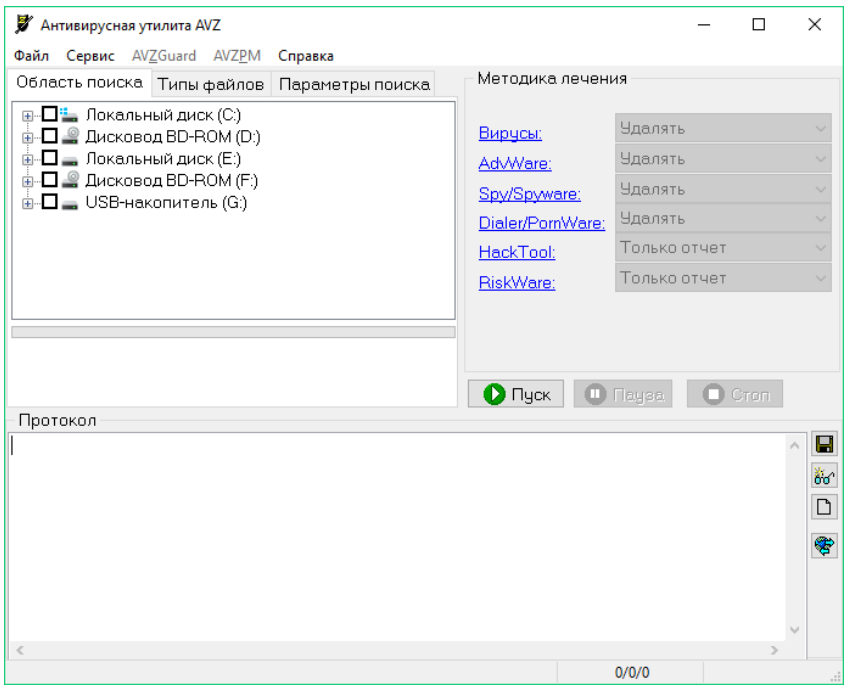


Рис. 1. – Главный экран AVZ

Запуск утилиты должен производиться от имени администратора.

Особенностями утилиты AVZ (помимо типового сигнатурного сканера) является:

- **Микропрограммы эвристической проверки системы**. Микропрограммы проводят поиск известных SpyWare и вирусов по косвенным признакам - на основании анализа реестра, файлов на диске и в памяти.
- **Обновляемая база безопасных файлов**. В нее входят цифровые подписи десятков тысяч системных файлов и файлов известных безопасных процессов. База подключена ко всем системам AVZ и работает по принципу "свой/чужой" - безопасные файлы не вносятся в карантин, для них заблокировано удаление и вывод предупреждений, база используется антируткитом, системой поиска файлов, различными анализаторами. В частности, встроенный диспетчер процессов выделяет безопасные процессы и сервисы цветом, поиск файлов на диске может исключать из поиска известные файлы (что очень полезно при поиске на диске троянских программ);
- **Встроенная система обнаружения Rootkit**. Поиск RootKit идет *без применения сигнатур* на основании исследования базовых системных библиотек на предмет перехвата их функций. AVZ может не только обнаруживать RootKit, но и производить корректную блокировку работы UserMode RootKit для своего процесса и KernelMode RootKit на уровне системы. Противодействие RootKit распространяется на все сервисные функции AVZ, в результате сканер AVZ может обнаруживать маскируемые процессы, система поиска в реестре "видит" маскируемые ключи и т.п. Антируткит снабжен анализатором, который проводит обнаружение процессов и сервисов, маскируемых RootKit. Одной из главных на мой взгляд особенностей системы противодействия RootKit является ее работоспособность в Win9X (распространеннное мнение об отсутствии RootKit, работающих на платформе Win9X глубоко ошибочно - известны сотни троянских программ, перехватывающих API функции для маскировки своего присутствия, для искажения работы API функций или слежения за их использованием). Другой особенностью является универсальная система обнаружения и блокирования KernelMode RootKit, работоспособная под Windows NT, Windows 2000 pro/server, XP, XP SP1, XP SP2, Windows 2003 Server, Windows 2003 Server SP1
- **Детектор клавиатурных шпионов (Keylogger) и троянских DLL**. Поиск Keylogger и троянских DLL ведется на основании анализа системы *без применения базы сигнатур*, что позволяет достаточно уверенно детектировать заранее неизвестные троянские DLL и Keylogger;

- **Нейроанализатор**. Помимо сигнатурного анализатора AVZ содержит нейроэмулятор, который позволяет производить исследование подозрительных файлов при помощи нейросети. В настоящее время нейросеть применяется в детекторе кейлоггеров.
- **Встроенный анализатор Winsock SPI/LSP настроек**. Позволяет проанализировать настройки, диагностировать возможные ошибки в настройке и произвести *автоматическое* лечение. Возможность автоматической диагностики и лечения полезна для начинающих пользователей (в утилитах типа LSPFix автоматическое лечение отсутствует). Для исследования SPI/LSP вручную в программе имеется специальный менеджер настроек LSP/SPI. На работу анализатора Winsock SPI/LSP распространяется действие антируткита;
- **Встроенный диспетчер процессов, сервисов и драйверов**. Предназначен для изучения запущенных процессов и загруженных библиотек, запущенных сервисов и драйверов. На работу диспетчера процессов распространяется действие антируткита (как следствие - он "видит" маскируемые руткитом процессы). Диспетчер процессов связан с базой безопасных файлов AVZ, опознанные безопасные и системные файлы выделяются цветом;
- **Встроенная утилита для поиска файлов на диске**. Позволяет искать файл по различным критериям, возможности системы поиска превосходят возможности системного поиска. На работу системы поиска распространяется действие антируткита (как следствие - поиск "видит" маскируемые руткитом файлы и может удалить их), фильтр позволяет исключать из результатов поиска файлы, опознанные AVZ как безопасные. Результаты поиска доступны в виде текстового протокола и в виде таблицы, в которой можно пометить группу файлов для последующего удаления или помещения в карантин
- **Встроенная утилита для поиска данных в реестре**. Позволяет искать ключи и параметры по заданному образцу, результаты поиска доступны в виде текстового протокола и в виде таблицы, в которой можно отметить несколько ключей для их экспорта или удаления. На работу системы поиска распространяется действие антируткита (как следствие - поиск "видит" маскируемые руткитом ключи реестра и может удалить их)
- **Встроенный анализатор открытых портов TCP/UDP**. На него распространяется действие антируткита, в Windows XP для каждого порта отображается использующий порт процесс. Анализатор опирается на обновляемую базу портов известных троянских/Backdoor программ и известных системных сервисов. Поиск портов троянских программ включен в основной алгоритм проверки системы - при обнаружении подозрительных портов в протокол выводятся предупреждения с указанием, каким троянских программам свойственно использование данного порта
- **Встроенный анализатор общих ресурсов**, сетевых сеансов и открытых по сети файлов. Работает в Win9X и в NT/W2K/XP.
- **Встроенный анализатор Downloaded Program Files (DPF)** - отображает элементы DPF, подключен ко всем системам AVZ.
- **Микропрограммы восстановления системы**. Микропрограммы проводят восстановления настроек Internet Explorer, параметров запуска программ и иные системные параметры, повреждаемые вредоносными программами. Восстановление запускается вручную, восстанавливаемые параметры указываются пользователем.
- **Эвристическое удаление файлов**. Суть его состоит в том, что если в ходе лечения удалялись вредоносные файлы и включена эта опция, то производится автоматическое исследование системы, охватывающее классы, BHO, расширения IE и Explorer, все доступные AVZ виды автозапуска, Winlogon, SPI/LSP и т.п. Все найденные ссылки на удаленный файл автоматически вычищаются с занесением в протокол информации о том,

что конкретно и где было вычищено. Для этой чистки активно применяется движок микропрограмм лечения системы;

- **Проверка архивов.** Начиная с версии 3.60 AVZ поддерживает проверку архивов и составных файлов. На настоящий момент проверяются архивы формата ZIP, RAR, CAB, GZIP, TAR; письма электронной почты и MHT файлы; CHM архивы
- **Проверка и лечение потоков NTFS.** Проверка NTFS потоков включена в AVZ начиная с версии 3.75
- **Скрипты управления.** Позволяют администратору написать скрипт, выполняющий на ПК пользователя набор заданных операций. Скрипты позволяют применять AVZ в корпоративной сети, включая его запуск в ходе загрузки системы.
- **Анализатор процессов.** Анализатор использует нейросети и микропрограммы анализа, он включается при включении расширенного анализа на максимальном уровне эвристики и предназначен для поиска подозрительных процессов в памяти.
- **Система AVZGuard.** Предназначена для борьбы с трудноудалимыми вредоносными программами, может кроме AVZ защищать указанные пользователем приложения, например, другие антишпионские и антивирусные программы.
- **Система прямого доступа к диску** для работы с заблокированными файлами. Работает на FAT16/FAT32/NTFS, поддерживается на всех операционных системах линейки NT, позволяет сканеру анализировать заблокированные файлы и помещать их в карантин.
- **Драйвер мониторинга процессов и драйверов AVZPM**. Предназначен для отслеживания запуска и остановки процессов и загрузки/выгрузки драйверов для поиска маскирующихся драйверов и обнаружения искажений в описывающих процессы и драйверы структурах, создаваемых DKOM руткитами.
- **Драйвер Boot Cleaner**. Предназначен для выполнения чистки системы (удаление файлов, драйверов и служб, ключей реестра) из KernelMode. Операция чистки может выполняться как в процессе перезагрузки компьютера, так и в ходе лечения.

Порядок выполнения практической работы:

1. Изучить теоретический материал.
2. Выполнить предлагаемые задания.
3. Ответить на контрольные вопросы и предоставить в тетради в виде отчета. Отчет должен включать:
    - номер, наименование практической работы и тему;
    - ответы на контрольные вопросы;
    - выводы.
4. Выполненную работу и отчет по проделанной работе предъявить преподавателю.

Задания для выполнения практической работы:

Изучить категории вредоносных программ и изучить работу с антивирусной утилитой AVZ.

Заполнить таблицу с описанием вирусов

Категории вредоносных программ	**Наименование и описание вируса**	**Видимые проявления**
Adware и SpyWare		
Backdoor		
Hoax		
Trojan		
Trojan-Clicker		
Trojan-Downloader		
Trojan-Spy		
Trojan-PSW		

Net-Worm		
Worm		
Trojan-Dropper		
Trojan-Proxy		
Email-Worm		
FraudTool		
Trojan-Ransom		

Запустить утилиту AVZ

Включить AVZGuard

Выполнить восстановление настроек системы: без «Полного пересоздания настроек SPI».

Выполнить резервное копирование с параметрами: настройки проводника, настройки рабочего стола и настройки Windows Firewall.

Используя «Мастер поиска и устранения проблем» произвести поиск проблем средней тяжести и исправить их.

Используя диспетчер процессов определить используемые модули для процесса «smss.exe».

Используя менеджер файла Hosts убедиться в отсутствии лишних записей.

Узнать какие порты TCP/UDP открыты.

Провести поиск на наличие уязвимостей и вирусов. Выставив следующие настройки:

а) методика лечения: удалять все

б) область поиска: все диски

в) эвристический анализ: средний уровень

г) Anti-RootKit: детектировать перехватчики

д) keylogger – включен

е) поиск портов TCP/UDP троянских программ – включен

ж) копировать подозрительные файлы в карантин

з) тип файлов: все файлы

Сохранить профиль настроек для дальнейшего использования.

Завершить работу с утилитой AVZ.

Оформление отчета

Отчет по выполненной работе представляется в печатном или рукописном виде и должен включать:

- титульный лист;
- теоретические сведения;
- описание работы утилиты AVZ;
- вывод по работе;
- ответы на контрольные вопросы.

Контрольные вопросы:

1. Какие существуют методы обнаружения вирусов?
2. Какие из методов позволяют определить неизвестные вирусы?
3. Какие существуют методы удаления последствий заражения вирусами?
4. Для чего предназначена антивирусная утилита AVZ?
5. Что такое руткит?

Лабораторная работа №6 «Установка и настройка антивируса. Настройка обновлений с помощью зеркала»

Цель работы: изучить системные требования антивируса и сравнить их с параметрами компьютера, на который он будет устанавливаться
Материально-техническое обеспечение: Компьютер, операционная система Windows 7, ESET Nod

Краткие теоретические сведения:
Понятие вируса.

Официальное появление *первого компьютерного вируса* датируется 1981 годом, задолго до выхода первой версии Microsoft Windows. Этот вирус, замаскированный под компьютерную игру, атаковал наиболее популярный компьютер того времени — Apple II. Распространялся он с черепашьей скоростью (с помощью дискет).

Согласно подсчетам экспертов, объем *malware* (общепринятое название всех видов вредоносных программ) возрастает более чем на 15 % в год. Согласно данным компании Sophos, разработчика антивирусных программ, каждый день появляются примерно 30 новых вирусов, а перечень активных вирусов пополняется 10 тыс. новых наименований в год.

Вирус — это часть программного кода, которая тиражируется путем добавления в другой объект, обычно незаметно и без разрешения пользователя.
Встреча компьютера с вирусом влечет несколько последствий.
• Появление необычных системных сообщений.
• Исчезновение файлов или увеличение их размеров.
• Замедление работы системы.
• Внезапный недостаток дискового пространства.
• Диск становится недоступным.

Классификация вирусов.

Вирусы могут быть *безвредными, малоопасными и разрушительными.*

Вирусы могут заражать программные файлы, документы (так называемые *макровирусы*) или файловые и дисковые структуры низкого уровня, такие как загрузочный сектор или таблица размещения файлов *(Boot – вирусы)*. *Файловые вирусы* заражают исполнимые файлы, имплантируя в них опасный код. Вирусы могут активизироваться при запуске инфицированной программы; также они могут постоянно находиться в памяти и заражать открываемые пользователем файлы или создавать свои собственные. Когда вирус проникает в компьютер, на котором установлена система Windows, он может изменять значения в системном реестре, замещать собой системные файлы и внедряться в почтовую программу с целью дальнейшего размножения (черви). *Сетевые вирусы* обитают в оперативной памяти компьютеров и не копируют себя на носители данных. Они обитают в сети, когда хотя бы один компьютер включен, поэтому не опасны для индивидуального пользователя. Вирус не обязательно представляет собой отдельную программу и не всегда является деструктивным по своей сути, все зависит от его конкретной разновидности. Хотя основную угрозу для пользователей представляют именно компьютерные вирусы, существует несколько видов вредоносных программ:

Троянский конь представляет собой компьютерную программу, которая маскируется или скрывается в части программы. Некоторые формы троянских коней могут быть запрограммированы на саморазрушение и не оставляют никаких следов, кроме причиненных ими разрушений. Некоторые хакеры используют троянских коней для получения паролей и отсылки их обратно хакеру. Кроме того, они могут использоваться для банковских мошенничеств, когда небольшие суммы денег снимаются с законных счетов и передаются на секретный счет.

Черви представляют собой программы, которые разрушают компьютерную систему. Они могут проникать в программы обработки данных и подменять или разрушать данные. Как вирусы, они могут причинять большие разрушения, если их не обнаружить вовремя. Намного проще ликвидировать червя или троянского коня, если существует только единственная копия программы-разрушителя.

Логические бомбы подобны программам, используемым для троянских коней. Однако логические бомбы имеют таймер, который взрывает их в заданную дату и время. Например, вирус Michelangelo имеет триггер, установленный на день рождения знаменитого художника Микеланджело – 6 марта. Логические бомбы часто используются недовольными служащими, которые могут установить их на активацию после того, как они оставят компанию. Например, логическая бомба может «взорваться», когда имя этого служащего исключается из платежной ведомости. Благодаря встроенному механизму задержки, логические бомбы активно используются для шантажа. Например, шантажист может послать сообщение, говорящее, что если ему будет выплачена определенная сумма денег, он предоставит инструкцию для отключения логической бомбы.

Смешанные коды представляют собой новый класс изощренных вредоносных программ, которые сочетают в себе характеристики вирусов, червей и 35ое35ия35, что позволяет злоумышленнику осуществить особо эффективную атаку. В отличие от большинства доморощенных вирусов, которые распространяются благодаря взлому адресных книг на компьютерах под управлением Windows, целью таких программ являются web-серверы и сети, что значительно повышает их опасность.

