Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет
им. Г.И. Носова»
Многопрофильный колледж

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

по ПМ.04 «Сопровождение и обслуживание программного обеспечения компьютерных систем»
МДК.04.02 Обеспечение качества функционирования компьютерных систем
для студентов специальности
09.02.07 Информационные системы и программирование
Квалификация: Программист

Магнитогорск, 2018

ОДОБРЕНО
Предметно-цикловой комиссией
«Информатика и вычислительная техника»
Председатель *И.Г.Зорина*
Протокол № 6 от 21.02.2018

Методической комиссией МпК

Протокол №4 от «01» марта 2018г

Разработчики:
преподаватель МпК ФГБОУ ВО «МГТУ им. Г.И. Носова» Денис Дмитриевич Тутаров

преподаватель МпК ФГБОУ ВО «МГТУ им. Г.И. Носова» Людмила Александровна Фетисова

Методические указания по выполнению практических и лабораторных работ разработаны на основе рабочей программы *ПМ.04 «Сопровождение и обслуживание программного обеспечения компьютерных систем»,* МДК.04.02 ОБЕСПЕЧЕНИЕ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ.

Содержание практических и лабораторных работ ориентировано на формирование общих и профессиональных компетенций по программе подготовки специалистов среднего звена по специальности 09.02.07 Информационные системы и программирование.

СОДЕРЖАНИЕ

1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Состав и содержание практических и лабораторных занятий направлены на реализацию Федерального государственного образовательного стандарта среднего профессионального образования.

Ведущей дидактической целью практических занятий является формирование профессиональных практических умений (умений выполнять определенные действия, операции, необходимые в последующем в профессиональной деятельности).

Ведущей дидактической целью лабораторных занятий является экспериментальное подтверждение и проверка существенных теоретических положений (законов, зависимостей).

В соответствии с рабочей программой ПМ.04 «Сопровождение и обслуживание программного обеспечения компьютерных систем»,МДК.04.02 ОБЕСПЕЧЕНИЕ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ, предусмотрено проведение практических и лабораторных занятий. В рамках практического или лабораторного занятия обучающиеся могут выполнять одну или несколько практических или лабораторных работ.

В результате их выполнения, обучающийся должен:

уметь:

-подбирать и настраивать конфигурацию программного обеспечения компьютерных систем;

-проводить инсталляцию программного обеспечения компьютерных систем;

-производить настройку отдельных компонентов программного обеспечения компьютерных систем;

-измерять и анализировать эксплуатационные характеристики качества программного обеспечения;

- использовать методы защиты программного обеспечения компьютерных систем;

- анализировать риски и характеристики качества программного обеспечения;

- выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами.

Содержание практических и лабораторных занятий ориентировано на формирование общих компетенций по профессиональному модулю программы подготовки специалистов среднего звена по специальности и овладению ***профессиональными компетенциями***:

Код	**Наименование вида деятельности и профессиональных компетенций**
ПК 4.1.	Осуществлять инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем.
ПК 4.2.	Осуществлять измерения эксплуатационных характеристик программного обеспечения компьютерных систем
ПК 4.4.	Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.

А также формированию ***общих компетенций***:

Код	***Наименование общих компетенций***
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для

	выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.
ОК 11.	Планировать предпринимательскую деятельность в профессиональной сфере

Выполнение обучающимися практических и лабораторных работ по ПМ.04 «Сопровождение и обслуживание программного обеспечения компьютерных систем», МДК.04.02 Обеспечение качества функционирования компьютерных систем, направлено на:

- обобщение, систематизацию, углубление, закрепление, развитие и детализацию полученных теоретических знаний по конкретным темам учебной дисциплины;
- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;
- формирование и развитие умений: наблюдать, сравнивать, сопоставлять, анализировать, делать выводы и обобщения, самостоятельно вести исследования, пользоваться различными приемами измерений, оформлять результаты в виде таблиц, схем, графиков;
- приобретение навыков работы с различными приборами, аппаратурой, установками и другими техническими средствами для проведения опытов;
- развитие интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструктивных и др.;
- выработку при решении поставленных задач профессионально значимых качеств, таких как самостоятельность, ответственность, точность, творческая инициатива.

Практическиеи лабораторные занятия проводятся после соответствующей темы, которая обеспечивает наличие знаний, необходимых для ее выполнения.

2. ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ ЗАНЯТИЙ

МДК.04.02 ОБЕСПЕЧЕНИЕ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ

Разделы/темы	**Темы лабораторных занятий**	**Количество часов**	**Требования ФГОС СПО (уметь)**
Раздел 2. Обеспечение качества компьютерных систем в процессе эксплуатации		**39**	
Тема 4.2.1 Основные методы обеспечения качества функционирования	Лабораторная работа №1,2 Тестирование программных продуктов	4	У1,У2, У3, У4, У5, У6, У10, У01.1,У01.2, У01.3, У02.1, У02.2, У02.3, У09.1, У09.2, У10.6,У03.2, У03.3, У04.1, У04.2, У04.5, У05.1, У05.3, У06.2,У07.2,У10.6
	Лабораторная работа №3,4 Сравнение результатов тестирования с требованиями технического задания и/или спецификацией	4	У1,У2, У3, У4, У5, У6, У10, У01.1,У01.2, У01.3, У02.1, У02.2, У02.3, У09.1, У09.2, У10.6,У03.2, У03.3, У04.1, У04.2, У04.5, У05.1, У05.3, У06.2,У07.2,У10.6
	Лабораторная работа №5,6 Анализ рисков	4	У1,У2, У3, У4, У5, У6, У10, У01.1,У01.2, У01.3, У02.1, У02.2, У02.3, У09.1, У09.2, У10.6,У03.2, У03.3, У04.1, У04.2, У04.5, У05.1, У05.3, У06.2,У07.2,У10.6
	Лабораторная работа №7,8 Выявление первичных и вторичных ошибок	3	У1,У2, У3, У4, У5, У6, У10, У01.1,У01.2, У01.3, У02.1, У02.2, У02.3, У09.1, У09.2, У10.6,У03.2, У03.3, У04.1, У04.2, У04.5, У05.1, У05.3, У06.2,У07.2,У10.6
Тема 4.2.2 Методы и средства защиты компьютерных систем	Лабораторная работа №1,2 Обнаружение вируса и устранение последствий его влияния	4	У1,У2, У3, У4, У5, У6, У10, У01.1,У01.2, У01.3, У02.1, У02.2, У02.3, У09.1, У09.2, У10.6,У03.2, У03.3, У04.1, У04.2, У04.5, У05.1, У05.3, У06.2,У07.2,У10.6
	Лабораторная работа №3,4,5 Установка и настройка антивируса. Настройка обновлений с помощью зеркала	6	У1,У2, У3, У4, У5, У6, У10, У01.1,У01.2, У01.3, У02.1, У02.2, У02.3, У09.1, У09.2, У10.6,У03.2, У03.3, У04.1, У04.2, У04.5, У05.1, У05.3, У06.2,У07.2,У10.6
	Лабораторная работа №6,7 Настройка политики	4	У1,У2, У3, У4, У5, У6, У10, У01.1,У01.2, У01.3,

	безопасности		У02.1, У02.2, У02.3, У09.1, У09.2, У10.6,У03.2, У03.3, У04.1, У04.2, У04.5, У05.1, У05.3, У06.2,У07.2,У10.6
	Лабораторная работа №8,9 Настройка браузера	4	У1,У2, У3, У4, У5, У6, У10, У01.1,У01.2, У01.3, У02.1, У02.2, У02.3, У09.1, У09.2, У10.6,У03.2, У03.3, У04.1, У04.2, У04.5, У05.1, У05.3, У06.2,У07.2,У10.6
	Лабораторная работа №10,11 Работа с реестром	4	У1,У2, У3, У4, У5, У6, У10, У01.1,У01.2, У01.3, У02.1, У02.2, У02.3, У09.1, У09.2, У10.6,У03.2, У03.3, У04.1, У04.2, У04.5, У05.1, У05.3, У06.2,У07.2,У10.6
	Лабораторная работа №12 Работа с программой восстановления файлов и очистки дисков	2	У1,У2, У3, У4, У5, У6, У10, У01.1,У01.2, У01.3, У02.1, У02.2, У02.3, У09.1, У09.2, У10.6,У03.2, У03.3, У04.1, У04.2, У04.5, У05.1, У05.3, У06.2,У07.2,У10.6
ИТОГО		**39**	

3 МЕТОДИЧЕСКИЕ УКАЗАНИЯ

Тема 4.2.1 Основные методы обеспечения качества функционирования

Лабораторная работа №1,2
Тестирование программных продуктов

Цель: изучить классификацию видов тестирования,
практически закрепить эти знания путем генерации тестов различных видов,
научиться планировать тестовые активности в зависимости от специфики поставляемой на тестирование функциональности.

Выполнив работу, Вы будете:

уметь:

- составлять тесты для ПО
- выбирать тесты, подходящие для специфики функциональности

Материальное обеспечение:

ПО: MSWindows 7,MSOffice

Теоретическое обоснование

Тестирование – процесс, направленный на оценку корректности, полноты и качества разработанного программного обеспечения.

Тестирование можно классифицировать по очень большому количествупризнаков. Далее приведен обобщенный список видов тестирования поразличным основаниям.

Типы тестов по покрытию (по глубине)

Smoketest – тестирование системы для определения корректной работыбазовых функций программы в целом, без углубления в детали. Припроведении теста определяется пригодность сборки для дальнейшеготестирования.

MinimalAcceptanceTest (MAT, Positivetest):тестированиесистемыили ее части только на валидных данных (валидные данные – это данные,которые необходимо использовать для корректной работы модуля/функции).При тестировании проверяется правильной работы всех функций и модулей свалидными данными.

Для крупных и сложных приложений используется ограниченныйнабор сценариев и функций.

AcceptanceTest (AT): полное тестирование системы или ее части как накорректных, так и на некорректных данных/сценариях. Вид теста,направленный на подтверждение того, что приложение можетиспользоваться по назначению при любых условиях.

Тест на этом уровне покрывает все возможные сценарии тестирования:проверку работоспособности модулей при вводе корректных значений;проверку при вводе некорректных значений; использование форматованных отличных от тех, которые указаны в требованиях; проверкуисключительных ситуаций, сообщений об ошибках; тестирование наразличных комбинациях входных параметров; проверку

всех классовэквивалентности; тестирование граничных значений интервалов; сценарии непредусмотренные спецификацией и т.д.

Тестовые активности (типы тестов по покрытию (по ширине)):

DefectValidation – проверка результата исправления дефектов.Включает в себя проверку на воспроизводимость дефектов, которые были исправлены в новой сборке продукта, а также проверку того, чтоисправление не повлияло на ранее работавшую функциональность**NewFeatureTest (NFT, ATofNF)** – определениекачествапоставленной на тестирование новой функциональности, которая ранее нетестировалась. Данный тип тестирования включает в себя: проведениеполного теста (АТ) непосредственно новой функциональности; тестированиеновой функциональности на соответствие документации; проверкувсевозможных взаимодействий ранее реализованной функциональности сновыми модулями и функциями.

