**Вопросы к дифференцированному зачету по МДК 04.01 Внедрение и поддержка компьютерных систем**

1. Понятие программный модуль, программный комплекс, программный продукт.

**Программный модуль** – конструкция, которая состоит из процедур или объявлений данных, которая может взаимодействовать с другими конструкциями

**Программный комплекс** – совокупность программных модулей, предназначенных для решения одной задачи.

**Программный продукт** – программный комплекс с соответствующей документацией, регламентирующей правила обращения с ним пользователя.

1. Назначение стандарта ГОСТ Р ИСО/МЭК 12207-2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств»

Стандарт используется при приобретении систем, ПП и услуг, при их поставке, разработке, применении по назначению, сопровождении и прекращении применения ПП и программных компонентов системы в самой организации и вне ее.

**Системная инженерия** – наука о создании крупных комплексных систем, которые соответствуют набору экономических и технических требований.

**Программная инженерия** – область компьютерной науки и технологии, которая занимается построением программных систем.

**Процессы ЖЦ программных средств:** 1) основные 2) вспомогательные 3) организационные

1. Перечислить основные процессы согласно стандарту ГОСТ Р ИСО/МЭК 12207-2010.

**Основные процессы** – относятся к ЖЦ информационной системы и является производственными процессами организации. (Заказ, поставка, разработка, эксплуатация, сопровождение)

1. Перечислить вспомогательные процессы согласно стандарту ГОСТ Р ИСО/МЭК 12207-2010.

**Вспомогательные процессы** – предназначены для поддержки основных процессов. (Документирование, управление конфигурацией, обеспечение качества, аттестация, совместный анализ, аудит, решение проблем)

1. Перечислить организационные процессы согласно стандарту ГОСТ Р ИСО/МЭК 12207-2010.

**Организационные процессы** – затрагивают персонал предприятия, происходит независимо от вспомогательных и основных процессов. (Управление, создание инфраструктуры, усовершенствование, обучение)

1. Понятие внедрение программного обеспечения, стратегии внедрения программного обеспечения, виды стратегий внедрения.

**Внедрение ПО** – процесс настройки ПО под условия использования с последующим обучением пользователей работе с установленным ПО.

**Стратегия внедрения ПО** – набор правил принятия решений, используемый для определения направлений деятельности по внедрению ПО в организации.

**Виды стратегий:** 1) опытные (пробные) 2) масштабные 3) конвейерные

1. Перечислить основные этапы внедрения ПП.
2. обследование
3. разработка технического задания
4. настройка системы
5. тестирование системы
6. опытная эксплуатация
7. промышленная эксплуатация
8. Понятие сценария внедрения. Последовательность шагов сценария внедрения ПО.

**Сценарий внедрения** – комплекс действий и задач, выполняемых и решаемых заказчиком, приобретающим ПО.

**Последовательность шагов сценария внедрения ПО:**

1) подготовка заявки на приобретение ПО

2) подготовка договора на приобретение ПО

3) контроль за деятельностью поставщика

4) составления актов приемки работ

1. Цель автоматизации информационных процессов. 2 системных аспектов разработки (проектировании) систем автоматизации информационных процессов.

**Цель автоматизации информационных процессов** – повышение производительности и эффективности труда работников, улучшение качества информационной продукции и услуг, повышение сервиса и оперативности обслуживания пользователей.

**2 системных аспекта разработки систем:**

1) анализ – выделение процессов, подлежащих автоматизации, их изучение, выявление определенных закономерностей, особенностей и др.

2) синтез – организация внедрения новой информационной технологии для осуществления, полученных в результате анализа, технических, технологических и программных решений.

1. Понятие сопровождение программного обеспечения. Кем может осуществляться сопровождение.

**Сопровождение ПО** – совокупность действий по обеспечению работы ПО, а также по внесению изменений в случае обнаружения ошибок в процессе эксплуатации, по адаптации ПО к новой среде функционирования, а также по повышению производительности или улучшению других характеристик ПО.

**Сопровождение осуществляется:**

1) организацией разработчика

2) сотрудниками организации заказчика

3) сторонней организацией, которая оказывает услуги в области сопровождения

1. Что включает процесс сопровождения ПО.

1) передача ПО от разработчика организации заказчику для сопровождения

2) принятие или отклонение запроса на модификацию

3) отслеживание запросов на модификацию и отчетах об ошибках

4) анализ возможных последствий изменений, вносимых в систему

5) поддержка ПО   
6) ведение контрактов и обязательств на уровне оказания услуг по сопровождению

1. В каких целях проводится Сопровождения системы.

