Министерство образования Иркутской области
Государственное бюджетное профессиональное образовательное учреждение Иркутской области
«Иркутский авиационный техникум»

УТВЕРЖДАЮ
Директор
ГБПОУИО «ИАТ»
_____ Якубовский А.Н.
«31» мая 2018 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

ОП.08 Информационные технологии в профессиональной деятельности

специальности

24.02.01 Производство летательных аппаратов

Иркутск, 2018

Рассмотрена
цикловой комиссией
С протокол №16 от 23.05.2018
г.

Председатель ЦК

/В.К. Задорожный /

№	Разработчик ФИО
1	Букова Ольга Михайловна

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Область применения фонда оценочных средств (ФОС)

ФОС по дисциплине является частью программы подготовки специалистов среднего звена по специальности 24.02.01 Производство летательных аппаратов

1.2. Место дисциплины в структуре ППССЗ:

ОП.00 Общепрофессиональный цикл.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины

В результате освоения дисциплины обучающийся должен	№ дидактической единицы	Формируемая дидактическая единица
Знать	1.1	основные понятия автоматизированной обработки информации;
	1.2	общий состав и структуру персональных компьютеров и вычислительных систем;
	1.3	состав, функции и возможности использования информационных и телекоммуникационных технологий в профессиональной деятельности;
	1.4	методы и средства сбора, обработки, хранения, передачи и накопления информации;
	1.5	базовые системные программные продукты и пакеты прикладных программ в области профессиональной деятельности;
	1.6	основные методы и приемы обеспечения информационной безопасности
Уметь	2.1	использовать технологии сбора, размещения, хранения, накопления, преобразования и передачи данных в профессионально ориентированных информационных системах;
	2.2	использовать в профессиональной деятельности различные виды программного обеспечения, в т.ч. специального;
	2.3	применять компьютерные и коммуникационные средства;

	2.4	уметь выполнять ассоциативные чертежи на основе созданных 3D моделей с необходимым числом видов, разрезов, сечений.
	2.5	оформлять ассоциативные чертежи, наносить размеры, заполнять технические требования
	2.6	уметь создавать компоненты сборки, накладывать зависимости совмещения, проводить анализ на пространственное пересечение компонентов

1.4. Формируемые компетенции:

ОК.1 Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК.2 Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК.3 Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК.4 Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.
ОК.5 Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК.6 Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК.8 Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ПК.1.1 Анализировать объект производства: конструкцию летательного аппарата, агрегатов, узлов, деталей, систем, конструкторскую документацию на их изготовление и монтаж.
ПК.2.1 Анализировать техническое задание для разработки конструкции несложных деталей и узлов изделия и оснастки. Производить увязку и базирование элементов изделий и оснастки по технологической цепочке их изготовления и сборки.
ПК.2.2 Выбирать конструктивное решение узла.
ПК.2.3 Выполнять необходимые типовые расчеты при конструировании.
ПК.2.4 Разрабатывать рабочий проект деталей и узлов в соответствии с требованиями ЕСКД.
ПК.3.2 Проверять качество выпускаемой продукции и/или выполняемых работ.

2. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ, ИСПОЛЬЗУЕМЫЙ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

2.1 Текущий контроль (ТК) № 1

Тема занятия: 2.1.4.Типы файлов и шаблоны в Inventor
Метод и форма контроля: Письменный опрос (Опрос)
Вид контроля: проверочная работа
Дидактическая единица: 1.1 основные понятия автоматизированной обработки информации;
Занятие(-я):
1.1.1.Введение. Общий состав и структура персональных компьютеров и вычислительных систем. Методы и средства сбора,обработки, хранения, передачи и накопления информации.
Задание №1
Дать ответы на вопросы

1. Сто называется информационным процессом? Что такое сбор информации?
2. Что такое формализация данных? Что такое фильтрация данных?
3. Что такое сортировка данных? Что такое защита данных?
4. Что такое архивация данных? Что такое транспортировка данных?

5. Что такое преобразование данных?

Оценка	*Показатели оценки*
3	получены правильные ответы на три вопроса
4	получены правильные ответы на четыре вопроса
5	получены правильные ответы на все вопросы

Дидактическая единица: 1.3 состав, функции и возможности использования информационных и телекоммуникационных технологий в профессиональной деятельности;
Занятие(-я):
2.1.1.Профессионально ориентированные информационные системы. Базовые системные программные продукты и пакеты прикладных программ в области профессиональной деятельности.
Задание №1

1. Перечислить задачи, решаемые САПР на стадиях проектирования и

подготовки производства.

2. Перечислить программы, используемые при машиностроительном проектировании.
3. Перечислить функции CAD-систем.

Оценка	***Показатели оценки***

3	Получен ответ на один вопрос из трех представленных: 1. Перечислить задачи, решаемые САПР на стадиях проектирования и подготовки производства. 2. Перечислить современные системы автоматизированного проектирования. 3. Основная цель создания САПР — повышение эффективности труда инженеров, включая: • сокращения трудоемкости проектирования и планирования; • сокращения сроков проектирования; • сокращения себестоимости проектирования; • повышения качества и технико-экономического уровня результатов проектирования; • сокращения затрат на натурное моделирование и испытания. В России и странах СНГ наиболее широко распространены: • программный пакет **AutoCAD** • **КОМПАС** - система автоматизированного проектирования, разработанная российской компанией <АСКОН> с возможностями оформления проектной и конструкторской документации согласно стандартам серии ЕСКД и СПДС. Существует в двух версиях: КОМПАС-График и КОМПАС-3D, соответственно предназначенных для плоского черчения и трехмерного проектирования. • **Autodesk Inventor** — система трехмерного твердотельного проектирования для разработки сложных машиностроительных изделий. Функции CAD-систем в машиностроении подразделяют на функции двухмерного*(2D)* и трехмерного *(3D)* проектирования. К функциям *2D* относятся черчение, оформление конструкторской документации; к функциям *3D* — получение трехмерных моделей, метрические расчеты, реалистичная визуализация, взаимное преобразование*2D* и *3D* моделей.

4	Получен ответ на два вопроса из трех представленных: 1. Перечислить задачи, решаемые САПР на стадиях проектирования и подготовки производства. 2. Перечислить современные системы автоматизированного проектирования. 3. Основная цель создания САПР — повышение эффективности труда инженеров, включая: • сокращения трудоемкости проектирования и планирования; • сокращения сроков проектирования; • сокращения себестоимости проектирования; • повышения качества и технико-экономического уровня результатов проектирования; • сокращения затрат на натурное моделирование и испытания. В России и странах СНГ наиболее широко распространены: • программный пакет **AutoCAD** • **КОМПАС** - система автоматизированного проектирования, разработанная российской компанией <АСКОН> с возможностями оформления проектной и конструкторской документации согласно стандартам серии ЕСКД и СПДС. Существует в двух версиях: КОМПАС-График и КОМПАС-3D, соответственно предназначенных для плоского черчения и трехмерного проектирования. • **Autodesk Inventor** — система трехмерного твердотельного проектирования для разработки сложных машиностроительных изделий. Функции CAD-систем в машиностроении подразделяют на функции двухмерного*(2D)* и трехмерного *(3D)* проектирования. К функциям *2D* относятся черчение, оформление конструкторской документации; к функциям *3D* — получение трехмерных моделей, метрические расчеты, реалистичная визуализация, взаимное преобразование*2D* и *3D* моделей.