Regressiontesting (регрессионное тестирование) – проводится сцелью оценки качества ранее реализованной функциональности. Включает всебя проверку стабильности ранее реализованной функциональности послевнесения изменений, например добавления новой функциональности,исправление дефектов, оптимизация кода, разворачивание приложения нановом окружении. Регрессионное тестирование может быть проведено науровнеSmoke, МАТилиАТ.

Типы тестов по знанию коду

Черный ящик – тестирование системы, функциональное илинефункциональное, без знания внутренней структуры и компонентовсистемы. У тестировщика нет доступа к внутренней структуре и кодуприложения либо в процессе тестирования он не обращается к ним.

Белый ящик – тестирование основанное на анализе внутреннейструктуры компонентов или системы. У тестировщика есть доступ квнутренней структуре и коду приложения.

Серый ящик – комбинация методов белого и черного ящика,состоящая в том, что к части кода архитектуры у тестировщика есть, а кчасти кода – нет.

Типы тестов по степени автоматизации

Ручное – тестирование, в котором тест-кейсы выполняютсятестировщиком вручную без использования средств автоматизации.

Автоматизированное – набор техник, подходов и инструментальныхсредств, позволяющий исключить человека из выполнения некоторых задач впроцессе тестирования. Тест-кейсы частично или полностью выполняетспециальное инструментальное средство.

Типы тестов по изолированности компонентов

Unit/component (модульное) – тестирование отдельных компонентов(модулей) программного обеспечения.

Integration (интеграционное) – тестируется взаимодействие междуинтегрированными компонентами или системами.

System (системное) – тестируется работоспособность системы в целомс целью проверки того, что она соответствует установленным требованиям.

Типы тестов по подготовленности.

Интуитивное тестирование выполняется без подготовки к тестам,без определения ожидаемых результатов, проектирования тестовыхсценариев.

Исследовательское тестирование – метод проектирования тестовыхсценариев во время выполнения этих сценариев. Тестировщик совершаетпроверки, продумывает их, придумывает новые проверки, часто используетдля этого полученную информацию.

Тестирование по документации – тестирование по подготовленнымтестовым сценариям, руководству по осуществлению тестов.

Титы тестов по месту и времени проведения

UserAcceptanceTesting (UAT) (приемочноетестирование) –формальное тестирование по отношению к потребностям, требованиям ибизнес процессам пользователя, проводимое с целью определениясоответствия системы критериям приёмки и дать возможностьпользователям, заказчикам или иным авторизованным лицам определить,принимать систему.

AlphaTesting (альфа-тестирование) – моделируемое илидействительное функциональное тестирование, выполняется в организации,разрабатывающей продукт, но не проектной командой (это может бытьнезависимая команда тестировщиков, потенциальные пользователи,заказчики). Альфа тестирование часто применяется к коробочномупрограммному обеспечению в качестве внутреннего приемочноготестирования.

BetaTesting (бета-тестирование) – эксплуатационное тестированиепотенциальными или существующими клиентами/заказчиками на внешнейстороне (в среде, где продукт будет использоваться) никак связанными сразработчиками, с целью определения действительно ли компонент илисистема удовлетворяет требованиям клиента/заказчика и вписывается вбизнес-процессы. Бета-тестирование часто проводится как форма внешнегоприемочного тестирования готового программного обеспечения для того,чтобы получить отзывы рынка.

Типы тестов по объекту тестирования

Functionaltesting (функциональное тестирование) – этотестирование, основанное на анализе спецификации, функциональностикомпонента или системы. Функциональным можно назвать любой видтестирования, который согласно требованиям проверяет правильную работу.

Safetytesting (тестирование безопасности) – тестированиепрограммного продукта с целью определить его безопасность (безопасность– способность программного продукта при использовании оговореннымобразом оставаться в рамках приемлемого риска причинения вреда здоровью,бизнесу, программам, собственности или окружающей среде.Securitytesting (тестирование защищенности) – это тестирование сцелью оценить защищенность программного продукта. Тестированиезащищенности проверяет фактическую реакцию защитных механизмов,встроенных в систему, на проникновение.

Compatibilitytesting (тестирование совместимости) – процесстестирования для определения возможности взаимодействия программногопродукта, проверка работоспособности приложения в различных средах(браузеры и их версии, операционные системы, их типа, версии иразрядность)

Виды тестов:

- кросс-браузерное тестирование (различные браузеры или версиибраузеров)

- кросс-платформенное тестирование (различные операционныесистемы или версии операционных систем)

Нефункциональное тестирование – это проверка характеристикпрограммы. Иначе говоря, когда проверяется не именно правильностьработы, а какие-либо свойства (внешний вид и удобство пользования,скорость работы и т.п.).

1. Тестирование пользовательского интерфейса (GUI) –тестирование, выполняемое путем взаимодействия с системой через

- графический интерфейс пользователя.
- навигация
- цвета, графика, оформление
- содержание выводимой информации
- поведение курсора и горячие клавиши
- отображение различного количества данных (нет данных, минимальное и максимальное количество)
- изменение размеров окна или разрешения экрана

2. Тестирование удобства использования (UsabilityTesting) –тестирование с целью определения степени понятности, легкости в изучениии использовании, привлекательности программного продукта дляпользователя при условии использования в заданных условиях эксплуатации.

- визуальное оформление
- навигация
- логичность

3. Тестирование доступности (Accessibilitytesting) – тестирование,которое определяет степень легкости, с которой пользователи сограниченными способностями могут использовать систему или еекомпоненты.

4. Тестирование интернационализации – тестирование способностипродукта работать в локализованных средах (способность изменять элементыинтерфейса в зависимости от длины и направления текста, менятьсортировки/форматы под различные локали и т.д.). (Максим Черняк).Интернационализация – это процесс, упрощающий дальнейшую адаптацию продукта к языковым и культурным особенностям региона,отличного от того, в котором разрабатывался продукт. Это адаптацияпродукта для потенциального использования практически в любом месте. Интернационализация производится на начальных этапах разработки, в товремя как локализация — для каждого целевого языка.

5. Тестирование локализации (Localizationtesting) – тестирование,проводимое с целью проверить качество перевода продукта с одного языкана другой.

6. Тестирование производительности или нагрузочноетестирование – процесс тестирования с целью определенияпроизводительности программного продукта.

Виды тестов:

- нагрузочное тестирование (PerformanceandLoadtesting) – видтестирования производительности, проводимый с целью оценки поведениякомпонента или системы при возрастающей нагрузке, например количествепараллельных пользователей и/или операций, а также определения какуюнагрузку может выдержать компонент или система;

- объемное тестирование (Volumetesting) – позволяет получитьоценку производительности при увеличении объемов данных в базе данныхприложения;
- тестирование стабильности и надежности (Stability / Reliabilitytesting) – позволяет проверять работоспособность приложения придлительном (многочасовом) тестировании со средним уровнем нагрузки.
- стрессовое тестирование (Stresstesting) – вид тестированияпроизводительности, оценивающий систему или компонент на граничныхзначениях рабочих нагрузок или за их пределами, или же в состоянииограниченных ресурсов, таких как память или доступ к серверу.

7. Тестирование требований (Requirementstesting) – проверкатребований на соответствие основным характеристикам качества.

8. Тестирование прототипа (Prototytetesting) – метод выявленияструктурных, логических ошибок и ошибок проектирования на раннейстадии развития продукта до начала фактической разработки.

9. Тестирование установки (Installabilitytesting) и лицензирования –процесс тестирования устанавливаемости программного продукта.

Виды тестов:

- формальный тест программы установки приложения (проверкапользовательского интерфейса, навигации, удобства пользования,соответствия общепринятым стандартам оформления);
- функциональный тест программы установки;тестирование механизма лицензирования и функций защиты отпиратства;
- проверка стабильности приложения после установки.

10. Тестирование на отказ и восстановление (FailoverandRecovery Testing) – тестирование при помощи эмуляции отказов системы или реальновызываемых отказов в управляемом окружении.

Тестирование программного продукта включает следующие этапы:

1. Изучение и анализ предмета тестирования.
2. Планирование тестирования.
3. Исполнение тестирования.

Изучение и анализ предмета тестирования начинается еще доутверждения спецификации и продолжается на стадии разработки(кодирования) программного обеспечения. Конечной целью этапа изучение ианализ предмета тестирования является получение ответов на два вопроса:- какие функциональности предстоит протестировать,- как эти функциональности работают.

Планирование тестирования происходит на стадии разработки(кодирования) программного обеспечения. На стадии планированиятестирования перед тестировщиком стоит задача поиска компромисса междуобъемом тестирования, который возможен в теории, и объемомтестирования, который возможен на практике. На данной стадии необходимоответить на вопрос: как будем тестировать? Результатом планированиятестирования является тестовая документация.

Выполнение тестирования происходит на стадии тестирования ипредставляет собой практический поиск дефектов с использованием тестовойдокументации,

составленной ранее.Для всех программных продуктов выполняют следующие типытестов и их композиции.

Для первого билда рекомендуется проводить Smoke+AT готовойфункциональности: поверхностное тестирование (SmokeTest) выполняетсядля определения пригодности сборки для дальнейшего тестирования; полноетестирование системы или ее части как на корректных, так и нанекорректных данных/сценариях (AcceptanceTest, AT) позволяет обнаружитьдефекты и внести запись о них в багтрэкинговую систему.

Для последующих билдов композиции тестов могут бытьследующими:

- Если не была добавлена новая функциональность, то: DV+MAT.T.e., выполняется проверка исправления дефектов программистом (DefectValidation, DV), а также проверка работоспособности остальнойфункциональности после исправления дефектов на позитивных сценариях(MinimalAcceptanceTest, MAT).
- Если была добавлена новая функциональность, то:Smoke+DV+NFT+RegressionTest. В частности, выполняется поверхностноетестирование (SmokeTest), проверка исправления дефектов программистом(DefectValidation, DV), тестирование новых функциональностей (NewFeatureTesting, NFT), проверка старых функциональностей, т.е.регрессионное тестирование (RegressionTest).
- Если была добавлена новая функциональность, то возможен такжевариант: DV+NFT+Resressiontest, т.е. без выполнения SmokeTest.В зависимости от типа и специфики приложения (web, desktop, mobile)выполняют специализированные тесты (например, кроссбраузерное или кроссплатформенное тестирование, тестирование локализации иинтернационализации и др.).

Порядок выполнения работы

1. Получить задание у преподавателя.
2. Выполнить генерацию тестов различных видов для конкретного объекта реального мира
3. Спланировать тестовые активности для следующих задач:

3.1 Поставлен на тестирование модуль 1, модуль 2, модуль 3.

3.2 Проведены исправления (fix) для заведенных дефектов, доставлена новая функциональность – модуль 4.

3.3 Заказчик решил расширять рынки сбыта и просит осуществить поддержку для Великобритании (кроме уже существующей Беларуси).

