**Практическая работа № 1-2**

**Тема: Тестирование программных продуктов**

Цель работы: 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.

Краткие теоретические сведения:

*Типы тестов по покрытию (по глубине):*

1.Smoke test – тестирование системы для определения корректной работы базовых функций программы в целом, без углубления в детали.

2.Minimal Acceptance Test (MAT, Positive test) - тестирование системы или ее части только на валидных данных

3.Acceptance Test (AT) - полное тестирование системы или ее части как на корректных, так и на некорректных данных/сценариях.

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

1.Defect Validation – проверка результата исправления дефектов.

2.New Feature Test (NFT, AT of NF) – определение качества поставленной на тестирование новой функциональности, которая ранее не тестировалась.

3.Regression testing (регрессионное тестирование) – проводится с целью оценки качества ранее реализованной функциональности.

*Типы тестов по знанию коду*

1.Черный ящик – тестирование системы, функциональное или нефункциональное, без знания внутренней структуры и компонентов системы. У тестировщика нет доступа к внутренней структуре и коду приложения либо в процессе тестирования он не обращается к ним.

2.Белый ящик – тестирование основанное на анализе внутренней структуры компонентов или системы. У тестировщика есть доступ к внутренней структуре и коду приложения.

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

*Типы тестов по степени автоматизации*

1.Ручное – тестирование, в котором тест-кейсы выполняются тестировщиком вручную без использования средств автоматизации.

2.Автоматизированное – набор техник, подходов и инструментальных средств, позволяющий исключить человека из выполнения некоторых задач в процессе тестирования.

*Типы тестов по изолированности компонентов*

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

2.Integration (интеграционное) – тестируется взаимодействие между интегрированными компонентами или системами.

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

*Типы тестов по подготовленности.*

1.Интуитивное тестирование выполняется без подготовки к тестам, без определения ожидаемых результатов, проектирования тестовых сценариев.

2.Исследовательское тестирование – метод проектирования тестовых сценариев во время выполнения этих сценариев. Тестировщик совершает проверки, продумывает их, придумывает новые проверки, часто использует для этого полученную информацию.

3.Тестирование по документации – тестирование по подготовленным тестовым сценариям, руководству по осуществлению тестов.

*Типы тестов по месту и времени проведения*

1.User Acceptance Testing (UAT) (приемочное тестирование) – формальное тестирование по отношению к потребностям, требованиям и бизнес процессам пользователя, проводимое с целью определения соответствия системы критериям приёмки и дать возможность пользователям, заказчикам или иным авторизованным лицам определить, принимать систему.

2.Alpha Testing (альфа-тестирование) – моделируемое или действительное функциональное тестирование, выполняется в организации, разрабатывающей продукт, но не проектной командой (это может быть независимая команда тестировщиков, потенциальные пользователи, заказчики).

3.Beta Testing (бета-тестирование) – эксплуатационное тестирование потенциальными или существующими клиентами/заказчиками на внешней стороне (в среде, где продукт будет использоваться) никак связанными с разработчиками, с целью определения действительно ли компонент или система удовлетворяет требованиям клиента/заказчика и вписывается в бизнес-процессы.

*Типы тестов по объекту тестирования*

1.Functional testing (функциональное тестирование) – это тестирование, основанное на анализе спецификации, функциональности компонента или системы.

2.Safety testing (тестирование безопасности) – тестирование программного продукта с целью определить его безопасность

3.Security testing (тестирование защищенности) – это тестирование с целью оценить защищенность программного продукта.

4.Compatibility testing (тестирование совместимости) – процесс тестирования для определения возможности взаимодействия программного продукта, проверка работоспособности приложения в различных средах

*Нефункциональное тестирование* – это проверка характеристик программы.

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
* изменение размеров окна или разрешения экрана

2. Тестирование удобства использования (Usability Testing) – тестирование с целью определения степени понятности, легкости в изучении и использовании, привлекательности

программного продукта для пользователя при условии использования в заданных условиях эксплуатации.

* визуальное оформление
* навигация
* логичность

3. Тестирование доступности (Accessibility testing) – тестирование, которое определяет степень

легкости, с которой пользователи с ограниченными способностями могут использовать систему или ее компоненты.

4. Тестирование интернационализации – тестирование способности продукта работать в локализованных средах

5. Тестирование локализации (Localization testing) – тестирование, проводимое с целью проверить качество перевода продукта с одного языка на другой.

6. Тестирование производительности или нагрузочное тестирование – процесс тестирования с целью определения производительности программного продукта.

*Виды тестов*:

* нагрузочное тестирование (Performance and Load testing) – вид тестирования производительности, проводимый с целью оценки поведения компонента или системы при возрастающей нагрузке, например количестве параллельных пользователей и/или операций, а также определения какую нагрузку может выдержать компонент или система;
* объемное тестирование (Volume testing) – позволяет получить оценку производительности при увеличении объемов данных в базе данных приложения;
* тестирование стабильности и надежности (Stability / Reliability testing) – позволяет проверять работоспособность приложения при длительном (многочасовом) тестировании со средним уровнем нагрузки.
* стрессовое тестирование (Stress testing) – вид тестирования производительности, оценивающий систему или компонент на граничных значениях рабочих нагрузок или за их пределами, или же в состоянии ограниченных ресурсов, таких как память или доступ к серверу.

7 .Тестирование требований (Requirements testing) – проверка требований на соответствие основным характеристикам качества.

8. Тестирование прототипа (Prototyte testing) – метод выявления структурных, логических ошибок и ошибок проектирования на ранней стадии развития продукта до начала фактической разработки.

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

*Виды тестов*:

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

10. Тестирование на отказ и восстановление (Failover and Recovery Testing) – тестирование при помощи эмуляции отказов системы или реально вызываемых отказов в управляемом окружении.