5	Получен ответ на три вопроса из трех представленных: 1. Перечислить задачи, решаемые САПР на стадиях проектирования и подготовки производства. 2. Перечислить современные системы автоматизированного проектирования. 3. Основная цель создания САПР — повышение эффективности труда инженеров, включая: • сокращения трудоемкости проектирования и планирования; • сокращения сроков проектирования; • сокращения себестоимости проектирования; • повышения качества и технико-экономического уровня результатов проектирования; • сокращения затрат на натурное моделирование и испытания. В России и странах СНГ наиболее широко распространены: • программный пакет **AutoCAD** • **КОМПАС** - система автоматизированного проектирования, разработанная российской компанией <АСКОН> с возможностями оформления проектной и конструкторской документации согласно стандартам серии ЕСКД и СПДС. Существует в двух версиях: КОМПАС-График и КОМПАС-3D, соответственно предназначенных для плоского черчения и трехмерного проектирования. • **Autodesk Inventor** — система трехмерного твердотельного проектирования для разработки сложных машиностроительных изделий. Функции CAD-систем в машиностроении подразделяют на функции двухмерного*(2D)* и трехмерного *(3D)* проектирования. К функциям *2D* относятся черчение, оформление конструкторской документации; к функциям *3D* — получение трехмерных моделей, метрические расчеты, реалистичная визуализация, взаимное преобразование*2D* и *3D* моделей.

2.2 Текущий контроль (ТК) № 2

Тема занятия: 2.1.14.Создание 3d модели используя команды Наклон и Оболочка.
Метод и форма контроля: Практическая работа (Сравнение с аналогом)
Вид контроля: Практическая работа с использованием ИКТ
Дидактическая единица: 1.2 общий состав и структуру персональных компьютеров и вычислительных систем;
Занятие(-я):
1.1.1.Введение. Общий состав и структура персональных компьютеров и вычислительных систем. Методы и средства сбора,обработки, хранения, передачи и накопления информации.
2.1.4.Типы файлов и шаблоны в Inventor
Задание №1

1. Перечислить состав персонального компьютера
2. Перечислить устройств ввода информации
3. Перечислить устройства вывода информации
4. Что понимается под архитектурой компьютера?
5. Что такое алгоритм и программа для ПК?

Оценка	***Показатели оценки***
3	получены правильные ответы на три вопроса
4	получены правильные ответы на четыре вопроса
5	получены правильные ответы на все вопросы

Дидактическая единица: 1.6 основные методы и приемы обеспечения информационной безопасности
Занятие(-я):
1.1.1.Введение. Общий состав и структура персональных компьютеров и вычислительных систем. Методы и средства сбора,обработки, хранения, передачи и накопления информации.
Задание №1

1. Что такое информационная безопасность?
2. Перечислить основные методы информационной безопасности. Перечислить основные организационно технические методы обеспечения информационной безопасности.
3. На какие классы можно разделить методы обеспечения информационной

безопасности

Оценка	***Показатели оценки***
3	Получен ответ на один вопрос из трех представленных: 1. Информационная безопасность это совокупность деятельности по недопущению вреда свойствам объекта безопасности обусловливаемым информацией и информационной инфраструктурой и субъектов а также средств этой деятельности. 2. Методы обеспечения информационной безопасности: • организационно правовые методы,(документы, регламентирующие все аспекты обеспечения информационной безопасности) • организационно технические методы.(Этот процесс никогда не закончится, так как совершенствуются методы нарушения информационной безопасности.) Перечислены основные организационно технические методы обеспечения информационной безопасности: 1. Авторизация. (позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.) 2. Иденификация и аутентификация.(Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам. Аутентификация-проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д.) 3. Экранирование – разделение информационных потоков между различными информационными системами. 4. Физическая защита. 1. Физические устройства доступности к сетевым узлам и линиям связи. 2. Противопожарные меры

3. Защита поддержки инфраструктуры (электропитание, кондиционирование…)
4. Защита мобильных и радио систем.
5. Защита от перехвата данных.

5. Поддержка текущей работоспособности.
    1. Резервное копирование.
    2. Управление носителями.
    3. Регламентированные работы.

В международных стандартах выделяют 7 классов безопасности систем, которые объединены в 4 уровня:
D — нулевой уровень безопасности;
C — системы с произвольным доступом;
B — системы с принудительным доступом;
A — системы с верифицируемой безопасностью.
Уровню D соответствуют системы, в которых слабо развита технология защиты. При такой ситуации любое постороннее лицо имеет возможность получить доступ к сведениям. Использование слаборазвитой технологии защиты чревато потерей или утратой сведений.
В уровне C есть следующие классы — C1 и C2. Класс безопасности C1 предполагает разделение данных и пользователей. Определенная группа пользователей имеет доступ только к определенным данным, для получения сведений необходима аутентификация — проверка подлинности пользователя путем запроса пароля. При классе безопасности C1 в системе имеются аппаратные и программные средства защиты. Системы с классом C2 дополнены мерами, гарантирующими ответственность пользователей: создается и поддерживается журнал регистрации доступа.
Уровень B включает технологии обеспечения безопасности, которые имеют классы уровня C, плюс несколько дополнительных. Класс B1 предполагает наличие политики безопасности, При классе B1 специалисты осуществляют тщательный анализ и тестирование исходного кода и архитектуры. Класс безопасности B2 характерен для многих современных систем и предполагает: Снабжение метками секретности всех ресурсов системы; Формальную политику безопасности; Высокую устойчивость систем к внешним атакам. Класс B3 предполагает, в дополнение к классу B1, оповещение

администратора о попытках нарушения политики безопасности, анализ появления тайных каналов, наличие механизмов для восстановления данных после сбоя в работе аппаратуры или программного обеспечения.
Уровень А включает один, наивысший класс безопасности — А. К данному классу относятся системы, прошедшие тестирование и получившие подтверждение соответствия формальным спецификациям верхнего уровня.

- Экранирование – разделение информационных потоков между различными информационными системами.
- Физическая защита.
    1. Физические устройства доступности к сетевым узлам и линиям связи.
    2. Противопожарные меры
    3. Защита поддержки инфраструктуры (электропитание, кондиционирование…)
    4. Защита мобильных и радио систем.
    5. Защита от перехвата данных.
- Поддержка текущей работоспособности.
    1. Резервное копирование.
    2. Управление носителями.
    3. Регламентированные работы.