3.4 Заказчик хочет убедиться, что ПО держит нагрузку в 2000 пользователей.

4. Оформить отчет и защитить лабораторную работу.

Форма представления результата

1. Цель работы.
2. Краткие теоретические сведения.
3. Сгенерированные тесты различных видов для выбранного объекта
4. реального мира.
5. Тестовые активности для сформулированных задач.

6. Выводы по работе.

Контрольные вопросы

1. Что такое тестирование?
2. Какие существуют типы тестов по покрытию? Дайте характеристику каждому.
3. Какие существуют тестовые активности? Дайте характеристику каждому.
4. Какие существуют типы тестов знанию кода? Дайте характеристику каждому.
5. Какие существуют типы тестов по степени автоматизации? Дайте характеристику каждому.
6. Какие существуют типы тестов по изолированности компонентов? Дайте характеристику каждому.
7. Какие существуют типы тестов по подготовленности? Дайте характеристику каждому.
8. Какие существуют типы тестов по месту и времени проведения? Дайте характеристику каждому.
9. Какие существуют типы тестов по объекту тестирования? Дайте характеристику каждому.
10. Какие существуют типы функциональных тестов? Дайте характеристику каждому.
11. Какие существуют типы нефункциональных тестов? Дайте характеристику каждому.
12. Какие этапы составляют процесс тестирования?
13. Что происходит на этапе изучения и анализа предмета тестирования?
14. Что происходит на этапе планирования тестирования?
15. Что происходит на этапе исполнения тестирования?
16. Какие типы тестов выполняют для первой поставки программного продукта?
17. Какие типы тестов выполняют для последующих поставок программного продукта?

Критерии оценки:

Оценка «5» ставится, если учащийся выполняет работу в полном объеме с соблюдением необходимой последовательности проведения опытов и измерений; самостоятельно и рационально монтирует необходимое оборудование; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдает требования правил безопасности труда; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей.

Оценка «4» ставится, если выполнены требования к оценке «5» , но было допущено два - три недочета, не более одной негрубой ошибки и одного недочёта.

Оценка «3» ставится, если работа выполнена не полностью, но объем выполненной части таков, позволяет получить правильные результаты и выводы: если в ходе проведения опыта и измерений были допущены ошибки.

Оценка «2» ставится, если работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов: если опыты, измерения, вычисления, наблюдения производились неправильно.

Лабораторная работа №3,4
Сравнение результатов тестирования с требованиями технического задания и/или спецификацией

Цель: составить итоговый отчето результатах тестирования web приложения.

Выполнив работу, Вы будете:

уметь:

- Анализировать результаты тестирования ПО
- Сравнивать результаты анализа тестирования ПО с требуемыми параметрами

Материальное обеспечение:

ПО: MSWindows 7, MSOffice, Internet

Теоретическое обоснование

Итоговый отчет о качестве проверенного функционала является неотъемлемой частью работы, которую каждый тестировщик должен выполнить по завершению тестирования.Итоговый отчет можно разделить на части с соответствующей информацией:

1.Общая информация.

2.Сведения о том, ктои когда тестировалпрограммный продукт.

3.Тестовое окружение.

4.Общая оценка качества приложения.5.Обоснование выставленного качества.

6.Графическое представление результатов тестирования.

7.Детализированный анализ качества по модулям.

8.ТОП-5 самых критичных дефектов.

9.Рекомендации.

Далее рассмотрим подробно каждую часть итогового отчета.

Общая информация включает:

- название проекта,
- номер сборки,
- модули, которые подверглись тестированию (в случае, если тестировался не весь проект),
- видытестовпоглубинепокрытия(Smoke Test, Minimal Acceptance Test, Acceptance Test),
- тестовыеактивности(New Feature Test, Regression Testing, Defect Validation),
- количествообнаруженныхдефектов,
- видрабочейтестовойдокументации(Acceptance Sheet, Test Survey, Test Cases).

Сведения о том, ктои когда тестировалпрограммный продукт, включают информацию о команде тестирования с указанием контактных данных и временном интервале тестирования.

Тестовое окружение содержит: ссылку на проект, браузер, операционную систему и другую информацию,конкретизирующую особенности конфигурации.Общая оценка качества приложениявыставляется на основании общего впечатления от работы с приложением и внесенных дефектов (количество, важность). Обязательно учитываетсяэтап разработки проекта –то, что не критично в началеработы, становится важным при выпуске программного продукта.

Уровни качества:

- Высокое(High),
- Среднее(Medium),
- Низкое(Low).

Обоснование выставленного качества является наиболее важнойчастью отчета, т.к. здесь отражается общее состояние сборки, а именно:

- качество сборки на текущий момент,
- факторы, повлиявшие на выставление именно такого качества сборки: указание функционала, который заблокирован для проверки, перечисление наиболее критичных дефектов и объяснение их важности для пользователя или бизнеса заказчика,
- анализ качества проверенного функционала: улучшилось оно или ухудшилось по сравнению с предыдущей версией,

если качество сборки ухудшилось, то обязательно должны бытьуказаны регрессионные места,наиболее нестабильные части функционала суказаниемпричин, по которымони таковыми являются.В данном разделе показывается аналитическая работа тестировщика, наиболее слабые места и наиболее критичные дефекты, динамика изменения качества проекта.Графическое представление результатов тестированияспособствует более полному и быстрому пониманию текстовой информации. Если необходимопродемонстрировать процентное соотношение, то целесообразноиспользоватькруговые диаграммы(например, процентное соотношение функциональных дефектов и дефектов GUI).Столбчатые диаграммы лучше подойдут там, где важно визуализировать количестводефектов в зависимости от степени их критичности или в зависимости от локализации (распределение дефектов по модулям).Отразитьв итоговомотчёте динамику качества по всем сборкам лучше всего удастся с помощью линейнографика.

Детализированный анализ качества по модулям.В анной части отчета описывается более подробная информация о проверенных частях функционала, устанавливается качество каждой проверенной части функционала(модуля) в отдельности, дается аргументация выставленного уровня качества. Как правило, данный раздел отчета представляется в табличной форме. В зависимости от вида проводимых тестовых активностей, этачасть отчета будет отличаться.

Порядок выполнения работы

1.Составить итоговый отчет по результатам тестирования web-приложения.

2.Указать общуюинформацию о тестируемом продукте (название, номер сборки, виды выполненных тестов, количество обнаруженных дефектов, вид рабочей тестовой документации).

3.Указать, кто и когда тестировал программный продукт.

4.Описать тестовое окружение (ссылку на web-приложение, браузер).

5.Указать общую оценку качества протестированного приложенияи подробно ее обосновать.

6.Графически (в виде круговой диаграммы) отразить процентное соотношение дефектов GUIи функциональных дефектов.

7.Графически(в виде столбчатой диаграммы) отразить распределениедефектов по различным степеням критичности.

8.Графически (в виде столбчатой диаграммы) отразить распределение дефектов по модулям.

9.Произвести детальный анализ качества всех модулей протестированного приложения с аргументацией выставленных уровней качества.

10.Привести список пяти наиболее критичных дефектов.

11.Сформулировать рекомендации по улучшению качества программного продукта.

12.Оформить отчет и защитить лабораторную работу.

Форма представления результата

1.Цель работы.

2.Итоговый отчет о результатах тестирования web-приложения.

3.Выводы по работе.

Контрольные вопросы

1.Какая структура итогового отчета о результатах тестирования?

2.Что содержится в разделе Общая информация?

3.Что содержится в разделе Тестовое окружение?

4.Как выставляется общая оценка качества приложения?

5.Как обосновать выставленную оценку качества?

6.Для чего используется графическое представление результатов тестированияв итоговом отчете?

7.Что содержится в разделе Детализированный анализ качества?

8.Что содержится в разделе Рекомендации?

Критерии оценки:

Оценка «5» ставится, если учащийся выполняет работу в полном объеме с соблюдением необходимой последовательности проведения опытов и измерений; самостоятельно и рационально монтирует необходимое оборудование; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдает требования правил безопасности труда; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей.

Оценка «4» ставится, если выполнены требования к оценке «5» , но было допущено два - три недочета, не более одной негрубой ошибки и одного недочёта.

Оценка «3» ставится, если работа выполнена не полностью, но объем выполненной части таков, позволяет получить правильные результаты и выводы: если в ходе проведения опыта и измерений были допущены ошибки.

Оценка «2» ставится, если работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов: если опыты, измерения, вычисления, наблюдения производились неправильно.

Лабораторная работа №5,6

Анализ рисков

Цель: Освоить технологии идентификации рисков. Качественного и количественного анализа

Выполнив работу, Вы будете:

уметь:

- Анализировать риски при разработке ПО
- Составлять стратегию управления рисками, минимизирующую их влияние

Материальное обеспечение:

ПО: MSWindows 7, MSOffice, Internet

Теоретическое обоснование

Проблема управления рисками проекта является одной изосновных и особо важных в общем перечне проблем и задачуправления проектами по созданию конкурентноспособной икачественной программной продукции. Пренебречь влиянием рисков- значит поставить под удар эффективность бизнес-процессов, чтоможет непосредственно отразиться на доходах и репутациикомпаний.

Управление рисками предприятия (EnterpriseRiskManagement,ERM) — это концепция, объединяющая методики и процессы,применяемые организациями для управления рисками ивозможностями достижения поставленных целей.Управление рисками позволяет организации определить, вкакой степени потенциальные события повлияют на достижение еёцелей. СогласнорекомендациямавторитетнойорганизацииCOSO(TheCommitteeofSponsoringOrganizationsoftheTreadwayCommission) **управление рисками организации**:

− представляет собой непрерывный процесс, охватывающийвсю организацию и осуществляемый на всех уровнях, включаявыработку стратегии;

− нацелено на определение событий, которые представляютопасность для организации.

У компании есть четыре варианта реакции на риск:

− принятие риска, когда не предпринимается никаких особыхдействий, связанных с данным риском;

− уменьшение риска посредством контроля за деятельностью ипроцессами либо принятия специальных мер;

− передача риска сторонней организации путём привлеченияпартнёров или страховых компаний;

− уклонение от риска — прекращение деятельности, ведущей криску.Остановимся особо на варианте уменьшения риска. Самаяочевидная реакция на риск — организовать контроль задеятельностью и процессами. Однако этого не всегда достаточно:нередко риск требует принятия специальных мер. Различаютнесколько видов рисков:

− присущий риск — это уровень риска, если непредпринимается никаких действий для изменения вероятности рискаили его влияния;

− остаточный риск — это уровень риска, остающийся послепринятия минимальных мер по реагированию на риск (как правило,сюда входит контроль за деятельностью и процессами предприятия);

− приемлемый остаточный риск — это уровень риска, равныйили ниже допустимого в данной организации и в данных условиях.Современный подход к управлению рисками рассматривает этудеятельность как непрерывный процесс, в котором риски регулярновыявляют и анализируют, измеряют, ищут способы работы с ними иоценивают эффективность уже принятых мер. Сам процессуправления рисками несложен и сводится к следующему простомуалгоритму:

− идентификация рисков: анализ ситуации, выявление причин,построение карты рисков, их детальное описание;

− анализ сценариев дальнейшего развития ситуации иопределение уровней рисков;

− проведение мероприятий по снижению уровней рисков.