*Тестирование программного продукта включает следующие этапы*:

1. Изучение и анализ предмета тестирования.

2. Планирование тестирования.

3. Исполнение тестирования.

**Порядок выполнения работы**

1. Получить индивидуальные задания у преподавателя.

2. Выполнить генерацию тестов различных видов для конкретного объекта реального мира (пример приведен на рисунке 1).

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 России).

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

4. Сделать выводы и оформить отчет 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?

**Практическая работа № 3-4**

**Тема: Анализ рисков**

Цель работы: изучение базовых принципов построения и приобретение

навыков использования модели угроз и уязвимостей ИС при анализе рисков

информационной безопасности в корпоративных информационных системах.

Краткие теоретические сведения:

Обеспечение безопасности информации носит комплексный характер и

основано, среди прочего, на анализе возможных негативных последствий развертывания и эксплуатации ИС.

Модель угроз и уязвимостей предназначена для оценки защищенности

ИС, при которой моделирование нарушений безопасности осуществляется на

базе анализа цепочки "уязвимость угроза-ресурс". При этом необходимо убедиться, что все ресурсы и уязвимости идентифицированы и сопоставлены

с угрозами. Важно иметь возможность при необходимости, не меняя самого

методического инструментария, вводить новые виды угроз и уязвимостей, которые станут известны вследствие развития знаний в этой области. В результате анализа по модели угроз и уязвимостей вычисляется уровень риска нарушения безопасности ИС и определяются его возможные причины.

*Понятийный базис модели*:

* угроза – действие, которое потенциально может привести к нарушению безопасности. Свойством угрозы является перечень уязвимостей, при помощи которых она может быть реализована;
* уязвимость - "слабое" место в ИС, которое может привести к нарушению безопасности путем реализации некоторой угрозы. Свойствами уязвимости являются вероятность (простота) и критичность реализации угрозы через данную уязвимость;
* вероятность реализации угрозы через данную уязвимость в течение года – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Измеряется в процентах;
* критичность реализации угрозы – степень влияния реализации угрозы на ресурс, т. е. как сильно реализация угрозы повлияет на работу ресурса. Задается в процентах. Допустимо рассматривать критичность реализации угрозы и по составляющим безопасности (конфиденциальности, целостности и доступности), и в целом (с учетом всех трех рисков);
* ресурс – часть ИС, предназначенная для хранения информации, подверженной угрозам ИБ (сервер, рабочая станция, мобильный компьютер,
* устройство хранения резервных копий и т. д.). Свойствами ресурса в данной модели являются перечень угроз, воздействующих на него, и критичность ресурса;
* критичность ресурса – степень значимости ресурса для ИС, т. е. насколько сильно реализация угроз безопасности на ресурс повлияет на работу всей ИС. Критичность ресурса оценивают в денежных единицах, относительных уровнях, условных единицах. Чаще всего она оценивается в

процентах, т. е. в уровнях от 1 до 100 по отношению к критичности других

ресурсов.

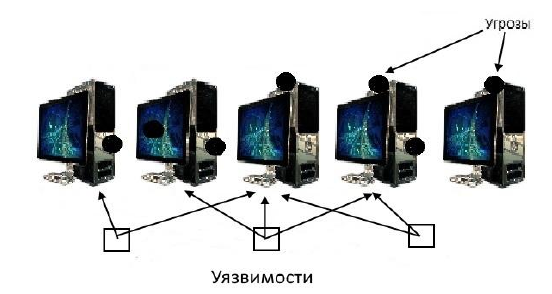
* максимальное критичное время простоя – значение времени простоя, которое является критичным для компании. Ущерб, нанесенный компании при простом ресурсе в течение этого времени, достигает максимального значения. При дальнейшем простое ущерб, наносимый компании, уже не увеличивается. Эта характеристика используется для оценки критичности ресурса по угрозе доступности.

Критичность ресурса оценивается, как правило, из ущерба, который понесет компания при осуществлении угроз нарушения конфиденциальности, доступности или целостности. При рассмотрении этой

характеристики необходимо определить шкалу, используемую для классификации критичности.

Для каждого из ресурсов определяются список угроз, действующих на

него, и список уязвимостей. Для нарушения безопасности по одной угрозе нарушитель может воспользоваться разными уязвимостями. Одна и та же уязвимость может привести к нарушению безопасности по нескольким угрозам.



**Порядок выполнения работы:**

1. Получить у преподавателя описание ИС.

2. Для данной ИС построить модель угроз и уязвимостей:

* выделить угрозы, применимые к рассматриваемой ИС;
* выделить уязвимости, через которые могут быть реализованы угрозы;
* определить угрозы, которые могут воздействовать на каждый из ресурсов в рамках ИС, и обосновать причины наличия этих угроз;
* определить уязвимости, через которые могут быть реализованы указанные угрозы.

3. Определить вероятности и критичности реализации угроз через уязвимости для каждой пары "угроза-уязвимость".

4. Определить функции для расчета рисков.

5. Рассчитать риски для всех ресурсов в рассматриваемой модели ИС.

6. Провести анализ полученных результатов. Выделить наиболее опасные уязвимости и предложить способы снижения вероятности и критичности. Предложить дальнейший план развития политики информационной безопасности для рассматриваемой ИС.

**Варианты заданий:**

Вариант 1. Тестовая информационная система ЗАО "ТестИС-Строй".

Основной вид деятельности ЗАО "ТестИС-Строй" – продажа строительных товаров на рынке "BusinesstoClient". Поставщиками являются частные лица и организации среднего и малого бизнеса. ЗАО "ТестИС-Строй" имеет четыре точки продаж, расположенные в пределах города. Каждая из этих точек – магазин площадью от 300 до2000 м2 . В каждом магазине работает до 100 сотрудников.