Перечислены основные методы обеспечения информационной безопасности:

1. Авторизация. (позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.)
2. Иденификация и аутентификация.(Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам. Аутентификация-проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д.)
3. Информационная безопасность это совокупность деятельности по недопущению вреда свойствам объекта

	безопасности обусловливаемым информацией и информационной инфраструктурой и субъектов а также средств этой деятельности. Методы обеспечения информационной безопасности 4. организационно правовые методы,(документы, регламентирующие все аспекты обеспечения информационной безопасности) 5. организационно технические методы.(Этот процесс никогда не закончится, так как совершенствуются методы нарушения информационной безопасности.)
4	Получен ответ на два вопроса из трех представленных: 1. Информационная безопасность это совокупность деятельности по недопущению вреда свойствам объекта безопасности обусловливаемым информацией и информационной инфраструктурой и субъектов а также средств этой деятельности. Методы обеспечения информационной безопасности 2. организационно правовые методы,(документы, регламентирующие все аспекты обеспечения информационной безопасности) 3. организационно технические методы.(Этот процесс никогда не закончится, так как совершенствуются методы нарушения информационной безопасности.) 4. Перечислены основные методы обеспечения информационной безопасности: 5. Авторизация. (позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.) 6. Иденификация и аутентификация.(Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам. Аутентификация-проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д.)

7. Экранирование – разделение информационных потоков между различными информационными системами.
8. Физическая защита.
    1. Физические устройства доступности к сетевым узлам и линиям связи.
    2. Противопожарные меры
    3. Защита поддержки инфраструктуры (электропитание, кондиционирование…)
    4. Защита мобильных и радио систем.
    5. Защита от перехвата данных.
9. Поддержка текущей работоспособности.
    1. Резервное копирование.
    2. Управление носителями.
    3. Регламентированные работы

Перечислены основные методы обеспечения информационной безопасности:

1. В международных стандартах выделяют 7 классов безопасности систем, которые объединены в 4 уровня:
   D — нулевой уровень безопасности;
   C — системы с произвольным доступом;
   B — системы с принудительным доступом;
   A — системы с верифицируемой безопасностью.
   Уровню D соответствуют системы, в которых слабо развита технология защиты. При такой ситуации любое постороннее лицо имеет возможность получить доступ к сведениям. Использование слаборазвитой технологии защиты чревато потерей или утратой сведений.
   В уровне C есть следующие классы — C1 и C2. Класс безопасности C1 предполагает разделение данных и пользователей. Определенная группа пользователей имеет доступ только к определенным данным, для получения сведений необходима аутентификация — проверка подлинности пользователя путем запроса пароля. При классе безопасности C1 в системе имеются аппаратные и программные средства защиты. Системы с классом C2 дополнены мерами, гарантирующими ответственность

пользователей: создается и поддерживается журнал регистрации доступа.
Уровень B включает технологии обеспечения безопасности, которые имеют классы уровня C, плюс несколько дополнительных. Класс B1 предполагает наличие политики безопасности, При классе B1 специалисты осуществляют тщательный анализ и тестирование исходного кода и архитектуры. Класс безопасности B2 характерен для многих современных систем и предполагает: Снабжение метками секретности всех ресурсов системы; Формальную политику безопасности; Высокую устойчивость систем к внешним атакам. Класс B3 предполагает, в дополнение к классу B1, оповещение администратора о попытках нарушения политики безопасности, анализ появления тайных каналов, наличие механизмов для восстановления данных после сбоя в работе аппаратуры или программного обеспечения.
Уровень A включает один, наивысший класс безопасности — A. К данному классу относятся системы, прошедшие тестирование и получившие подтверждение соответствия формальным спецификациям верхнего уровня.

2. Экранирование – разделение информационных потоков между различными информационными системами.
3. Физическая защита.
    1. Физические устройства доступности к сетевым узлам и линиям связи.
    2. Противопожарные меры
    3. Защита поддержки инфраструктуры (электропитание, кондиционирование…)
    4. Защита мобильных и радио систем.
    5. Защита от перехвата данных.
4. Поддержка текущей работоспособности.
    1. Резервное копирование.
    2. Управление носителями.
    3. Регламентированные работы.
5. Авторизация. (позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.)

	6. Иденификация и аутентификация.(Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам. Аутентификация-проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д.) 7. Информационная безопасность это совокупность деятельности по недопущению вреда свойствам объекта безопасности обусловливаемым информацией и информационной инфраструктурой и субъектов а также средств этой деятельности. Методы обеспечения информационной безопасности 8. организационно правовые методы,(документы, регламентирующие все аспекты обеспечения информационной безопасности) 9. организационно технические методы.(Этот процесс никогда не закончится, так как совершенствуются методы нарушения информационной безопасности.)
5	Получен ответ на три вопроса из трех представленных: 1. Информационная безопасность это совокупность деятельности по недопущению вреда свойствам объекта безопасности обусловливаемым информацией и информационной инфраструктурой и субъектов а также средств этой деятельности. Методы обеспечения информационной безопасности 2. организационно правовые методы,(документы, регламентирующие все аспекты обеспечения информационной безопасности) 3. организационно технические методы.(Этот процесс никогда не закончится, так как совершенствуются методы нарушения информационной безопасности.) 4. Перечислены основные методы обеспечения информационной безопасности: 5. Авторизация. (позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к

сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.)

6. Иденификация и аутентификация.(Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам. Аутентификация-проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д.)
7. Экранирование – разделение информационных потоков между различными информационными системами.
8. Физическая защита.
    1. Физические устройства доступности к сетевым узлам и линиям связи.
    2. Противопожарные меры
    3. Защита поддержки инфраструктуры (электропитание, кондиционирование…)
    4. Защита мобильных и радио систем.
    5. Защита от перехвата данных.
9. Поддержка текущей работоспособности.
    1. Резервное копирование.
    2. Управление носителями.
    3. Регламентированные работы.

Информационная безопасность это совокупность деятельности по недопущению вреда свойствам объекта безопасности обусловливаемым информацией и информационной инфраструктурой и субъектов а также средств этой деятельности.
Методы обеспечения информационной безопасности

1. организационно правовые методы,(документы, регламентирующие все аспекты обеспечения информационной безопасности)
2. организационно технические методы.(Этот процесс никогда не закончится, так как совершенствуются методы нарушения информационной безопасности.)

Перечислены основные методы обеспечения информационной безопасности:

- Авторизация. (позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.)
- Иденификация и аутентификация.(Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам. Аутентификация-проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д.)
- Экранирование – разделение информационных потоков между различными информационными системами.
- Физическая защита.
    1. Физические устройства доступности к сетевым узлам и линиям связи.
    2. Противопожарные меры
    3. Защита поддержки инфраструктуры (электропитание, кондиционирование…)
    4. Защита мобильных и радио систем.
    5. Защита от перехвата данных.
- Поддержка текущей работоспособности.
    1. Резервное копирование.
    2. Управление носителями.
    3. Регламентированные работы.