Первоочередные меры реагирования на риск — контроль заходом деятельности и процессами организации. Это снижаетприсущий уровень риска, но если остаточный риск все же выше, чемприемлемый для организации, то необходимо предусмотретьспециальные меры реагирования на риск. В идеале эти меры должныбыть достаточными, чтобы уменьшить остаточный риск доприемлемого уровня. Уровень риска, который организация готовапринять, называется толерантностью к риску. Это индивидуальнаяхарактеристика: одни организации готовы рисковать чуть больше внадежде получить большую премию за риск, в то время как другие всячески обходят риски стороной.

Порядок выполнения работы

В ходе лабораторной работы необходимо выполнитьследующие этапы:

− Обозначить экономический объект, на котором будетпроводиться риск – менеджмент. Описать предметную область.− Выстроить процесс предметной области и описатьвозможные риски, проклассифицировать их.

− К каждому риску определить ряд последствий. Обозначитьвероятность рисков. Сделать вывод об общей картине влияния рисковна экономический объект.

− Выстроить стратегию управления рисками на основе одногоиз метода: уклонения, локализации, диверсификации, компенсации.

В результате выполнения лабораторной работы составить отчетв электронном виде.

Форма представления результата

Отчет выполнения лабораторной работы. Ответы на вопросы.

Контрольные вопросы

1. Какие бывают риски?
2. Какие бывают меры реагирования на риски?
3. Что такое стратегия управления рисками?
4. Что такое метод уклонения от рисков?

Критерии оценки:

Оценка «5» ставится, если учащийся выполняет работу в полном объеме с соблюдением необходимой последовательности проведения опытов и измерений; самостоятельно и рационально монтирует необходимое оборудование; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдает требования правил безопасности труда; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей.

Оценка «4» ставится, если выполнены требования к оценке «5» , но было допущено два - три недочета, не более одной негрубой ошибки и одного недочёта.

Оценка «3» ставится, если работа выполнена не полностью, но объем выполненной части таков, позволяет получить правильные результаты и выводы: если в ходе проведения опыта и измерений были допущены ошибки.

Оценка «2» ставится, если работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов: если опыты, измерения, вычисления, наблюдения производились неправильно.

Лабораторная работа №7,8
Выявление первичных и вторичных ошибок

Цель: протестировать web-приложение и описать найденные дефекты.

Выполнив работу, Вы будете:

уметь:

- Находить ошибки в процессе тестирования программного продукта
- Определять класс ошибки программного продукта

Материальное обеспечение:

ПО: MS Windows 7, MS Office, Internet

Теоретическое обоснование

Дефекты, обнаруженные тестировщиком, должны быть корректно и понятно описаны, чтобы разработчик смог воспроизвести данный дефект и устранить его. Описание каждого дефекта сохраняется в специализированной –багтрэкинговой –системе (например,JIRA, Bugzilla, Mantis, Redmineи др.) или в предварительно созданном в программной среде MicrosoftExcelфайле.

Описание дефекта включает следующие обязательные поля:

1.Headline–название дефекта.

2.Severity–степень критичности (важность дефекта).

3.Description–алгоритм воспроизведения.

4.Result–фактический результат.

5.Expectedresult–ожидаемый результат.

6.Attachment–прикреплённые файлы(приложение).

В багтрэкинговых системах для каждого дефекта автоматически генерируется его уникальный номер, в случае использования MicrosoftExcelномер дефекту необходимо присваивать вручную.Требование спецификации, которое нарушает обнаруженный дефект, можно дополнительно вынести в примечание.Дополнительно в описании дефекта может быть указана Priority–степень срочности исправления дефекта разработчиком.

Порядок выполнения работы

1.Выбрать объект реального мира(например, холодильник, блендер, лифт и др.), выделить в нем модули.

2.Разработать 20 и более тестовых проверок для выбранного объекта реального мира с указаниемтестируемого модуля иглубины тестового покрытия (Smoke, MAT, AT).3.Сформулировать по два возможных дефекта на каждый уровень Severity(Critical, Major, Average, Minor, Enhancement) для выбранного объекта реального мира.

4.Описать по одному дефекту на каждый уровень Severity(Critical, Major, Average, Minor, Enhancement) для выбранного объекта реального мира.

5.Протестировать web-приложение в соответствии с составленной ранее тестовой документацией.

6.Описать все найденные дефектыв отчете о дефектахв среде MicrosoftExcel.

7.В отчете о дефектах указать номер тестируемой сборки, название приложения, период времени тестирования, ФИО тестировщика, тестовое окружение (операционная система, браузер).

8.Для каждого дефекта указатьего порядковый номер, заголовок, важность, алгоритмвоспроизведения, фактический результат, ожидаемый результат, приложение, примечание.

9.Для каждого дефекта обязательно сделатьскриншоты.

10.В рабочую тестовую документацию внести результаты тестирования с указанием напротив соответствующей проверки степени критичности обнаруженного дефекта, его номера и заголовка.

11.Оформить отчет и защитить лабораторную работу.

Форма представления результата

Содержание отчета:

1.Цель работы.

2.Отчет о результатах тестирования выбранного объекта реального мира с перечислением тестовых проверок, сформулированныхдефектов на каждый уровень Severity, описания дефектов.

3.Отчет о найденных дефектахweb-приложения.

4.Рабочая тестовая документация с внесенными дефектамиweb-приложения.

5.Выводы по работе.

Контрольные вопросы

1.Что такое дефект?

2.Какие характеристики необходимо указать при описании дефекта?

3.Что такое Headline/Summary в описании дефекта?

4.На какие три вопроса должен отвечать Headline/Summary?

5.Что такое Severity в описании дефекта?

6.Какие существуют степени Severity? Приведите примеры.

7.Что такое Description в описании дефекта?

8.Что такое Expectedresult в описании дефекта?

9.Зачем нужен Attachment при описании дефекта?

10.Какие существуют рекомендации по описанию дефектов?

Критерии оценки:

Оценка «5» ставится, если учащийся выполняет работу в полном объеме с соблюдением необходимой последовательности проведения опытов и измерений; самостоятельно и рационально монтирует необходимое оборудование; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдает требования правил безопасности труда; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей.

Оценка «4» ставится, если выполнены требования к оценке «5» , но было допущено два - три недочета, не более одной негрубой ошибки и одного недочёта.

Оценка «3» ставится, если работа выполнена не полностью, но объем выполненной части таков, позволяет получить правильные результаты и выводы: если в ходе проведения опыта и измерений были допущены ошибки.

Оценка «2» ставится, если работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов: если опыты, измерения, вычисления, наблюдения производились неправильно.

Тема 4.2.2 Методы и средства защиты компьютерных систем

Лабораторная работа №1,2
Обнаружение вируса и устранение последствий его влияния

Цель: Изучить технологию тестирования компьютера на наличие вируса и профилактические меры. Познакомиться со способами лечения зараженных объектов.

Выполнив работу, Вы будете:

уметь:

- Обнаруживать компьютерный вирус специализированным ПО
- Лечить компьютерный вирус

Материальное обеспечение:

ПО: MSWindows 7, MSOffice, антивирус Касперского

Теоретическое обоснование

Компьютерный вирус – это специально написанная, небольшая по размерам программа (т.е. некоторая совокупность выполняемого кода), которая может “ приписывать” себя к другим программам (“заражать” их), создавать свои копии и внедрять их в файлы, системные области компьютера и т.д., а также выполнять различные нежелательные действия на компьютере.

Программа, внутри которой находится вирус, называется “зараженной” Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и заражает другие программы, а также выполняет какие-нибудь вредные действия (портит файлы или таблицу размещения файлов на диске, “засоряет” оперативную память и т.д.).

Признаки заражения

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка CD-ROM-устройства;
- произвольный, без вашего участия, запуск на компьютере каких-либо программ;

Есть также косвенные признаки заражения вашего компьютера:

- частые зависания и сбои в работе компьютера;
- прекращение работы или неправильная работа ранее успешно работавших программ;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размеров свободной оперативной памяти;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- MicrosoftInternetExplorer "зависает" или ведет себя неожиданным образом.

В 90% случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении. Несмотря на то, что подобные симптомы с малой

вероятностью свидетельствуют о заражении, при их появлении рекомендуем вам провести полную проверку вашего компьютера.

Антивирусные программы.

Для обнаружения, удаления и защиты от компьютерных вирусов разработаны специальные антивирусные программы. Различают следующие виды антивирусных программ:

Программы-детекторы осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатки: могут находить только те вирусы, которые известны разработчикам этой программы, поэтому быстро устаревают и требуют регулярного обновления.

Программы-доктора или фаги не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы-вируса, возвращая файл в исходное состояние. Полифаги – программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Недостатки те же, что и у программ-детекторов.

Программы-ревизоры относятся к самым надежным средствам защиты. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора.

Программы-фильтры или «сторожа» представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов (попытки коррекции файлов с расширением EXE или COM, изменение атрибутов файла, запись в загрузочные сектора и т.п.). При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Эти программы способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако они не лечат файла и диски. Для уничтожения вируса требуется применить другие программы.

Вакцины или иммунизаторы это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, лечащие этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. Имеют ограниченное применение.

Порядок выполнения работы

1. Вставьте диск в дисковод.
2. Запустите имеющуюся у вас антивирусную программу, например AVP Касперского.
3. Задайте область проверки —, режим проверки — лечение зараженных файлов и нажмите кнопку Проверить.
4. Обратите внимание на индикатор процесса сканирования. Если антивирусная программа обнаружила вирусы и произвела лечение файлов (что видно в отчете о

сканировании), запустите процесс сканирования дискеты еще раз и убедитесь, что все вирусы удалены.

5. Составьте отчет о проделанной работе, описав каждый пункт выполнения задания.
6. Выполните дополнительные задания.
7. Запишите ответы на контрольные вопросы в тетрадь для лабораторных работ.

Запустите имеющуюся у вас антивирусную программу и проверьте наличие вирусов на локальном диске С:.

Форма представления результата

Отчет о лабораторной работе

Контрольные вопросы

1. Что такое компьютерный вирус?
2. На какие типы разделяют компьютерные вирусы в различных видах классификации?
3. Чем отличаются макровирусы от обычных загрузочных вирусов?
4. Каковы основные пути проникновения вирусов в компьютер?
5. По каким признакам можно судить о поражении компьютера вирусом?
6. Какие типы антивирусных программ вам известны?
7. Каковы назначение и основные функции Антивируса Касперского Personal?
8. Как проверить CD-диск или дискету на наличие вируса с помощью программы Антивирус Касперского?
9. В каком файле содержится информация о зараженных и вылеченных объектах?
10. Перечислите профилактические меры для борьбы с заражением вирусами.