Пути проникновения вирусов в компьютер.

Вирусы попадают в вашу компьютерную систему из множества разнообразных *источников* – исполняемых программ, программ и файлов, передаваемых вам, или программного обеспечения, приобретаемого в архивированной форме.

Гибкие диски и компакт-диски могут хранить файлы данных, программ и программное обеспечение операционных систем. Гибкий диск состоит из загрузочного сектора и данных. При необходимости, в загрузочном секторе может храниться информация, нужная для загрузки компьютера. Кроме того, здесь же хранится информация о разделах, информация по управлению загрузкой и информация о размещении файлов. Данные представляют собой всю ту содержательную информацию, которая храниться на гибком диске. Очень легко распространяются вирусы с флеш-карт.

Излюбленным местом обитания вирусов являются загрузочные сектора и исполняемые файлы, хранимые на гибком диске. Помещенные в загрузочном секторе, вирусы могут запускаться при загрузке системы с дискеты. Вирусы, помещенные в исполняемые файлы, запускаются вместе с зараженной программой, после чего начинают свою деятельность.

Если в *локальной сети* заражён хотя бы один компьютер, то вирус моментально распространится и на все остальные компьютеры.

Интернет предоставил пользователям новые возможности, которые увеличивают потенциальную опасность прорех в системе защиты от вирусов.

Места обитания вирусов.

Место обитания вируса связано с его функционированием самым непосредственным образом (как и у настоящих живых вирусов). Вирусные атаки можно даже классифицировать по месту их расположения в компьютере. Типы вирусных атак: *атака загрузочного сектора; инфицирование файла; атака с использованием макросов.*

Вирусы загрузочного сектора инфицируют загрузочный сектор или главную загрузочную запись компьютерной системы. Когда компьютер загружается, вирусная программа активируется. Вирусы загрузочного сектора прежде всего перемещают в другое место записывают исходный загрузочный код и замещают его инфицированным загрузочным кодом. Информация исходного загрузочного сектора переносится на другой сектор диска, который помечается как дефектная область диска и далее не используется.

Поскольку загрузочный сектор – первый элемент, загружаемый при запуске компьютера, обнаружение вирусов загрузочного сектора может оказаться нелегкой задачей. Вирусы загрузочного сектора – один из самых популярных типов вирусов. Они могут распространяться путем использования инфицированных гибких дисков при загрузке компьютера. Это может легко произойти, если при перезагрузке компьютера гибкий диск вставлен в дисковод.

Вирусы, инфицирующие файлы, поражают *исполняемые файлы*. Они могут активироваться только при исполнении файла. Чаще прочих поражаются файлы типов COM, EXE, DLL, BIN, SYS и VXD. Вирусы, инфицирующие файлы, могут становиться резидентными и присоединяться к другим исполняемым программам. Вирусы, инфицирующие файлы, обычно заменяют инструкции загрузки программы исполняемого файла собственными инструкциями. Затем они переносят исходную инструкцию загрузки программы в другой раздел файла. Этот процесс увеличивает размер файла, что может помочь обнаружению вируса.

Вирусы в основе которых лежат макросы (*макровирусы),* исполняют непредусмотренные действия путем использования макроязыка приложения для своего распространения документы. Они могут, например, инфицировать файлы .DOT и .DOC приложения Microsoft Word, а также файлы Microsoft Excel. Эти вирусы относятся к межплатформенным вирусам и могут инфицировать как системы Macintosh, так и PC.

Прочие вирусы могут иметь черты одного или нескольких описанных выше типов.

Вирусы-невидимки (жаргонное название – «стелс-вирусы») при работе пытаются вся как от операционной системы, так и антивирусных программ. Чтобы перехватить все попытки использования операционной системы, вирус должен находиться в памяти. Вирусы невидимки могут скрывать все изменения, которые они вносят в размеры файлов, структуру каталогов или иные разделы операционной системы. Это значительно затрудняет их обнаружение. Чтобы блокировать вирусы-невидимки, их следует обнаружить, когда они находятся в памяти.

Зашифрованные вирусы во время работы шифруют свой вирусный код, что позволяет им предотвратить обнаружение и распознание вируса.

Полиморфные вирусы могут изменять свой внешний вид при каждом инфицировании. Для изменения внешнего вида и затруднения обнаружения они используют механизмы мутаций. Полиморфные вирусы способны принимать более двух миллиардов различных форм, поскольку при каждом инфицировании изменяют алгоритм шифрование.

Многокомпонентные вирусы инфицируют как загрузочные секторы, так и исполняемые файлы. Это один из самых сложных для обнаружения вирусов, поскольку многокомпонентные вирусы могут сочетать некоторые или все методы скрытия своей деятельности, присущие вирусам-невидимкам и полиморфным вирусам.

Самообновляющиеся вирусы, которые появились в самое последнее время, способные скрытно обновляться через Интернет во время сеансов связи.

Проблемы.

Новые вирусы. Сигнатуры новых вирусов появляются постоянно. Когда разрабатывается новый вирус, разработчики антивирусных программ должны «разобрать» его на составные части, проанализировать поведение, добавить его сигнатуру в базу данных антивируса и опубликовать данное обновление. Даже если ваша антивирусная программа настроена на регулярное обновление, какой-то короткий период времени вы не защищены от новейших вирусов. Эта проблема может показаться не столь серьезной в момент начала распространения вируса.

Поскольку новые вирусы появляются непрерывно, никогда не стоит рассчитывать только на антивирусную программу. Для создания нескольких уровней защиты необходимо блокировать исполняемые почтовые вложения и установить все необходимые обновления безопасности.

Ложные тревоги. Иногда антивирусный сканер может принять обычный файл за инфицированный, если база данных антивируса содержит некорректное описание вирусной программы или если алгоритм эвристического анализатора сканера содержит ошибки.

Действия антивирусных программ.

Антивирусная программа должна выполнять *три основные задачи*: обнаружение вируса, удаление вируса, превентивная защита.

Чтобы предотвратить вирусную атаку, антивирусная программа реализует *множество различных методов* обнаружения. Различные антивирусные программы используют некоторые или все методы из следующей группы.

Сканирование цифровой сигнатуры используется для идентификации уникального цифрового кода вируса. Цифровая сигнатура представляет собой предварительно установленный шестнадцатеричный код, наличие которого в файле свидетельствует о его заражении вирусом. Сканирование цифровой сигнатуры представляет собой в высшей степени успешный метод идентификации вирусов. Он, однако, всецело зависит от поддержки базы данных с цифровыми сигнатурами вирусов и тонкостей механизма сканирования. Возможно ложное обнаружение вируса в неповрежденном файле.

Эвристический анализ (или сканирование по заданным правилам) выполняется быстрее, чем сканирование большинством традиционных методов. Этот метод использует набор правил для эффективного анализа файлов и быстро обнаруживает подозрительный вирусный код. Как отмечено в [9], все эвристические методы в той или иной форме выполняют эмулирование исполнения кода вируса. Поэтому, при наличии некоторого опыта, разработчик вируса может защитить свое «изделие» от обнаружения эвристическим анализом. Эвристический анализ склонен к ложным тревогам, и, к сожалению, зависит от корректности набора правил выявления вируса, которые все время изменяются.

Исследование памяти — еще один метод, обычно успешно применяемый для обнару37ое37ия вирусов. Он зависит от распознания местоположения известных вирусов и их кодов, когда они находятся в памяти. И хотя исследование памяти обычно приводит к успеху, использование такого метода может потребовать значительных ресурсов компьютера. Кроме того, он может вмешиваться в нормальный ход выполнения операций компьютера.

Мониторинг прерываний работает путем локализации и предотвращения вирусных атак, использующих вызовы прерываний. Вызовы прерываний представляют собой запросы различных функций через системные прерывания. Мониторинг прерываний, подобно исследованию памяти, также может отвлечь значительные системные ресурсы. Он может стать причиной проблем при легальных системных вызовах и замедлить работу системы. Из-за большого числа вирусов и легальных системных вызовов, мониторинг прерываний может испытывать трудности в локализации вирусов.

Контроль целостности (известный также как *вычисление контрольных сумм)* просматривает характеристики файлов программ и определяет, были ли они модифицированы вирусным кодом. Этот метод не нуждается в обновлении программного обеспечения, поскольку не зависит от цифровых подписей вирусов. Однако он требует от вас поддержания базы данных контрольных сумм файлов, свободных от вирусов. Контроль целостности не способен обнаруживать пассивные и активные вирусы-невидимки. Кроме того, он не может идентифицировать обнаруженные вирусы по именам или типам.

Непрерывной контроль может быть неподходящим средством для домашнего использования, поскольку может привести к обработке слишком большого объема информации, а это замедляет работу компьютера. На клиентской машине предпочтительнее конфигурировать антивирусную программу на запуск в определенное время. Например, она может запускаться при загрузке компьюте37о или считывании

нового файла с гибкого диска. В некоторых пакетах (например, Norton AntiVirus и MacAfee VimsScan) используют метод, известный как сканирование по расписанию, для выполнения поиска вирусов на жестком диске в заданные периоды времени. Еще один метод заключается в использовании антивирусной программы в период простоя компьютера. Например, его можно использовать как часть программы экранной заставки.

Основные принципы компьютерной безопасности.

1. Обучите всех, кто пользуется вашим компьютером или сетью, основным принципам обеспечения компьютерной безопасности.
2. Установите антивирусную программу на компьютер. Установите на компьютер персональный брандмауэр.
3. Настройте почтовый клиент таким образом, чтобы он блокировал или помещал в отдельный каталог все потенциально опасные вложения.
4. Не пользуйтесь дисками, дискетами, флеш-картами, которыми Вы пользовались в заражённых ПК, не проверив их на наличие вирусов и не вылечив их.
5. Не поддавайтесь на сомнительные предложения в Интернете: просмотр интересного фильма или установка бесплатной программы и т.п.
6. Настройте свое антивирусное ПО таким образом, чтобы выполнялось регуляр38ое обновление, как минимум раз в неделю.
7. Используйте авторитетные источники информации о компьютерных вирусах и «ложных тревогах».
8. Пользуйтесь программами для резервного копирования данных. Разработайте план восстановления системы на случай вирусной атаки.

Замечание*: В* РФ отношения производителей и распространителей вирусов с обществом регулируются статьей 273 Уголовного кодекса, гласящей следующее: «*Создание программ для ЭВМ или внесение изменений в уже существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации или копированию информации, нарушению рабов ЭВМ, систем ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами наказывается лишением свободы на срок до 3-х лет со штрафом от 200 до 500 минимальных размеров оплаты труда…*». Аналогичные законы приняты и в других странах.

Порядок выполнения практической работы:

1. Изучить теоретический материал.
2. Выполнить предлагаемые задания.
3. Ответить на контрольные вопросы и предоставить в тетради в виде отчета. Отчет должен включать:
   - номер, наименование практической работы и тему;
   - ответы на контрольные вопросы;
   - выводы.
4. Выполненную работу и отчет по проделанной работе предъявить преподавателю.

Задания для выполнения практической работы:

1. Посмотрите, какие антивирусные программы установлены на Вашем ПК.

2. Откройте программу ESET NOD32 Antivirus и изучите окно программы (Рис.1).

3. Почитайте информацию на вкладках: Состояние защиты, Обновление, Настройка, Служебные программы, Справка и поддержка.

4. Посмотрите на вкладке Настройка, все ли опции включены: Защита в режиме реального времени, Защита электронной почты, Защита доступа в Интернет.

5. Включите вкладку Сканирование ПК. Выберите выборочное сканирование. Просканируйте диск локальный D.

6. Пока идёт сканирование, изучите содержимое вкладки Служебные программы. Какие файлы были помещены на карантин?

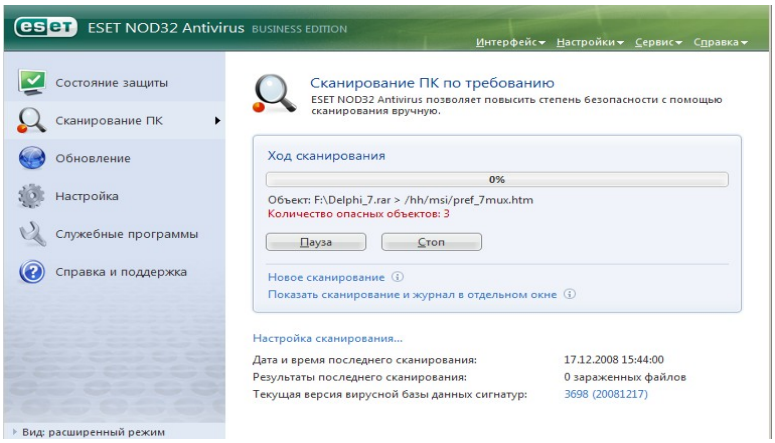


Рис.1

7. После окончания сканирования локального диска просканируйте свою дискету. Результаты сканирования диска и дискеты запишите в отчёт.
8. В разделе Справочной системы программы найдите информацию о том, какие *три уровня очистки* поддерживает программа и запишите эту информацию в отчёт.
9. Изучите раздел справки *Введение в интерфейс пользователя*.
10. Изучите раздел справки *Предупреждения и уведомления*.
11. В служебных программах в Планировщике почитайте, какие задачи запланированы на ближайшее время и запишите эту информацию в отчёт.

Требования к отчёту:

1. Запишите, где могут обитать вирусы.
2. Запишите, как вирусы могут проникнуть в ПК.
3. Запишите, какие типы вредоносных программ Вы изучили.
4. Запишите результаты выполнения пункта 7.
5. Запишите информацию из пункта 8 выполнения работы.
6. Запишите информацию из пункта 10 выполнения задания: о чём может предупреждать программа пользователя.
7. Запишите информацию из пункта 11 выполнения задания.

Контрольные вопросы:

1. Что такое вирус?
2. Какие разновидности вирусов Вы знаете?
3. Как вирусы классифицируются по среде обитания?
4. Как вирусы классифицируются по степени вредного воздействия?
5. Какие виды вредоносных программ Вы знаете?
6. Как вирусы маскируются?
7. Когда обнаружили первый вирус?
8. Как Вы думаете, зачем изобретают вирусы?
9. Какие действия могут выполнять антивирусные программы?
10. Какие три задачи должна выполнять антивирусная программа?
11. Как обеспечить безопасность своей информации?

Лабораторная работа №7 «Настройка политики безопасности»

Цель работы: «получение навыков работы с редактором групповой политики, изучение конфигурации групп пользователей и компьютеров»
Материально-техническое обеспечение: Компьютер, операционная система Windows 7

Краткие теоретические сведения:

Групповая политика – это набор правил, в соответствии с которыми производится настройка рабочей среды Windows. Групповые политики создаются в домене и реплицируются в рамках домена. Объект групповой политики (Group Policy Object, GPO) состоит из двух физически раздельных составляющих: контейнера групповой политики (Group Policy Container, GPC) и шаблона групповой политики (Group Policy Template, GPT). Эти два компонента содержат в себе всю информацию о параметрах рабочей среды, которая включается в состав объекта групповой политики. Продуманное применение объектов GPO к объектам каталога Active Directory позволяет создавать эффективную и легко управляемую компьютерную рабочую среду на базе ОС Windows.

Групповая политика в Windows XP предназначена для определения конфигурации групп пользователей и компьютеров. Конфигурация для группы пользователей и компьютеров создаётся с помощью оснастки «Групповая политика» консоли управления (MMC). Параметры групповой политики хранятся в объекте групповой политики, который в свою очередь связан с выбранными контейнерами Active Directory, например сайтами, доменами или подразделениями. Оснастка «Групповая политика» позволяет определить параметры политики для следующих элементов:

1 Политики из системного реестра;

К ним относятся групповые политики для операционной системы Windows 7 и её компонентов, а также для приложений. Для управления этими параметрами используется узел «Административные шаблоны» оснастки «Групповая политика».

2 Параметры безопасности;

В эту категорию входят параметры безопасности для локального компьютера, домена и сети.