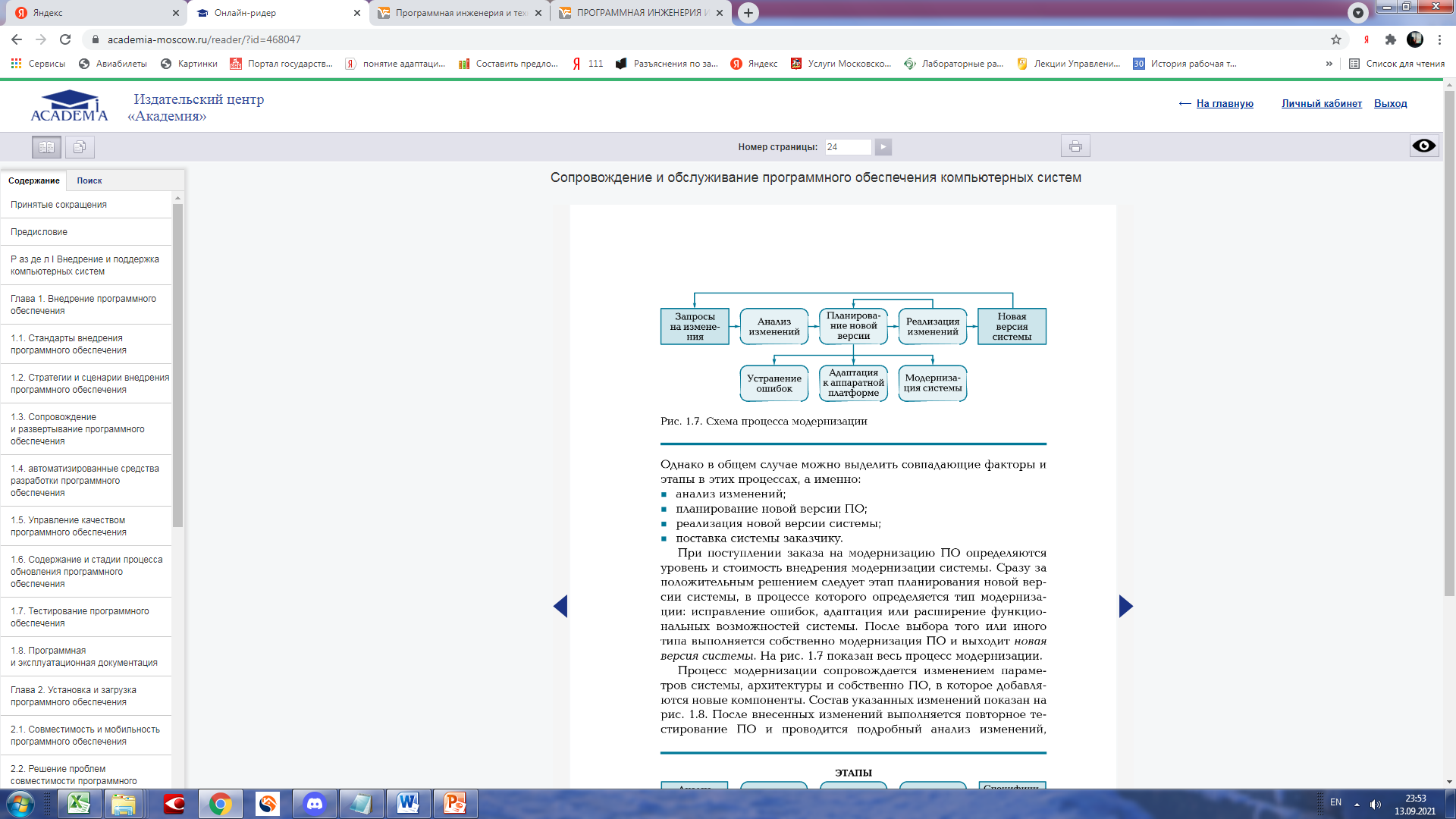
1) исправления ошибок

2) адаптации ПО к условиям эксплуатации, т.е. настройки продукта в изменившихся условиях эксплуатации или в новой среде выполнения ПО

3) изменения функциональных возможностей

1. Понятие модернизации ПО. Схема модернизация ПО.

**Модернизация** – изменение параметров системы, архитектуры и ПО, в которое добавляются новые компоненты.



1. Понятие развертывание ПО. Этапы развертывание ПО.

**Развертывание ПО** – действия, которые делают программную систему готовой к использованию.

**Этапы развёртывания:**

1) составление плана развертывания ПО

2) разработка спецификаций требований

3) установка отдельных подсистем

1. Понятие качество программного продукта. Характеристики качества ПО.

**Качество ПП** – способность удовлетворять установленным или предполагаемым потребностям.

**Характеристики качества**:

1) функциональность – способность ПО решать задачи, которые соответствуют потребностям пользователя при заданных условиях использования ПО.

2) надежность – св-во выполнять задачи в заданных условиях работы и на заданной вычислительной машине в определенный промежуток времени.

3) удобство использования – возможность комфортного изучения ПО пользователем

4) эффективность – способность ПО обеспечивать требуемый уровень производительности в соответствии с выделенными ресурсами, временем и другими условиями.

5) мобильность – перенос ПО с одного окружения в другое.

6) удобство сопровождения – легкость, с которой ПО может анализироваться, тестироваться и изменять для исправления ошибок, для реализации требований, облегчения сопровождения и адаптации к условиям.

1. Управление качеством. Этапы управления качеством ПО.

**Управление качеством** – возможность контроля за процессом разработки ПО.

**Процесс управления качеством состоит из трех видов деятельности:**

1) обеспечение качества. Определение множества организационных процедур и стандартов в целях создания ПО высокого качества.

2) планирование качества. Выделение стандартов и процедур и их адаптация к проекту разработки ПО.

3) контроль качества. Определение и проведение мероприятий по выполнению нормативных процедур и стандартов качества членами группы разработчиков.

1. Контроль качества. Два взаимодополняющих подхода к процессу контроля качества.

**Контроль качества** – набор процедур и отчетов, которые могут быть использованы в процессе разработки ПО.

**2 подхода к процессу контроля качества:**

1) группа разработчиков анализирует документацию, сопровождающую ПП, проверяет соответствие документа стандартам.

2) ПП и его документация проверяется компьютерной программой на соответствие стандарту.

1. Понятие обновление ПО. Виды обновлений ПО.

**Обновление ПО** – дополнения к ПО, устраняющие неполадки, повышающие безопасность или улучшающие производительность компьютерной системы.

**Виды обновлений:**

1) обновление для ОС и серверного ПО применяются в целях поддержки надлежащего уровня безопасности и устранения «дыр» защиты.

2) обновление прикладного ПО необходимы для решения возникших проблем

1. Понятие пакеты обновлений. Виды пакеты обновлений.

**Пакеты обновлений** – наборы обновлений, исправлений и улучшений ПО, поставляемые в виде единого установочного дистрибутива.

**Виды пакетов обновлений:**

1) разностные пакеты – содержат обновления, которых не было в предыдущих пакетах обновлений.

2) суммарные пакеты – включают в себя содержимое предыдущих обновлений.

1. Понятие Patch Management. Перечислить этапы Patch Managment.

**Patch Management** – процесс управления обновлениями ПО.

**Этапы:**

1) подготовка тестовых клиентов. (на машину для тестирования обновлений устанавливается образ ОС с приложениями и утвержденными ранее протестированными обновлениями)

2) создание листов обновлений или патч-листов. (включает обновления, вышедшие в текущем месяце и подходящие под определение «требуемые обновления»

3) развертывание в тестовой среде. (При добавлении пакета к коллекции тестовых клиентов автоматически начинается развертывание. Если выбрать нужные обновления и начнется их установка, после чего произойдёт перезагрузка системы)

4) развертывание на пилотных пользователях. (готовится список протестированных обновлений, который отправляется на клиенты пилотных пользователей, которые разбираются в ПО.

1. Проверка корректности установки обновлений.

Чтобы протестировать корректность обновлений необходимо:

1) перезагрузить систему и, войдя в нее под тестовой учетной записью, убедиться в отсутствии сообщений об ошибках\предупреждениях системы.

2) убедиться, что системная переменная PATH не содержит символов и знаков, которые могут привести к проблемам.

3) проверить журнал системных событий и убедиться в успешности установки всех обновлений и отсутствии

1. Понятие Валидация и Верификация программной системы.

**Валидация программной системы** – доказательство того, что в результате разработки ПО достигнуты цели, которые планировали достичь благодаря ее использованию.

**Верификация** – достижение гарантии того, что верифицируемый объект соответствует требованиям; реализован без непредусмотренных функций и удовлетворяет проектным спецификациям и стандартам.

1. Понятие Тестирование и отладка программного обеспечения.

**Тестирование ПО** – процесс исследования ПО с целью получения информации о качестве продукта.

**Отладка** – поиск местоположения ошибок в программном коде и их исправление.

1. Классификация по объекту тестирования.

1) функциональность

2) надёжность

3) удобство использования

4) производительность

5) удобство сопровождения

6) переносимость

1. Тестирование чёрного ящика, белого ящика, серого ящика.

**Тестирование чёрного ящика** – методика, изучающая функциональность ПО без необходимости знания внутренней структуры кода.

**Тестирование белого ящика** – метод тестирования ПО, который проверяет внутренние структуры или работу приложения.

**Тестирование серого ящика** –метод тестирования ПО, позволяющий протестировать ПП или приложение с частичным знанием внутренней структуры приложения.

1. Ручное тестирование, Автоматизированное тестирование, Полуавтоматизированное тестирование.

**Ручное тестирование** – проверка ПО вручную, без использования автоматизированных инструментов. Тестировщик взаимодействует с программой как обычный пользователь.

**Автоматизированное тестирование** – метод тестирования ПО, который выполняется с использованием специальных программных средств, которые, необходимы для выполнения набора тестовых примеров.