Критерии оценки:

Оценка «5» ставится, если учащийся выполняет работу в полном объеме с соблюдением необходимой последовательности проведения опытов и измерений; самостоятельно и рационально монтирует необходимое оборудование; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдает требования правил безопасности труда; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей.

Оценка «4» ставится, если выполнены требования к оценке «5» , но было допущено два - три недочета, не более одной негрубой ошибки и одного недочёта.

Оценка «3» ставится, если работа выполнена не полностью, но объем выполненной части таков, позволяет получить правильные результаты и выводы: если в ходе проведения опыта и измерений были допущены ошибки.

Оценка «2» ставится, если работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов: если опыты, измерения, вычисления, наблюдения производились неправильно.

Лабораторная работа №3,4,5

Установка и настройка антивируса. Настройка обновлений с помощью зеркала

Цель: научиться устанавливать, настраивать антивирусные программы.

Выполнив работу, Вы будете:

уметь:

- Устанавливать антивирусное ПО
- Настраивать Антивирус

Материальное обеспечение:

ПО: MS Windows 7, MS Office, NOD32, VirtualBox

Теоретическое обоснование

Антивирусные программы - это программы, основной задачей которых является защита именно от вирусов, или точнее, от вредоносных программ.

Методы и принципы защиты теоретически не имеют особого значения, главное чтобы они были направлены на борьбу с вредоносными программами. Но на практике дело обстоит несколько иначе: практически любая антивирусная программа объединяет в разных пропорциях все технологии и методы защиты от вирусов, созданные к сегодняшнему дню.

Из всех методов антивирусной защиты можно выделить две основные группы:

Сигнатурные методы - точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов

Эвристические методы - приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен

Порядок выполнения работы

Установка антивируса ESET NOD32

1. Запустите установочный файл. Файл установки имеет вид ess_nt32.msi. Предлагается два типа установки с разным указанием подробностей об установке:

- обычная установка
- пользовательская установка

Обычная установка рекомендуется для пользователей, предпочитающих установить ESET SmartSecurity со стандартными параметрами. Стандартные параметры по умолчанию обеспечивают наивысшую степень безопасности. Этот вариант рекомендуется для пользователей, которые не хотят выполнять подробную настройку программы вручную.

Для установки ознакомьтесь с условиями лицензионного соглашения и выберите «Я принимаю условия лицензионного соглашения», если вы согласны с ними.

2. На следующем шаге установки предлагается ввести имя пользователя и пароль, необходимые для получения автоматических обновлений программы. В соответствующих полях введите свои имя пользователя и пароль, то есть те самые

данные, которые были получены при приобретении или регистрации программы. Если имя пользователя и пароль еще неизвестны, выберите «Установить параметры обновления позже».
3. Следующим шагом является настройка системы своевременного обнаружения ThreatSense.Net. Система своевременного обнаружения ThreatSense.Net предназначена для своевременного и постоянного информирования компании ESET о появлении новых угроз. Она позволяет быстро реагировать и защищать пользователей. Система предусматривает передачу образцов злонамеренного кода в лабораторию ESET. Там они анализируются, обрабатываются и добавляются в базы данных сигнатур вирусов.

Для активизации этой функции установите флажок «Включить систему своевременного обнаружения». Для изменения параметров передачи подозрительных файлов нажмите «Дополнительные настройки».
4. Следующим шагом установки является настройка защиты от потенциально нежелательного программного обеспечения. Выберите «Включить обнаружение потенциально нежелательного ПО», чтобы разрешить обнаружение системой ESET SmartSecurity такого типа угроз. Рекомендуется включить эту функцию.
5. Последним шагом обычной установки является подтверждение установки. Для этого нажмите кнопку «Установить».

Если в системе уже установлена программа ESET SmartSecurity, мастер установки предложит удалить ее. Выберите «Удалить», если нужно удалить программу ESET SmartSecurity с компьютера.

Обновление программы

Регулярные обновления системы являются основой для обеспечения максимально возможного уровня безопасности, который предоставляется программой ESET SmartSecurity. Модуль обновления предназначен для получения регулярных обновлений программы. При этом обновляются как базы данных сигнатур вирусов, так и компоненты системы. Процесс обновления можно запустить немедленно с помощью функции «Обновить базу данных сигнатур вирусов». Кроме того, там расположены основные параметры обновления, например имя пользователя и пароль для доступа к серверам обновлений компании ESET. Имя пользователя и пароль предоставляются компанией ESET после приобретения программы ESET SmartSecurity.

Настройка

Настройка включает в себя три пункта:

- Антивирус;
- Персональный файервол;
- Антиспам.

Сам пункт «Настройка» показывает состояние защиты от вирусов и шпионских программ, сосятоние персонального файервола», а также модуля защиты программ.

Наибольшая степень защиты гарантируется, когда включены все пункты.

Персональный файервол – это устройство, выполняющее функции драйвера сетевого трафика и управляющее взаимодействием в рамках локальной сети или Интернета. При помощи заранее определенных правил файервол анализирует это взаимодействие и принимает решение о его разрешении или запрете. Самая основная функция файервола – защита частных сетей или компьютеров от вторжения со стороны потенциально опасных внешних сетей и компьютеров.

Доступны три отдельных режима работы файервола. Чтобы изменить поведение файервола, выберите нужный режим фильтрации. Для изменения режима фильтрации выполните следующие действия:

1. Переключитесь в «Расширенный режим», щелкнув переключатель расширенного режима в нижнем левом углу или нажав сочетание клавиш CTRL+M.

2. Выберите «Настройка» - «Персональный файервол», а затем щелкните пункт «Расширенная настройка персонального файервола...» в нижней части главного окна программы.

3. Откроется окно расширенной настройки. В расположенном справа раскрывающемся меню «Режим фильтрации» выберите нужный режим фильтрации и нажмите кнопку «OK».

Планировщик задач

Для того чтобы создать новую задачу в планировщике, нажмите кнопку «Добавить» или щелкните правой кнопкой мыши и выберите команду «Добавить» в контекстном меню. Доступны пять типов задач:

- Запуск внешнего приложения;
- Обслуживание журнала;
- Проверка файлов, исполняемых при запуске системы;
- Сканирование компьютера по требованию;
- Обновление.

Зеркало обновлений

ESET EndpointAntivirus дает возможность создавать копии файлов обновлений, которые могут использоваться для обновления других рабочих станций в сети. Использование зеркала (копии файлов обновлений в локальной сети) позволяет избежать загрузки одних и тех же обновлений с сервера производителя всеми рабочими станциями. Обновления загружаются на локальный сервер зеркала, а затем распространяются на рабочие станции. Это позволяет избежать перерасхода трафика. Обновление клиентских рабочих станций с зеркала оптимизирует трафик в сети и сокращает объем потребляемого интернет-трафика.

Настроить локальный сервер зеркала можно в расширенных параметрах в разделе Обновление. Чтобы попасть в этот раздел, нажмите клавишу F5 (откроется меню «Расширенные параметры»), щелкните Обновление > Профили и разверните элемент Зеркало обновлений.

Чтобы создать зеркало на клиентской рабочей станции, установите флажок Создать зеркало обновления. После этого станут доступными другие параметры настройки зеркала, такие как способ доступа к файлам обновлений и путь к файлам зеркала.

Доступ к файлам обновления

Включить HTTP-сервер. Если этот параметр активирован, файлы обновлений будут доступны по протоколу HTTP без необходимости указывать учетные данные.

Способы доступа к серверу зеркала детально описаны в статье Обновление с зеркала. Есть два основных способа доступа к зеркалу: папка с файлами обновлений может использоваться как общая сетевая папка или клиенты могут получить доступ к зеркалу на HTTP-сервере.

Папка, предназначенная для хранения файлов обновлений для зеркала, указывается в разделе Папка для хранения копий файлов. Чтобы выбрать другую папку, щелкните Очистить для удаления предварительно заданной папки C:\ProgramData\ESET\ESET EndpointAntivirus\mirror, а затем щелкните Изменить для выбора папки на локальном компьютере или общей сетевой папки. Если для указанной папки нужна авторизация, данные аутентификации должны быть указаны в полях Имя пользователя и Пароль. Если выбранная папка назначения расположена на сетевом диске компьютера под управлением ОС Windows NT/2000/XP, указанные имя пользователя и пароль должны принадлежать пользователю с правами на запись в указанную папку. Имя пользователя и пароль следует вводить в формате Домен/Пользователь или Рабочая_группа/Пользователь. Не забудьте ввести соответствующие пароли.

Форма представления результата

Отчет о лабораторной работе содержащий основные окна настроенной антивирусной программы

Контрольные вопросы

1. В каких случаях применяют специализированные программы защиты от компьютерных вирусов?
2. .На какие виды можно подразделить программы защиты от компьютерных вирусов?
3. Как действуют программы-детекторы?
4. Что называется сигнатурой?
5. Всегда ли детектор распознает зараженную программу?
6. Каков принцип действия программ-ревизоров, программ-фильтров, программ-вакцин?
7. Как выглядит многоуровневая защита от компьютерных вирусов с помощью антивирусных программ?
8. Перечислите меры защиты информации от компьютерных вирусов.
9. Каковы современные технологии антивирусной защиты?

Критерии оценки:

Оценка «5» ставится, если учащийся выполняет работу в полном объеме с соблюдением необходимой последовательности проведения опытов и измерений; самостоятельно и рационально монтирует необходимое оборудование; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдает требования правил безопасности труда; в отчете правильно и аккуратно выполняет все

записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей.

Оценка «4» ставится, если выполнены требования к оценке «5» , но было допущено два - три недочета, не более одной негрубой ошибки и одного недочёта.

Оценка «3» ставится, если работа выполнена не полностью, но объем выполненной части таков, позволяет получить правильные результаты и выводы: если в ходе проведения опыта и измерений были допущены ошибки.

Оценка «2» ставится, если работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов: если опыты, измерения, вычисления, наблюдения производились неправильно.

Лабораторная работа №6,7
Настройка политики безопасности

Цель: приобретение обучаемыми необходимого объёма знаний и практических навыков в области политики безопасности.

Выполнив работу, Вы будете:

уметь:

- Настраивать политики безопасности Windows
- Настраивать параметры безопасности Windows

Материальное обеспечение:

ПО: MS Windows 7, MS Office, VirtualBox

Теоретическое обоснование

Политика безопасности, права пользователей.

Политика безопасности системы является одной из важнейших со-ставляющих в обеспечении надежной и защищенной работы Windows XP. Настройка политики безопасности осуществляется в программе LocalSecuritySettings: Пуск\Панель управления\Администрирование\Локальная политика безопасности\Назначение прав пользователя

После запуска программы Назначение прав пользователя появится окно Локальные параметры безопасности

Основные пункты политики безопасности.