3 Параметры установки и обслуживания программ;

Служат для централизованного управления установкой, обновлением и удалением программ.

4 Параметры сценариев;

Сценарии для запуска компьютера и завершения его работы, входа пользователей в систему и окончания сеансов.

5 Параметры перенаправления папок;

Позволяют администратору перенаправлять специальные папки пользователей в сеть.

Благодаря групповой политике можно один раз определить конфигурацию рабочей среды пользователя, после чего операционная система будет применять заданные политики.

Порядок выполнения практической работы:

1. Изучить теоретический материал.
2. Выполнить предлагаемые задания.
3. Ответить на контрольные вопросы и предоставить в тетради в виде отчета. Отчет должен включать:
    - номер, наименование практической работы и тему;
    - ответы на контрольные вопросы;
    - выводы.
4. Выполненную работу и отчет по проделанной работе предъявить преподавателю.

Задания для выполнения практической работы:

Задание 1

Чтобы запустить редактор групповой политики, выполните следующие действия:

ПРИМЕЧАНИЕ. Чтобы использовать редактор групповой политики, необходимо войти в систему с учётной записью, обладающей привилегиями администратора.

1 Откройте *«Консоль управления MMC»*. Для этого нажмите на кнопку *«Пуск»*, в поле поиска введите **mmc** , а затем нажмите на кнопку *Enter*.

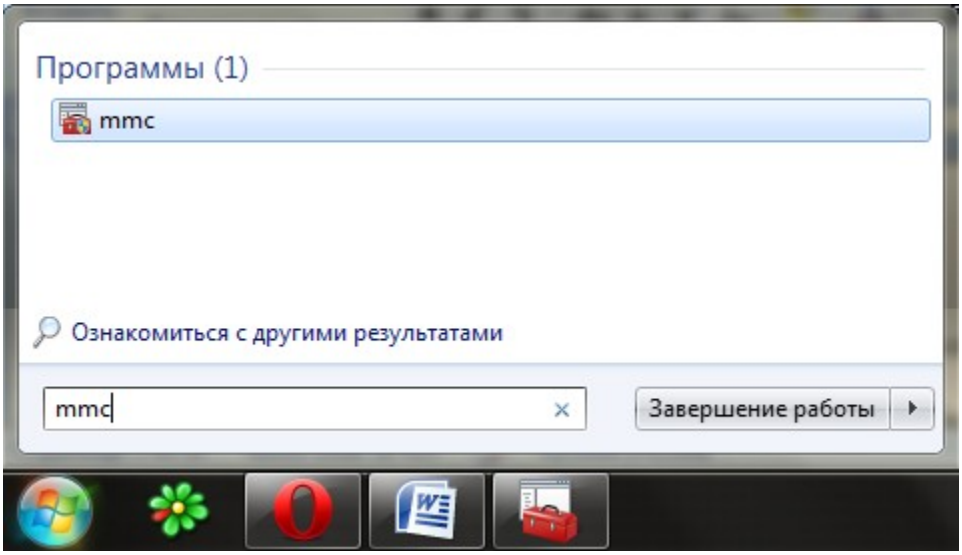


Рисунок 1 – Поиск «mmc»

2 Откроется пустая консоль *MMC*. В меню *«Консоль»* выберите команду *«Добавить или удалить оснастку»* или воспользуйтесь комбинацией клавиш *Ctrl+M.*

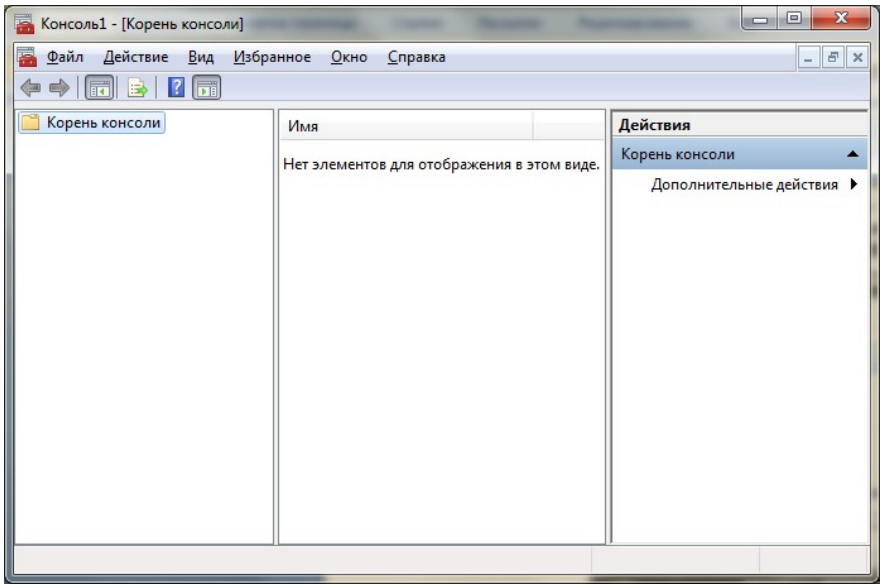


Рисунок 2 – Добавление оснастки

3 В диалоге *«Добавление и удаление оснасток»* выберите оснастку *«Редактор объектов групповой политики»* и нажмите на кнопку *«Добавить»*.

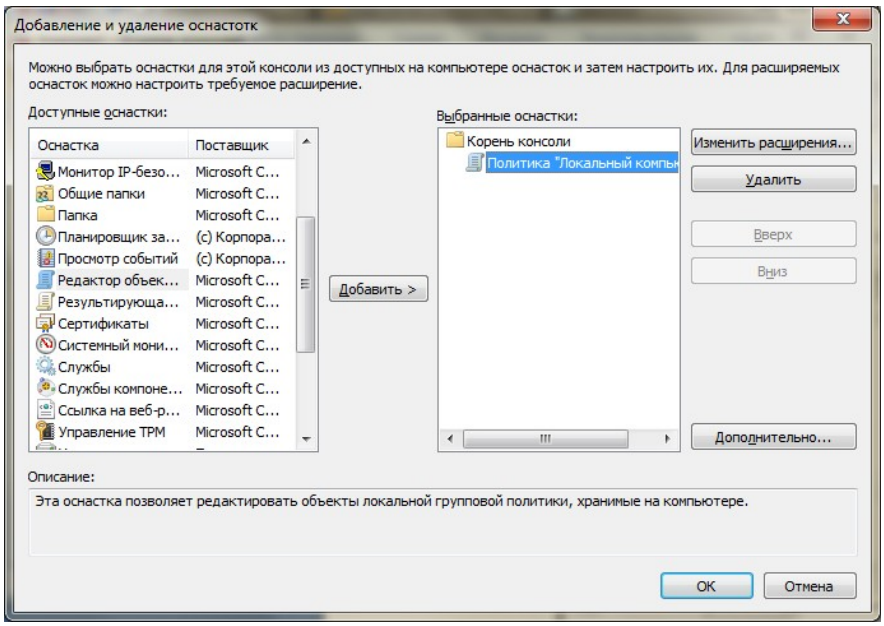


Рисунок 3 – Выбор «Редактора объектов групповой политики»

4 Для того чтобы выбрать нужный объект групповой политики, в появившемся диалоге *«Выбор объекта групповой политики»* нажмите на кнопку *«Обзор»*.

5 В диалоге *«Поиска объекта групповой политики»* можно перейти на вкладку *«Пользователи»* и выбрать объект, над которым будут проводиться настройки групповой политики, например *«Не администраторы»*.

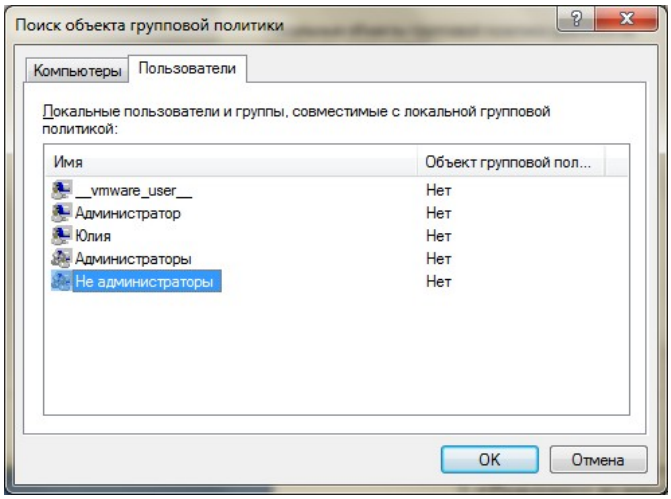


Рисунок 4 – Выбор объекта, над которым будут проводиться настройки «Групповой политики»

6 Нажмите на кнопку *«ОК»* в диалоге *«Поиск объекта групповой политики»*, в диалоге *«Выбор объекта групповой политики»* нажмите на кнопку *«Готово»,* а после этого нажмите на кнопку *«ОК»* диалога *«Добавление и удаление оснасток»*.

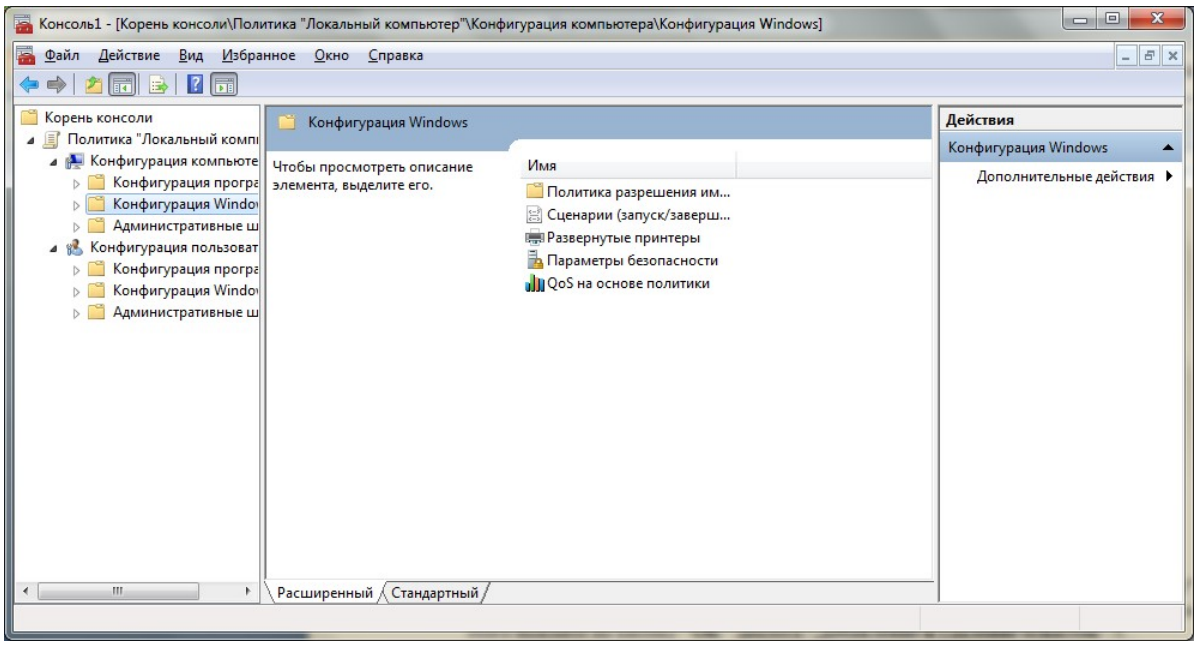


Рисунок 5 – Завершение выбора объекта

Задание №2

Чтобы использовать редактор групповой политики, выполните следующие действия:

1 Разверните нужный объект групповой политики, например *«Политика «Локальный компьютер»;*

2 Разверните нужный узел, например, «*Конфигурация компьютера»;*

3 Разверните нужный вложенный элемент, например, *«Конфигурация Windows»;*

4 Откройте папку, которая содержит нужный параметр политики. Элементы политики отображаются на правой панели оснастки в редакторе групповой политики;

5 В списке *«Параметр»* два раза щёлкните нужный элемент политики;

6 Настройте параметры политики в открывшемся диалоговом окне и нажмите кнопку «ОК»;

7 Выполнив необходимые действия, закройте консоль управления;

Конфигурация компьютера

Этот узел служит для настройки политик, применяемых к компьютеру независимо от того, кто входит в систему. Узел *«Конфигурация компьютера»*, как правило, содержит вложенные элементы для параметров программ, параметров Windows и административных шаблонов.

Конфигурация Windows

Узел, расположенный в дереве *\Конфигурация компьютера \ Конфигурация Windows*, содержит параметры, применяющиеся ко всем пользователям, входящим в систему на данном компьютере. Он включает две подпапки: *«Параметры безопасности»* и «*Сценарии»*.

Сценарии запуск/завершение

Администраторы используют это расширение для указания сценариев, которые выполняются при запуске или завершении работы системы. Сценарии выполняются в контексте локального компьютера.

- ***Автозагрузка –*** содержит сценарии загрузки компьютера;
- ***Завершение работы*** – содержит сценарии завершения работы компьютера.

Параметры безопасности

С помощью параметров безопасности можно изменить политику безопасности для подразделения, домена или узла с любого компьютера, присоединённого к домену. Администратор безопасности с помощью компонента «Параметры безопасности» может изменить параметры безопасности, назначенные объекту групповой политики.

Политика учётных записей

Представляет собой набор параметров для настройки политики паролей и блокировки учётных записей.

Параметры безопасности были рассмотрены в предыдущей лабораторной работе.

Задание №3

1 Откройте оснастку *«Групповая политика».*

2 В дереве консоли щёлкнуть «*Сценарии (запуск/завершение)»*.

3 Дважды щёлкнуть «*Автозагрузка»*.

4 В диалоговом окне «*Свойства: Автозагрузка»* нажать кнопку «*Добавить»*.

5 В диалоговом окне «*Добавление сценария»* ввести «*Имя сценария»* и «*Параметры»*, нажать кнопку «*ОК»*.

Административные шаблоны

Узел *«Административные шаблоны»* содержит всю информацию о политиках системного реестра.

Компоненты Windows – содержат параметры для компонентов операционной системы.

1) *Пересылка событий*;

- ***диспетчер подписки*** – позволяет настроить адрес сервера, интервал обновления и центр сертификации, выдающий сертификаты для диспетчера подписки. Диспетчер подписки – это компьютер, которому пересылаются события;
- ***ForwarderResourceUsage*** – управляет использованием ресурсов сервера пересылки. Каждый параметр применяется ко всем подпискам сервера пересылки.

2) *Каналы RSS;*

- ***отключить синхронизацию каналов в фоновом режиме –*** определяет, включена ли синхронизация каналов в фоновом режиме. Если параметр включён, то возможность синхронизации каналов в фоновом режиме отключена. При отключённом или ненастроенном параметре пользователям будет позволено синхронизировать их каналы в фоновом режиме;
- ***отключить добавление и удаление каналов*** – запрещает пользователям подписываться на канал и удалять каналы, на которые они уже подписаны;
- ***отключить загрузку вложений*** – запрещает загрузку вложений (вложенных файлов) из канала на компьютер;
- ***отключить обнаружение каналов*** – запрещает пользователям включать автоматическое обнаружение доступных на соответствующей веб-странице каналов обозревателем Internet Explorer;
- ***отключить список каналов*** – запрещает пользователям использовать Internet Explorer в качестве средства чтения каналов. Этот параметр не влияет на платформу RSS.