**Полуавтоматизированное тестирование** – ручное тестирование с частичным использованием средств автоматизации ПО для контроля выполнения тестов, сравнения полученных результатов с эталонными, установки предусловий тестов и других функций контроля тестирования и организации отчетов.

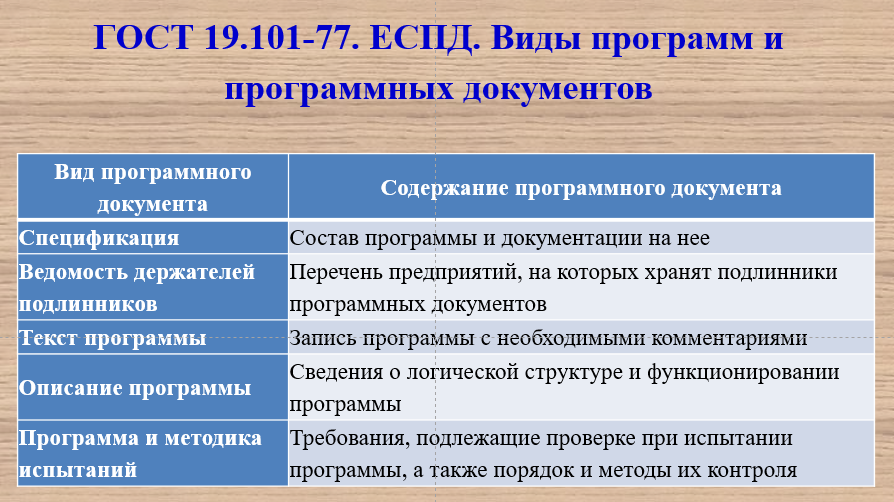
1. Альфа – тестирование. Бета – тестирование.

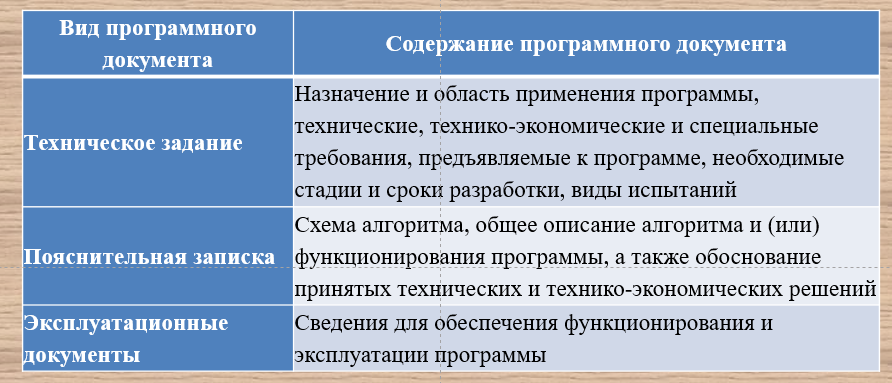
**Альфа-тестирование** – тестирование, проводимое на ранней стадии разработки продукта и включающее имитацию использования продукта разработчиками или реальное использование клиентами.

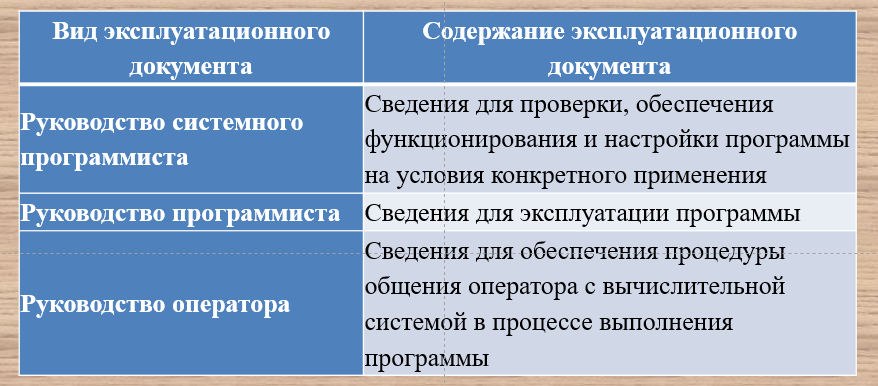
**Бета-тестирование** – использование почти готовой версии продукта с целью выявления максимального числа ошибок его работе для их последующего устранения перед окончательным выходом.

1. Назначение ЕСПД. ГОСТ 19.101-77. ЕСПД. Виды программ и программных документов.

**Единая система программной документации** – комплекс государственных стандартов, устанавливающих взаимосвязанные правила разработки, оформления и обращения программ и программной документации.







1. Понятие программная и аппаратная конфигурация.

**Программная конфигурация** – состав ПО компьютера.

**Аппаратная конфигурация** – совокупность аппаратных средств компьютера.

1. Дать характеристику уровням программного обеспечения (прикладной уровень; служебный уровень; системный уровень; базовый уровень).

**Базовый уровень** отвечает за взаимодействие с аппаратными средствами и хранится в ПЗУ.

**Системный уровень** обеспечивает взаимодействие других программ компьютера с базовым уровнем и с аппаратным обеспечением.

**Служебный уровень** автоматизирует работы по проверке и настройке компьютерной системы.

**Прикладной уровень** представляет собой комплекс прикладных программ, с помощью которых выполняются конкретные задачи.

1. Основные направления изменения конфигурации.

1) замена устаревших компонентов и расширением возможностей называется модернизацией (апгрейдом).

2) повышение производительности системы может достигаться за счет искусственного увеличения тактовой частоты микропроцессоров – «разгона».

3) изменение внешнего вида компьютера называется моддингом.

1. Виды аппаратных конфигураций.

1) Минимальная конфигурация ПК – связывается с конкретным типом ЦП, стандартными или минимальными для него размерами внутренней и внешней памяти, клавиатурой и монитором.

2) базовая конфигурация ПК – минимальный комплект аппаратный средств, достаточный для начала работы с компьютером.

3) оптимальная конфигурация ПК – комплектующие подобранные для какой-то задачи.

1. Понятие и виды совместимости.

**Совместимость** – способность аппаратных или программных компонентов взаимодействовать друг с другом.

**Виды совместимости:**

1) аппаратная– способность одного компьютера работать с узлами или устройствами, входящими в состав другого компьютера.

2) информационная– способность компьютеров, или систем адекватно воспринимать одинаково представленные данные.

3) программная– способность выполнения одних и тех же программ на разных компьютерах с получением одинаковых результатов.

1. Совместимость драйверов. Процесс совместимости драйверов устройств.

**Совместимость драйверов** – часть кода ОС, отвечающая за взаимодействия ПО с физической или виртуальной аппаратурой.



1. Методы уменьшения проблем с совместимостью.

1) изменения конфигурации существующего приложения для обнаружения проблем и создания исправления данного приложения.

2) применение пакетов обновлений или обновлений к приложению.

3) апгрейд приложений для совместимого релиза (лучшее решение – обновить до более новой версии).

4) изменения конфигурации безопасности (например: добавить сайт в список надежных сайтов или выключить защищенный режим).

5) запуск приложения в виртуализированной среде (запустить приложение в другой ОС, используя инструменты виртуализации).

6) использование функции совместимости приложения: запуск приложения в режиме эмуляции, применение мастера совместимости программ.

7) выбор другого приложения, которое выполняет ту же функцию, но не имеет проблем с совместимостью.