ЗАО "ТестИС-Строй" имеет центральный офис в центре города, где располагается дата-центр, включающий центральную базу данных товаров и

серверы баз данных бухгалтерии, отдела кадров и т. д. В центральном офисе

и на каждой из точек продаж развернуты локальные вычислительные сети (ЛВС). Каждая из ЛВС точек продаж связана с центральным офисом посредством сети Интернет. В точках продаж функционируют 1-2 сервера, обеспечивающих синхронизацию с центральной базой данных, и до 20 рабочих станций: компьютеры директора магазина, секретаря, терминалы в

торговых залах.

В дата-центре установлены Web-сайт электронного магазина и почтовый сервер. К терминалам торговых залов исключена возможность подключения внешних носителей. В дата-центре все серверы размещены в несгораемых сейфах, доступ в помещение контролируется физически(охраняемое помещение). В торговых точках все серверы находятся в кабинетах, закрываемых на ключ. На всех компьютерах, кроме терминалов в торговых залах, установлено антивирусное ПО.

На серверах дата-центра установлен межсетевой экран. На сервере базы данных бухгалтерии дополнительно установлена система обнаружения

вторжений. Для подключения к дата-центру используется защищенное VPN-

соединение. Для подключения к центральной базе товаров предусмотрен резервный канал. Загрузка терминалов торговых залов обеспечивается только

после введения пароля в BIOS.

Вариант 2. Тестовая информационная система издательства газеты "ТестИС-Пресс". Редакция газеты ТестИС-Пресс" занимается публикацией новостей из мира информационных технологий.

Читатели и конкуренты не должны иметь возможности узнать о публикуемых новостях ранее выпуска номера (факторы актуальности и эксклюзивности).

Издательство "ТестИС-Пресс" включает подразделения: руководство (директор и заместитель, главный редактор), IT-отдел (администраторы), бухгалтерия (главный бухгалтер и бухгалтеры),журналисты, редакторы, наборщики, верстальщики. Типография также входит в состав издательства

(сотрудниками являются инженеры по печати и переплету). Всего в редакции

работают 60 сотрудников.

В бухгалтерии используются два сервера: для хранения бухгалтерской

базы данных и ее резервных копий. Каждый редактор, журналист, наборщик

и верстальщик работает на своей рабочей станции. В издательстве используется несколько серверов: для хранения материалов готовящегося к выходу номера, хранения архивов номеров. Почта и web-сайт издательства

функционируют на двух выделенных серверах. Доступ в Интернет осуществляется через Провайдера. Издательство готово к сотрудничеству с

внешними аудиторами.

В издательстве используется система криптозашиты электронной почты. На рабочих станциях редакторов и журналистов настроена система

автоматической блокировки станции при отсутствии сотрудника на рабочем

месте. В бухгалтерии установлена система видеонаблюдения. Доступ в серверную комнату обеспечивается только по пропускам. Предусмотрено резервное копирование бухгалтерской базы данных.

Вариант 3. Тестовая информационная система компании по обслуживанию средств электронной коммерции "ТестИС-Е".

Компания "ТестИС-Е" осуществляет деятельность в рамках продаж и

обслуживания оборудования электронной коммерции. В компании существуют три отдела: бухгалтерия (главный бухгалтер, бухгалтеры), отдел технического анализа (руководитель отдела, инженеры), отдел продаж (руководитель отдела, заместитель, менеджеры). Для всех сотрудников предоставлена рабочая станция с выходом в Интернет. В конференц-зале установлена рабочая станция (ноутбук), которую используют только члены совета директоров (финансовый директор, генеральный директор и его заместитель).

В компании определена должность администратора, имеющего доступ

ко всем ресурсам системы за исключением сервера коммерческих данных.

В отделе технического анализа расположен сервер-хранилище информации. Доступ к нему имеют только сотрудники этого отдела. Почтовым сервером, расположенным в серверном помещении, пользуются сотрудники отдела продаж, дирекция и бухгалтерия. К серверу коммерческих данных, расположенному в серверном помещении, имеют доступ только члены совета директоров и главный бухгалтер (администратор не имеет доступа к этому серверу). Резервное копирование этого сервера выполняется на CD-R-носители, хранимые в сейфе генерального директора.

Для доступа в Интернет используется шлюз в виде отдельного сервера,

размещенного в серверном помещении. На нем установлена служба VPN-доступа, Web-прокси, служба фильтрации запросов, система учета трафика и

система обнаружения вторжений. В компании не используется антивирусное программное обеспечение.

Внутренние документы и настройки безопасности рабочих станций запрещают запускать любые программы, кроме, установленных на компьютерах. Запрещена инициация соединений с рабочими станциями пользователей внешней сети. На почтовом сервере используется система антивирусной защиты электронной почты и защиты от спама.

Вариант 4. Тестовая информационная система компании по разработке программного обеспечения "ТестИС-Солюшн".

Компания "ТестИС-Солюшн" занимается разработкой программного

обеспечения, используемого в банках. Руководство компании "ТестИС- Солюшн" представлено генеральным директором, его заместителем и техническим директором. Штатный состав компании составляет 70 человек.

Разработки компании имеют закрытый тип. Для их контроля и контроля используемых ресурсов в штатном расписании предусмотрены следующие должности: главный администратор, администратор файловых

серверов, сетевой администратор. Остальные сотрудники – инженеры по разработке ПО, тестировщики, разработчики и руководители проектов. В бухгалтерии работает один человек – главный бухгалтер. База данных бухгалтерии находится на его рабочей станции.

Информация, обрабатываемая в системе – результаты и данные разработки программных продуктов: исходные коды, документация, результаты тестирования.

В компании используется антивирусная защита, все серверы расположены в серверном помещении, закрываемом на ключ. На серверах

установлены системы контроля версий; почтовый и файловый серверы защищены межсетевым экраном. Сервер системы контроля версий доступен

тестировщикам из Интернет по VPN-соединению. Компьютер главного бухгалтера не имеет дисководов и устройств подключения USB, кроме того,

он не включен в основную сеть. Резервное копирование не производится.