3) *Internet Explorer – содержит параметры политики для IE:*

- ***отключить отображение меню «Справка» в IE*** – позволяет отключить меню «Справка» в Internet Explorer;
- ***включение полноэкранного режима*** – панель навигации содержит средства просмотра веб-страниц, поиска в сети с помощью выбранных инструментов поиска, просмотра журнала, печати и доступа к почте и группам новостей. Строка меню содержит меню с раскрывающимися списками соответствующих функций. Среди них печать, настройка Internet Explorer, копирование и вставка текста, управление избранным и справка. С помощью панели команд осуществляется управление и доступ к избранному, веб-каналам, закладкам и т. д. Полноэкранный режим отключает эти три панели, и обозреватель переходит в полноэкранный режим. Ярлыки этих панелей перестают работать;
- ***настроить строку обозревателя*** – позволяет задавать строку, которую Internet Explorer будет отправлять веб-серверам в заголовке запроса HTTP User Agent в качестве версии обозревателя;

- ***отключить проверку настроек безопасности*** – отключает функцию проверки безопасности параметров, которая определяет, когда параметры ставят безопасность Internet Explorer под угрозу;
- ***отключить управление фильтром фишинга*** – позволяет пользователям включить фильтр фишинга, предупреждающий о попытках незаконного сбора персональной информации с помощью фишинга при посещении веб-узла;
- ***задать параметры прокси для компьютера*** – применяет параметры прокси ко всем пользователям на данном компьютере;
- ***отключить изменение параметров подключений*** – запрещает пользователям изменять параметры удалённого доступа;
- ***отключить изменение параметров прокси*** – задаёт подключение к Интернету с указанными параметрами прокси-сервера. Прокси-сервер действует как посредник между внутренней сетью (интрасетью) и Интернетом, получая файлы с удалённых веб-серверов. Этот параметр указывает, хочет ли пользователь подключаться к адресам локальной интрасети с помощью прокси-сервера или в обход него для адресов интрасети;
- ***отключить настройку журнала*** – задаёт, сколько дней Internet Explorer отслеживает просмотренные страницы в списке журнала. Получить доступ к параметру «Удалить журнал обозревателя» можно, выбрав «Служебные программы», «Параметры обозревателя» и вкладку «Общие». В Internet Explorer 7 он доступен также как параметр «Удалить историю» прямо в «Служебных программах», «Удалить историю просмотра»;
- ***запретить удаление временных файлов Интернета и файлов cookies*** – используется для управления временными файлами Интернета и файлами cookie, связанными с историей просмотра Интернета и доступными при выборе в Internet Explorer 7 команд «Средства», «Параметры Интернета», «Удалить историю просмотра»;
- ***отключить возможность «Удаление паролей»*** – запрещает пользователям очищать пароли. Эта возможность доступна через параметр «Удалить пароли» в диалоговом окне «Удалить журнал обозревателя» в Internet Explorer 7, кроме того, можно щёлкнуть кнопку «Очистить пароли» в группе «Очистка журнала автозаполнения» диалогового окна «Настройка автозаполнения», вызываемого на вкладке «Содержание» в свойствах обозревателя.

4) ***Совместимость приложений:***

- ***процессы IE –*** позволяет избегать запросов на разрешение, когда сценарии, запущенные внутри процесса Internet Explorer, пытаются выполнять операции с буфером обмена (например, вырезание, копирование, вставку), а также действия для URL в зоне, настроенной на отображение запроса;
- ***список процессов*** – позволяет администраторам задавать приложения, для которых это средство запрещено или разрешено;
- ***все процессы*** – позволяет запретить или разрешить эту функцию для всех процессов, запущенных на компьютере. Если включить этот параметр политики, сценарий любого процесса компьютера сможет выполнять операции с буфером обмена без запроса на разрешение. Т.е. если поведение зоны настроено на запрос разрешения, эта настройка не будет учитываться, а операция будет разрешена. Если отключить этот параметр политики, сценарий любого процесса компьютера не сможет выполнять операции вырезания, копирования или вставки из буфера обмена без запроса на разрешение.

5) ***Панель управления браузером:***

Содержит параметры для добавления или удаления вкладок диалогового окна свойств обозревателя:

- ***отключить страницу «Общие»*** **–** удаляет вкладку «Общие» из диалогового окна свойств обозревателя;
- ***отключить страницу «Безопасность»*** – удаляет вкладку «Безопасность» из диалогового окна свойств обозревателя;

- ***отключить страницу «Содержание», «Подключение», «Программы», «Конфиденциальность», «Дополнительно»*** – удаляет одноимённые вкладки из диалогового окна свойств обозревателя;
- ***отправлять международные доменные имена*** – разрешает Internet Explorer преобразовывать имена доменов в формате Unicode в формат IDN (Punycode) перед посылкой на серверы службы доменных имён (DNS) или прокси-серверы;
- ***использовать кодировку UTF-8 для почтовых ссылок*** – позволяет задать, использует ли Internet Explorer кодировку UTF-8 для почтовых ссылок;
- ***запретить пропуск ошибок сертификата*** – Internet Explorer обрабатывает как критические любые ошибки сертификатов SSL/TLS (Secure Socket Layer/Transport Layer Security), прерывающие переход (такие как «истёк срок действия», «сертификат отозван», «несоответствие имён»).

6) *Панели инструментов:*

- ***средство обновления панели инструментов*** проверяет установленные панели инструментов и вспомогательные объекты обозревателя на совместимость при запуске Internet Explorer. При обнаружении несовместимой панели инструментов пользователь получит запрос на её обновление или отключение. Отдельные панели инструментов и вспомогательные объекты обозревателя, включённые или отключённые политикой, не будут подвергнуты этой проверке.

Задание №4

1 Откройте оснастку «Групповая политика».

2 В узле «Конфигурация компьютера» выберите Административные шаблоны.

3 Далее выберите «Компоненты Windows» – «Internet Explorer» – «Удалить журнал браузера» – «Запретить удаление временных файлов Интернета и файлов cookies».

4 В завершении установите необходимые параметры

7) *Совместимость приложений:*

- ***включить обработчик совместимости приложений –*** управляет состоянием обработчика совместимости приложений на компьютере. Обработчик, являющийся частью загрузчика, просматривает базу данных совместимости при каждом запуске приложения на компьютере. Если обнаружено соответствие для приложения, оно обеспечивает либо исполняемые решения или исправления совместимости, либо отображается справочное сообщение приложения, если известна причина неполадок;
- ***включить мастер совместимости программ*** – управляет состоянием мастера совместимости программ. Когда эта политика включена, она отключает начальную страницу мастера в центре справки и поддержки и в меню «Пуск».

8) *Просмотр событий:*

- ***URL-адрес EVANTS.ASP –*** это URL-адрес, передаваемый в область описания события в диалоговом окне свойств события. Измените это значение, если хотите использовать другой веб-сервер для обработки запросов дополнительной информации о событиях;
- ***программа EVANTS.ASP*** – это программа, которая будет вызвана, если пользователь щёлкнет ссылку EVENTS.ASP;
- ***параметры командной строки программы EVANTS.ASP*** – задаёт параметры командной строки, передаваемые программе EVENTS.ASP.

9) *Службы IIS:*

- ***запрет установки IIS*** – когда этот параметр включён, запрещается установка служб IIS, а также установка компонентов Windows или приложений, которым требуется IIS. Пользователи, устанавливающие компоненты Windows или приложений, которым требуется IIS, могут не получить предупреждение о невозможности установки IIS из-за данной групповой политики. Включение данного параметра не влияет на IIS, если службы IIS уже установлены на компьютере.

10) *Центр обеспечения безопасности:*

- ***включить «Центр обеспечения безопасности» (только для компьютеров в домене)*** – указывает, включён ли «Центр обеспечения безопасности» на пользовательских компьютерах, которые присоединены к домену Active Directory. Когда «Центр обеспечения безопасности» включён, он наблюдает за основными параметрами безопасности (брандмауэр, антивирус, автоматическое обновление), и уведомляет пользователей, если их компьютеры подвержены опасности. Категория «Центр обеспечения безопасности» в панели управления также содержит секцию состояния, где пользователи могут найти рекомендации по повышению безопасности своего компьютера. Если «Центр обеспечения безопасности» отключён, то ни уведомления, ни раздел состояния не отображаются.

11) ***Планировщик заданий (управляет возможностью пользователей управлять заданиями).***

- ***скрывать страницы свойств*** – запрещает пользователям просматривать и изменять свойства существующего задания. Эта политика удаляет команду «Свойства» из меню «Файл» в окне «Назначенные задания» и из контекстного меню, которое появляется при выполнении правого щелчка на задании. В результате пользователи не могут изменять свойства заданий. Они могут просматривать только те свойства, которые отображаются в окне назначенных заданий при использовании команды «Таблица» в меню «Вид»;
- ***запретить запуск и завершение задач*** – запрещает пользователям запускать или останавливать задания вручную. Эта политика удаляет команды «Выполнить» и «Завершить задание» из контекстного меню, которое появляется при выполнении правого щелчка мышью на задании. В результате пользователи не могут запускать задания вручную или принудительно завершать задания до окончания их выполнения;
- ***запретить перетаскивание с помощью мыши*** – запрещает пользователям добавлять и удалять задания с помощью перемещения или копирования программ в папку «Назначенные задания». Эта политика отключает команды «Вырезать», «Копировать», «Вставить» и «Вставить ярлык» в контекстном меню и в меню «Правка» в папке «Назначенные задания». Она также отключает возможности перетаскивания объектов с помощью мыши в эту папку;
- ***запретить создание новых заданий –*** удаляет элемент «Добавить задание» из папки назначенных заданий, которая запускает «Мастер планирования заданий». Кроме того, система не позволяет переместить или скопировать с помощью буфера обмена или мыши программы или документы в папку «Назначенные задания»;
- ***запретить удаление заданий*** – удаляет команду «Удалить задание» из меню «Правка» папки назначенных заданий и из контекстных меню, которые открываются правым щелчком мыши на задании. Кроме того, система не позволяет удалить задание из папки «Назначенные задания» с помощью вырезания существующего задания в буфер обмена или перетаскивания его мышью;
- ***скрыть флажок дополнительных свойств в мастере планирования заданий*** удаляет флажок «Установить дополнительные параметры» после нажатия кнопки «Готово» с последней страницы мастера планирования заданий. Она предназначена для того, чтобы упростить создание заданий для начинающих пользователей;
- ***запретить обзор –*** ограничивает выбор назначаемых для выполнения по расписанию программ теми, которые указаны в меню «Пуск» пользователя, и запрещает пользователю изменять расписание выполнения уже назначенных заданий. Эта политика удаляет кнопку «Обзор» из мастера назначения заданий и вкладки «Задание» диалогового окна свойств задания. Кроме того, пользователи не могут изменять значение поля «Выполнить» и «Рабочая папка», которые определяют программу и путь для выполняемого задания.

Задание №5

1 Откройте оснастку *«Групповая политика».*

2 В узле *«Конфигурация компьютера»* выберите «*Административные шаблоны».*

3 Далее выберите «*Компоненты Window»s* – «*Все параметры»* – «***Удалить элемент «Отключение сеанса»*** из диалога завершения работы.

4 В завершении установите необходимые параметры.

12) ***Смарт-карта:***

- ***разрешить перенаправление часового пояса –*** разрешено ли клиентским компьютерам перенаправлять их параметры часового пояса в сеанс службы терминалов;
- ***не разрешать перенаправление буфера обмена*** – указывает, следует ли отключать совместное использование содержимого буфера обмена (перенаправление буфера обмена) удалёнными компьютерами и клиентскими компьютерами для сеанса служб терминалов;
- ***не разрешать перенаправление устройства чтения смарт-карт –*** указывает, следует ли предотвращать сопоставление устройств чтения смарт-карт (перенаправление устройства смарт-карт) в сеансе службы терминалов. Компьютер клиента должен работать под управлением Windows 2000 Server, Windows XP Professional или семейства Windows Server 2003;
- ***разрешать перенаправление звука –*** указывает, могут ли пользователи выбирать, где будет воспроизводиться звук с удалённого компьютера в сеансе службы терминалов (перенаправление звука);
- ***не разрешать перенаправление клиентских принтеров*** – эта политика может использоваться для запрещения пользователям перенаправление заданий на печать с удалённого компьютера на принтер, подключённый к их локальному (клиентскому) компьютеру.

13) ***Шифрование и безопасность:***

- ***всегда запрашивать пароль у клиента при подключении*** – указывает, всегда ли службы терминалов запрашивают пароль клиента при подключении.
- ***установить уровень шифрования для клиентских подключений –*** указывает службам терминалов на необходимость применения указанного уровня шифрования для всех данных, передаваемых между клиентом и удалённым компьютером во время сеанса работы со службами терминалов;
- ***безопасный сервер –*** указывает, требует ли сервер терминалов безопасные подключения RPC от всех клиентов либо допускает небезопасные подключения.

14) ***Лицензирование:***

- ***группа безопасности сервера лицензий –*** указывает серверы терминалов и серверы лицензий, которым сервер лицензирования сервера терминалов предоставляет лицензии. С помощью этого параметра можно определять, каким серверам будут выдаваться лицензии. По умолчанию сервер лицензирования служб терминалов выдаёт лицензию любому запросившему её компьютеру;
- ***запретить повышение лицензий –*** управляет тем, как сервер лицензий распределяет обновления лицензий для серверов терминалов, работающих под управлением Windows 2000. Сервер лицензий пытается предоставлять наиболее подходящие клиентские лицензии (CAL) для подключения.

15) ***Временные папки:***

- ***не использовать временные папки для сеанса*** – указывает, следует ли службам терминалов создавать временные папки сеансов. Используя этот параметр, можно запретить создание на удалённом компьютере отдельных временных папок для каждого сеанса;
- ***не удалять временные папки при выходе –*** указывает, сохраняются ли временные папки служб терминалов после завершения сеансов пользователями. Этот параметр позволяет управлять временными папками сеансов пользователей на удалённом компьютере, даже если пользователь завершает сеанс.

16) ***Клиент:***

- ***запретить сохранение паролей*** – указывает, могут ли сохраняться на этом компьютере пароли клиентов сервера терминалов.

17) ***Каталог сеансов:***

- ***задать ограничение по времени для отключённых сеансов –*** этот параметр можно использовать для указания наибольшего количество времени, в течение которого отключённый сеанс остаётся открытым на сервере;
- ***задать ограничение по времени для активных сеансов*** – используя этот параметр, можно задать наибольший интервал времени, в течение которого сеанс служб терминалов может быть активен до автоматического отключения;
- ***задать ограничение по времени для бездействующих сеансов –*** параметр можно использовать для указания наибольшего количество времени, в течение которого активный сеанс может оставаться бездействующим (без участия пользователя) до автоматического отключения;
- ***разрешать переподключение только от исходного клиента*** – указывает, могут ли пользователи переподключаться к отключённому сеансу служб терминалов, используя другой компьютер (не тот, с которого был начат сеанс);
- ***завершать сеанс при достижении ограничения по времени*** – этот параметр используется, чтобы указать, что при достижении ограничений по времени для активных или бездействующих сеансов эти сеансы следует завершать (то есть выполнить выход пользователя, а сеанс удалить с сервера).

Задание №6

1 Откройте оснастку *«Групповая политика».*

2 В узле *«Конфигурация компьютера»* выберите *Административные шаблоны.*

3 Далее выберите *«Все параметры»* – ***«Запретить сохранение паролей».***

4 В завершении установите необходимые параметры.

18) ***Проводник:***

- ***отключить защищённый режим протокола оболочки*** – позволяет настраивать функциональные возможности протокола оболочки. При использовании всех возможностей протокола приложения могут открывать папки и запускать файлы. Защищённый режим уменьшает возможности протокола, позволяя приложениям открывать только некоторые папки. Приложения не смогут запускать файлы в защищённом режиме. Рекомендуется использовать протокол в защищённом режиме для повышения безопасности Windows.

19) ***Установщик Windows:***

- ***запретить использование установщика*** – эта политика может запретить пользователям устанавливать программы или разрешить устанавливать только программы, предложенные администратором;
- ***ведение журнала –*** указывает типы событий, записываемых установщиком Windows в журнал транзакций для каждой установки. Журнал, Msi.log, находится в папке Temp на системном томе;
- ***запретить установки для пользователей –*** позволяет настраивать установки для пользователей. Для этого следует включить эту политику и выбрать в раскрывающемся списке желаемое поведение;
- ***отключить создание контрольных точек восстановления системы –*** восстановление системы позволяет пользователям, в случае возникновения проблем, восстанавливать состояние своего компьютера на некоторый предшествующий момент, не теряя при этом личных файлов с данными. По умолчанию, установщик Windows Installer автоматически создает контрольную точку восстановления системы всякий раз при установке приложения, так что пользователи могут восстановить состояние компьютера до состояния, предшествовавшего установке этого приложения;

- ***запретить удаление обновлений*** **–** эта политика управляет тем, имеют ли право обычные пользователи или администраторы удалять обновления, установленные с помощью установщика Windows***;***
- ***максимальный размер кэша базисных файлов*** **–** эта политика задаёт процент свободного места на диске, доступного для кэша базисных файлов установщика Windows.