1. Пункт Доступ к компьютеру из сети – определяет, какие именно пользователи и группы поль-зователей могут получать доступ к данному компьютеру по компьютерной се-ти. Если компьютер не подключен к локальной сети, рекомендуется запретить доступ пользователей извне, это позволит избежать атак взломщиков и их проникновение в систему при работе в Интернете.
2. Пункт Разрешать вход в систему через службу терминалов является аналогичным предыдущему, но вход пользователей в систему осуществляется в качестве клиентов терминал-сервера. Если данный сервис не используется, то рекомендуется аналогичным мето-дом запретить вход в систему всех пользователей, убрав их из значения данного пункта как клиентов терминал-сервера. В случае необходимости всегда можно добавить нужных пользователей и их группы при помощи кнопки Добавить пользователя или группу
3. Пункт Изменение системного времени, позволяющий пользователям, перечисленным в нем, менять системное время, а также просматривать календарь, появляющийся на экране при двойном щелчке по текущему времени на панели задач. По умолчанию данной возможностью обычные пользователи не смогут воспользоваться. Для разрешения пользователям выполнять такое действие следует их внести в список данного пункта политики безопасности при помощи кнопки Добавить пользователя или группу

4. Пункт Отладка программ позволяет указать пользователей, которые смогут подсоединять свой отладчик к процессам и производить их отладку. Следует включать в этот пункт только тех пользователей, которым это действи-тельно нужно, например, системный админи-стратор и системные программисты. Не следует давать это право другим пользователям, так как этой возможностью могут воспользоваться вирусы для заражения системы, запущенные под одной из пользовательских записей, имеющей право на отладку процессов.
5. Пункт Отказ в доступе к компьютеру из сети содержит пользователей и их группы, которым запрещен вход в систему по компьютерной сети. При необходимости можно добавить пользователей, которым запрещен доступ к компьютеру с помощью кнопки Добавить пользователя или группу
6. Пункт Отклонить локальный вход содержит пользователей и их группы, ко-торым запрещен локальный вход в систему. При необходимости можно добавить пользователей, которым запрещен доступ к компьютеру с помощью кнопки Добавить пользователя или группу
7. Пункт Запретить вход через службу терминалов также содержит пользователей и их группы, которым запрещен вход в систему как клиентов терминал-сервера. При необходимости можно добавить пользователей, которым запрещен доступ к компьютеру с помощью кнопки Добавить пользователя или группу
8. Пункт Принудительное удаленное завершение является очень важным в настройке локальной политики безопасности, так как если его не настроить соответствующим образом, то система может получить команду на выключение или перезагрузку от удаленно пользователя. Поэтому в данном пункте следует указывать только пользователей, которым действительно может потребоваться с машин, находящихся в локаль-ной сети, выключить или перезапустить систему.
9. Пункт Загрузка и выгрузка драйверов устройств позволяет указать, кто из пользователей может динамически устанавливать и выгружать драйвера устройств. Это право необходимо для установки драйверов устройств, имеющих спецификацию PlugandPlay.
10. Пункт Локальный вход в систему является очень важным и определяет, какие пользователи и их группы могут локально входить в систему.
11. Пункт Управление аудитом и журналом безопасности относится к механизму аудита системы и определяет, какие пользователи и их группы могут уста-навливать аудит доступа к определенным объектам, таким как файлы, ключи реестра и пр. По умолчанию в данном пункте перечислена лишь одна группа локальных системных администраторов.
12. Пункт Изменение параметров среды оборудования определяет пользователей, которые будут иметь право в Windows XP менять значения системных переменных. По умолчанию на это имеют право только пользователи, при-надлежащие локальной группе администраторов.
13. Пункт Запуск операций по обслуживанию тома позволяет указать пользовате-лей и их группы, которые будут иметь право выполнять задачи по поддержанию работы накопителей, такие как очистка диска или его

дефрагментация. Вы-полнение данных задач, по умолчанию, доверяется только пользователям из группы системных администраторов.

14. Пункт Восстановление файлов и каталогов позволяет указывать пользователей и их группы, которые могут выполнять операцию восстановления файлов и директорий из сохраненных копий, а также ставить им необходимые права доступа. По умолчанию в системе такими пользователями являются члены группы системных администраторов, а также операторы сохранения данных.
15. Пункт Завершение работы системы указывает, кто из локальных пользователей, имеющих учетные записи в системе, имеет право на ее выключение или перезагрузку. По умолчанию на это имеют право все пользователи. Однако, в ряде случаев, может потребоваться запретить выполнять данные функции некоторым пользователям. Например, если нужно, чтобы компьютеры работали в то время, когда некоторые пользователи их пытаются отключить. В этом случае нужно убрать этих пользователей из данного пункта. Особенно это может быть полезно, если определенные пользователи пытаются выключить компьютер, на котором находится информация, используемая удаленно другими пользователями.
16. Пункт Овладение файлами или иными объектами отвечает за возможность пользователей, перечисленных в нем, брать на себя право становиться владельцами файлов и объектов. Этими объектами могут быть структуры ActiveDirectory, ключи реестра, принтеры и процессы. По умолчанию на это имеют право только пользователи группы системных администраторов. Добавление к этому пункту пользователей означает предос-тавление им всех прав по доступу к различным объектам.

Порядок выполнения работы

1. Произвести настройку Политики безопасности на своем ПК.
2. Произвести настройку Параметров безопасности на своем ПК.
3. Произвести настройку Политики обновления на своем ПК.

Форма представления результата

Отчет о лабораторной работе

Контрольные вопросы

1. Определите назначение политики безопасности системы.
2. Где производится настройка политики безопасности системы?
3. Как запретить доступ сетевых пользователей к компьютеру?
4. Как разрешить доступ сетевым пользователям, которым разрешено работать в системе к компьютеру?
5. Определите назначения пункта политики безопасности Разрешать вход в систему через службу терминалов.
6. Как предоставить определенной группе пользователей вносить изменения в системное время?
7. Определите назначение пункта политики безопасности Отладка программ.
8. Каким образом запретить вход определенной группе пользователей в систему по локальной сети?

9. Определите назначение пункта политики безопасности Принудительное удаленное завершение.
10. Как установить пользователей и их группы, которые могут локально входить в систему?
11. Как запретить определенной группе пользователей завершать работу системы, и в каких случаях это актуально?
12. В каком разделе производится настройка глобальных параметров безопасности?
13. Определите назначение политики обновления.
14. Как произвести настройку политики обновления?

Критерии оценки:

Оценка «5» ставится, если учащийся выполняет работу в полном объеме с соблюдением необходимой последовательности проведения опытов и измерений; самостоятельно и рационально монтирует необходимое оборудование; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдает требования правил безопасности труда; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей.

Оценка «4» ставится, если выполнены требования к оценке «5» , но было допущено два - три недочета, не более одной негрубой ошибки и одного недочёта.

Оценка «3» ставится, если работа выполнена не полностью, но объем выполненной части таков, позволяет получить правильные результаты и выводы: если в ходе проведения опыта и измерений были допущены ошибки.

Оценка «2» ставится, если работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов: если опыты, измерения, вычисления, наблюдения производились неправильно.

Лабораторная работа №8,9

Настройка браузера

Цель: настроить параметры web-браузера

Выполнив работу, Вы будете:

уметь:

- Настраивать основные параметры web-браузера

Материальное обеспечение:

ПО: MS Windows 7, MS Office, Internet, Google chrome

Теоретическое обоснование

Браузер GoogleChrome в настоящее время обладает наибольшими функциональными возможностями и широко распространяется в

сети Интернета. Популярность браузера связана с широким распространением многофункциональной поисковой системы Google.com

(для России имеется русская версия Google.ru).

Порядок выполнения работы

1. Запускаем браузер GoogleChrome. Нажимаем на настройки иуправления и выбираем из списка параметры
2. Вкладка «Основные».Для начала рассмотрим действия браузера при запуске, а именноразделы «Начальная группа». В разделе «Начальная группа» можно выбрать, что будет отображать браузер при запуске. При выборе пункта «Главная страница»необходимо задать, какая страница будет запускаться автоматически при запуске браузера. либо использовать страницу быстрого доступа.Страница быстрого доступа появляется при открытии новой вкладкиGoogleChrome. С ее помощью можно быстро переходить на любимыесайты и приложения. При выборе «Главная страница» на панели инструментов браузера добавляется кнопка «Главная страница», которая даст возможность открывать страницу одним нажатием созданной кнопки. Для удобства доступа к своим избранным сайтам можно закрепить панель закладок под адресной строкой. Для этого необходимо установить флажок «Всегда показывать панель закладок». На панели закладок содержатся все закладки и папки с закладками, созданные в GoogleChrome.В разделе «Поиск» для браузера можно задать поисковую систему, которая будет использоваться в адресной строке по умолчанию. Для изменения поисковой системы следует выбрать ее из списка и нажать на поле, которое требуется изменить. Выбрать поисковую систему, которую требуется использовать в качестве поисковой системы по умолчанию и нажать появившуюся в строке кнопку «Использовать по умолчанию»
3. Вкладка «Персональные».Нажатием на кнопку «Вход в Chrome» вызвать окно, в которомможно создать аккаунт Google. Для добавления пользователя необходимо в разделе «Пользователи» нажать на кнопку «Добавить пользователя» и вызвать диалоговое окно, где в дальнейшем можно ввести пользовательские данные. Раздел «Пароли» предназначен для управления

паролями. В этом разделе возможно управление паролями – предлагатьсохранение паролей или не сохранять их. Также возможно дополнительное управление сохраненными паролями. Автозаполнение позволяет заполнять формы всего одним кликом. Нажатием на кнопку настройки автозаполнения выводятся параметры автозаполнения, где пользователь после нажатия на кнопку может добавить почтовый адрес и внести свои персональные данные.Раздел «Импорт» предназначен для импорта данных из InternetExplorer или других браузеров. Темы изменяют внешний вид GoogleChrome, чтобы сделать егоеще более стильным и привлекательным. Нажатием кнопки «Выбратьтему» переходим в каталог тем.

4. Вкладка «Дополнительные». Если нажать на кнопку «Настройка контента» раздела «Личные данные», вызовется диалоговое окно настройки содержимого браузера. Файлы cookies – это файлы, создаваемые посещаемыми вами вебсайтами для хранения пользовательской информации, например настроек веб-сайта или данных о профиле. По умолчанию они включены. Нажатием кнопки «Управление исключениями» вызываем диалоговое окно исключения для файлов cookie и данных сайта. Для просмотра всех cookies и данных сайтов необходимо нажать на кнопку «Все файлы cookie и данные сайта», вызвав при этом окно «Файлы cookie и другие данные». С помощью подключаемых модулей браузером обрабатываются специальные типы веб-содержания, например файлы Flash и WindowsMedia. Для отключения ненужных нажатием кнопки «Отключить отдельные модули» вызывается диалоговое окно, в котором выбираем программы, которые желаем отключить. В разделе «Местоположение» можно полностью управлять настройками доступа веб-сайтов к сведениям о местоположении. Нажатием на кнопку «Очистить историю» можно вызвать диалоговое окно, в котором указано, что будет удалено из истории пользования браузером.
5. Вкладка «Расширения». Расширения – это дополнительные функции, которые легко подключить к GoogleChrome. Расширения позволяют добавлять в GoogleChrome только нужные функции, избегая тех, которые не требуются.