1. Режим совместимости Windows 10.

**Режим совместимости Windows 10** – позволяет запустить старую программу, работающую в одной из предыдущих версий Windows, обеспечивая её стабильную работу в новой версии Widows 10

1. Основные этапы перехода на последнюю версию ПО.

1) апгрейд. Обмен одного из имеющихся у пользователя продукта на новый.

2) установка. Проведение самих работ, результат – рабочая новая версия ПО, которую можно сразу использовать.

3) перенос данных. Необходимый этап в рамках, которого информация со старой версии переносится на новую.

4) освоение. Научиться работать с новой системой можно: - самостоятельно, для этого выпускается специализированная литература - в специально созданных учебных центрах - индивидуально, с квалифицированным специалистом.

1. Пошаговая модель перехода на новое ПО.

Шаг 1: определение приоритетности бизнес-мероприятий. Проведение обновления является уникальным для каждой организации, которая внедряет решение. Выбор различных параметров, от способов доставки до конечных устройств, будет зависеть от таких факторов, как потребности различных типов пользователей внутри организации, задачи, которые они выполняют, и места, в которых они работают.

Шаг 2: сбор данных. Прежде чем приступить к анализу вашей среды, важно собрать актуальные данные относительно пользователей, приложений и устройств.

Шаг 3: анализ среды и сегментирование пользователей. Чтобы переход к более новой версии ПО и трансформация ИТ-отделов прошли максимально успешно, необходимо полное понимание среды.

Шаг 4: рационализирование приложения. Сделайте проект проще, сократив список приложений до необходимого минимума.

Шаг 5: решайте связанные с совместимостью приложений вопросы в удобном темпе.

1. Способы обновление Windows 10.

1) встроенными средствами ОС. С помощью центра обновление Windows можно обновить до последней версии Windows.

2) скачивание и установка обновлений вручную.

3) загрузка обновлений с ручной установкой.

1. Чистая загрузка Windows 10. Причины использования Чистой загрузки.

**Чистая загрузка Windows** – загрузка ОС Windows с программами и драйверами, которые поддерживают ее нормальное функционирования.

**Причины использования чистой загрузки:**

1) при чистом запуске ОС компьютер загружает все установленные драйвера, включая сторонние, но не загружает сторонние программы и утилиты.

2) если системе не удается установить или удалить программы «штатными средствами» или, когда возникают проблемы с запуском приложения от стороннего разработчика, которые не связаны с отсутствием исполняемых файлов.

3) когда необходимо определить программу из списка «Автозагрузки», из-за которой загрузка проблематична.

4) система «захватила и не отдает» ресурс пользователя.

1. Понятие статистических и динамических библиотек.

**Статические (LIB) библиотеки** – набор исходных кодов, подключаемых программистом в свою программу, либо набор заранее скомпилированных объектных файлов, связываемых вместе на этапе компиляции.

**Динамические (DLL) библиотеки** – загружаются ОС по «требованию» запущенной программы уже в ходе ее выполнения.

1. Технология реализации модульного принципа программирования.

1) задача разбивается на простые и самостоятельные фрагменты. Критериями качества разбиения являются: ■ решение задачи до конца каждым выделяемым фрагментом ■ возможность запрограммировать модуль в заданный срок ■ минимум связей с остальными модулями ■ проверяемость входных данных и результатов выполнения модуля.

2) формируются требования к модулям. Для каждой задачи выполняемой программы должна существовать цепочка последовательно выполняемых модулей, решающая данную задачу.

3) разрабатывается межмодульный интерфейс – правила вызова модулей, передачи им параметров и данных.

4) проводится комплексная отладка. В ходе отладки проверяется возможность совместной работы модулей, правильность решения всех задач ПП.

1. Понятие виртуальная машина и перечислить типы виртуализации.

**Виртуальная машина** – программная или аппаратная среда, исполняющая некоторый код (например, машинный код реального процессора), или спецификация системы (например: «виртуальная машина языка программирования Си»).

**Типы виртуализации:**

1) эмуляция оборудования

2) полная виртуализация

3) паравиртуализация

1. Причины использование виртуальных машин.

**Причины использования виртуальной машины:**

1) защита информации и ограничения возможностей процессов

2) для исследования производительности ПО или новой компьютерной архитектуры.

3) для эмуляции различных архитектур (например, эмулятор игровой приставки).

4) оптимизация использования ресурсов мощных компьютеров

5) для моделирования систем с клиент-серверной архитектурой на одной ЭВМ (эмуляция компьютерной сети с помощью нескольких виртуальных машин).

6) для упрощения управления кластерами – виртуальные машины могут мигрировать с одной физической машины на другую во время работы.

1. Понятие Образа диска и ISO- диска.

**Образ диска** – файл, содержащий в себе полную копию содержания и структуры файловой системы и данных, находящихся на диске.

**ISO-образ** – термин для обозначения образа оптического диска, содержащего файловую систему стандарта ISO 9660.

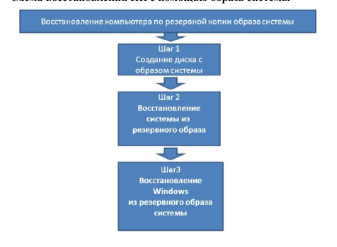
1. Использование образа диска.

1) распространение программного обеспечения. Образы дисков используются для распространения больших программных пакетов через интернет.

2) виртуальные диски. Образы дисков могут использоваться в качестве устройства хранения для эмуляторов и виртуальных машин.

3) тиражирование однотипных систем

1. Схема восстановления ПК с помощью образа системы.



1. Понятие Система обслуживания образов развертывания (DISM).

Система обслуживания образов развертывания (DISM) используется для изменения в образе Windows программ по умолчанию, связанных с расширениями имен файлов или протоколов.

1. Понятие групповой политики. Использование групповой политики в доменах Windows.

**Групповая политика** – совокупность параметров, используемых для конфигурирования рабочего окружения пользователя или компьютера.

**Групповая политика в доменах Windows применяется к основным категориям сетевых объектов:**

1) пользователи. Групповая политика регламентирует окружение конкретных пользователей независимо от того, на каком компьютере эти пользователи работают

2) компьютеры. Групповая политика определяет параметры системы, влияющие на окружение пользователей, для конкретных компьютеров независимо от того, какие пользователи на них работают.

1. Создание объекта групповой политики. Перечислить пункты консоли Объектов групповой политики.

Для создания объектов групповой политики используется специальная оснастка консоли управления Windows – mmc.

«Конфигурация пользователя» данный узел содержит элементы «Конфигурация программ» «Конфигурация Windows» и «Административные шаблоны»

«Конфигурация компьютера» Данный узел содержит подузлы «Конфигурация программ», «Конфигурация Windows» и «Административные шаблоны».

«Редактор объектов групповой политики» допускает добавление или удаление расширений.

1. Понятие Безопасный режим Windows 10. Применение безопасного режима работы.

**Безопасный режим Windows 10** – диагностический режим загрузки ОС, предназначенный для поиска и решения многих проблем в ОС с целью вернуть ее к работоспособному состоянию.

**Безопасный режим полезен для:**

1) удаления вирусов

2) исправления ошибок с драйверами, возникших из-за их несовершенства или неполной совместимости

3) устранения причины возникновения синих экранов и зависаний

4) удаления программ

5) тестирования совместимости ПП

6) восстановления системы

7) активации аккаунта администратора

1. Восстановление системы. Точки восстановления.