20) ***Windows Messenger:***

- ***запретить выполнение Windows Messenger*** – позволяет отключить Windows Messenger;
- ***не запускать Windows Messenger автоматически при входе*** **–** Windows Messenger автоматически загружается и начинает выполняться при входе пользователя в Windows XP. Эта политика может использоваться для того, чтобы отменить автоматический запуск Windows Messenger при входе в систему.

21) ***Windows Update:***

- ***не отображать параметр «Установить обновления и завершить работу» в диалоговом окне завершения работы Windows*** **–** позволяет выбрать, будет ли отображаться параметр «Установить обновления и завершить работу» в диалоговом окне завершения работы Windows;
- ***настройка автоматического обновления*** – указывает, будет ли данный компьютер получать обновления системы безопасности и другие важные обновления с помощью службы автоматического обновления Windows. Этот параметр позволяет указать, разрешается ли автоматическое обновление для данного компьютера;
- ***указать размещение службы обновлений Microsoft в интрасети*** **–** указывает сервер интрасети, на котором находятся обновления, полученные с веб-узлов обновлений Microsoft. Затем эту службу обновления можно использовать для автоматического обновления системы на всех компьютерах сети. Эта политика позволяет указать сервер в сети, на котором будет работать внутренняя служба обновлений. Клиентская программа автоматического обновления будет искать в этой службе обновлений, применимые для компьютеров сети;
- ***не выполнять автоматическую перезагрузку при автоматической установке обновлений, если в системе работают пользователи*** **–** указывает, что для завершения запланированной установки программа автоматических обновлений подождёт перезагрузки компьютера кем-либо из пользователей вместо принудительного автоматического перезапуска.

22) ***Удалённое управление Windows:***

- ***разрешить обычную проверку подлинности*** – позволяет определить, будет ли клиент службы удалённого управления Windows (WinRM) использовать обычную проверку подлинности;
- ***разрешить незашифрованный трафик*** **–** позволяет определить, будет ли клиент службы удалённого управления Windows посылать и принимать через сеть незашифрованные сообщения;
- ***надёжные сайты*** **–** позволяет определить, будет ли клиент службы удалённого управления Windows использовать список, заданный в списке надёжных сайтов, чтобы определить степень надёжности целевого сайта;
- ***запретить проверку подлинности согласованием*** **–** позволяет указать, что клиент службы удалённого управления Windows (WinRM) не будет использовать проверку подлинности согласованием;
- ***запретить проверку подлинности по протоколу Kerberos*** **–** позволяет указать, что клиент службы удалённого управления Windows (WinRM) не будет использовать проверку подлинности Kerberos непосредственно;
- ***запретить краткую проверку подлинности*** **–** позволяет указать, что клиент службы удалённого управления Windows (WinRM) не будет использовать краткую проверку подлинности.

23) ***Удалённая оболочка Windows:***

- ***тайм-аут простоя*** – задаёт в миллисекундах максимальное время, в течение которого удалённая оболочка при отсутствии активности пользователей остаётся открытой, а затем удаляется;
- ***тайм-аут оболочки*** – определяет максимальное время в миллисекундах, которое отводится на выполнение удалённой команды или сценария;
- ***разрешить доступ к удалённой оболочке –*** настраивает доступ к удалённым оболочкам;
- ***максимальный объём памяти в мегабайтах для одной оболочки –*** задаёт максимальный общий объём памяти, которую можно выделить для любой активной удалённой оболочки и её дочерних процессов;
- ***максимальное число удалённых оболочек для одного пользователя –*** задаёт максимальное количество одновременно запущенных оболочек, которые любой пользователь может удалённо открыть на одном компьютере;
- ***максимальное количество процессов для одной оболочки –*** задаёт максимальное количество процессов, разрешенное к запуску для удалённой оболочки;
- ***MaxConcurrentUsers –*** задаёт максимальное количество пользователей, которые могут параллельно выполнять удалённые операции в одной системе с помощью удалённой оболочки CMD.

24) ***Проигрыватель Windows Media:***

- ***не создавать ярлык на рабочем столе –*** запрещает добавление значка ярлыка проигрывателя на рабочий стол пользователя;
- ***не создавать ярлык на панели быстрого запуска –*** запрещает добавление ярлыка проигрывателя на панель быстрого запуска;
- ***не отображать диалоговые окна первого пользования –*** запрещает отображение диалоговых окон «Параметры конфиденциальности» и «Параметры установки» при первом запуске проигрывателя Windows Media;
- ***запрещение предоставления общего доступа к библиотеке –*** запрещает общий доступ к любой библиотеке проигрывателя Windows Media на этом компьютере с других компьютеров и устройств в домашней сети. Кроме того, флажок «Общий доступ по умолчанию» и кнопка «Запретить доступ» будут недоступны;
- ***запретить сглаживание изображения –*** запрещает сглаживание изображения, в результате чего улучшается качество воспроизведения на компьютерах с ограниченными ресурсами. Кроме того, флажок «Использовать сглаживание изображения» в диалоговом окне «Настройка ускорения видео» в проигрывателе снят и недоступен;
- ***запретить автоматическое обновление –*** запрещает обновление проигрывателя и отключает запросы на обновление для пользователей с правами администратора, когда появляется новая версия. Команда «Проверка наличия обновлений» в меню «Справка» в проигрывателе недоступна. Кроме того, ни один из временных интервалов не выбран и не доступен в разделе «Проверка обновлений» на вкладке «Проигрыватель».

Задание №7

1 Необходимо открыть оснастку *«Групповая политика»*.

2 В дереве консоли выбрать *Конфигурация компьютера – Административные шаблоны – Компоненты Windows – Проигрыватель Windows Media*.

3 Далее дважды щёлкнуть в правой части окна по пункту «*Не создавать ярлык на рабочем столе»*.

4 Установить флажок *«Включён».*

Система

Разрешает настройку параметров различных компонентов системы:

- ***предотвращение доступа к потенциально небезопасным функциям справки HTML для указанных папок*** – можно ограничить выполнение определённых команд справки HTML, чтобы они выполнялись только для файлов справки HTML (.chm) в указанных папках и их подпапках. Можно также отключить выполнение этих команд для всей системы. Настоятельно рекомендуется добавлять в эту политику только папки, требующие административных привилегий;
- ***не отображать страницу «Управление данным сервером» при входе –*** указывает, следует ли отключить автоматическое отображение страницы «Управление данным сервером»;
- ***отображать диалог слежения за завершением работы –*** диалог слежения за событиями завершения работы может отображаться при завершении работы рабочей станции или сервера. В нем содержится ряд вопросов, которые отображаются при вызове завершения работы компьютера, что используется для сбора сведений о том, почему выполняется завершение работы компьютера;
- ***включить постоянную временную метку*** – постоянный штамп времени позволяет системе обнаруживать время неожиданного отключения за счет записи на диск текущего времени по расписанию, которое определяется интервалом штампа времени;
- ***указать расположение установочных файлов Windows –*** указывает другое размещение для установочных файлов Windows;
- ***указать размещение установочных файлов пакета обновления Windows –*** указывает другое размещение для установочных файлов пакета обновления Windows;
- ***отключить сообщения о состоянии загрузки, завершения работы, входа и выхода из сети –*** подавляет сообщения о состоянии системы;
- ***подробные сообщения о состоянии –*** указывает системе, что следует отображать наиболее подробные сообщения о состоянии;
- ***отключить автозапуск –*** отключает возможность автозапуска. Автозапуск приводит к тому, что система приступает к чтению данных с устройства сразу же после того, как носитель вставлен в это устройство. В результате немедленно запускается файл программы установки для программных дисков или начинается воспроизведение музыки для звуковых носителей;
- ***не выключайте питание компьютера после завершения работы Windows –*** позволяет настроить автоматическое выключение питания компьютера после завершения работы Windows. Она не влияет на поведение завершения работы Windows, когда работа завершается вручную из меню Пуск или из диспетчера задач. Некоторые приложения, такие как программа обеспечения поддержки источника бесперебойного питания (ИБП), могут зависеть от поведения завершения работы Windows;
- ***отключить запрос на использование Windows Update при поиске драйверов –*** указывает, будет ли выдаваться запрос администратору о выполнении поиска драйверов на узле Windows Update через Интернет.

1) ***<u>Сценарии:</u>***

- ***синхронное выполнение сценариев входа в систему –*** указывает, что системе следует дождаться завершения работы сценариев входа перед тем, как будет запущен интерфейс «Проводника Windows» и создан рабочий стол;
- ***асинхронное выполнение сценариев загрузки –*** позволяет системе асинхронное, одновременное выполнение сценариев загрузки. Сценарии загрузки представляют собой пакетные файлы, состоящие из команд, выполняемых системой при загрузке системы, перед тем как будет выдано приглашение для входа пользователя в систему. По умолчанию, система ожидает завершения выполнения каждого из сценариев загрузки перед запуском следующего сценария загрузки***;***
- ***выполнять сценарии загрузки с отображением команд –*** отображает команды сценариев загрузки во время их выполнения;

- ***выполнять сценарии завершения работы с отображением команд*** – отображает команды сценариев завершения работы во время их выполнения;
- ***максимальное время выполнения сценариев групповой политики*** – определяет, как долго система ожидает выполнения сценария, применяемого групповой политикой.

2) ***Вход в систему:***

- ***всегда использовать классический вход в систему*** – вынуждает пользователя выполнять вход в систему с помощью классического окна входа в систему;
- ***запускать указанные программы при входе*** – указывает дополнительные программы или документы, которые Windows будет автоматически запускать или открывать при входе пользователя в систему.

3) ***Дисковые квоты:***

- ***включить дисковые квоты*** – включает и отключает управление дисковыми квотами на всех NTFS-томах этого компьютера и запрещает пользователям изменять этот параметр;
- ***задать предел дисковой квоты*** – задаёт обязательное применение дисковых квот и запрещает пользователям изменять этот параметр;
- ***предел квоты по умолчанию и уровень предупреждения*** – указывает значение предела дисковой квоты и уровня предупреждения по умолчанию для новых пользователей тома;
- ***применять политику к съемным носителям*** – распространяет политики дисковой квоты из этой папки на все тома с файловой системой NTFS на съемных носителях.

4) ***Групповая политика:***

- ***отключить фоновое обновление групповой политики*** – предотвращает обновление групповой политики во время использования компьютера. Эта политика применима к групповым политикам для компьютеров, пользователей и контроллеров домена;
- ***интервал обновления групповой политики для компьютеров*** – определяет частоту обновления групповой политики для компьютеров во время работы (в фоновом режиме). Эта политика указывает частоту фонового обновления только для групповых политик в папке «Конфигурация компьютера»;
- ***обнаружение медленных подключений для групповой политики*** – определяет медленное подключение для применения или обновления групповой политики;
- ***обработка политики реестра*** – определяет порядок обновления политик работы с реестром;
- ***обработка политики настройки IE*** –определяет порядок обновления политик настройки Internet Explorer;
- ***обработка политики установки программ*** – определяет порядок обновления политик установки программ. Оказывает влияние на все политики, использующие компонент установки программ из групповой политики, в том числе, политики, находящиеся в разделе «Конфигурация программ \ Установка программ»;
- ***обработка политики сценариев*** – определяет, когда обновляются политики, которые назначают выполнение общих сценариев;
- ***всегда использовать локальные файлы ADM для редактора объектов групповой политики*** – разрешение использовать локальные ADM-файлы для оснастки групповой политики. По умолчанию при редактировании объекта групповой политики используется оснастка редактора объекта групповой политики; ADM-файлы загружаются из объекта групповой политики в оснастку редактора.

25) ***Удалённый помощник:***

- ***запрошенная удалённая помощь*** **–** определяет, можно ли пользователю запрашивать удалённую помощь с этого компьютера;
- ***разрешить предложение удалённой помощи*** **–** определяет, может ли персонал службы поддержки или сетевой администратор (в дальнейшем «эксперт») предлагать удалённую помощь для пользователя этого компьютера, если пользователь первым явно не запросил помощь через канал связи, электронную почту или службу мгновенных сообщений.

26) ***Восстановление системы:***

- ***отключить восстановление системы*** **–** восстановление системы позволяет пользователям, в случае возникновения проблем, восстанавливать состояние своего компьютера на некоторый предшествующий момент, не теряя при этом личных файлов с данными;
- ***отключить конфигурацию*** **–** позволяет отключать интерфейс конфигурации для восстановления системы.

Задание №8

1 В дереве консоли выбрать «*Конфигурация компьютера» – «Административные шаблоны» – «Система» – «Восстановление системы».*

2 Далее дважды щёлкнуть в правой части окна по пункту «*Отключить конфигурацию».*

3 Задать параметр «*Включён».*

27) ***Отчёт об ошибках:***

- ***отображать уведомления об ошибках*** **–** используется для управления тем, будет ли пользователь иметь возможность отправлять отчёт об ошибках;
- ***настроить отчёты об ошибках*** **–** задаёт параметры отправки отчёта об ошибках и того, какая информация отправляется в этих отчётах, если включена отправка отчётов об ошибках. Эта политика не включает и не отключает отправку отчётов об ошибках, для этого следует использовать политику «Отключить отчёты об ошибках Windows» в папке «Конфигурация компьютера/Административные шаблоны/Система/Управление связью через Интернет/Параметры связи через Интернет»;
- ***сообщать о системных ошибках*** **–** эта политика управляет тем, следует ли добавлять сообщения об ошибках в работе операционной системы в отчёт, если включена отправка отчётов об ошибках;
- ***список приложений, для которых нужно отправлять отчёт об ошибках*** **–** задаёт приложения, для которых всегда нужно отправлять отчёт об ошибках;
- ***список приложений, для которых не нужно отправлять отчёт об ошибках*** **–** управляет рапортованием об ошибках для обычных приложений, когда рапортование об ошибках включено.

28) ***Защита файлов Windows:***

- ***установить частоту сканирования защиты файлов*** **–** определяет, когда средство защиты файлов Windows сканирует защищённые файлы. Этот параметр заставляет средство защиты файлов Windows выполнять перечисление и сканирование всех системных файлов с целью обнаружения изменений;
- ***скрывать окно индикации сканирования файлов*** **–** скрывает окно индикации выполнения сканирования файлов. Это окно обеспечивает дополнительную информацию о состоянии, которая может потребоваться только опытным пользователям;
- ***ограничить размер кэша защиты файлов*** **–** указывает наибольший объём места на диске, который может использоваться для файлового кэша защиты файлов Windows.

29) ***Служба времени Windows:***

- ***глобальные параметры конфигурации*** **–** задаёт набор параметров для всех поставщиков времени, установленных на компьютере;

- ***включить Windows NTP-клиента*** – указывает, включён ли NTP-клиент Windows. Включение NTP-клиента Windows позволяет компьютеру выполнять синхронизацию часов компьютера с другими NTP-серверами;
- ***настроить Windows NTP-клиента –*** указывает, выполняет ли NTP-клиент Windows синхронизацию времени с доменной иерархией или настроенным вручную NTP-сервером. Указывает, может ли клиент синхронизовать время из источника, находящегося за пределами своего сайта, как долго NTP-клиент Windows ожидает перед тем, как попытаться заново разрешить не разрешенное ранее имя NTP-сервера, и степень подробности протоколирования событий NTP-клиента;
- ***включить Windows NTP-сервер –*** указывает, включён ли NTP-сервер Windows. Включение NTP-сервера Windows позволяет компьютеру обслуживать NTP-запросы от других компьютеров.