Форма представления результата

Отчет о лабораторной работе со скриншотами настроенного браузера

Контрольные вопросы

1. Порядок настройки браузеров.
2. Настройка домашней страницы.
3. Настройка подключения к сети Интернет.
4. Настройка безопасности работы в Интернете.
5. Настройка дополнительных параметров браузера.

Критерии оценки:

Оценка «5» ставится, если учащийся выполняет работу в полном объеме с соблюдением необходимой последовательности проведения опытов и измерений; самостоятельно и рационально монтирует необходимое оборудование; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдает требования правил безопасности труда; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей.

Оценка «4» ставится, если выполнены требования к оценке «5» , но было допущено два - три недочета, не более одной негрубой ошибки и одного недочёта.

Оценка «3» ставится, если работа выполнена не полностью, но объем выполненной части таков, позволяет получить правильные результаты и выводы: если в ходе проведения опыта и измерений были допущены ошибки.

Оценка «2» ставится, если работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов: если опыты, измерения, вычисления, наблюдения производились неправильно.

Лабораторная работа №10,11
Работа с реестром

Цель: Получение основных сведений о структуре и функциях системного реестра операционной системы Windows

Выполнив работу, Вы будете:

уметь:

- Работать с реестром ОС Windows

Материальное обеспечение:

ПО: MS Windows 7, MS Office, VirtualBox

Теоретическое обоснование

На смену ini-файлам, имеющим ряд концептуальных ограничений, еще в Windows 3.1 было введено понятие реестра – регистрационной базы данных, хранящей различные настройки ОС и приложений. Изначально реестр был предназначен только для хранения сведений об объектах OLE (ObjectLinkingandEmbedding — связь и внедрение объектов) и сопоставлений приложений расширениям имен файлов, однако позже его структура и границы использования расширились. Реестры разных версий Windows имеют различия; это нужно помнить при импорте reg-файлов. В Windows XP в архитектуру реестра были введены важные новшества, улучшающие функциональность данного компонента ОС. Реестр хранится в бинарном (двоичном) виде, поэтому для ручной работы с ним необходима специальная программа — редактор реестра. В XP это Regedit.exe, в других версиях NT ими являются Regedit.exe и Regedt32.exe, имеющий дополнительные возможности работы с реестром (Regedt32.exe есть и в XP, но на самом деле он всего лишь вызывает Regedit.exe). Есть и другие программы, в том числе и консольные (Reg.exe). Ручным модифицированием параметров реестра мы займемся чуть позже, а сейчас рассмотрим основные группы сведений, хранящихся в этой базе данных.

- **Программы установки**. Любая грамотно написанная программа под Windows должна иметь свой инсталлятор-установщик. Это может быть встроенный в ОС MicrosoftInstaller либо любой другой. В любом случае инсталлятор использует реестр для хранения своих настроек, позволяя правильно устанавливать и удалять приложения, не трогая совместно используемые файлы.
- **Распознаватель**. При каждом запуске компьютера программа NTDETECT.COM и ядро Windows распознает оборудование и сохраняет эту информацию в реестре.
- **Ядро ОС**. Хранит много сведений в реестре о своей конфигурации, в том числе и данные о порядке загрузки драйверов устройств.
- **Диспетчер PnP (Plug and Play).** Абсолютно необходимая вещь для большинства пользователей, которая избавляет их от мук по установке нового оборудования (не всегда, правда:)). Неудивительно, что он хранит свою информацию в реестре.
- **Драйверы устройств**. Хранят здесь свои параметры.
- **Административные средства**. Например, такие, как Панель управления, MMC (Micro-softManagementConsole) и др.
- **Пользовательские профили**. Это целая группа параметров, уникальная для каждого пользователя: настройки графической оболочки, сетевых соединений, программ и многое другое.
- **Аппаратные профили**. Позволяют создавать несколько конфигураций с различным оборудованием.

- **Общие настройки программ**. Почему общие? Потому, что у каждого пользователя есть профиль, где хранятся его настройки для соответствующей программы.

Таким образом, выше приведены данные о предназначении реестра. Теперь обратим внимание на логическую структуру реестра. Для лучшего понимания материала рекомендуется запустить Regedit.exe.

Структура реестра

Реестр Windows имеет древовидную структуру, схожую со структурой файловой системы. Папкам здесь соответствуют ключи (keys) или разделы (ветви), а файлам — параметры (values). Разделы могут содержать как вложенные разделы (subkeys), так и параметры. На верхнем уровне этой иерархии находятся корневые разделы (rootkeys). Они перечислены в таблице 1

Таблица 1. Корневые разделы

Имя корневого раздела	**Описание**
HKEY_LOCAL_MACHINE	Содержит глобальную информацию о компьютерной системе, включая такие данные об аппаратных средствах и операционной системе, в том числе: тип шины, системная память, драйверы устройств и управляющие данные, используемые при запуске системы. Информация, содержащаяся в этом разделе, действует применительно ко веем пользователям, регистрирующимся в системе Windows NT/2000. На верхнем уровне иерархии реестра для этого раздела имеются три псевдонима: HKEY CLASSES ROOT, HKEY CURRENT CONFIG и HKEY_DYN_DATA
HKEY_CLASSES_ROOT	Содержит ассоциации между приложениями и типами файлов (по расширениям имени файла). Кроме того, этот раздел содержит информацию OLE (ObjectLinkingandEmbedding), ассоциированную с объектами COM, а также данные по ассоциациям файлов и классов (эквивалент реестра ранних версий. Windows, служивших настройкой над MS-DOS). Параметры этого раздела совпадают с параметрами, расположенными в разделе HKEY_LOCAL_MACHINE\Software\Classes. Подробную информацию о разделе HKEY_CLASSES_ ROOT можно найти в руководстве OLE Programmer'sReference, входящем в состав продукта Windows NT 4.0 SoftwareDevelopmentKit (SDK)
HKEY_CURRENT_CONFIG	Содержит конфигурационные данные для текущего аппаратного профиля. Аппаратные профили представляют собой наборы изменений, внесенных в стандартную конфигурацию сервисов и устройств, установленную данными разделов Software и System корневого раздела HKEY_LOCAL_MACHINE. В разделе HKEY_CURRENT_ CONFIG отражаются только изменения. Кроме того, параметры этого раздела появляются также в разделе HKEY_LOCAL_MACHINE\System \CurentControlSet\HardwareProfites\CuiTent
HKEY_CURRENT_USER	Содержит, профиль пользователя, на данный момент

	.зарегистрировавшегося в системе, включая переменные окружения, настройку рабочего стола, параметры настройки сети, принтеров и приложений. Этот раздел представляет собой ссылку на раздел HKEY USERS\username, где username — имя пользователя, зарегистрировавшегося в системе на текущий момент
HKEY_USERS	Содержит все активно загруженные пользовательские профили, включая HKEY_CURRENT_USER, а также профиль по умолчанию. Пользователи, получающие удаленный доступ к серверу, не имеют профилей, содержащихся в этом разделе; их профили загружаются в реестры на их собственных компьютерах. Windows NT/2000 требует наличия учетных записей для каждого пользователя, регистрирующегося в системе. Раздел HKEY_USERS содержит вложенный раздел \Default, а также другие разделы, определяемые идентификатором безопасности (Security ID) каждого пользователя

Типы данных

Все параметры реестра имеют фиксированный тип. В таблице 2 приводится полный список используемых типов. Не все из них используются в разных версиях NT — REG_QWORD явно предназначен для 64-битной версии XP. Следует учесть, что ряд типов используется только системой в некоторых разделах, и создать свой параметр такого типа с помощью редактора реестра не получится.

Таблица 2. Типы параметров

Тип данных	**Описание**
REG_BINARY	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 Unicode переменной длины. Этот тип данных включает переменные, обрабатываемые программой или службой
REG_MULTI_SZ	Многострочный текст Unicode. Этот тип, как правило, имеют списки и другие записи в формате, удобном для чтения. Записи разделяются пробелами, запятыми или другими символами
REG_SZ	Текстовая Unicode строка фиксированной длины
REG_DWORD_LITTLE_ENDIAN	32-разрядное число в формате

	“остроконечников” — младший байт хранится первым в памяти. Эквивалент REG_DWORD
REG_DWORD_BIG_ENDIAN	32-разрядное число в формате “тупоконечников” — старший байт хранится первым в памяти
REG_LINK	Символическая ссылка Unicode. Только для внутреннего использования (некоторые корневые разделы являются такой ссылкой на другие подразделы)
REG_NONE	Параметр не имеет определенного типа данных
REG_QWORD	64-разрядное число
REG_QWORD_LITTLE_ENDIAN	64-разрядное число в формате “остроконечников”. Эквивалент REG_QWORD
REG_RESOURCE_LIST	Список аппаратных ресурсов. Используется только в разделе HKLM\HARDWARE
REG_FULL_RESOURCE_DESCRIPTOR	Дескриптор (описатель) аппаратного ресурса. Применяется только в HKLM\HARDWARE.
REG_RESOURCE_REQUIREMENTS_LIST	Список необходимых аппаратных ресурсов. Используется только в HKLM\HARDWARE.

Хранение реестра

Элементы реестра хранятся в виде атомарной структуры. Реестр разделяется на составные части, называемые ульями (hives), или кустами. Ульи хранятся на диске в виде файлов. Некоторые ульи, такие, как HKLM\HARDWARE, не сохраняются в файлах, а создаются при каждой загрузке, то есть являются изменяемыми (vola-tile). При запуске системы реестр собирается из ульев в единую древовидную структуру с корневыми разделами. Перечислим ульи реестра и их местоположение на диске (для NT старше версии 4.0) в таблице 3

Таблица 3. Ульи реестра

Улей	**Расположение**
HKLM\SYSTEM	%SystemRoot%\system32\config\system
HKLM\SAM	%SystemRoot%\system32\config\SAM
HKLM\SECURITY	%SystemRoot%\system32\config\SECURITY
HKLM\SOFTWARE	%SystemRoot%\system32\config\software
HKLM\HARDWARE	Изменяемый улей
HKLM\SYSTEM\Clone	Изменяемый улей
HKU\<SID_пользователя>	%USERPROFILE%\ntuser.dat
HKU\<SID_пользователя>_Classes	%USERPROFILE%\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
HKU\.DEFAULT	%SystemRoot%\system32\config\default

Кроме этих файлов, есть ряд вспомогательных, со следующими расширениями:

- ALT – резервная копия улья HKLM\SYSTEM (отсутствует в XP).
- LOG – журнал транзакций, в котором регистрируются все изменения реестра.
- SAV – копии ульев в том виде, в котором они были после завершения текстовой фазы установки.