Дирекция и руководители проектов имеют доступ в Интернет с рабочих мест. Только разработчики могут вносить изменения в систему контроля версий.

**Практическая работа № 7-8**

**Тема: Выявление первичных и вторичных ошибок**

Цель работы: изучить первичные и вторичные ошибки, научиться применять методы и способы выявления ошибок, оформлять отчет о дефектах программного продукта.

Краткие теоретические сведения:

При отладке и тестировании сначала обнаруживаются вторичные ошибки, т.е. результаты проявления исходных дефектов, которые являются первичными ошибками или причинами обнаруженных аномалий. Проявления дефектов и ошибок в разной степени влияют на работоспособность программы.

По величине ущерба проявления дефектов и вторичных ошибок их делят на:

1. сбои, которые не отражаются существенно на работоспособности программы и ущербом, от которых можно пренебречь.  
2. ординарные отказы, ущерб от которых находится в допустимых пределах;  
3. катастрофические отказы, ущерб от которых так велик, что определяет безопасность применения данного комплекса программ.

Первичные ошибки в ПС в порядке усложнения их обнаружения можно разделить на следующие виды:

1. технологические – это ошибки подготовки машинных носителей, документации и ошибки ввода программ в память ПК и вывода их на средства отображения;

2. программные ошибки из-за неправильной записи исходного текста программ на языке программирования и ошибок трансляции программ в объектный код;

3. алгоритмические ошибки, связанные с неполным формированием необходимых условий решения и некорректно поставленных задач;  
4. системные ошибки, обусловленные отклонением функционирования ПС в реальной системе и отклонением характеристик внешних объектов от предполагаемых при проектировании.

*Методы обнаружения ошибок:*

### Инспекции исходного текста

### Сквозные просмотры

### Проверка за столом

**Порядок выполнения работы:**

Задание 1: Произвести отладку программного продукта на основании отчета по тестированию работоспособности, сделанного в предыдущих практических работах.

**Практическая работа № 9-10**

**Тема: Обнаружение вируса и устранение последствий его влияния**

Цель работы: изучение [методов обнаружения вирусов и методов](http://www.vossta.ru/o-vozmojnostyah-razlichnih-metodov-obnarujeniya-i-ustraneniya.html) удаления последствий заражения вирусами с использованием антивирусной утилиты

Краткие теоретические сведения:

*Методы обнаружения вирусов*: сканирование, обнаружение изменений, эвристический анализ, использование резидентных сторожей, вакцинирование программ, аппаратно-программная защита от вирусов.

*Методы удаления последствий заражения вирусам*:

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

2. позволяет восстанавливать файлы и загрузочные сектора, зараженные неизвестными вирусами (для восстановления файлов программа восстановления должна заблаговременно создать и хранить информацию о файлах, полученную в условиях отсутствия вирусов.

**Порядок выполнения работы:**

Задание 1. Изучить категории вредоносных программ и изучить работу с [антивирусной утилитой](http://www.vossta.ru/3-trebovaniya-nastoyashej-instrukcii-obyazateleni-dlya-vipolne.html). Заполнить таблицу с описанием вирусов.

|  |  |  |
| --- | --- | --- |
| Категории вредоносных программ | Наименование и описание вируса | Видимые проявления |
| Adware и SpyWare |  |  |
| Backdoor |  |  |
| Hoax |  |  |
| Trojan |  |  |
| Trojan-Clicke |  |  |
| Trojan-Downloader |  |  |
| Trojan-Spy |  |  |
| Trojan-PSW |  |  |
| Net-Worm |  |  |
| Worm |  |  |
| Trojan-Dropper |  |  |
| Trojan-Proxy |  |  |
| Email-Worm |  |  |
| FraudToo |  |  |
| Trojan-Ransom |  |  |

Задание 2. Проверить компьютер на наличие вирусов. В случае обнаружения, устранить последствия их влияния.

**Практическая работа №11**

**Тема: Работа с реестром**

Цель работы: научится использовать реестр, для просмотра и настройки безопасности системы, ознакомиться с операциями, направленными на оптимизацию работы операционной системы.

Краткие теоретические сведения:

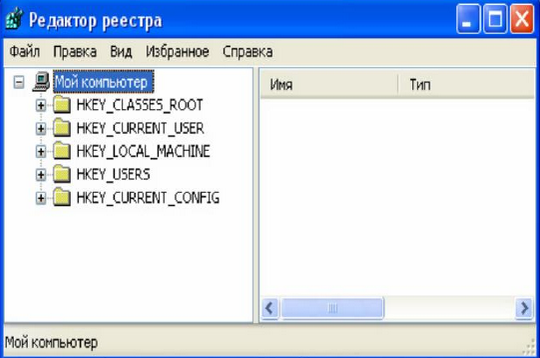
Реестр операционной системы Windows – это большая база данных, где

хранится информация о конфигурации системы. Этой информацией пользуются как операционная система Windows, так и другие программы. В некоторых случаях восстановить работоспособность системы после сбоя можно, загрузив работоспособную версию реестра, но для этого необходимо иметь копию реестра.

Реестр можно рассматривать как записную книжку Windows - как только системе нужна какая-то информация, она ищет ее в реестре. Реестр очень обширен, и дать однозначное его определение невозможно. В целом реестр очень напоминает файловую систему с той разницей, что вместо файлов на нижнем уровне содержатся параметры.