В международных стандартах выделяют 7 классов безопасности систем, которые объединены в 4 уровня:
D — нулевой уровень безопасности;
C — системы с произвольным доступом;
B — системы с принудительным доступом;
A — системы с верифицируемой безопасностью.
Уровню D соответствуют системы, в которых слабо развита технология защиты. При такой ситуации любое постороннее лицо имеет возможность получить доступ к сведениям. Использование слаборазвитой технологии защиты чревато потерей или утратой сведений.
В уровне C есть следующие классы — C1 и C2. Класс безопасности C1 предполагает разделение данных и пользователей. Определенная группа пользователей имеет доступ только к определенным данным, для получения сведений

	необходима аутентификация — проверка подлинности пользователя путем запроса пароля. При классе безопасности С1 в системе имеются аппаратные и программные средства защиты. Системы с классом С2 дополнены мерами, гарантирующими ответственность пользователей: создается и поддерживается журнал регистрации доступа. Уровень В включает технологии обеспечения безопасности, которые имеют классы уровня С, плюс несколько дополнительных. Класс В1 предполагает наличие политики безопасности, При классе В1 специалисты осуществляют тщательный анализ и тестирование исходного кода и архитектуры. Класс безопасности В2 характерен для многих современных систем и предполагает: Снабжение метками секретности всех ресурсов системы; Формальную политику безопасности; Высокую устойчивость систем к внешним атакам. Класс В3 предполагает, в дополнение к классу В1, оповещение администратора о попытках нарушения политики безопасности, анализ появления тайных каналов, наличие механизмов для восстановления данных после сбоя в работе аппаратуры или программного обеспечения. Уровень А включает один, наивысший класс безопасности — А. К данному классу относятся системы, прошедшие тестирование и получившие подтверждение соответствия формальным спецификациям верхнего уровня.

Дидактическая единица: 2.1 использовать технологии сбора, размещения, хранения, накопления, преобразования и передачи данных в профессионально ориентированных информационных системах;

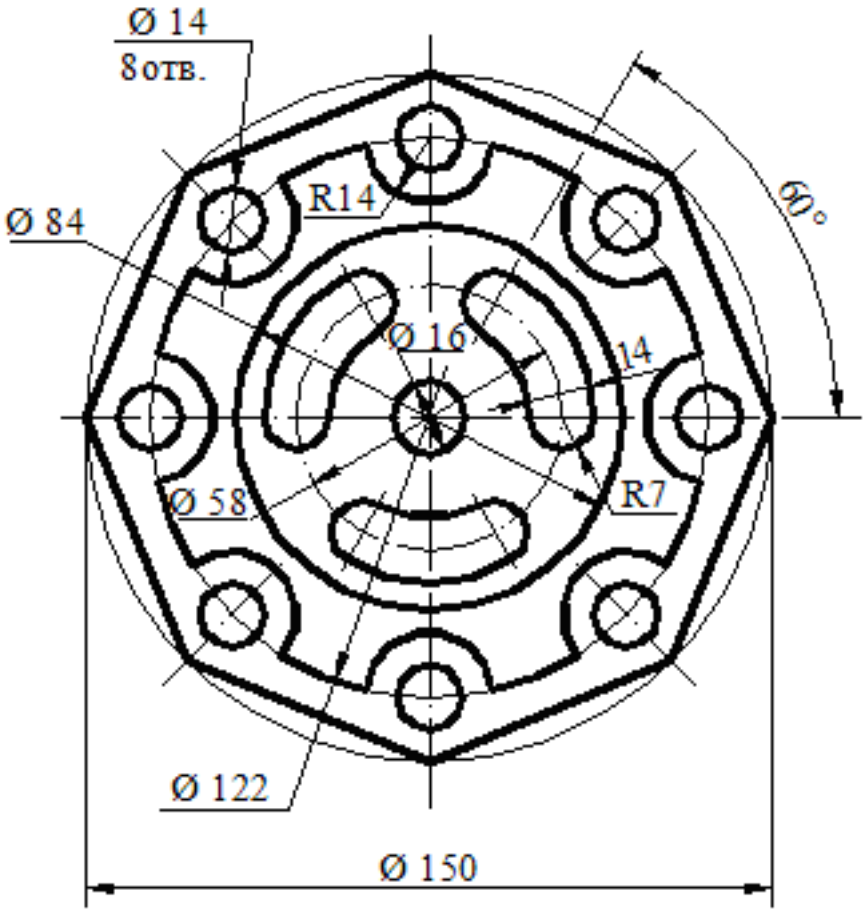
Занятие(-я):

1.1.1.Введение. Общий состав и структура персональных компьютеров и вычислительных систем. Методы и средства сбора,обработки, хранения, передачи и накопления информации.

2.1.1.Профессионально ориентированные информационные системы. Базовые системные программные продукты и пакеты прикладных программ в области профессиональной деятельности.

Задание №1

Вычертить контур плоской детали с элементами деления окружности, сопряжений, нанесением размеров (Задания выдаются по вариантам).



Оценка	*Показатели оценки*
3	1. На созданном по умолчанию формате листа построены элементы чертежа не требующие дополнительных построений. 2. Построены сопряжения, и выполнено деление окружности на равные части используя соответствующие инструменты САПР. 3. Нанесены размеры согласно ГОСТ 2.307-2011. 4. Заполнена основная надпись.
4	1. Выбран масштаб детали. 2. Выбран формат листа в зависимости от масштаба детали. 3. Построены элементы чертежа не требующие дополнительных построений. 4. Построены сопряжения, и выполнено деление окружности на равные части используя соответствующие инструменты САПР. 5. Построены центровые линии. 6. Нанесены размеры согласно ГОСТ 2.307-2011. 7. Заполнена основная надпись

5	1. Выбран масштаб детали. 2. Измен формат листа в зависимости от масштаба детали с помощью инструмента Редактировать лист выбранного из контекстного меню Раскладка. 3. Построены элементы чертежа не требующие дополнительных построений. 4. Построены сопряжения, и выполнено деление окружности на равные части используя соответствующие инструменты САПР. 5. Построены центровые и осевые линии используя соответствующие инструменты САПР. 6. Нанесены размеры согласно ГОСТ 2.307-2011. 7. Заполнена основная надпись.

2.3 Текущий контроль (ТК) № 3

Тема занятия: 2.1.23.Создание чертежа детали Вал. Создание чертежа детали Плита. Создание чертежа детали Рычаг. Создание чертежа детали из листового металла. в Autodesk Inventor.

Метод и форма контроля: Практическая работа (Информационно-аналитический)

Вид контроля: практическая работа с использованием ИКТ

Дидактическая единица: 1.5 базовые системные программные продукты и пакеты прикладных программ в области профессиональной деятельности;

Занятие(-я):

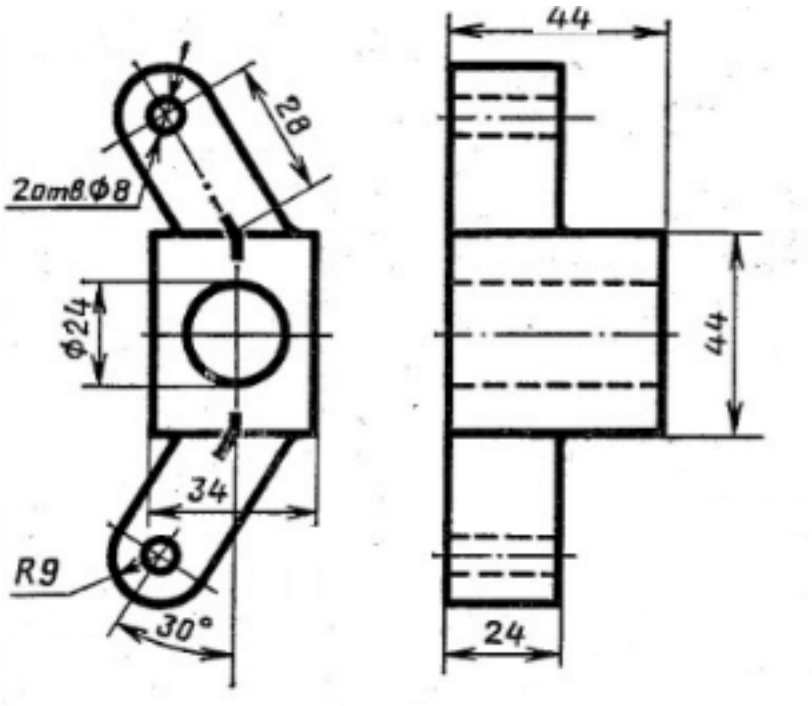
2.1.1.Профессионально ориентированные информационные системы. Базовые системные программные продукты и пакеты прикладных программ в области профессиональной деятельности.