Дополнительные сведения

Реестр является настоящей базой данных, поэтому в нем используется технология восстановления, похожая на оную в NTFS. Уже упомянутые LOG-файлы содержат журнал транзакций, который хранит все изменения. Благодаря этому реализуется атомарность реестра – то есть в данный момент времени в реестре могут быть либо старые значения, либо новые, даже после сбоя. Как видим, в отличие от NTFS, здесь обеспечивается сохранность не только структуры реестра, но и данных. К тому же, реестр поддерживает такие фишки NTFS, как управление избирательным доступом и аудит событий – система безопасности пронизывает всю NT снизу доверху. Да, эти функции доступны только из Regedt32.exe или Regedit.exe для XP. А еще весь реестр или его отдельные части можно экспортировать в текстовые reg-файлы (Unicode для Windows 2000 и старше), редактировать их в блокноте, а затем экспортировать обратно. Во многих редакторах реестра можно подключать любые доступные ульи реестра, в том числе и на удаленных машинах (при соответствующих полномочиях). Есть возможность делать резервные копии с помощью программы NTBackup.

Порядок выполнения работы

1. Изучить теоретическую часть;
2. Запустить редактор реестра.

– Перейти в раздел реестра **HKEY_CURRENT_USER;**
– Найти ключ, отвечающий за настройки Рабочего стола;
– Ознакомиться со списком вложенных ключей;
– Для произвольно выбранных из списка 5 ключей исследовать, аналогом каких настроек Панели управления они являются;
– Перейти в раздел реестра **HKEY_CLASSES_ROOT;**
– Выбрать из списка 5 ключей и описать, для файлов с какими расширениями они используются, и какие параметры для них установлены;

Результаты внести в отчет.

Форма представления результата

Отчет о лабораторной работе

Контрольные вопросы

1. Что такое системный реестр Windows?
2. Расскажите о структуре реестра.
3. Поясните особенности «троянских программ».
4. Почему профилактика «троянских программ» связана с системным реестром?
5. Какие разделы и ключи являются потенциальными местами записей «троянских программ»?

Критерии оценки:

Оценка «5» ставится, если учащийся выполняет работу в полном объеме с соблюдением необходимой последовательности проведения опытов и измерений; самостоятельно и рационально монтирует необходимое оборудование; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдает требования правил безопасности труда; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей.

Оценка «4» ставится, если выполнены требования к оценке «5» , но было допущено два - три недочета, не более одной негрубой ошибки и одного недочёта.

Оценка «3» ставится, если работа выполнена не полностью, но объем выполненной части таков, позволяет получить правильные результаты и выводы: если в ходе проведения опыта и измерений были допущены ошибки.

Оценка «2» ставится, если работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов: если опыты, измерения, вычисления, наблюдения производились неправильно.

Лабораторная работа №12
Работа с программой восстановления файлов и очистки дисков

Цель: научиться работать с программой восстановления файлов и очистки дисков

Выполнив работу, Вы будете:

уметь:

- Работать с программой восстановления файлов и очистки дисков

Материальное обеспечение:

ПО: MSWindows 7, MSOffice, EasyRecovery

Теоретическое обоснование

EasyRecoveryPro на сегодняшний день - это одна из лучших программ своего класса. Облегченный вариант - EasyRecoveryLite - входит в состав пакета комплексного обслуживания системы Fix-ItUtilities. EasyRecovery умеет работать почти со всеми более-менее распространенными файловыми системами: FAT12, FAT16, FAT32, NTFS, Novell, стандартами ZIP и JAZприводов, поддерживаются также и SCSI-жесткие диски. Одно из важнейших достоинств программы заключается в том, что у нее не только удобный и понятный Windows-интерфейс, доступный неопытным пользователям, но и есть возможность создать комплект загрузочных дискет с полноценной DOS-версией EasyRecovery. Сделано это для того, чтобы в случае серьезных неполадок, когда нет возможности загрузить Windows (а, соответственно, и "виндовскую" версию EasyRecovery), вас всегда был бы доступ к жесткому диску, и вы могли бы восстанавливать файлы непосредственно из MS-DOS. Такой режим наиболее предпочтителен при крупных сбоях - на сбойный диск ничего не записывается, EasyRecovery работает для него в режиме Readonly («Только чтение»), поэтому и файлы на нем будут в большей сохранности. Первое, что бросается в глаза сразу после запуска программы - очень долгий процесс сканирования диска. Однако это не является недостатком, а совсем наоборот - свидетельствует о ее неслабых возможностях. Дело в том, что как уже отмечалось, быстрые, простые программы получают информацию об удаленных файлах и шансах на их восстановление из структуры директорий таблицы размещения файлов. Времени это, конечно, занимает очень мало, но ведь файл может еще быть на диске даже в том случае, если больше никаких его следов не осталось, да и сама таблица размещения файлов и корневая директория могут быть разрушены. Вот тут-то и спасет вас EasyRecovery - она просканирует целиком весь жесткий диск, кластер за кластером, пытаясь собрать все кусочки каждого файла воедино. При этом допускается полная потеря обоих копий таблицы FAT, повреждение RootFolder и загрузочного сектора диска. Разумеется, если что-то из этого все-таки сохранилось, то будет в полной мере использовано. Кстати, если вы регулярно дефрагментируете диск, то шансы на успех еще больше увеличиваются - файл, у которого используемые кластеры идут друг за другом, восстановить проще. Таким образом, EasyRecovery - это одна из немногих программ, которая справляется не только с восстановлением ошибочно удаленных файлов, но и восстанавливает информацию на диске после повреждения его вирусами, форматирования, переразбиения на разделы, порчи при скачках напряжения питания, сбоях аппаратного оборудования или программ. Из "виндовского" интерфейса вы, разумеется, тоже получите все эти возможностей, но только в том случае, если диск с

операционной системой невредим. Поэтому целесообразно сделать заранее загрузочные дискеты EasyRecovery - с ними ваши данные будут иметь как бы дополнительный "спасательный круг". Правда, поскольку EasyRecovery с поврежденным диском работает только на чтение, то придется запастись вторым винчестером или другим носителем, прежде чем приступать к восстановлению больших объемов данных. Причем доступ к диску вы, скорее всего, получите, даже если ваша ОС его не обнаруживает. Конечно, с DOS-вариантом программы работать сложнее, поэтому желательно предварительно изучить инструкцию, чтобы разобраться во всех многочисленных опциях EasyRecovery. Приятных и полезных дополнительных функций у EasyRecovery немало: так, например, "виндовская" версия умеет проводить диагностический тест диска, аналогичный тому, что используется стандартным ScanDisk. При восстановлении файлов сохраняются длинные имена. В соответствии с последними стандартами, программа способна обновляться через Интернет.

Порядок выполнения работы

Восстановление файлов с помощью EasyRecovery

Запустите EasyRecovery (Пуск – Тема – Осмотр носителя – 4 Восстановление данных – EasyRecoveryProfessional). После загрузки программы на экране появляется окно, в левой части которого размещено меню в виде кнопок, обеспечивающих доступ к четырем категориям функций, а также к двум дополнительным сервисам:

- Диагностика диска – утилиты для проверки физических параметров диска и целостности файловой системы;
- Восстановление данных – утилиты для поиска и восстановления удаленных и поврежденных данных;
- Восстановление файлов – специализированные утилиты для восстановления файлов, созданных приложениями из семейства MS Office (кроме Outlook), а также ZIPархивов;
- Восстановление Email – специализированная утилита для восстановления файлов Outlook;
- Обновление программы – сервисные функции, позволяющие получать информацию и выполнять обновление лицензионной версии EasyRecovery через Интернет;
- Кризисный центр – набор функций, обеспечивающих доступ к сервисным вебслужбам компании Ontrack.

В меню выберите Восстановление данных и далее DeletedRecovery. В левой части выберите диск D:\.

Примечание. Если вы удалили один или несколько файлов, быстрое сканирование должно найти эти файлы. Поиск будет производиться только в файловой системе (это должно продолжаться всего несколько секунд). В случае, когда вы удалили целые каталоги, используйте опцию полного поиска. Для этого выберите опцию CompleteScan. Нажмите кнопку Далее, чтобы начать сканирование диска. Вы увидите окно прогресса сканирования.

- Processingblock показан сканированный блок диска и число всех блоков до момента сканирования
- Elapsedtime время, которое прошло от момента начала сканирования

- Remainingtime предполагаемое время, которое осталось до окончания операции
- Directoriesfound количество найденных на диске каталогов
- Filesfound количество найденных файлов
- Lastfile название последнего найденного файла

После окончания сканирования вы увидите список найденных файлов. Однако надо помнить, что не каждый найденный с помощью EasyRecovery файл возможно восстановить.

Поле Condition в списке файлов показывает в каком состоянии находится найденный файл.

Выберите файлы, которые хотите восстановить и щелкните Далее.

В следующем окне в поле RecoveryStatistics находится короткая статистика о восстановленных файлах, включающая количество файлов, которые вы выбрали для восстановления, а также их полный размер. Выберите директорию, в которую их надо записать (RecovertoLocalDrive). Вы также можете отправить восстановленные файлы непосредственно на сервер FTP (Recovertoan FTP Server). Помните, что EasyRecovery не позволит записать файлы в раздел, с которого происходит восстановление данные. Версия Professional предлагает возможность компрессии восстановленных файлов в архив ZIP (Create ZIP). На ваше усмотрение вы можете установить лимит размера файла ZIP (ZIP FileSizeLimit), а также создать отчет о восстановлении файлов (GenerateRecoveryReport). Выберите для восстановления диск C:\, нажмите Далее

EasyRecovery может записать установки восстановления, чтобы потом вы смогли продолжить операцию восстановления других файлов. Нажмите кнопку No. Вы восстановили данные. Просмотрите восстановленный файл. Внесите данные в отчет.

Форма представления результата

Отчет о лабораторной работе

Контрольные вопросы

1. В чем назначение программы EasyRecovery?
2. Какие действия необходимо выполнить перед началом работы с программой EasyRecovery?
3. Как осуществляется проверка целостности жесткого диска с помощью программы EasyRecovery?
4. Перечислите известные вам программы по обслуживанию жестких дисков в процессе их эксплуатации и определите их назначение.
5. Опишите последовательность восстановления удаленной информации, если

а) Файл удален в Корзину.

б) Файл удален в Корзину и затем очистили Корзину.

Критерии оценки:

Оценка «5» ставится, если учащийся выполняет работу в полном объеме с соблюдением необходимой последовательности проведения опытов и измерений; самостоятельно и рационально монтирует необходимое оборудование; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдает требования правил безопасности труда; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей.

Оценка «4» ставится, если выполнены требования к оценке «5» , но было допущено два - три недочета, не более одной негрубой ошибки и одного недочёта.

Оценка «3» ставится, если работа выполнена не полностью, но объем выполненной части таков, позволяет получить правильные результаты и выводы: если в ходе проведения опыта и измерений были допущены ошибки.

Оценка «2» ставится, если работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов: если опыты, измерения, вычисления, наблюдения производились неправильно.