Информация, хранящаяся в иерархической базе данных реестра, собрана в разделы (ключи, key), которые содержат один или более подразделов (subkey). Каждый подраздел содержит параметры (значения, value)

Основным средством для просмотра и редактирования записей реестра служит специализированная утилита «*Редактор реестра*». Файл редактор реестра находится в папке *C:\Windows*. Называется он *REGEDIT.EXE*. после запуска появится окно редактора реестра. Вы увидите список из 5 разделов:



Работа с разделами реестра аналогична работе с папками в *Проводнике*. Конечным элементом дерева реестра являются ключи или параметры. Реестр содержит шесть корневых разделов (ветвей), каждый из них включает подразделы, отображаемые в левой части окна в виде значка папки.

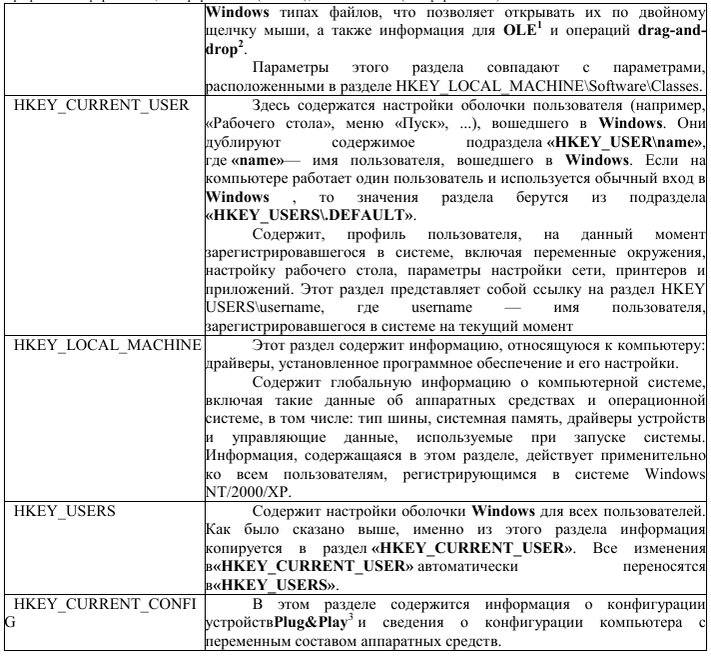
**Порядок выполнения работы:**

*Указания*: Перед выполнением заданий создайте точку восстановления системы.

Задания 1. С помощью редактора реестра изучить корневые разделы системного реестра.

Таблица 1 Корневые разделы реестра:





Регистр букв в ключах и параметрах не имеет значения. Прописные буквы употребляются только для удобства восприятия информации.

Задание 2. Экспорт реестра

*Указание*: по ходу выполнения заданий сделайте несколько скриншотов, добавьте в них комментарии и пояснения, внесите в отчет.

Для экспорта ветвей реестра выполните следующие действия:

1. щелкните мышью на разделе (ключе), находящемся в вершине ветви, выбранной самостоятельно, которую необходимо экспортировать (например, HKEY\_CURRENT\_USER);

2. в меню «ФАЙЛ» выберите пункт «ЭКСПОРТ», чтобы вывести на экран диалоговое окно «ЭКСПОРТ ФАЙЛА РЕЕСТРА»;

3. в поле «ИМЯ ФАЙЛА» введите имя файла для экспорта;

4. выберите диапазон экспорта: чтобы создать копию всего реестра, щелкните на «ВЕСЬ РЕЕСТР», чтобы создать копию выделенной ветви, щелкните на «ВЫБРАННАЯ ВЕТВЬ»;

5. в выпадающем списке «Тип файла» выберите тип файла для экспорта: «Файлы Реестра \*.reg», «Файлы кустов Реестра \*.\*», «Текстовые файлы \*.txt» или «Файлы Реестра Win9x/NT4 \*.reg»;

6. экспортируйте ветвь, мышью щелкнув на кнопке «*Сохранить*».

Последовательность вышеописанных действий фактически представляет собой один из способов создания резервной копии Реестра ОС. Сохранение Реестра перед редактированием является принципиальным, поскольку обеспечивает дополнительный шанс на его восстановление в случае выхода системы из строя посредством непродуманных действий пользователя.

Задание 3. Внесение в системный реестр настроек, запрещающих пользователю полное или частичное изменение свойств *Рабочего стола*.

*Указание*: в отчет внести скриншот и полученные выводы.

1. С помощью *Проводника* найти в папке Windows файл *regedit.exe* и запустить его.

2. Перейти в раздел реестра HKEY\_CURRENT\_USERS\SOFTWARE\ MICROSOFT\WINDOWS\CURRENT VERSION\POLICIES\SYSTEM.

Если при открытии раздела POLICIES окажется, что в нем отсутствует раздел *SYSTEM*, создать его, используя команду *Правка – Создать – Раздел*.

3.Свернуть окно редактирования реестра и, щелкнув правой кнопкой мыши в свободном месте *Рабочего стола*, с помощью контекстного меню открыть окно *Свойства: Экран*. Записать перечень закладок окна с настройками экрана, доступными для пользователя, и закрыть окно.

4. Развернуть окно редактирования реестра и в разделе *System* с помощью

команды *Правка – Создать – Параметр Dword* создать ключ *NODISPSettingsPage* и, щелкнув по его имени правой кнопкой мыши, выбрать в появившемся меню команду *Изменить*. Используя окно *Изменение Параметра Dword* (вызов осуществляется через контекстное меню), присвоить созданному ключу значение «1» в шестнадцатеричной системе.

5. Свернуть окно редактирования реестра и вновь открыть окно *Свойства: Экран*. Изучить перечень закладок, доступных пользователю, и сделать вывод о назначении ключа *NODISPSettingsPage*. Закрыть окно свойств экрана.

6. Повторить действия, описанные в пунктах 4 и 5, присваивая значение «1»

следующим ключам: *NODISPBackgroundPage; NODISPAppearancePage; NODISPScrSavPage; NODISPCPL*.

Сделать вывод об их назначении.