**Восстановление системы** – компонент ОС Windows, предназначенный для восстановления работоспособности ОС путем отката.

Точки восстановления создаются:

■ когда программа устанавливается с помощью Windows Installer, Package Installer или других установщиков

■ Windows Update устанавливает новые обновления

■ пользователь устанавливает драйвер без цифровой подписи Windows Hardware Quality Labs

■ система запускается, будучи отключенной более 24 ч

■ по требованию пользователя.

1. Понятие производительности ПК. Назовите наиболее характерные узкие места, снижающие производительность.

**Производительность компьютера** – скорость выполнения им операций.

**Узкие места, снижающие производительность:**

1) ЦП

2) память

3) подсистема ввода-вывода

4) неисправные компоненты

5) приложения.

1. Средства мониторинга и анализа производительности.

1) системный монитор Windows используется для анализа влияния работы программ на производительность компьютера в реальном времени и посредством сбора данных журнала для последующей обработки.

2) оценка производительности аппаратной части ПК – утилита обладает полной совместимостью с Windows 10.

3) монитор ресурсов – позволяет наблюдать статистику использования ресурсов компьютера.

4) журнал событий – способ записи и централизованного хранения об аппаратных и программных событиях.

1. Понятие Оптимизации ПК. 2 способа, с помощью которых можно произвести оптимизацию ПК.

**Оптимизация** – модификация компьютера для улучшения его эффективности работы.

**Оптимизацию компонентов компьютера можно произвести с помощью:** 1) BIOS. От системы ввода-вывода зависят надежность и стойкость работы системы, поэтому оптимизацию имеет смысл производить именно с BIOS. 2) программ для оптимизации ПК. Программы для оптимизации windows могут увеличить быстродействие и производительность системы, очистить реестр от устаревших записей, ошибок, мусора и неактуальных данных.

1. Приемы оптимизации.

1) устранение недостатков конструкции компьютера, негативно сказывающихся на его работе

2) оптимизация параметров BIOS – базовой системы ввода-вывода. Она управляет работой большинства ключевых компонентов системы, определяя их производительность

3) использование программ и утилит, позволяющих оптимизировать компоненты штатными средствами.

4) регулярная проверка жесткого диска: дефрагментация, выявление и устранение ошибок

5) оптимизация настроек ОС. Основные области оптимизации – настройка виртуальной памяти, работающих служб и автоматически запускаемых программ.

6) очистка системы от вирусов, троянов и вредоносного ПО

7) оптимизация количества и режима работы установленных в системе программ

8) выработка оптимальных приемов работы на ПК с ограниченными системными ресурсами.

1. Понятие Оптимизации сетевой инфраструктуры приложений.

**Оптимизация сетевой инфраструктуры приложений** – комплекс систем доставки приложений, которые работают вместе, чтобы обеспечить высокую доступность, лучшую производительность, безопасность приложений и управление доступом.

1. Понятие Конфликта оборудования. Какими тремя характерными признаками отличаются конфликты.

**Конфликты** – результат неудачно проведенной модернизации компьютера.

**Конфликты отличаются характерными признаками:**

1) в систему было установлено новое устройство или программа

2) проблема возникла после установки нового устройства или программы

3) до установки нового устройства или программы система работала нормально.

1. Перечислите основные признаки конфликтов.

■ компьютер зависает в процессе выполнения POST или инициализации ОС

■ система зависает при выполнении прикладной программы

■ система зависает при использовании конкретного устройства

■ компьютер зависает без предупреждения и независимо от исполняемой программы

■ компьютер может и не зависать, но новое устройство не работает.

■ компьютер может не зависать, но устройства или программы, ранее работавшие нормально, теперь не функционируют

1. Основное правило разрешения конфликта и быстрый способ его устранения.

Основное правило разрешения конфликта: то, что было подключено последним, отключается первым. Самым быстрым способом устранения конфликта является удаление из системы устройства или программы, которая его вызвала.

1. Программные конфликты. Аппаратные конфликты.

**Аппаратные конфликты** – конфликты, не приводящие к полной потере работоспособности системы.

**Программные конфликты** – ситуация, возникающая в результате несовместимости результатов действий различных программ/алгоритмов.

1. Понятие Диагностики аппаратно-программных средств. Средства диагностики.

**Диагностика** – тестирование компонентов компьютера с целью выяснения соответствия их характеристик заявленным производителем, а также определения производительности (скорости работы) и сравнения показателей с эталонным оборудованием.

**Средства диагностики подразделяют на программные и сервисную диагностическую аппаратуру.**

Диагностическое ПО включает в себя стандартное ПО, встроенное в состав ОС, и сторонние утилиты.

К аппаратным средствам диагностики неисправностей СВТ относятся:

1) универсальные измерительные приборы (тестеры, осциллографы, мультиметры и др.)

2) сервисная аппаратура для СВТ.

1. Комплексные программы и специализированные программы диагностики.

**Комплексные программы** – предназначены для получения подробной информации об установленных компонентах, определения производительности и сравнения с эталонным оборудованием

**Специализированные** – позволяют получить наиболее полную информацию о компонентах, а также включать/отключать режимы работы, которые недоступны при помощи стандартных средств.

1. Классификация диагностических программ по их возможностям.

1) программы, тестирующие быстродействие и производительность системы

2) программы, проверяющие на наличие ошибок и конфликтов

3) информационные программы, выдающие информацию об устройстве

4) программы, позволяющие управлять работой устройства, изменять параметры.

1. Понятие сервера и рабочей станции, отчего зависит их конфигурация.

**Сервер** – специализированный многопользовательский мощный компьютер в средних и крупных информационных системах.

**Рабочая станция** – клиентские рабочие места в информационных системах, для которых применяют ПК.

**При расчете параметров технических средств учитывают:**

1) предполагаемые объемы баз данных

2) сложность алгоритмов обработки данных по каждой задаче

3) кол-во пользователей и интенсивность их работы с базой данных

4) требуемый уровень надежности всех элементов системы и др.

1. Аппаратные платформы компьютеров.

Платформа IBM. Платформа IBM-совместимых компьютеров включает в себя громадный спектр различных компьютеров, от домашних до сложных серверов.

Платформа Apple. Компания Apple делала ставку на закрытую архитектуру – комплектующие и программы для этих компьютеров выпускались небольшим числом авторизованных производителей. Компьютеры Macintosh стоили дороже PC-совместимых конкурентов, что, компенсировалось их высокой надежностью и удобством.

1. Понятие Серверное программное обеспечение. Принцип работы Серверное программное обеспечение.

**Серверное ПО** – программный компонент вычислительной системы, выполняющий обслуживающие функции по запросу клиента, предоставляя ему доступ к определенным ресурсам или услугам.

**Принцип работы:** Для взаимодействия с клиентом (или клиентами, если поддерживается одновременная работа с несколькими клиентами) сервер выделяет необходимые ресурсы (разделяемая память, сокет и др.) и ожидает запросы на открытие соединения (или запросы на предоставляемый сервис). В зависимости от типа ресурса сервер может обслуживать процессы в пределах одной компьютерной системы или процессы на других машинах через каналы передачи данных или сетевые соединения. Формат запросов клиента и ответов сервера определяется протоколом.