2.1.2.Интерфейс Autodesk Inventor 2016. Зависимости в Autodesk Inventor 2016.

2.1.3.Разделы справки в Autodesk Inventor .

2.1.8.Команды редактирования: Перенос, Копировать, Поворот, Команды редактирования: Обрезать, Удлинить, Разделить; редактирование эскиза в Autodesk Inventor.

Задание №1



Построить 3D модель детали Распорка используя команды редактирования: Обрезать, Удлинить,Повернуть, Перенос;

Оценка	*Показатели оценки*
3	Построена 3D модель детали Распорка без использования команд редактирования: Обрезать, Удлинить,Повернуть, Перенос;
4	Построена 3D модель детали Распорка с частичным использования команд редактирования;
5	Построена 3D модель детали Распорка с использованием команды редактирования: Обрезать, Удлинить,Повернуть, Перенос;

Дидактическая единица: 2.3 применять компьютерные и коммуникационные средства;

Занятие(-я):

2.1.10.Выполнение практического задания №1. Выполнение практического задания №2 в Autodesk Inventor.

2.1.18.Создание 3d модели используя команду Пружина, Рельеф, Массив вдоль кривой.

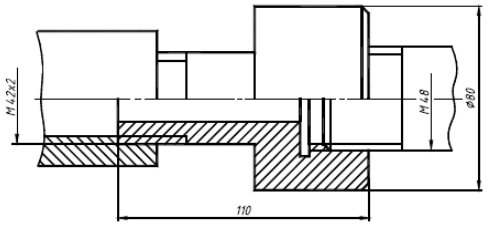
2.1.19.Создание 3 D моделей с использованием различных типов скруглений: полное круговое сопряжение и сопряжение с переменным радиусом.

2.1.20.Создание простой детали. Создание детали средней сложности.

Задание №1

1. Ответить на вопрос: что такое *компьютерные коммуникации*
2. Начертить резьбовое соединение в по приведенному описанию, нанести размеры резьбы, габаритные размеры и оформить изображение в виде рабочего чертежа на формате А4.

Деталь цилиндрической формы расположена горизонтально. Левая часть детали – цилиндр 42 мм, длиной 60 мм. На нем с левой стороны на длину 35 мм нарезана метрическая резьба с мелким шагом 2 мм. Правая часть – цилиндр 80 мм, длиной 60 мм. Слева направо в детали проходит цилиндрическое отверстие 16 мм. Справа налево в детали просверлено отверстие 48 мм и глубиной 30 мм, в котором нарезана метрическая резьба с круп-ным шагом. Отверстие заканчивается канавкой 52 мм и шири-ной 5 мм. На цилиндр 42 мм навернута на глубину 15 мм втул-ка 60 мм, в которой на всю длину нарезана резьба. Длина втул-ки не задается, и она показывается на чертеже с обрывом. В от-верстие 48 мм с правой стороны ввернут на глубину 20 мм стержень, на котором нарезана резьба на длину 30 мм. Длина са-мого стержня не задается, и он показывается на чертеже с обры-вом. Цилиндр 80 мм с правой стороны имеет фаску размером 3 мм под углом 45о. Стержень 48 мм с левой стороны имеет фас-ку размером 2 мм под углом 45о.



Оценка	*Показатели оценки*
3	Начерчено резьбовое соединение в по приведенному описанию
4	Начерчено резьбовое соединение в по приведенному описанию нанесены размеры
5	Начерчено резьбовое соединение по приведенному описанию правильно нанесены размеры, получен правильный ответ на вопрос

1. Пример выполнения задания показан на рис.

2.4 Текущий контроль (ТК) № 4

Тема занятия: 2.1.27.Создание чертежа Плиты нижней, чертежа Прокладки,

чертежа Плиты верхней.
Метод и форма контроля: Практическая работа (Информационно-аналитический)
Вид контроля: Практическая работа с использованием ИКТ
Дидактическая единица: 2.2 использовать в профессиональной деятельности различные виды программного обеспечения, в т.ч. специального;
Занятие(-я):
2.1.5.Создание простого параметрического эскиза в Autodesk Inventor.
2.1.6.Создание параметрического эскиза средней сложности в Autodesk Inventor.
2.1.7.Создание сложного параметрического эскиза в Autodesk Inventor.
2.1.8.Команды редактирования: Перенос, Копировать, Поворот, Команды редактирования: Обрезать, Удлинить, Разделить; редактирование эскиза в Autodesk Inventor.
2.1.9.Команды: Масштаб, Растянуть, Смещение, Круговой массив, Прямоугольный массив, Зеркальное отражение в Autodesk Inventor.
2.1.11.Создание детали типа призма, создание 3d модели типа Вал в Autodesk Inventor.
2.1.12.Создание 3D модели Крышка в Autodesk Inventor.
2.1.13.Создание 3d модели используя команду Сдвиг в Autodesk Inventor.
2.1.15.Создание рабочих плоскостей. Создание рабочих точек и осей в Autodesk Inventor.
2.1.16.Создание 3d модели используя команда Лофт (создание элементов по сечениям).
2.1.17.Создание 3d модели используя команду Проецирование геометрии.
2.1.21.Создание 3D модели сложной детали.
2.1.22.Создание детали из листового металла.
2.1.23.Создание чертежа детали Вал. Создание чертежа детали Плита. Создание чертежа детали Рычаг. Создание чертежа детали из листового металла. в Autodesk Inventor.
2.1.24.Создание 3d модели Вала используя элементы Проектирование «Вал». Создание чертежа вала.
2.1.25.Создание сборки Опора: Создание 3D модели Плита нижняя. Создание детали Прокладка. Создание детали Плита верхняя.
2.1.26.Создание сборки Опора.
Задание №1
Разработать параметрическую электронную модель "Шатун"

Оценка	***Показатели оценки***
3	Разработана модель "Шатун" с ордним набором размеров
4	Разработана параметрическая модель "Шатун"

5	Разработана параметрическая модель "Шатун" с наложением всех зависимостей

2.5 Текущий контроль (ТК) № 5

Тема занятия: 2.1.29.Создание сборки механизма с помощью команды Соединение. Создание сборки механизма с помощью команды Зависимость.
Метод и форма контроля: Практическая работа (Информационно-аналитический)
Вид контроля: Практическая работа с использованием ИКТ
Дидактическая единица: 1.4 методы и средства сбора, обработки, хранения, передачи и накопления информации;
Занятие(-я):
1.1.1.Введение. Общий состав и структура персональных компьютеров и вычислительных систем. Методы и средства сбора,обработки, хранения, передачи и накопления информации.
Задание №1

1. Что относится к аппаратным средствам создания и обработки графических изображений?
2. Что относится к программным средствам создания и обработки графических изображений?
3. В каком виде может быть представлено ПО?