30) ***Управление связью через Интернет:***

- ***ограничить связь через Интернет –*** указывает, может ли Windows использовать доступ к Интернету для выполнения задач, требующих обращения к ресурсам Интернета;
- ***отключить веб-публикацию в списке задач для файлов и папок –*** указывает, отображаются ли задачи «Опубликовать файл в вебе», «Опубликовать эту папку в вебе», «Опубликовать выделенные объекты в вебе» в разделе задач для файлов и папок в окне Проводника Windows. «Мастер веб-публикаций» используется для загрузки списка поставщиков услуг и позволяет публиковать информацию на вебе;
- ***отключить загрузку из Интернета для мастеров веб-публикаций и заказа отпечатков –*** указывает, нужно ли загружать список поставщиков услуг для мастеров веб-публикации и заказа отпечатков;
- ***отключить заказ отпечатков через Интернет в списке задач для изображений –*** указывает, надо ли отображать «Заказ отпечатков через Интернет» в списке задач для изображений;
- ***отключить участие в программе улучшения поддержки пользователей Windows Messenger –*** указывает, выполняет ли Windows Messenger сбор анонимной информации о том, как используется программное обеспечение и служба Windows Messenger;
- ***отключить службу сопоставления файлов Интернета –*** указывает, нужно ли использовать веб-службу Майкрософт для поиска приложений, подходящих для открытия файлов, которым ещё не сопоставлено приложение. Когда пользователь открывает файл, расширение имени которого не сопоставлено ни одному из приложений на этом компьютере, имеется возможность выбрать либо одно из локальных приложений, либо обратиться в веб-службу для поиска подходящего приложения;
- ***отключить выполнение печати через HTTP-протокол –*** указывает, следует ли разрешить выполнение печати от этого клиента через HTTP-протокол. Выполнение печати через HTTP позволяет клиентам выполнять печать на принтерах, находящихся как в интрасети, так и в Интернете.

31) ***DCOM (параметры совместимости приложений):***

- ***разрешать локальные исключения проверки безопасности при активации –*** позволяет указать, что локальные администраторы компьютера могут предоставлять список для политики «Задать исключения проверки безопасности при активации»;
- ***задать исключения проверки безопасности при активации –*** позволяет просматривать и изменять список кодов приложения DCOM-сервера (appid), исключённых из проверки безопасности при активации DCOM. DCOM использует два списка: один настроен через групповую политику с использованием этой политики; другой – действиями локальных администраторов компьютера.

Конфигурация пользователя

Этот узел служит для настройки политик, применяемых к пользователям независимо от того, на каком компьютере они входят в систему. Узел «Конфигурация пользователя», как правило, содержит вложенные элементы для параметров программ, параметров Windows и административных шаблонов.

Конфигурация Windows

Узел, расположенный в дереве \Конфигурация пользователя \Конфигурация Windows, содержит параметры, применяющиеся к пользователям вне зависимости от того, с какого компьютера они входят в систему. Он включает три подпапки: «Перенаправление папки», «Параметры безопасности» и «Сценарии».

Сценарии вход/выход из системы

Администраторы используют это расширение для указания сценариев, которые выполняются при входе пользователя в систему или выходе из неё. Сценарии выполняются в пользовательском контексте.

- ***Вход в систему –*** содержит сценарии входа в систему пользователя.
- ***Выход из системы –*** содержит сценарии выхода пользователя.

Параметры безопасности

Параметры безопасности были рассмотрены в предыдущей лабораторной работе.

Административные шаблоны

Узел «Административные шаблоны» содержит всю информацию о политиках системного реестра.

Как правило, узел «Административные шаблоны» не всегда содержит полный перечень политик. Для того чтобы получить полный доступ к политикам данной категории необходимо подключить файл, содержащий административные шаблоны. Сделать это можно следующим образом:

- разверните узел «*Конфигурация пользователя»* (если он не развёрнут);
- в узле «*Конфигурация пользователя»* нажмите ПКМ на элемент «*Административные шаблоны»;*
- выберите пункт меню «*Добавление и удаление шаблонов»;*
- нажмите кнопку *«Добавить»;*
- выберите файл system.adm;
- нажмите кнопку «*Открыть»*.

Теперь, имея доступ ко всем административным шаблонам, рассмотрим принцип работы некоторых из них.

Компоненты Windows

1) ***NetMeeting. Общий доступ к приложениям;***

- ***открыть общий доступ к приложениям –*** запрещает общий доступ к приложениям с помощью NetMeeting. Пользователи не смогут предоставлять общий доступ к своим приложениям или пользоваться доступом к чужим приложениям;
- ***запретить предоставление общего доступа –*** запрещает пользователям предоставлять общин доступ. Однако они смогут пользоваться общим доступом к чужим приложениям или рабочему столу;
- ***запретить предоставление общего доступа к рабочему столу –*** запрещает пользователям предоставлять общин доступ к рабочему столу. Однако они смогут предоставлять общин доступ к отдельным приложениям;
- ***запретить предоставление общего доступа к командной строке –*** запрещает пользователям предоставлять общин доступ к командной строке. Таким образом, предотвращается возможность непредусмотренного предоставления доступа к другим приложениям, поскольку командная строка может использоваться для запуска других приложений;
- ***запретить предоставление общего доступа к окнам Проводника –*** запрещает пользователям предоставлять общин доступ к окнам Проводника. Таким

образом, предотвращается возможность непредусмотренного предоставления доступа к другим приложениям, поскольку окно Проводника может использоваться для запуска других приложений;

- ***запретить общий доступ к приложениям в режиме True Color –*** запрещает пользователям предоставлять общий доступ к приложениям в режиме True Color. В этом режиме приложение требует большей пропускной способности канала связи.

Контрольные вопросы:

1. Что подразумевается под «параметрами» Групповой политики?
2. Какой узел используют администраторы для задания политик, применяемых к компьютерам, независимо от того, кто осуществил вход в систему и каким образом?
3. Какой узел используется для задания политик, применяемых к пользователям, независимо от того, с какого компьютера ими осуществлён вход в систему?
4. Чем отличается содержание папки «Конфигурация программ», расположенная в узле *Конфигурация компьютера*\ *Конфигурация программ* от содержания папки, расположенной в узле \ *Конфигурация пользователя*\ *Конфигурация программ*.

Лабораторная работа №8 «Настройка браузера»

Цель работы: работа по настройке браузера
Материально-техническое обеспечение: Компьютер, операционная система Windows 7, Microsoft Internet Explorer

Краткие теоретические сведения:

1. Запуск браузера Microsoft Internet Explorer

Для запуска браузера выполните команды:
Пуск-> Программы -> Internet Explorer.

2. Настройка панелей инструментов браузера

Вид -> Панели инструментов. Всегда должны быть отмечены опции **Строка меню** и **Адресная Строка.**

Вид -> Строка состояния. В строке состояния показываются URL выделенных на Web-странице объектов.

Вид -> **Панели обозревателя.** Можно включать панели **Поиск, Избранное, Журнал, Папки.**

3. Удаление временных файлов Интернета

Браузер сохраняет просмотренные страницы в специальную папку Temporary Internet Files (временные файлы Интернета), чтобы ее очистить от устаревших страниц, войдите в меню **Сервис -> Свойства обозревателя** -> вкладка **Общие** -> в разделе **Временные файлы Интернета** нажмите кнопку **Удалить файлы** -> <поставьте флажок **удалить это содержимое> -> ОК.**

4. Кнопки панели управления браузера Internet Explorer

- **Назад** — открывает предыдущую просмотренную сегодня Web-страницу;
- **Вперед** — открывает следующую по списку Web-страницу, из тех, что вы сегодня уже открывали;
- **Остановить** — останавливает загрузку Web-страницы;
- **Обновить** — заново загружает текущую Web-страницу;
- **Домой** — возвращает на *домашнюю страницу браузера,* эта страница автоматически открывается при запуске браузера. ***Установка домашней страницы:*** **Сервис -> Свойства обозревателя** -> на вкладке **Общие** в разделе **Домашняя страница** напишите адрес нужной страницы -> **ОК;**
- **Поиск** — открывает окно для поиска информации;
- **Избранное** — открывает список избранных страниц, адреса которых вы сами помещаете в этот список;
- **Журнал** — показывает список всех страниц, на которых вы побывали за последние дни;
- **Печать** — выводит на принтер текущую Web-страницу.

5. Открытие Web-страницы

В Адресной строке удалите все символы и введите нужный вам адрес, например ***www.lenta.ru***, нажмите клавишу **Enter** или кнопку **Переход.**

6. Добавление ссылки на Web-страницу в папку Избранные

Если вы часто обращаетесь к одной и той же странице, имеет смысл сохранить ссылку на эту страницу в специальной папке **Избранное.**

Добавление ссылки в избранное. Откройте какую-нибудь страницу -> войдите в меню **Избранное -> Добавить в избранное** -> в поле **Имя** напишите название страницы -> ОК.

Посмотрите результат: войдите в меню **Избранное** и щелкните по ссылке (в выпадающем списке внизу).

Создание вложенной папки в папке Избранное. Для создания вложенной папки выполните действия: **Избранное -> Добавить в избранное** -> <нажмите кнопку **Создать папку>** -> <в поле **Имя папки** введите название папки > -> ОК -» ОК.

Добавление ссылки во вложенную папку. Для добавления ссылки откройте нужную страницу -> **Избранное -> Добавить в избранное** -> <нажмите кнопку **Добавить в>** -> <в окне **Добавить в** откройте нужную папку двойным щелчком> -> <в поле **Имя** введите название страницы> -> ОК.

Чтобы открыть страницу, ссылка на которую находится во вложенной папке, войдите в меню **Избранное,** укажите мышью на нужную папку, правее появится список ссылок, которые вы туда поместили, щелкните по нужной ссылке.

Удаление ненужных ссылок из папки Избранное. Для удаления ненужных ссылок выполните действия: **Избранное -> Упорядочить избранное** -> <выделите ненужные ссылки или папки> -> <нажмите кнопку **Удалить> -> Закрыть.**

7. ***Поиск информации во Всемирной паутине***

Если вы не знаете, на каком сайте может находиться нужная вам информация, то воспользуйтесь **поисковыми серверами** или **каталогами:** ***yandex.ru, rambler.ru, google.ru, altavista.com, yahoo.com*** и др.

В Адресной строке введите адрес поискового сервера (например, www.rambler.ru).

На первой странице поискового сервера в поле Я **ищу** (иногда здесь написано **Найти)** введите *ключевое слово,* которое достаточно точно описывает нужную вам информацию, например *породы кошек.*

Нажмите клавишу **Enter** или кнопку **Найти** (правее поля запроса).

Результаты поиска отобразятся на новой странице в виде списка ссылок на web-страницы с краткими комментариями, поясняющими содержимое страницы. Чтобы открыть заинтересовавшую вас web-страницу, щелкните по ссылке на нее (подчеркнутый синий текст названия страницы).

8. Сохранение информации с Web-страницы

Сохранение текста. Чтобы сохранить информацию с Web-страницы, выполните действия: <выделите текст на Web-странице> -> **Правка -> Копировать** -> <откройте Microsoft Word > -> **Правка -> Вставить** -> сохраните текст как документ Word **(Файл -> Сохранить).**

Сохранение Web-страницы полностью. Для сохранения Web-страницы выполните действия: **Файл -> Сохранить как** -> <в поле **Папка** выберите свою рабочую папку> -> <в поле **Имя файла** можно ввести любое имя Web-страницы> -> **Сохранить.**

Сохранение рисунка. Для сохранения рисунка необходимо выполнить следующие действия: <щелкните правой кнопкой мыши по рисунку> -> <в контекстном меню выберите команду **Сохранить рисунок как...>** -> <откройте свою папку, если хотите, измените имя файла> -> **Сохранить.**

Порядок выполнения практической работы:

1. Изучить теоретический материал.
2. Выполнить предлагаемые задания.
3. Ответить на контрольные вопросы и предоставить в тетради в виде отчета. Отчет должен включать:
   - номер, наименование практической работы и тему;
   - ответы на контрольные вопросы;
   - выводы.
4. Выполненную работу и отчет по проделанной работе предъявить преподавателю.

Задания для выполнения практической работы:

Задание 1. Знакомство с окном браузера (обозревателя Web-страницы)

1. Создайте папку *Интернет* на своем рабочем диске.

2. Запустите программу-браузер **Internet Explorer** для работы со службой **WWW** (найдите ярлык на рабочем столе или **Пуск -> Программы).**

1. Ознакомьтесь с содержимым пунктов **главного меню** браузера **(Файл, Правка, Вид,**

Избранное, Сервис, Справка).

3. Ознакомьтесь с назначением наиболее часто используемых кнопок **Панели инструментов:**

•с помощью кнопок **Назад** и **Вперед** можно листать открытые сегодня Web-страницы;

•с помощью кнопки **Остановить** останавливается загрузка Web-страницы;

•с помощью кнопки **Обновить** еще раз с Web-сервера загружается текущая Web-страница;

•с помощью кнопки **Домой** открывается *основная страница (основная страница* автоматически открывается при запуске обозревателя);

•с помощью кнопки **Поиск** можно просмотреть список популярных англоязычных поисковых серверов;

•с помощью кнопки **Избранное** можно сформировать список часто используемых сайтов или конкретных Web-страниц;

•с помощью кнопки **Журнал** можно просмотреть список всех страниц, на которых вы побывали за несколько последних дней;

•с помощью кнопки **Почта** можно запустить из браузера программу для работы с электронной почтой;

•с помощью кнопки **Печать** можно вывести на принтер открытую Web-страницу.

Все эти кнопки находятся на панели инструментов **Обычная,** которая включается в меню **Вид.**

5. Ознакомьтесь с **Адресной строкой (**Адресная строка находится над или под кнопками Панели инструментов в зависимости от версии установленного браузера).

Обмен информации в **WWW** реализован на основе протокола HTTP (Hyper Text Transfer Protocol) — «Запрос — Ответ». Для просмотра Web-страницы в **Адресной строке** необходимо написать требуемый адрес, например http://www.rambler.ru *(http://* — эту часть адреса можно опустить).

6. Измените размер окна браузера, выполнив действия:

- **Вид** -> **Во весь экран** (окно браузера раскрылось на весь экран);
- вернитесь к прежнему размеру окна (кнопка в верхней части окна).

Задание 2. Настройка браузера

Ознакомьтесь с основными настройками браузера.

1. Настройка (отключение и включение) **Панели инструментов** и **Адресной строки (Вид -> Панели инструментов).**

Настройка общих свойств браузера **(Сервис -> Свойства обозревателя... -> Общие):**

- настройка **Домашней страницы (Домашняя страница** -> **С пустой);** Такая настройка выполняется в том случае, когда при каждом входе в Интернет вы загружаете разные Web-страницы. В результате этой настройки в адресном поле появится запись *«about.blank».* В том случае, если вы начинаете работу в Интернете с одной и той же Web-страницы, то в адресном поле надо установить адрес этой страницы;
- настройка **Временных файлов Интернета** — просматриваемые страницы копируются в особую папку для ускорения их последующего просмотра **(Временные файлы Интернета -> Параметры -> Проверять наличие обновления сохраненных страниц: -> автоматически -> Занимать на диске не более:** -> устанавливается необходимый объем диска>); Чем больше объем выделенного под временные файлы дискового пространства, тем быстрее работает браузер. Обычно рекомендуют выделять в пределах 1—2 % от объема диска. В случае затруднения эту настройку можно оставить по умолчанию;
- настройка **Журнала (Сервис -> Свойства обозревателя... -> Общие -> Журнал -> Сколько дней хранить ссылки** -> Остановите число 10>);

Эта настройка указывает, в течение какого времени сохранять в журнале адреса открываемых Web-страниц (например, в течение 10 дней);

- настройка **Цвета, Шрифтов, Языка, Оформления (кнопки Цвета..., Шрифты..., Языки..., Оформление....).**

3. Настройка вкладки **Программы (Сервис -> Свойства обозревателя... -> Программы):**

- просмотрите приложения Windows, которые будут использоваться автоматически;
- проверьте, установлена ли программа Outlook Express для электронной почты и групп новостей.

4. Настройка вкладки **Дополнительно (Сервис -> Свойства обозревателя... -> Дополнительно):**

- ознакомьтесь со списком настройки этой вкладки (рекомендуется все настройки этой вкладки делать опытным пользователям, кроме раздела **Мультимедиа);**
- Ознакомьтесь с флажками раздела **Мультимедиа** и снимите их, если у вас «медленная связь» (в противном случае Web-страницы будут загружаться очень медленно).