1. Перечислите виды серверов.
2. универсальные серверы
3. сервер маршрутизации
4. файл-серверы
5. Клиентское программное обеспечение. Компоненты клиентского ПО.

**Клиентское ПО** – ПО обеспечивающее доступ к ресурсам, расположенным на сетевом сервере.

**Компоненты клиентского ПО:**

1) редиректор – сетевое ПО, которое принимает запросы ввода-вывода для удаленных файлов, именованных каналов или почтовых слотов и переназначает их сетевым сервисам другого компьютера.

2) распределитель – часть ПО, управляющая присвоением букв накопителя локальным и удаленным сетевым ресурсам или разделяемым дисководам, что помогает во взаимодействии с сетевыми ресурсами.

3) имена UNC – стандартный способ именования сетевых ресурсов. Способные работать с UNC приложения и утилиты командной строки используют имена UNC вместо отображения сетевых дисков.

1. Сетевая операционная система. Главная задача сетевой ОС. Два класса сетевой ОС.

**Сетевая ОС** – ОС, которая обеспечивает обработку, хранение и передачу данных в информационной сети.

Главной задачей сетевой ОС являются **разделение ресурсов сети и администрирование сети**.

**Сетевые ОС, и сети подразделяются на 2 класса:** одноранговые и сети с выделенными серверами.

**Сети с выделенным сервером**. Если компьютер предоставляет свои ресурсы другим пользователям сети, то он играет роль сервера. При этом компьютер, обращающийся к ресурсам другой машины, является клиентом. Компьютер, работающий в сети, может выполнять функции клиента или сервера, либо совмещать обе эти функции. Если выполнение каких-либо серверных функций является основным назначением компьютера, то такой компьютер называется выделенным сервером. В зависимости от того какой ресурс сервера является разделяемым, он называется файл-сервером, факс-сервером, принт-сервером, сервером приложений, сервером базы данных, веб-сервером и др.

**Одноранговые сети**. В одноранговых сетях все компьютеры равны в правах доступа к ресурсам друг друга. Каждый пользователь может по своему желанию объявить какой-либо ресурс своего компьютера разделяемым, после чего другие пользователи могут его эксплуатировать. В таких сетях на всех компьютерах устанавливается одна и та же ОС, которая предоставляет всем компьютерам в сети равные возможности.

**Вопросы к дифференцированному зачету по МДК 04.02. Обеспечение качества функционирования компьютерных систем**

1. Понятие моделей качества. Назовите наиболее известные модели качества.

**Модели качества** – иерархические модели на основе критериев качества и связанных с ними показателей (метрик).

**Модели качества:**

1) модель МакКола

2) модель Боэма

3) модель качества ISO 9126

1. Категории моделей качества.

1) теоретические модели – основаны на гипотезе отношений между переменными качества.

2) модели управления данными – основаны на статистическом анализе.

3) комбинированная модель – интуиция исследователя используется для определения вида модели, а анализ данных применяется для определения констант модели качества.

1. Что такое Многоуровневый подход к моделям качества.

**Многоуровневый подход** – подход, который содержит число уровней 2 (модели МакКола и Боэма) или 3 (модели МакКола и Боэма + метрики).

1. Назовите характеристики качества.

1)использование (корректность, надежность, эффективность, целостность, практичность);

2)модификация (тестируемость, гибкость) – факторы качества, важные для разработки новой версии ПО;

3)переносимость – факторы качества, важные для переносимости ПП на другие аппаратные и программные платформы.

4)практичность – как легко, надежно и эффективно может быть использован пакет программ;

5)сопровождаемость – насколько легко изменить и протестировать пакет программ;

6)мобильность – как пакет программ может использоваться при изменении программных и аппаратных средств.

1. Понятие надежности.

**Надёжность** – свойство ПО сохранять значения параметров, характеризующих способность выполнять требуемые функции в заданных условиях применения.

1. Понятие сбоя. Виды сбоев.

**Сбой** – самоустраняющийся отказ или однократный отказ, устраняемый вмешательством оператора.

**Виды сбоев:**

• в системном ПО.

• в прикладном ПО

• возникающие вследствие непредусмотренного порядка действий пользователя при работе с системой.

1. Понятие отказа. Виды отказов.

**Отказ** – событие, при котором вся система или ее часть выходят из работоспособного состояния.

**Виды отказов:**

• ресурсный

• конструктивный

• производственный

• эксплуатационный

1. Что такое явный и скрытый отказ.

**Явный отказ** – отказ, обнаруживаемый визуально или штатными методами и средствами контроля и диагностирования при подготовке ПО к применению или в процессе его применения.

**Скрытый отказ** – отказ, не обнаруживаемый визуально или штатными методами и средствами контроля и диагностирования, но выявляемый при проведении технического обслуживания или методами диагностики.

1. Понятие Уязвимости ПО.

**Уязвимости ПО** – слабые стороны ПО, которые позволяют злоумышленнику нарушить его целостность, доступность и конфиденциальность.

1. Внутренние источники угроз надежности.

■системные ошибки проектирования – при постановке целей и задач создания ПС, при формулировке требований к функциям и характеристикам решения задач, определении условий и параметров внешней среды, в которой предстоит применять ПС

■алгоритмические ошибки – разработки при спецификации функций ПО, при определении структуры и взаимодействия компонентов комплексов программ, а также при использовании информации баз данных

■ошибки программирования в текстах программ и описаниях данных, также в документации на компоненты и ПО

■недостаточная эффективность используемых методов и средств оперативной защиты программ и данных от сбоев и отказов (и обеспечения надежности функционирования ПО в условиях негативных воздействий.)

1. Внешние дестабилизирующие факторы надежности.

■ошибки оперативного и обслуживающего персонала в процессе эксплуатации ПС

■искажения в каналах телекоммуникации информации, поступающей от внешних источников и передаваемой потребителям

■сбои и отказы в аппаратуре вычислительных средств

■изменения состава и конфигурации комплекса взаимодействующей аппаратуры информационной системы.

1. Основные методы предотвращения угроз надежности.

■предотвращение ошибок за счет структурного программирования

■сокрытие и дозированный доступ к данным со стороны

■отладка и диагностика выполнения ПО

■обработка исключительных ситуаций и локализация ошибок и сбоев

■восстановление программы после сбоя.

1. Назовите оперативные методы повышения надежности ПО.

1. временная избыточность – обеспечение запаса производительности вычислительной системы в целях выделения части этого запаса для контроля исполнения программ, их диагностики и реализации восстановления вычислительного процесса.

2. информационная избыточность – определение обрабатываемых программами данных, которые влияют на нормальное функционирование программного средства и требуют времени для восстановления.

3. программная избыточность – используется для контроля и обеспечения достоверности наиболее важных решений по обработке информации.

1. Способы обеспечения и повышения надежности ПО.

■усовершенствование технологии программирования (описание этапов программирования с помощью языка UML)

■ выбор алгоритмов, не чувствительных к нарушениям вычислительного процесса (использование алгоритмической избыточности)

■резервирование программ – N-версионное программирование

■верификация и валидация программ с последующей коррекцией.

1. Что такое Модель надежности ПО. Аналитические и Эмпирические модели надежности ПО.