Оценка	*Показатели оценки*
3	Получен ответ на один вопроса из трех представленных: 1. К аппаратным средствам создания и обработки графических изображений относятся: • монитор и видеокарта, поддерживающая графический режим отображения; • видеоадаптеры (видеоускорители), ускоряющие выполнение графических операций и тем самым «разгружающие» центральный процессор; • манипуляторы «мышь», без которых не мыслится работа большинства современных программных средств работы с графикой; • сканеры как устройства оцифровки графических

	изображений; • дигитайзеры (совместно со световым пером и графическим планшетом), преобразующие в векторный формат изображение, полученное в результате передвижения руки оператора; • принтеры и графопостроители (плоттеры) в качестве основных устройств вывода графических изображений. 2.К программным средствам создания и обработки графических изображений относятся: • графические редакторы; • аниматоры; • программные средства для работы с трехмерной графикой; • средства деловой графики; • средства для создания презентаций, функции которых часто совмещаются с функциями вышеперечисленных средств. 3. ПО может быть представлено в виде: • отдельных самостоятельных программ (чаще всего это графические редакторы); • отдельных модулей, входящих в состав других программных средств (например, «Мастер диаграмм» как составная часть текстового процессора или электронных таблиц); • сложного комплекса программных модулей (большинство ПО для работы с трехмерной графикой, средства автоматизированного проектирования и т.п.).
4	Получен ответ на два вопроса из трех представленных: К аппаратным средствам создания и обработки графических изображений относятся: • монитор и видеокарта, поддерживающая графический режим отображения; • видеоадаптеры (видеоускорители), ускоряющие

	выполнение графических операций и тем самым «разгружающие» центральный процессор; • манипуляторы «мышь», без которых не мыслится работа большинства современных программных средств работы с графикой; • сканеры как устройства оцифровки графических изображений; • дигитайзеры (совместно со световым пером и графическим планшетом), преобразующие в векторный формат изображение, полученное в результате передвижения руки оператора; • принтеры и графопостроители (плоттеры) в качестве основных устройств вывода графических изображений. К программным средствам создания и обработки графических изображений относятся: - графические редакторы; - аниматоры; - программные средства для работы с трехмерной графикой; - средства деловой графики; - средства для создания презентаций, функции которых часто совмещаются с функциями вышеперечисленных средств. 3. ПО может быть представлено в виде: • отдельных самостоятельных программ (чаще всего это графические редакторы); • отдельных модулей, входящих в состав других программных средств (например, «Мастер диаграмм» как составная часть текстового процессора или электронных таблиц); • сложного комплекса программных модулей (большинство ПС для работы с трехмерной графикой, средства автоматизированного проектирования и т.п.).
5	Получен ответ на три вопроса из трех представленных: К аппаратным средствам создания и обработки графических изображений относятся: • монитор и видеокарта, поддерживающая графический режим отображения;

	• видеоадаптеры (видеоускорители), ускоряющие выполнение графических операций и тем самым «разгружающие» центральный процессор; • манипуляторы «мышь», без которых не мыслится работа большинства современных программных средств работы с графикой; • сканеры как устройства оцифровки графических изображений; • дигитайзеры (совместно со световым пером и графическим планшетом), преобразующие в векторный формат изображение, полученное в результате передвижения руки оператора; • принтеры и графопостроители (плоттеры) в качестве основных устройств вывода графических изображений. К программным средствам создания и обработки графических изображений относятся: - графические редакторы; - аниматоры; - программные средства для работы с трехмерной графикой; - средства деловой графики; - средства для создания презентаций, функции которых часто совмещаются с функциями вышеперечисленных средств. 3. ПО может быть представлено в виде: • отдельных самостоятельных программ (чаще всего это графические редакторы); • отдельных модулей, входящих в состав других программных средств (например, «Мастер диаграмм» как составная часть текстового процессора или электронных таблиц); • сложного комплекса программных модулей (большинство ПС для работы с трехмерной графикой, средства автоматизированного проектирования и т.п.).

Дидактическая единица: 2.2 использовать в профессиональной деятельности различные виды программного обеспечения, в т.ч. специального;
Занятие(-я):
2.1.27.Создание чертежа Плиты нижней, чертежа Прокладки, чертежа Плиты верхней.

2.1.28.Создание Сборочного чертежа Опоры. Два способа создания спецификации.

Задание №1

Дана сборка реального производства (например штуцер). Произвести обмер каждой детали. Построить ассоциативный чертеж, Оформить чертеж согласно ГОСТ 2.305-2008. Размеры нанести согласно ГОСТ 2.307-2011

Оценка	***Показатели оценки***
3	Проанализирован состав сборки (каждя деталь мысленно разбита на элементарные составляющие элементы). Произведен обмер каждой детали с помощью штангенциркуля. Согласно размерам построены 3 D модели каждой детали и собраны в сборку. Согласно размерам сборки произведено оформление чертежа согласно ГОСТ 2.103-68, 2.104-2006, 2.302-68, 2.303-68, 2.304-81 Оформление чертежа произведено согласно ГОСТ 2.305-2008
4	Проанализирован состав сборки (каждя деталь мысленно разбита на элементарные составляющие элементы). Произведен обмер каждой детали с помощью штангенциркуля. Согласно размерам построены 3 D модели каждой детали и собраны в сборку. Согласно размерам сборки произведено оформление чертежа согласно ГОСТ 2.103-68, 2.104-2006, 2.302-68, 2.303-68, 2.304-81 Оформление чертежа произведено согласно ГОСТ 2.305-2008
5	Проанализирован состав сборки (каждя деталь мысленно разбита на элементарные составляющие элементы). Произведен обмер каждой детали с помощью штангенциркуля. Согласно размерам построены 3 D модели каждой детали и собраны в сборку. Согласно размерам сборки произведено оформление чертежа согласно ГОСТ 2.103-68, 2.104-2006, 2.302-68, 2.303-68, 2.304-81 Оформление чертежа произведено согласно ГОСТ 2.305-2008 Размеры нанесены согласно ГОСТ 2.307-2011

2.6 Текущий контроль (ТК) № 6

Тема занятия: 2.1.32.Создание видов в сборке. Выполнение половинного сечения и сечения в три четверти сборки.

Метод и форма контроля: Практическая работа (Информационно-аналитический)

Вид контроля: Практическая работа с использованием ИКТ

Дидактическая единица: 2.4 уметь выполнять ассоциативные чертежи на основе созданных 3D моделей с необходимым числом видов, разрезов, сечений.

Занятие(-я):

2.1.27.Создание чертежа Плиты нижней, чертежа Прокладки, чертежа Плиты верхней.