Задание 4. Создание файлов редактирования реестра, один из которых разрешает, а другой запрещает пользователю изменение настроек Рабочего стола.

*Указание*: внести в отчет скриншот и полученные выводы.

1. Хотя файлы редактирования реестра могут создаваться в любом текстовом

Редакторе (например, Блокнот), удобнее получить шаблон такого файла, используя *regedit*. Для этого, не закрывая редактор *regedit* после выполнения задания 3, в разделе *System* удалить все ключи кроме последнего *NODISPCPL*.

2. Щелкнув мышью по строке с названием раздела *System*, выполнить команду *Файл – Экспорт* и, указав имя создаваемого файла f*ile1*, сохранить его в папке *Мои документы*.

3. Закрыть программу *regedit*.

4. Перейти в папку *Мои документы* и, щелкнув правой кнопкой мыши по файлу *file1.reg*, выполнить команду *Открыть с помощью – Блокнот*

5. Изучить структуру файла *file1.reg*. Его содержимое должно быть примерно

следующим: Windows Registry Editor Version 5 [HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System] "NODISPCPL"=dword:00000001

6. Заменить в последней строке файла значение параметра *DWORD* c 00000001 на 00000000 и, используя команду *Файл – Сохранить как*, сохранить внесенные изменения в файле *file2.reg*.

7. Закрыть *Блокнот*. Поочередно запуская двойным щелчком на выполнение

файлы *file1.reg и file2.reg*, произвести попытку редактирования настроек *Рабочего стола*. Сделать выводы, удалить оба файла.

Задание 5. Настройка визуальных опций ОС с помощью системного Реестра.

*Указание*: в отчет внести выводы по задачам № 1 и 2, скриншоты по заданиям № 3 и 4

В диалоговом окне «*Изменение строкового параметра*» ключа *HKCU\Control Panel\Desktop* измените значение параметра *MenuShowDelay* на любое число, менее 400. Сделайте вывод о том, как различные значения этого параметра влияют на раскрытие вложенных списков меню *Пуск*.

Скрыть все значки с рабочего стола. Для этого в разделе *HREY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\*

*Explorer* создать параметр *DWORD NoDesktop =1* (=0 - все значки видны). При необходимости выполните перезагрузку виртуальной машины.

Запретить следующие команды в меню *Пуск*. В разделе *HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer* если параметр имеет равен 1, то команда запрещена, 0 - разрешена

−NoTrayContextMenu - запретить контекстное меню панели задач,

−NoChangeStartMenu - запретить контекстное меню в меню *Пуск*

−NoStartMenuSubfolders- скрыть подкаталоги в меню *Пуск*.

−NoRun - скрыть меню *Выполнить* в меню *Пуск*.

−NoFind скрыть меню *Найти* в меню *Пуск*.

−NoLogOff скрыть меню *Завершение сеанса* в меню *Пуск*.

−NoClose скрыть меню *Завершение работы* в меню *Пуск*.

Удалить стрелки у ярлыков:

HKLM\SOFTWARE\Classes\lnkfile - ярлыки Windows

STRING IsShortcut - удаление этого параметра - отключает стрелки на ярлыках.

Не добавлять "ЯРЛЫК ДЛЯ..." для создаваемых ярлыков:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer BINARY link, значение hex:00,00, 00,00 - не добавлять.

Задание 6. Создание в системном реестре собственного обработчика произвольного расширения.

*Указание:* внести в отчет скриншот полученного результата

1. выберите самостоятельно произвольное расширение, состоящее из трех

символов, обработчик которого предполагается создать,

2. в разделе *HKCR Реестра* ОС создайте новый раздел с названием выбранного ранее расширения; при этом обратите внимание на то, как это уже сделано для других расширений в системе,

3. значение строкового параметра (по умолчанию), соответствующего созданному разделу, должно содержать ссылку вида *\*\*\*file, где \*\*\** – символы выбранного расширения, на раздел обработчика данного расширения,

4. в разделе *HKCR Реестра* ОС создайте новый раздел обработчика расширения следующего вида *\*\*\*file\shell\open\command* – для команды открытия и *\*\*\*file\shell\list\command* – для команды просмотра файла;

5. в разделах *command*, каждой из ветвей, создайте по одному расширяемому

строковому параметру типа *REG\_EXPAND\_SZ* с наименованием (по умолчанию),

6. удалите старые строковые параметры *REG\_SZ*, создаваемые в разделе

*command* по умолчанию,

7. в расширяемом строковом параметре раздела *\*\*\*file\shell\list* измените

данные значения по умолчанию на «*Мой просмотр*»,

8. в соответствующих разделах *command* измените значения расширяемых

строковых параметров на команды для открытия файла и его просмотра. В частности, для открытия текстового файла можно воспользоваться приложением *Wordpad.Exe*, а для его просмотра выбрать *Notepad.Exe*,

9 проверьте работоспособность обработчика, выполнив следующее:

−выберите какой-либо файл с его стандартным расширением,

−поменяйте стандартное расширение на то, обработчик которого Вы только что создали,

−правой кнопкой манипулятора мышь выберите из контекстного меню команду с именем того файла (filename.\*\*\*), который Вы собираетесь открыть или команду «*Мой просмотр*», чтобы просмотреть файл; при этом должно загрузиться соответствующее приложение обработчика.

**Практическая работа №12**

**Тема: Работа с программой восстановления файлов и очистки дисков**

Цель работы: изучить программы по восстановлению файлов, научиться использовать специализированные программы для сервисного обслуживания компьютера и операционной системы.

Краткие теоретические сведения:

Все программы по восстановлению утерянных файлов работают благодаря особенности записи данных на ПК. Физический ресурс памяти компьютера поделен на логические части. Пользователь видит их в виде «диск С», «диск D» и далее. Каждый имеет свой шаблон записи или файловую систему. На одном компьютере может работать несколько систем сохраняющих контент каждая по-своему.