**Модель надежности ПО** – математическая модель, построенная для оценки надежности ПС от известных или оцененных в ходе тестирования параметров.

**Аналитическая модель** – показатель надежности определяется на основании данных о поведении программы в процессе тестирования.

**Эмпирическая модель** – возможность предсказывать показатели надежности на основе данных о метрических свойствах программы.

1. Понятие Программная ошибка. Основная особенность процесса выявления ошибок в программах.

**Программная ошибка** – искажение работы программы, исходными эталонами для любого ПО являются спецификации требований заказчика, предъявляемых к сопровождаемым программам.

Важной особенностью процесса выявления ошибок в программах является отсутствие программы-эталона, которой должны соответствовать текст и результаты функционирования разрабатываемой программы.

1. Понятие первичных и вторичных ошибок.

**Вторичные ошибки** – обнаруживаемые при отладке и тестировании ПО.

**Первичные ошибки** – обнаруживаемые в результате функционирования программы.

1. Понятие: небольшие ошибки, умеренные ошибки, критические ошибки.

**Небольшие ошибки** – ошибки, на которые пользователь не обратит внимания при применении программного продукта вследствие отсутствия их проявления.

**Умеренные ошибки** влияют на конечного пользователя, но имеются слабые последствия или обходные пути, позволяющие сохранить функциональность ПП.

**Критические ошибки** – ошибки с высоким влиянием, останавливают выпуск версии программного продукта.

1. Предназначение математических моделей ошибок в программах.

Математические модели описывают закономерности изменения суммарного кол-ва вторичных ошибок в программах. Эти математические модели предназначены для оценки:

- надежности работы ПО в процессе отладки, испытаний и эксплуатации;

- числа ошибок, оставшихся не выявленными в анализируемых программах;

- времени, требующегося для обнаружения следующей ошибки в функционирующей программе;

- времени, необходимого для поиска всех ошибок с заданной вероятностью.

1. Понятие риска. Основная причина возникновения рисков.

**Риск** – возможность понести потери.

Причиной возникновения рисков являются неопределенности, существующие в проекте.

1. Понятие известные и неизвестные риски.

**Известные риски** – риски, которые определены и оценены, для которых возможно планирование.

**Неизвестные риски** – риски, которые не идентифицированы и не могут быть спрогнозированы.

1. Перечислить этапы Методики анализа рисков.

Этап 1. Подготовка исходных данных для анализа

Этап 2. Идентификация угроз и рисков качества ПО

Этап 3. Оценка опасности угроз и выбор мер для их сокращения

Этап 4. Устранение опасных рисков качества проекта

Этап 5. Контроль, мониторинг и утверждение допустимого риска качества проекта

1. Понятие Планирование реагирования на риски. Матрица компромиссов рисков.

**Планирование реагирования на риски** – определение процедур и методов по ослаблению отрицательных последствий рисковых событий и использованию возможных преимуществ.

Все риски оцениваются в матрице компромиссов:

|  |  |  |  |
| --- | --- | --- | --- |
| Риск | Последствия | Меры по предотвращению | Меры по минимизации |
|  |  |  |  |

1. Назовите преимущества программного обеспечения, способного к адаптации.

1. Способное к адаптации ПО решает широкий круг задач в интересах пользователей.

2. Вокруг адаптируемого приложения возникает сообщество людей (занимающихся адаптацией), которое заинтересовано в увеличении числа пользователей и распространении приложения.

1. Назовите технологии, которые можно применять при адаптации ПО.

1) Технология СОМ – технологический стандарт от компании Microsoft, предназначенный для создания ПО на основе взаимодействующих компонентов объекта, каждый из которых может использоваться во многих программах одновременно.

2) Технология VBA – позволяет решать проблемы адаптируемости приложений.

3) Технология ActiveX Scripting – предоставляет приложениям возможность запускать программы на скриптовых языках VBScript, JScript.

1. Что называется, компьютерным вирусом и вредоносной программой.

**Компьютерный вирус** – программа, способная внедряться в другие программы, хранящиеся на дисках запоминающих устройств компьютера и умеющая самовоспроизводиться.

**Вредоносная программа** – компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в КС.

1. Стадии вирусов

**Пассивная стадия** – вирус практически не проявляет себя, стараясь оставаться незаметным для пользователя.

**Активная стадия** – вирусная атака может начинаться одновременно на всех пораженных компьютерах или в разное время.

1. Какая программа называется "зараженной". Что называется, сигнатурой вируса.

Программа, внутри которой находится вирус, называется «зараженной».

Сигнатура вируса – программный код вируса (тело вируса).

1. Назовите этапы Жизненного цикла вируса.

1. Проникновение на компьютер

2. Активация вируса

3. Поиск объектов для заражения

4. Подготовка вирусных копий

5. Внедрение вирусных копий

1. Каковы последствия заражения компьютерным вирусом.

• медленная работа компьютера;

• невозможность загрузки ОС;

• исчезновение файлов и каталогов или искажение их содержимого;

• изменение даты и времени модификации файлов;

• изменение размеров файлов;

• увеличение количества файлов на диске;

• уменьшение размера свободной оперативной памяти;

• вывод на экран непредусмотренных сообщений или изображений;

• подача непредусмотренных звуковых сигналов;

• зависания и сбои в работе компьютера.

1. Как классифицируются вирусы по среде обитания.

**Файловые вирусы** – различными способами внедряются в выполняемые файлы, создают файлы-двойники, используют особенности организации файловой системы.

**Загрузочные вирусы** – записывают себя в загрузочный сектор диска, или в сектор, содержащий системный загрузчик винчестера, или меняют указатель на активный boot-сектор.

**Файлово-загрузочные** – заражают файлы и загрузочные сектора дисков.

**Макровирусы** – заражают файлы-документы и электронные таблицы популярных редакторов.

**Сетевые вирусы** – используют для распространения протоколы или команды компьютерных сетей и электронной почты.

1. Какие типы компьютерных вирусов выделяются по способу заражения.

**Резидентные вирусы** – оставляют свою резидентную часть, которая потом перехватывает обращение ОС к объектам заражения и внедряются в них.

**Не резидентные вирусы** – не заражают память компьютера неограниченное время.

1. Как классифицируются вирусы по степени опасности.

**Безвредные вирусы** – никак не влияют на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения).

**Неопасные вирусы** – влияние, которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми эффектами.

**Опасные вирусы** – могут привести к серьезным сбоям в работе компьютера.

**Очень опасные вирусы** – в алгоритм их работы заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть для работы компьютера информацию, записанную в системных областях памяти.

1. Как классифицируются вирусы по алгоритму функционирования.

**Простейшие вирусы** – вирусы, которые при распространении своих копий изменяют содержимое дисковых секторов или файлов, поэтому его легко обнаружить.

**Вирусы-невидимки** – файловый вирус, остающийся «невидимым» для антивирусных программ.

**Вирусы-черви** – разновидность вредоносной программы, распространяющейся через локальные и глобальные компьютерные сети.

**Троянские программы** – модули, присоединяемые к программам, распространяемым по сети, или «забрасываемые» в компьютер несанкционированным способом.

1. Назовите вирусоподобные программы.

К вредоносным программам относятся компьютерные вирусы, трояны, сетевые черви.

1. Какие методы защиты от компьютерных вирусов можно использовать.