5. Настройку вкладок **Подключение, Безопасность** и **Содержание** лучше делать опытным пользователям.

6. Закройте окно **Свойства обозревателя...** .

Задание 3. Навигация в сети Интернет по гиперссылкам на Web-страницах. Работа с папкой *Избранное. Сохранение рисунка* ***с*** *Web-страницы* ***в*** *файле*

1. Откройте сайт РУДН (<в **Адресной строке** удалите все символы> -> <введите адрес: **www.rudn.ru** > -> клавиша **Enter).**

В течение нескольких секунд происходит подключение компьютера к тому компьютеру, на котором расположен сайт (индикатор прогресса на панели состояния в нижней части окна отражает процесс подключения);

Если Web-страница долго не открывается (более 2—3 мин), то ее можно перезагрузить (кнопка **Остановить** -> кнопка **Обновить);**

В случае появления нечитаемых выражений необходимо изменить кодировку символов **(Вид -> Вид кодировки -> кириллица (Windows) или кириллица (КОИ8-Р)).**

2. Найдите и откройте Web-страницу с информацией о любом факультете.

Указатель мыши в области гиперссылки приобретает вид ладони с указательным пальцем.

Открыть Web-страницу с адресом, указанным в гиперссылке, можно двумя способами:

1-й способ: **один раз щелкнуть левой кнопкой мыши по гиперссылке.** При этом новая Web-страница будет загружена или в текущее окно браузера или в новое окно (это зависит от решения разработчика сайта);

2-й способ: **щелкнуть правой кнопкой мыши на гиперссылке** —> <выбрать режим открытия документа (открыть в новом окне или в текущем окне браузера) >;

Не рекомендуется открывать более 2—3 окон из-за возможного замедления работы.

Кнопка **Назад** на Панели инструментов используется для возврата к предыдущей Web-странице.

3. Найдите слово *кафедра* на открытой странице с информацией о любом факультете **(Правка -> Найти на этой странице... -> Поиск -> Найти:** ***кафедра*** -> < выбрать направление **вверх** или **вниз> -> Найти далее** -> <закройте окно поиска>).

4. Сохраните адрес сайта РУДН в папке с именем «РУДН» в папке **Избранное** (если вы часто обращаетесь к одной и той же странице, то ее адрес можно записать в папке **Избранное** или в своей собственной папке, созданной в папке **Избранное):**

- **Избранное -> Добавить в Избранное... -> Создать папку... -> Имя папки:** *РУДН* -> ОК -> ОК;
- перейдите на **Домашнюю страницу.**

5. Откройте сайт РУДН из папки **Избранное.**

5. Сохраните рисунок РУДН в файле РУДН.*jpg* в папке Интернет (<наведите курсор на рисунок РУДН> -> <щелкните по рисунку правой кнопкой мыши> -> **Сохранить рисунок как** -> <введите имя: *РУДН*> -> <выберите папку Интернет> -> кнопка **Сохранить).**

6. Перейдите на **Домашнюю страницу.**

Задание 4. Работа с поисковой системой Yandex. Сохранение информации с Web-страницы в виде файла Word

1..Откройте Web-страницу поисковой системы Yandex (в Адресное поле введите адрес: **www.yandex.ru** -> кл. **Enter**).

2. Для формирования сложного запроса ознакомьтесь с языком запросов (<гиперссылка **Помощь** (в конце страницы) -> раздел **Как искать** -> гиперссылка **Дополнительные возможности -> Язык запросов**).

3. Вернитесь на стартовую страницу поисковой системы Yandex.

4. Найдите материал для реферата на тему ***«Защита информации в Интернете».*** Например, можно сформировать такой запрос: *(защита информации в Интернете) & реферат.*

5. Найдите материал для реферата, сформировав другие запросы на эту тему.

6. Сохраните информацию для реферата в файле *Реферат.doc*

- выделите информацию для реферата;
- скопируйте ее в буфер обмена;
- откройте **Word (Пуск -> Программы -► Microsoft Office -> Microsoft Word);**
- откройте новый документ;
- скопируйте туда информацию из буфера обмена;
- сохраните эту информацию в файле *Реферат.doc* в папке Интернет;
- закройте **Word.**

7. Закройте браузер.

Контрольные вопросы:

1. Что такое браузер?
2. Какие браузеры Вы знаете?
3. Какие настройки Вы можете установить в браузере?

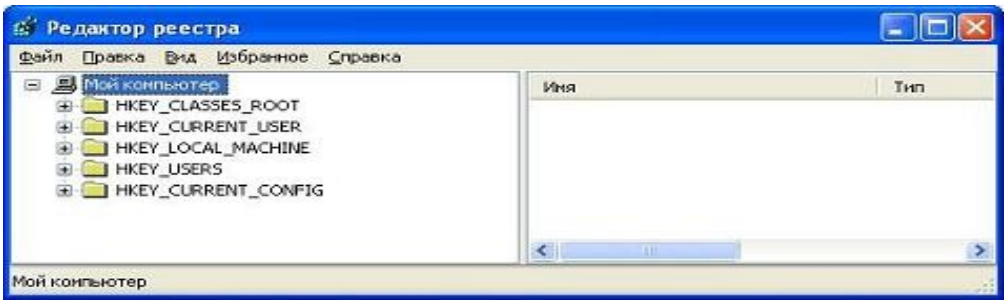
Лабораторная работа №9 «Работа с реестром»

Цель работы: «изучить назначение реестра, его структуру, редакторы реестра, приемы восстановления системы при повреждении реестра; сформировать навыки и умения работать с редактором реестра»
Материально-техническое обеспечение: Компьютер, операционная система Windows 7

Краткие теоретические сведения:

Реестр операционной системы.

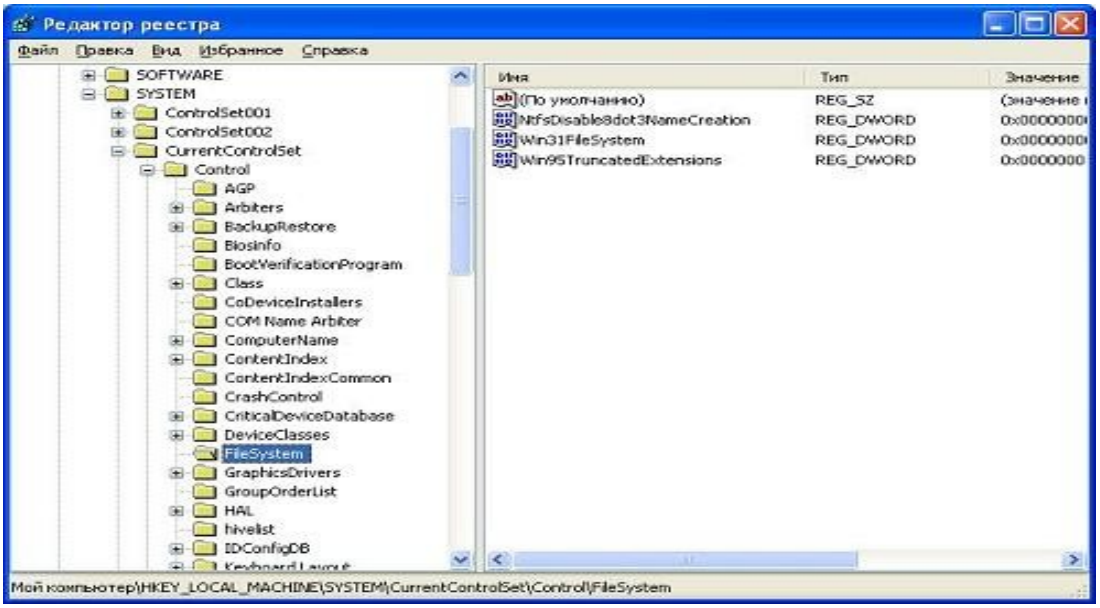
Все настройки операционной системы вместе с конфигурацией персонального компьютера собраны в единой базе данных, именуемой системным реестром. С момента запуска компьютера и вплоть до его отключения операционная система непрерывно использует эту базу данных, контролируя настройки профилей всех пользователей, параметры программ, типы документов, сетевые настройки и т.д. Для работы с системным реестром в операционной системе Microsoft Windows 7 пользователю предлагается использовать встроенную утилиту Regedit (см рис.).



Реестр имеет иерархическую структуру, состоящую из 5 корневых ключей.

- **HKEY_CLASSES_ROOT –** информация об ассоциациях файлов с приложениями, ярлыками, объектами
- **HKEY_CURRENT_USER –** информация настроек для зарегистрированного в системе пользователя
- **HKEY_LOCAL_MACHINE –** информация об установленном аппаратном программном обеспечении
- **HKEY_USERS –** информация о конфигурациях пользовательских профилей, системных переменных среды, раскладке клавиатуры и т.п.
- **HKEY_CURRENT_CONFIG –** текущая конфигурация программного и аппаратного обеспечения.

В левой части окна редактора реестра в виде дерева отображаются поддеревья и разделы реестра, в правой - параметры конкретного раздела реестра. Полный путь к выбранному разделу выводится в строке состояния.



Физически реестр состоит из нескольких файлов двоичного (нетекстового формата), которые хранятся в каталоге *Winnt|System32|Config (Windows 2000), .*

Редакторы реестра позволяют просматривать и модифицировать реестр. Они не являются «услужливыми» программами, не распознают ошибки, не предупреждают о них пользователя, не имеют команды undo (отменить). Программа **regedt32.exe** автоматически устанавливается в папку **%systemroot%\system32**. Программа **regedit.exe** устанавливается в папку **%systemroot%**.

Использование редактора реестра для настройки операционной системы.

Существует множество программ для редактирования реестра. Однако, несмотря на то, что все программы, позволяющие осуществлять настройки реестра, просты в использовании и обладают обширными возможностями, все то, что умеют эти утилиты, можно сделать и вручную. До того как начать работу с реестром, настоятельно рекомендуется сделать его резервную копию, создать точку отката в Windows 7 или создать образ диска с операционной системой. Эту процедуру необходимо осуществить в том случае, если при неправильном редактировании реестра произошли изменения, повлекшие за собой некорректную работу ОС, и вернуть исходные настройки представляется весьма затруднительным. Имея резервную копию, вы всегда сможете восстановить исходные значения всех ключей реестра. Для тех, кто заранее не заботился о сохранности реестра, единственный выход из сложившейся ситуации - переустановка операционной системы с нуля.

Внесение в реестр неправильных изменений может серьезно повредить систему. Реестр является важнейшим компонентом, от которого зависит работоспособность системы. Неумелое обращение с реестром может привести к краху операционной системы.

Запуск редактора реестра.

В меню **Пуск** выберите пункт **Выполнить**, введите команду **regedit.exe** и нажмите **OK**.

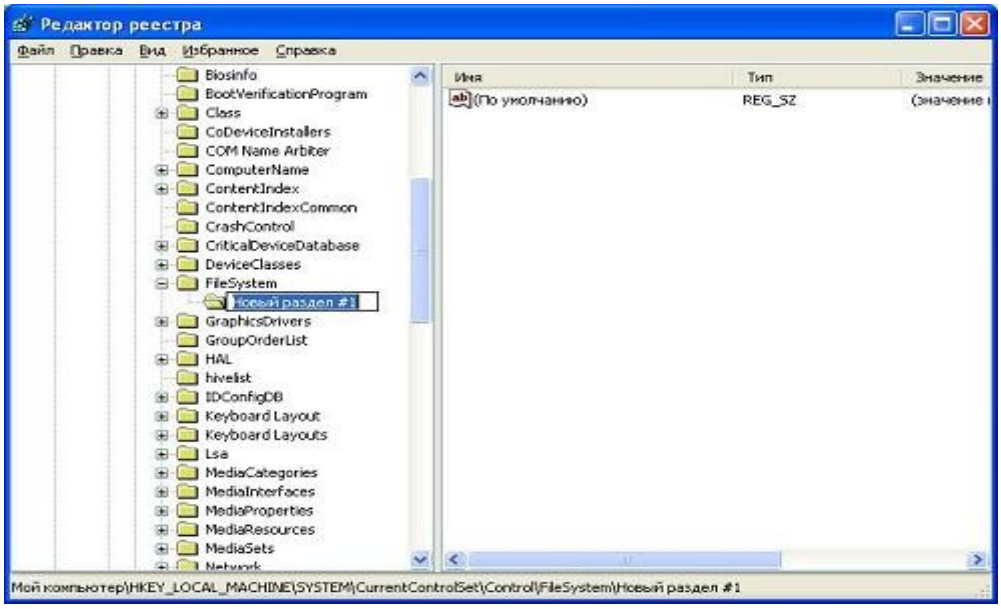
Перед вами предстанет окно редактора реестра.

Работа с редактором реестра сводится к выполнению следующих задач:

- управление разделами реестра;
- управление параметрами;
- экспорт и импорт данных.

1. Управление разделами реестра.

Чтобы создать новый подраздел, найдите в дереве реестра нужный раздел, выделите его и в меню ***Правка*** выберите ***Создать -> Раздел***.



Введите имя нового раздела.

Чтобы удалить раздел, найдите его в дереве реестра, выделите и в меню **Правка** выберите **Удалить**. После дополнительного подтверждения раздел, включая все подразделы и параметры во всех подразделах, будет удален.

При удалении разделов реестра удаляются все его подразделы и параметры во всех подразделах. Кроме того, операция удаления не может быть отменена.

2. Управление параметрами и их значениями.

Редактор реестра regedit.exe поддерживает работу с параметрами следующих типов:

Тип данных	**Описание**
REG_BINARY	Необработанные двоичные данные. Большинство сведений об аппаратных компонентах хранится в виде двоичных данных и выводится в редакторе реестра в шестнадцатеричном формате.
REG_DWORD	Данные, представленные целым числом (4 байта). Многие параметры служб и драйверов устройств имеют этот тип и отображаются в двоичном, шестнадцатеричном или десятичном форматах.
REG_EXPAND_SZ	Строка данных переменной длины. Этот тип данных включает переменные, обрабатываемые при использовании данных программой или службой.
REG_MULTI_SZ	Многострочный текст. Этот тип, как правило, имеют списки и другие записи в формате, удобном для чтения. Записи разделяются пробелами, запятыми или другими символами.
REG_SZ	Текстовая строка фиксированной длины.
REG_FULL _RESOURCE_DESCRIPTOR	Последовательность вложенных массивов, разработанная для хранения списка ресурсов аппаратного компонента или драйвера.

Чтобы *создать новый параметр* в разделе, найдите в дереве реестра нужный раздел, выделите его и нажмите правую кнопку мыши. В контекстном меню выберите **Создать**, а

в нем - **Строковый параметр**, Двоичный параметр, Параметр DWORD, Мультистроковый параметр или Расширяемый строковый параметр, в зависимости от того, параметр какого типа хотите создать. Будет создан новый параметр с именем Новый параметр #1 , которое можно сразу изменить. После нажатия клавиши **Enter** параметр будет сохранен с новым именем.

Чтобы *изменить имя параметра*, найдите в дереве реестра нужный раздел, выделите его и найдите нужный параметр в списке справа. Выделите этот параметр и нажмите правую кнопку мыши. В контекстном меню выберите **Переименовать**. Заменить имя параметра также можно, нажав клавишу **F2**. Теперь вы можете изменить имя параметра непосредственно в списке параметров. После изменения нажмите клавишу **Enter**, и новое название параметра будет сохранено.

Чтобы *удалить параметр*, найдите в дереве реестра нужный раздел, выделите его и найдите нужный параметр в списке справа. Выделите этот параметр и нажмите правую кнопку мыши. В контекстном меню выберите **Удалить**. Кроме того, можно использовать клавишу **Delete** . После дополнительного подтверждения параметр будет удален.

Чтобы *изменить значение параметра*, найдите в дереве реестра нужный раздел, выделите его и найдите нужный параметр в списке справа. Выделите этот параметр и нажмите правую кнопку мыши. В контекстном меню выберите **Изменить**. Кроме того, можно использовать клавишу **Enter**. В появившемся окне исправьте или введите новое значение параметра и щелкните кнопку **ОК**.