Невидимыми для пользователя являются метаданные. Они располагаются на том же уровне, что и логические диски и хранят сведения о структуре расположения папок и документов, их имена, тип файловой системы.

Эта служебная информация необходима компьютеру для лучшей организации работы и не показывается на экране. Каждый логический диск тоже имеет скрытые сведения и копии этих сведений.

Технические сведения полезны т.к. содержат точный физический адрес файла. Утилита обращается к этим записям и восстанавливает материал. Если метаданные повреждены, утилита обращается к одной из копий.

Когда происходит визуальное удаление материала, на самом деле изменяется только техническая информация о файле или папке. Если не произошла на его место перезапись нового файла, первоначальная информация по-прежнему содержится в компьютере.

Поиск по техническим сведениям помогает воссоздать содержимое в исходном виде.

Если произошло разрушение метаданных, то утилита восстановит материал, но содержаться он будет не под своим, а под виртуальным именем (набор цифр и букв).

Еще один принцип работы заключается в обращении к сигнатуре. Это сведения о расширении. Например, запись о музыке в формате MP3 начинается с обозначения ID3… Программа ищет все известные расширения и реанимирует их по категориям: музыка, фото, Pdf — документы, txt, и так далее.

Недостаток этого метода в отсутствии первоначальной структуры. Все «возвращенное» будет в хаотичном порядке и под чужим (произвольным) именем. Но этот способ позволяет восстановить гораздо больше информации, чем первый.

## *Восстановление файлов при повреждении жесткого диска*

Чаще всего пользователи хранят важные сведения на [жестком диске](https://pchelp.one/zhelezo/kak-vybrat-zhestkij-disk.html). Но если он повреждается, то это влечет частичную потерю информации, которую можно восстановить при помощи софта. Но это подходит только в случае целостности дисков.

Когда жесткий диск поврежден механически — разорваны дорожки, или аппаратно — не определяется компьютером, то лучше обратиться в специальные лаборатории.

***Важное предостережение: перед началом восстановления информации с жесткого диска следует создать его образ.***

Клонировать содержимое диска можно при помощи этих же программ. Это защитит первоисточник от перезаписи и позволит экспериментировать с различными вариантами работы приложения.

Не следует сохранять восстановленную информацию на этот же диск; необходимо найти другой носитель.

*Примеры программ*:

## R-studio - В случае удаления важного контента с внутренней памяти компьютера

1. Recuva – многофункциональная утилита.
2. Recovery-software составляет целую группу программ, специализирующихся на [восстановлении флешек](https://pchelp.one/%d0%bf%d1%80%d0%be%d0%b3%d1%80%d0%b0%d0%bc%d0%bc%d1%8b-%d0%b4%d0%bb%d1%8f-%d0%b2%d0%be%d1%81%d1%81%d1%82%d0%b0%d0%bd%d0%be%d0%b2%d0%bb%d0%b5%d0%bd%d0%b8%d1%8f-%d1%84%d0%bb%d0%b5%d1%88%d0%b5%d0%ba/), так и жестких дисков.
3. **Data Rescue** специализируется на поврежденных или переформатированных носителях.
4. **UndeletPlus** отличается большим спектром выбора носителя: жесткие диски, карты памяти фотоаппаратов, мультимедийные плееры, почтовые аккаунты, флешкарты.

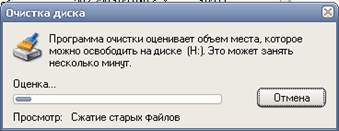
**Порядок выполнения работы:**

Задание 1. **Использование программы очистки диска. Произвести очистку диска.**

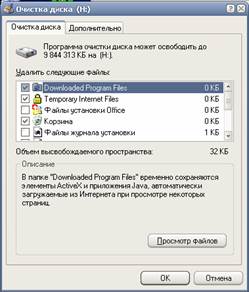
Программа очистки диска помогает очистить пространство на жестком диске. Программа очистки диска проверяет диск и выводит перечень временных файлов, файлов кэша Интернета, а также ненужных программных файлов, удаление которых не приведет к негативным последствиям. Можно выбрать удаление некоторых или всех этих файлов.

Для выполнения некоторых задач может потребоваться войти в систему с учетной записью «Администратор» или члена группы «Администраторы».

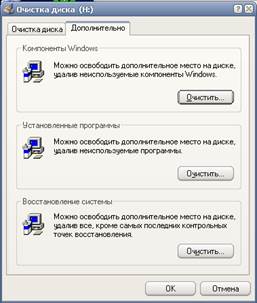
1.Запустите программу Очистка диска.



2.После оценки объема места, которое можно освободить на диске, отметить файлы к удалению и нажать ОК.



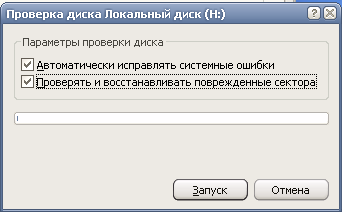
3.При необходимости провести дополнительную очистку диска, удалив неиспользуемые компоненты Windows, неиспользуемое программное обеспечение.



4.Провести анализ освободившегося пространства.

Задание 2. С помощью меню сервис выполнить проверку диска

1.Запустить программу проверки диска. Установить флажки автоматического исправления ошибок, проверки и восстановления поврежденных секторов.

****

2.Описать процедуру проверки, сделать анализ

**Задание 3. Произвести дефрагментацию жесткого диска**

Программа «Дефрагментация диска» — это системная служебная программа, выполняющая анализ локальных томов с последующим поиском и объединением фрагментированных файлов и папок.

Программа дефрагментации объединяет фрагментированные файлы и папки на жестком диске компьютера, после чего каждый файл или папка тома занимает единое непрерывное пространство. В результате доступ к файлам и папкам выполняется эффективнее. Объединяя отдельные части файлов и папок, программа дефрагментации также объединяет в единое целое свободное место на диске, что делает менее вероятной фрагментацию новых файлов.