Задание №1

Создать ассоциативный чертеж детали Шатун с необходимым числом видов, разрезов, сечений. Нанести размеры

Оценка	*Показатели оценки*
3	Создан ассоциативный чертеж детали Шатун. Нанесено 30% размеров.
4	Создан ассоциативный чертеж детали Шатун с необходимым числом видов, разрезов, сечений. Нанесено 70% размеров.
5	Создан ассоциативный чертеж детали Шатун с необходимым числом видов, разрезов, сечений. Нанесены все размеры.

2.7 Текущий контроль (ТК) № 7

Тема занятия: 2.1.33.Сборка плиты нижней и плиты верхней. Создание компонентов сборки в самой сборке. Команда Болтовое соединение.

Метод и форма контроля: Практическая работа (Информационно-аналитический)

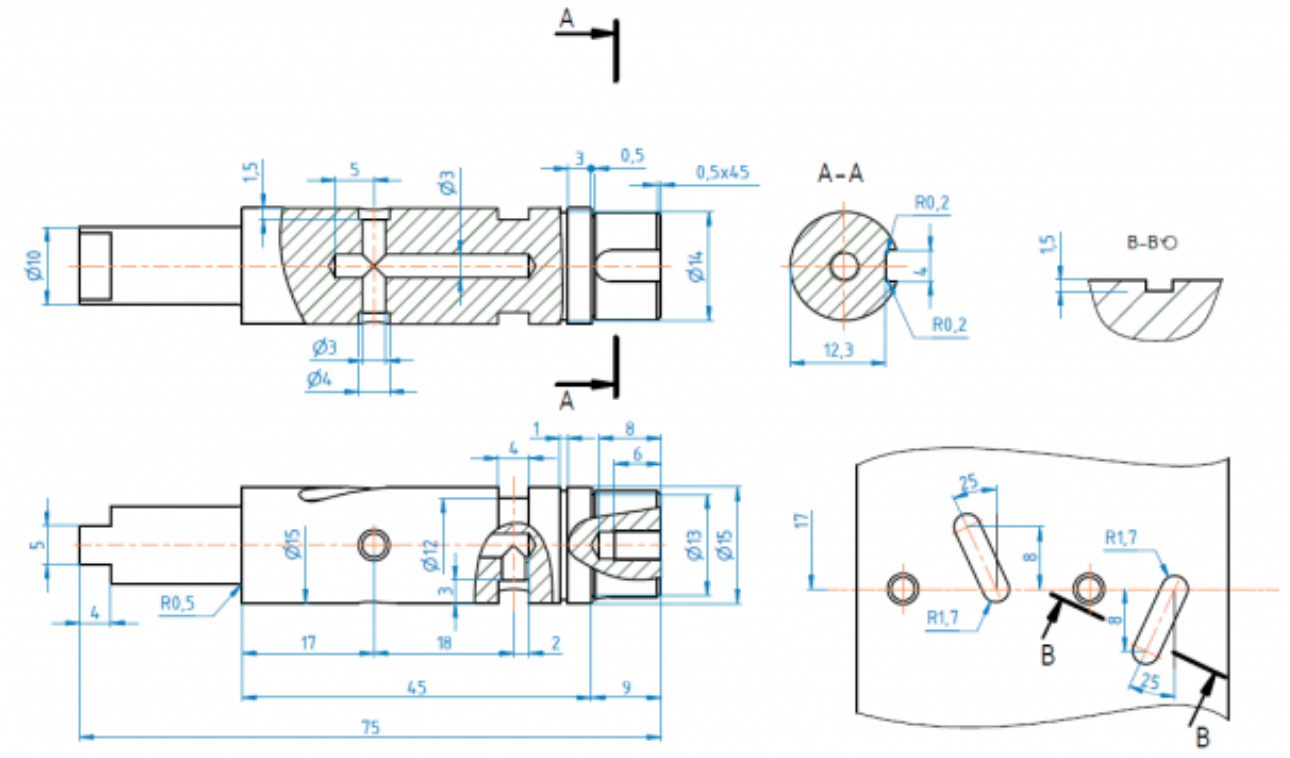
Вид контроля:

Дидактическая единица: 2.5 оформлять ассоциативные чертежи, наносить размеры, заполнять технические требования

Занятие(-я):

2.1.23.Создание чертежа детали Вал. Создание чертежа детали Плита. Создание чертежа детали Рычаг. Создание чертежа детали из листового металла. в Autodesk Inventor.

Задание №1



Создать ассоциативный чертеж вала, нанести размеры, заполнить технические требования

Оценка	*Показатели оценки*
3	Создан ассоциативный чертеж вала
4	Создан ассоциативный чертеж вала, правильно нанесены размеры.
5	Создать ассоциативный чертеж вала, правильно нанести размеры, заполнены технические требования

2.8 Текущий контроль (ТК) № 8

Тема занятия: 3.1.1.Методы обеспечения информационной безопасности
Метод и форма контроля: Практическая работа (Опрос)
Вид контроля: защита
Дидактическая единица: 1.5 базовые системные программные продукты и пакеты прикладных программ в области профессиональной деятельности;
Занятие(-я):

Задание №1
Что такое профиль эскиза?
Что такое траектория эскиза?

На что влияют зависимости в эскизе?