2 Создание копии реестра. Резервную копию можно сохранить в нужном месте, например в папке на жестком диске или на съемном носителе. Затем эту резервную копию можно импортировать, чтобы отменить внесенные изменения.

1. Откройте редактор реестра. Для этого нажмите кнопку Пуск, введите regedit в поле поиска и затем нажмите клавишу ВВОД. Если отображается запрос на ввод пароля администратора или его подтверждения, укажите пароль или предоставьте подтверждение.
2. Найдите и выберите раздел или подраздел реестра, резервную копию которого необходимо создать.
3. Откройте вкладку Файл и нажмите кнопку Экспорт.
4. В поле Папка выберите расположение, в которое следует сохранить резервную копию, и в поле Имя файла введите имя файла.
5. Щелкните Сохранить.

Порядок выполнения практической работы:

1. Изучить теоретический материал.
2. Выполнить предлагаемые задания.
3. Ответить на контрольные вопросы и предоставить в тетради в виде отчета. Отчет должен включать:
   - номер, наименование практической работы и тему;
   - ответы на контрольные вопросы;
   - выводы.
4. Выполненную работу и отчет по проделанной работе предъявить преподавателю.

Задания для выполнения практической работы:

1. Открыть справку WINDOWS, найти информацию по реестру, занести в конспект информацию о том, что такое реестр, «Восстановление реестра».

2 Измените некоторые системные настройки посредством реестра

2.1 Выполнить экспорт реестра в текстовый файл на свой раздел диска. Имя файла – MYREG.REG.

2.2 Добавьте сообщение, отображаемое при регистрации пользователя в системе:

- Вызовите редактор REGEDIT.

- Раскройте ключ реестра HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ WindowsNT\CurrentVersion\WinLogon
- Найдите параметр *LegalNoticeCaption.* Раскройте его и введите «Заголовок окна». Введенная фраза будет отображаться в заголовке информационного окна.
- Найдите параметр *LegalNoticeText.* Раскройте его и введите «Вас приветствует администратор».
- Закройте окно редактора. Перезагрузите систему, продемонстрируйте результат вашей работы.
- Проделайте шаги 1 – 5, очистив значения *LegalNoticeCaption* и *LegalNoticeText.*
- Какие изменения вы заметили?

2.3 Измените значок мусорной корзины (пустой и заполненной):

- В реестре найдите ключ
- **HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\ CURRENTVERSION\EXPLORER\CLSID\645FF040-5081-101B-9F08-00AA002F954E.**
  - Прямо под ним – ключ *Defaulticon*. Откройте его. В правом окне элементы *FULL* и *EMPTY*.Номера 31 и 32 соответствуют пиктограммам. Замените их на 64 и 65 соответственно.
  - Создайте на рабочем столе новую папку и удалите ее. Посмотрите, изменилась ли пиктограмма корзины.
  - Продемонстрируйте преподавателю результат вашей работы.
  - Верните прежние пиктограммы для корзины.

2.4 ***Удалите стрелки с ярлыков***.

- Создайте на рабочем столе 2 любых ярлыка. Убедитесь, что на ярлычках имеются маленькие стрелочки
- Вызовите редактор реестра
- Найдите ключ **HKEY_CLASSES_ROOT\lnkfile**
- Запишите тип параметра IsShortcut в тетрадь (для дальнейшего восстановления), удалите этот параметр
- Найдите ключ **HKEY_CLASSES_ROOT\piffile**
- Удалите параметр IsShortcut
- Перезагрузите Windows. Убедитесь, что стрелочки у ярлычков отсутствуют
- Продемонстрируйте преподавателю результат вашей работы.
- Верните прежние установки (параметры IsShortcut).

2.5 Измените фоновый рисунок экрана входа Windows LogOn (На своем рабочем столе вы можете поместить любой рисунок, то почему бы не сделать то же самое со своим экраном входа в Windows 7)?

1. Зайдите в реестр и пройдите к записи HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Authentication/ LogonUI/Background.
2. Найдите в правой панели ключик “OEMBackground”. Если этого ключа нет, то создайте его. Для этого кликните правой кнопкой мыши по правой панели, выберите Создать и затем Параметр DWORD (32 бита). Созданный ключик необходимо назвать соответственно “OEMBackground”.
3. Дважды кликните по ключику, чтобы открыть его.
4. Теперь в поле Значение введите 1.
5. Кликните OK.
6. С помощью проводника Windows пройдите в папку Windows/System32/oobe. Если в этой папке вы найдете папку с названием info, то войдите в нее. Если же в info есть папка с названием backgrounds, то войдите и в нее. Если две последние папки не существуют, то создайте их.
7. Скопируйте желаемое изображение (это должен быть JPEG-файл с размером менее

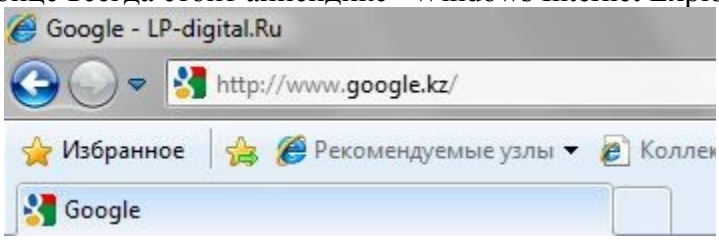
256KB) в папку info/backgrounds.
8. Затем переименуйте скопированный собой файл в backgroundDefault.jpg. (Заметьте, что если размер изображения отличается от разрешения вашего рабочего стола, то изображение будет подогнано под ваш стол – с возможной потерей его качества. Папка info/background также поддерживает 12 других файлов под определенные разрешения. Файлы должны иметь название backgroundXXXXX.jpg, где вместо XXXXX следует вставить разрешения 900x1440, 960x1280, 1024x1280, 1280x1024, 1024x768, 1280x960, 1600x1200, 1440x900, 1920x1200, 1280x768 и 1360x768. (Так, например, файл background1920x1200.jpg будет использоваться на разрешении 1920x1200).

При следующей перезагрузке компьютера в окне входа Windows LogOn вы увидите свою картинку. Если выбранная вами картинка мешает вам читать надписи на кнопках экрана, то попробуйте настроить вид кнопок. Для этого:

1. Пройдите к ключику HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Authentication/LogonUI.
2. В правой панели создайте параметр DWORD с названием ButtonSet.
3. Измените его значение на 1 (тени текста при этом станут темнее, а кнопка светлее. Параметр предназначен для светлых рисунков) или на 2 (нет теней и непрозрачные кнопки – для темных рисунков) или на 0, что Windows принимает по умолчанию.

2.6 Персонализация строки заголовка IE8

В своей Windows 7 вы используете Internet Explorer 8? Тогда вы, скорее всего, знакомы со строкой заголовка браузера, где в независимости от странички, на который вы находитесь, в конце всегда стоит аппендикс “Windows Internet Explorer”.



Так почему бы не изменить его на что-либо более интересное?

1. Перейдите к записи HKEY_CURRENT_USER/Software/Microsoft/Internet Explorer/Main.
2. Кликните правой кнопкой мыши по правой панели, выберите Создать и затем Строковый параметр.
3. Назовите только что созданный собой параметр “Window Title” (вместе с пробелом!).
4. Дважды кликните по нему мышью.
5. Введите в поле значения свой “аппендикс”… и кликните OK.

2.7 Изменение поведения стековой кнопки на панели задач

По умолчанию панель задач группирует несколько окон одного приложения под одной кнопкой и затем при клике по этой кнопке показывает их миниатюры. Если же вы думаете, что было бы лучше, чтобы при клике по кнопке операционная система автоматически переходила на последнее открытое окно, то вы можете это сделать. Для этого:

1. Пройдите к записи HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/Advanced.

2. Кликните правой кнопкой мыши по правой панели, выберите Создать и затем Параметр DWORD (32 бита).
3. Переименуйте созданный параметр в “LastActiveClick”.
4. Дважды кликните по LastActiveClick, чтобы открыть его.
5. Измените число в поле значения на 1.
6. Кликните OK.

2.8 Изменение размера кнопок панели задач

По умолчанию Windows 7 всегда объединяет кнопки панели задач от одной программы и никогда не отображает их лэйблы. Если же вы только что полностью отключили объединение окон или заставили операционную систему объединять их только при заполнении панели задач, то вы также можете изменить размер иконок, чтобы скрыть их лэйблы. Для этого:

1. Пройдите к записи HKEY_CURRENT_USER/Control Panel/Desktop/WindowMetrics.
2. Найдите в правой панели ключ “MinWidth”. Если его там нет, то вам придется создать его самостоятельно. Кликните правой кнопкой мыши по правой панели, выберите Создать и затем Строковый параметр. После чего переименуйте созданный собой параметр в MinWidth.
3. Дважды кликните по MinWidth, чтобы открыть его.
4. Измените число в поле значения. Для небольших иконок введите сюда 38. Для более крупных введите 52.
5. Кликните OK.

Контрольные вопросы:

1. Какие корневые ключи имеет реестр, в чем их назначение?
2. Как сохранить реестр перед редактированием?
3. Как восстановить реестр?
4. Запишите названия ключей, параметров и значений, которые вы использовали при выполнении заданий, в чем их назначение?
5. Как деинсталлировать программы, которые не отображаются в меню "Установка или удаление программ"? (Напишите путь в реестре).
6. Почему перед редактированием создается точка отката в Windows?

Лабораторная работа №10 «Работа с программой восстановления файлов и очистки дисков»

Цель работы: «познакомится с работой программ восстановления файлов и очистки дисков»
Материально-техническое обеспечение: Компьютер, операционная система Windows 7

Порядок выполнения практической работы:

1. Изучить теоретический материал.
2. Выполнить предлагаемые задания.
3. Ответить на контрольные вопросы и предоставить в тетради в виде отчета. Отчет должен включать:
    - номер, наименование практической работы и тему;
    - ответы на контрольные вопросы;
    - выводы.
4. Выполненную работу и отчет по проделанной работе предъявить преподавателю.

Задания для выполнения практической работы:

Выполните следующие задания.

1. Используя задания Сведения о системе, определите следующие параметры компьютерной системы: Мультимедиа, запоминающие устройства, системные драйверы, группы программ, автоматически загружаемые программы.

Для запуска программы **Сведения о системе** выберите в меню Пуск команду **Программы-Стандартные-Служебные-Сведения о системе**.

Для получения сведений об устройствах мультимедиа выберите в дереве категорий в левой области окна программы категорию Компоненты, а в ней подкатегорию Мультимедиа. Выбирая в этой подкатегории элементы мультимедиа аудио- и видеокодеки, CD-ROM, звуковое устройство, дисплей, просмотрите в правой части окна программы сведения, относящиеся к элементу, выделенному в дереве категорий.

Для просмотра сведений о запоминающих устройствах выберите в левой части окна категорию Запоминающие устройства. Выбирая в этой категории различные подкатегории, в области сведений просмотрите информацию об устройствах внешней памяти.

Для просмотра сведений о системных драйверах выберите категорию Программная среда, а в ней подкатегорию Системные драйверы.

Для просмотра данных о группах программ найдите в категории Программная среда подкатегорию Группы программ, чтобы вывести сведения о них в правой области окна.

Аналогично найдите сведения о программах, автоматически загружаемых при старте Windows XP.

Закройте окно программы **Сведения о системе**.

2. Используя стандартную программу Windows **Проверка диска**, проверьте диск A: на наличие поврежденных секторов и ошибок файловой системы. При этом если будут обнаружены ошибки, то задайте режим восстановления поврежденных секторов диска автоматического исправления системных ошибок.

Перед запуском проверки диска закройте все файлы на нем. Открыв окно *Мой компьютер*, выберите локальный диск A:, затем в меню **Файл** выберите команду **Свойства**. На вкладке **Сервис**в группе **Проверка диска** нажмите кнопку «Выполнить проверку». В группе **Параметры проверки диска** установите флажки **Автоматически исправлять системные ошибки** и **Проверять и восстанавливать поврежденные сектора**.

Для начала процесса сканирования диска на наличие ошибок щелкните на кнопке «Запуск». По окончании проверки диска на экран будет выведено сообщение об окончании проверки диска.

3. Используя стандартную программу **Очистка диска**, выполните очистку диска C:.

Для запуска программы выберите в меню **Пуск** команду **Программы-Стандартные-Служебные-Очистка диска**. В рабочем окне программы выберите логический диск C:, который будет подвергнут процедуре очистки, и щелкните на кнопке «ОК». После этого мастер очистки диска перейдет к процедуре проверки состояния файлов на данном диске. После завершения анализа текущего состояния диска программа представит отчет о проделанной работе, указав, сколько места можно освободить. Определив, что подлежит удалению при очистке диска, щелкните на кнопке «ОК», а затем подтвердите удаление файлов при очистке диска, щелкнув на кнопке «Да». После этого запускается процесс очистки диска.

4. Используя стандартную программу **Дефрагментация диска**, выполните оценку фрагментированности файлов на диске C: и, если требуется, то выполните дефрагментацию этого диска.

Для запуска программы Дефрагментации диска выберите в меню **Пуск** команду **Программы-Стандартные-Служебные-Дефрагментация диска**. После этого выберите диск C: и нажмите кнопку «Анализ». По завершении анализа тома программа дефрагментации диска выведет результаты анализа и сообщение о том, нуждается ли данный том в дефрагментации. Если в окне сообщения программа рекомендует выполнить дефрагментацию диска, то щелкните на кнопке «Дефрагментация», если иначе - щелкните кнопку «Закрыть». Если была запущена процедура дефрагментации, то после ее окончания результаты будут отображены в графическом представлении с цветовой кодировкой в полях результатов анализа и дефрагментации. Чтобы просмотреть подробный отчет о дефрагментации, нажмите кнопку «Вывести отчет». Закройте окно программы **Дефрагментация диска**.

Защита и восстановление данных на компьютере

Выполните следующие задания.

1. Используя служебную программу **Архивация данных**, архивируйте данные из папки C:\Program Files\Microsoft Office\Templates в архив с именем Templates на диске D:.

Для запуска приложения Архивация данных выберите в меню **Пуск** команды **Программы-Стандартные-Служебные-Архивация данных**. Если программа архивации запускается в режиме мастера, то для переключения в расширенный режим нажмите кнопку «Расширенный» в окне мастера архивации.

Для архивации выбранных файлов и папок на жестком диске перейдите на вкладку **Архивация** и установите флажок в списке Установите флажки для папки C:\ Program Files\Microsoft Offlce\ Templates, данные из которой вы хотите заархивировать.

Задайте в качестве носителя диск D: и имя файла для архива Templates, нажмите на кнопку «Архивировать», а затем в окне *Сведения о задании архивации* выберите вариант **Затереть данные носителя этим архивом**.

Щелчком на кнопке «Архивировать» запустите процедуру архивации. После этого в окне *Ход архивации* пронаблюдайте за процессом архивации, по окончании которого будет выведено окно сообщения о завершении архивации с краткими сведениями. Для просмотра подробного текста отчета щелкните на кнопке «Отчет».

2. Используя служебную программу **Архивация данных**, создайте архив системных файлов и дискету аварийного восстановления, которые могут быть использованы в целях восстановления системы в случае ее отказа.

Приготовьте чистую дискету емкостью 1,44 Мбайта для сохранения параметров системы, затем запустите приложение Архивация в режиме **Расширенный**. В меню **Сервис** выберите команду **Мастер аварийного восстановления системы**. Следуйте инструкциям, появляющимся на экране. Для перехода к следующему шагу

мастера щелкайте на кнопке «Далее». Выбрав тип носителя для системного архива и имя носителя для хранения архивных данных, например, D:\Arxiv\Backup.bkf, щелкните на кнопке «Далее» для создания архива. После этого будет выполнена архивация системных файлов, необходимых для загрузки системы, и создание дискеты аварийного восстановления.

По окончании процесса архивации в ответ на предложение вставить дискету вставьте чистую дискету, после этого будет создана дискета аварийного восстановления. Для просмотра подробного отчета щелкните на кнопке «Отчет». Закройте окно программы **Архивация данных**.

Контрольные вопросы:

1. Для чего необходимо восстановление файлов?
1. Какие утилиты для восстановления файлов вы знаете?