1.Откройте программу Дефрагментация диска.

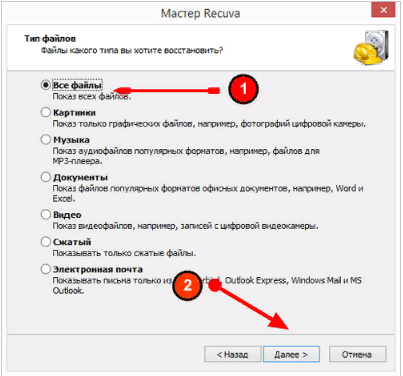
Дефрагментацию дисков можно запустить из командной строки с помощью команды defrag или нажмите кнопку ***Пуск*** *-* ***Все программы –Стандартные –Служебные – Дефрагментация диска***.

2.Для получения сведений об использовании программы дефрагментации дисков выберите команду ***Справка*** в меню ***Действие*** этой программы.

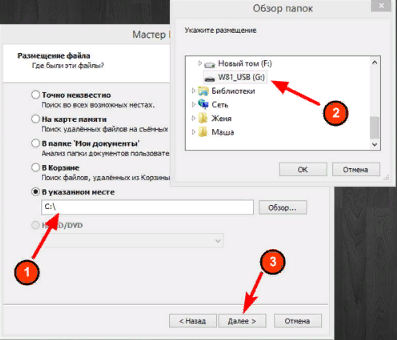
Задание 4. С помощью программы Recuva восстановить данные

1.Запустить программу Recuva.

2. После установки и запуска программы выберете тип восстанавливаемых данных. Если вы, к примеру, хотите восстановить только музыку, удаленную с флешки, выбирайте третий пункт. Если же желаете увидеть все найденные к восстановлению данные, оставляйте флажок на первом пункте «все файлы», и нажимайте «далее»

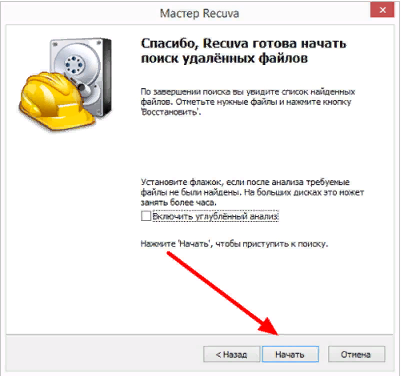


3. Если вы точно знаете месторасположение удаленных файлов (например, флешка), выбирайте пятый пункт «В указанном месте», отмечайте двойным кликом в появившемся списке нужный диск/папку и нажимайте «Далее».

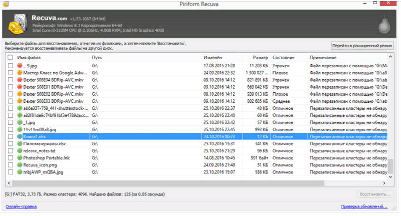


4. После того, как вы выбрали нужный диск/папку, перед вами появится окно завершения работы мастера Recuva, где он предложит вам включить углубленный анализ.

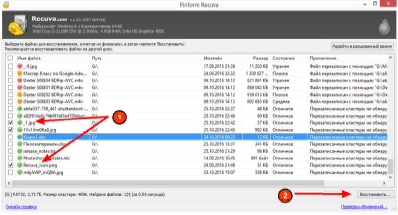
При первичном проходе делать этого не рекомендуется, т.к. включение данной функции сильно увеличит время сканирования, при этом результаты не факт что будут отличаться. Так что оставляйте пока как есть и нажимайте «Начать».



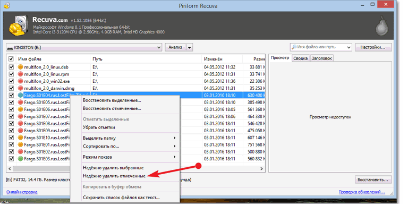
5. После того, как закончится сканирование, перед вами появится окно в найденными удаленными файлами. Как видите, есть три типа цветовой индикации найденных файлов — красные (восстановить не получится), желтые (возможно частичное восстановление) и зеленые (могут быть восстановлены полностью).



6. Отмечайте искомые файлы, нажимайте «Восстановить…» и выбирайте папку, куда будут помещены восстановленные файлы.



7. В том же окне выбора файлов отметьте те, которые хотите удалить навсегда, вызовите правой кнопкой мыши контекстное меню и выбирайте пункт «Надежно удалить отмеченные». Через некоторое время Recuva удалит эти файлы без возможности восстановления.



# Информационное обеспечение обучения по дисциплине

1. Вичугова А.А. Инструментальные средства разработки компьютерных систем и комплексов [Электронный ресурс]: учебное пособие для СПО/ Вичугова А.А.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 135 c.— Режим доступа: http://www.iprbookshop.ru/66387.html.— ЭБС «IPRbooks»

2. Гвоздева, В. А. Основы построения автоматизированных информационных систем: учебник / В. А. Гвоздева, И. Ю. Лаврентьева. -М.: ФОРУМ-ИНФРА-М, 2017.-256 с.

3.Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. — СПб.: Питер, 2018. — 992 с

4.Разработка, внедрение и адаптация программного обеспечения отраслевой направленности. Учебное пособие/ Федорова Г.И. Изд.: КУРС, Инфра-М. Среднее профессиональное образование. 2016. - 336 с.

### 5. [Черников Б.В.](https://znanium.com/spec/catalog/author/?id=cb16e0d8-f075-11e3-b92a-00237dd2fde2) Управление качеством программного обеспечения: Учебник / Б.В. Черников. - М.: ИД ФОРУМ: ИНФРА-М, 2017. - 240 с.