1)не использовать сомнительные носители

2)ограничить доступ к файлам программ, устанавливая для них статус «только для чтения»

3)при работе в сети не вызывайте программы из памяти других компьютеров.

4)храните программы и данные на разных носителях.

5)не копируйте программы для собственных нужд со случайных копий.

6)имейте антивирусную программу

7)не заходить на сомнительные сайты и не скачивать оттуда информацию

1. Понятие антивирусная программа. Основные задачи антивирусных программ.

**Антивирусная программа** – программа для обнаружения компьютерных вирусов, а также нежелательных вредоносных программ и восстановления заражённых программами файлов и профилактики.

Основные задачи антивирусных программ:

•препятствование проникновению вирусов в компьютерную систему

•обнаружение наличия вирусов в компьютерной системе

•устранение вирусов из компьютерной системы без нанесения повреждений другим объектам системы

•минимизация ущерба от действий вирусов

1. Назовите Технологии обнаружения вирусов.

1. Сигнатурный анализ – метод обнаружения вирусов, заключающийся в проверке наличия в файлах сигнатур вирусов.

2. Технологии вероятностного анализа, которые подразделяются на 3 категории:

•Эвристический анализ

•Поведенческий анализ

•Анализ контрольных сумм

1. Факторы, определяющие качество антивирусных программ.

1. Надежность и удобство работы.

2. Качество обнаружения вирусов.

3. Существование версий антивируса под популярные платформы.

4. Скорость работы и полезные особенности, функции.

1. На какие виды можно подразделить антивирусные программы.

1) программы-детекторы;

2) программы-доктора или фаги;

3) программы-ревизоры;

4) программы-фильтры;

5) программы-вакцины или иммунизаторы.

1. Как действуют программы-детекторы, доктора, фаги?

**Детекторы** осуществляют поиск характерного для конкретного вируса кода в оперативной памяти и в файлах, и при обнаружении выдают сообщение.

**Доктора** – программа находит зараженные вирусами файлы и удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние.

**Фаги** осуществляют последовательный просмотр файлов на предмет нахождения в них вирусных программ. Если сигнатура вируса была обнаружена, то производится процедура удаления вирусного кода из тела программы или документа.

1. Каков принцип действия программ-ревизоров, программ-фильтров, программ- вакцин?

**Ревизоры** запоминают исходное состояние программ, каталогов и системных областей диска, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным.

**Программы-фильтры** – предназначены для обнаружения подозрительных действий при работе компьютера, характерных для вирусов.

**Вакцина** модифицирует программу или диск, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится.

1. Понятие межсетевой экран. Основная задача межсетевого экрана.

**Межсетевой экран** – комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа.

1. Возможности межсетевого экрана.

1) фильтрация доступа к незащищенным службам;

2) препятствование получению закрытой информации из защищенной подсети, а также внедрению в защищенную подсеть ложных данных с помощью уязвимых служб;

3) контроль доступа к узлам сети;

4) регистрирует попытки доступа извне и из внутренней сети, что позволяет вести учёт использования доступа в Интернет отдельными узлами сети;

5) регламентирование порядка доступа к сети;

6) уведомление о подозрительной деятельности, атаки на узлы сети или сам экран.

1. Понятие: традиционный сетевой (или межсетевой) экран, персональный сетевой экран, вырожденный случай.

**Традиционный сетевой** (или межсетевой) экран – программа (или часть ОС) на шлюзе (сервере, передающем трафик между сетями) или аппаратное решение, контролирующие входящие и исходящие потоки данных между подключенными сетями.

**Персональный сетевой экран** – программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа этого компьютера.

**Вырожденный случай** – использование традиционного сетевого экрана сервером, для ограничения доступа к собственным ресурсам.

1. Понятие политики ИБ. Уровни политики ИБ.

**Политика безопасности** – совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.

Верхний уровень – решения, затрагивающие организацию в целом.

Средний уровень – вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам.

1. Понятие идентификации. Виды идентификаторов.

**Идентификация** – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

**Виды идентификаторов:**

1. Набор символов (пароль, секретный ключ, персональный идентификатор), который пользователь запоминает или использует средства хранения

2. Физиологические параметры человека или особенности поведения (особенности работы на клавиатуре).

1. Понятие аутентификации и механизм аутентификации.

**Аутентификация** (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

**Механизм аутентификации:**

1) пользователь предоставляет системе свой личный идентификатор

2) система сравнивает полученный идентификатор со всеми хранящимися в ее базе идентификаторами

3) если результат сравнения успешный, то пользователь получает доступ к системе в рамках установленных полномочий

4) в случае отрицательного результата система сообщает об ошибке и предлагает повторно ввести идентификатор;

5) если пользователь превышает лимит ввода информации, система временно блокируется и выдается сообщение о несанкционированных действиях.

1. Понятие протоколирование и аудита.

**Протоколирование** – сбор и накопление информации о событиях, происходящих в информационной системе.

**Аудит** – анализ накопленной информации, проводимый в реальном времени или периодически.

1. Задачи протоколирования и аудита.

1) обеспечение подотчетности пользователей и администраторов

2) обеспечение возможности реконструкции последовательности событий

3) обнаружение попыток нарушений информационной безопасности

4) предоставление информации для выявления и анализа проблем

1. Методы аудита.

Статистические методы основаны на накоплении среднестатистических параметров функционирования подсистем и сравнении текущих параметров с ними.

Эвристические методы используют модели сценариев несанкционированных действий, которые описываются логическими правилами или модели действий, приводящие к несанкционированным действиям.

1. Понятие криптография и криптоанализ

**Криптография** – наука о способах преобразования информации с целью ее защиты от незаконных пользователей

**Криптоанализ** – наука о методах и способах вскрытия шифров

1. Применение криптографических методов защиты.

1)шифрование

2)цифровая подпись кода

3)управление идентичностью

4)управление авторством

5)доверенная платформа

6)построение VPN

7)разграничение доступа

8)защита от кражи носителя

9)уничтожение информации

1. Симметричные и асимметричные (с открытым ключом) криптосистемы.

1. Симметричные криптосистемы - способ шифрования, в котором для шифрования и дешифрования применяется один и тот же криптографический ключ.

2. Криптосистемы с открытым ключом – методика шифрования данных, с применением открытого и закрытого ключа.

1. Понятие Электронная цифровая подпись и ее применение.

**Электронная цифровая подпись** (ЭЦП) – ПО, подтверждающее достоверность информации документа, его реквизитов и факта подписания конкретным лицом.

Применение ЭЦП позволяет сократить время движения документов в процессе оформления отчетов и обмена документацией.

1. Понятие шифрование и дешифрование данных.

**Шифрование** – вид криптографического закрытия, при котором преобразованию подвергается каждый символ защищаемого сообщения.

**Дешифрование** – вид криптографического раскрытия, при котором преобразованию подвергается каждый символ защищаемого сообщения.

1. Понятие кодирование и рассечение-разнесение данных.

**Кодирование** – вид криптографического закрытия, когда элементы защищаемых данных заменяются выбранными кодами (цифровыми, буквенными, буквенно-цифровыми сочетаниями).

**Рассечение-разнесение данных** – массив защищаемых данных делится на элементы, каждый из которых не позволяет раскрыть содержание защищаемой информации.