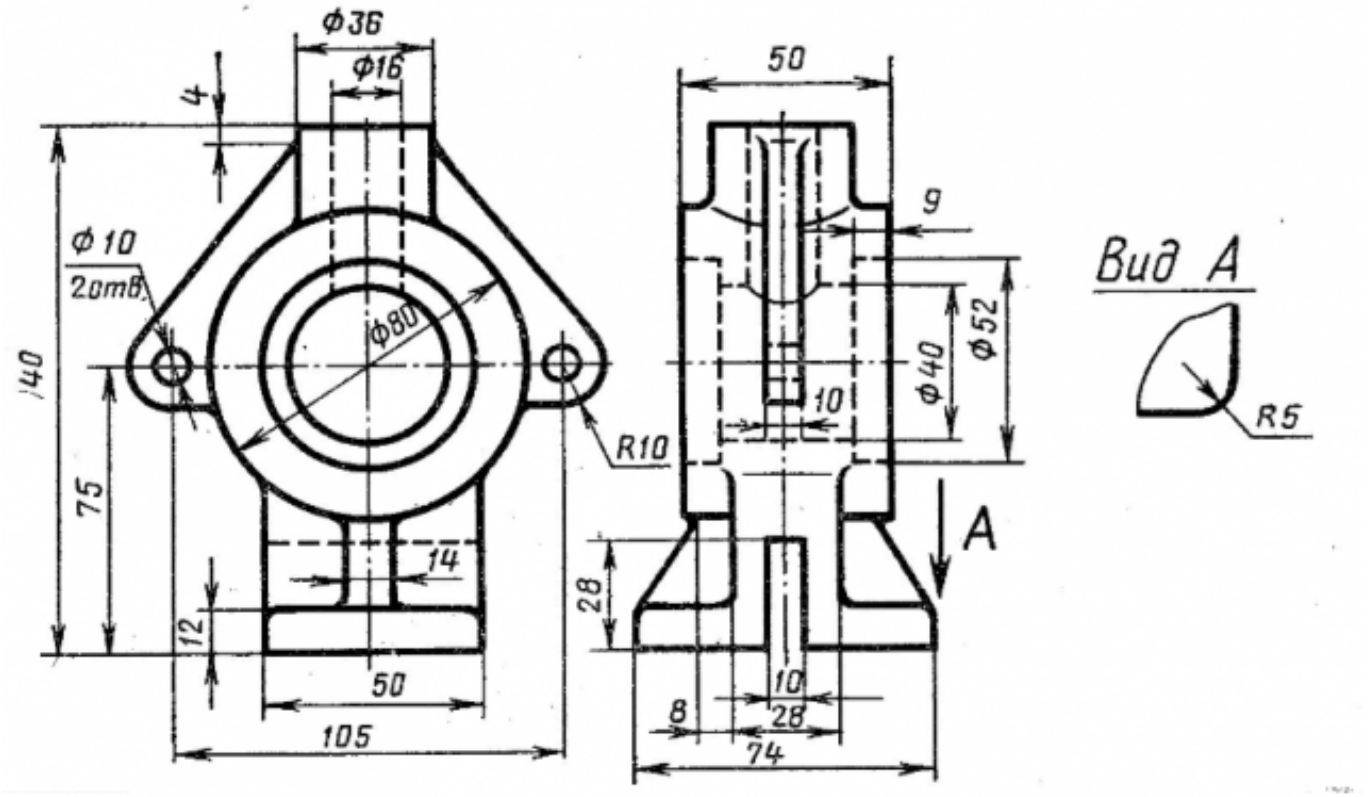
Оценка	***Показатели оценки***
3	Получен ответ на один из трех представленных вопросов. 1. Профиль эскиза — это замкнутый контур, определенный эскизной или ссылочной геометрией, которая представляет поперечное сечение элемента. 2. Траектория эскиза — это траектория элемента сдвига. Траекторией может являться замкнутый или разомкнутый контур, состоящий из линий, дуг, эллипсов и окружностей с указанной начальной точкой. 3. Зависимости влияют на следующие факторы: • ориентацию геометрии в системе координат эскиза. (при построении практически вертикальной линии Inventor автоматически создает ее по вертикали); • связь между геометрией эскиза.(зависимости можно добавлять для создания перпендикулярных, параллельных, касательных или концентрических форм или линий). Можно также задавать пропорциональные связи между кривыми эскиза. Либо использовать размерные зависимости для стабилизации эскизов. Параметрические размеры определяют размер и положение геометрии эскиза и помогают предотвратить искажение при изменении размера элементов эскиза.

4	Получены два ответа из трех представленных вопросов. 1. Профиль эскиза — это замкнутый контур, определенный эскизной или ссылочной геометрией, которая представляет поперечное сечение элемента. 2. Траектория эскиза — это траектория элемента сдвига. Траекторией может являться замкнутый или разомкнутый контур, состоящий из линий, дуг, эллипсов и окружностей с указанной начальной точкой. 3. Зависимости влияют на следующие факторы: • ориентацию геометрии в системе координат эскиза. (при построении практически вертикальной линии Inventor автоматически создает ее по вертикали); • связь между геометрией эскиза.(зависимости можно добавлять для создания перпендикулярных, параллельных, касательных или концентрических форм или линий). Можно также задавать пропорциональные связи между кривыми эскиза. Либо использовать размерные зависимости для стабилизации эскизов. Параметрические размеры определяют размер и положение геометрии эскиза и помогают предотвратить искажение при изменении размера элементов эскиза.

5	Получены три ответа из трех представленных вопросов. Профиль эскиза — это замкнутый контур, определенный эскизной или ссылочной геометрией, которая представляет поперечное сечение элемента. Траектория эскиза — это траектория элемента сдвига. Траекторией может являться замкнутый или разомкнутый контур, состоящий из линий, дуг, эллипсов и окружностей с указанной начальной точкой. Зависимости влияют на следующие факторы: • ориентацию геометрии в системе координат эскиза. (при построении практически вертикальной линии Inventor автоматически создает ее по вертикали); • связь между геометрией эскиза.(зависимости можно добавлять для создания перпендикулярных, параллельных, касательных или концентрических форм или линий). Можно также задавать пропорциональные связи между кривыми эскиза. Либо использовать размерные зависимости для стабилизации эскизов. Параметрические размеры определяют размер и положение геометрии эскиза и помогают предотвратить искажение при изменении размера элементов эскиза.

Дидактическая единица: 2.4 уметь выполнять ассоциативные чертежи на основе созданных 3D моделей с необходимым числом видов, разрезов, сечений.
Занятие(-я):

Задание №1



Построить ассоциативный чертеж 3D модели Стойки с необходимым числом видов, разрезов, сечений.

Оценка	***Показатели оценки***
3	Построен ассоциативный чертеж 3D модели Стойки с видами.
4	Построен ассоциативный чертеж 3D модели Стойки с необходимым числом видов.
5	Построен ассоциативный чертеж 3D модели Стойки с необходимым числом видов, разрезов, сечений.

Дидактическая единица: 2.6 уметь создавать компоненты сборки, накладывать зависимости совмещения, проводить анализ на пространственное пересечение компонентов

Занятие(-я):

2.1.32.Создание видов в сборке. Выполнение половинного сечения и сечения в три четверти сборки.

Задание №1

В сборке Редуктор построить компанент "Прокладка" , нанести необходимые зависимости

Оценка	*Показатели оценки*
3	В сборке Редуктор построен компанент "Прокладка"
4	В сборке Редуктор построен компанент "Прокладка" , нанесены зависимости
5	В сборке Редуктор построен компанент "Прокладка" , нанесены все необходимые зависимости

3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ, ИСПОЛЬЗУЕМЫЙ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

№ семестра	Вид промежуточной аттестации
2	Дифференцированный зачет

Дифференцированный зачет может быть выставлен автоматически по результатам текущих контролей
Текущий контроль №1
Текущий контроль №2
Текущий контроль №3
Текущий контроль №4
Текущий контроль №5
Текущий контроль №6
Текущий контроль №7
Текущий контроль №8

Метод и форма контроля: Практическая работа (Информационно-аналитический)
Вид контроля: по выбору выполнить два теоретических и два практических задания
Дидактическая единица для контроля:
1.1 основные понятия автоматизированной обработки информации;
Задание №1 (из текущего контроля)
Дать ответы на вопросы

1. Сто называется информационным процессом? Что такое сбор информации?
2. Что такое формализация данных? Что такое фильтрация данных?
3. Что такое сортировка данных? Что такое защита данных?
4. Что такое архивация данных? Что такое транспортировка данных?

5. Что такое преобразование данных?

Оценка	*Показатели оценки*
3	получены правильные ответы на три вопроса
4	получены правильные ответы на четыре вопроса
5	получены правильные ответы на все вопросы

Дидактическая единица для контроля:
1.2 общий состав и структуру персональных компьютеров и вычислительных систем;
Задание №1 (из текущего контроля)

1. Перечислить состав персонального компьютера
2. Перечислить устройств ввода информации
3. Перечислить устройства вывода информации
4. Что понимается под архитектурой компьютера?
5. Что такое алгоритм и программа для ПК?

Оценка	***Показатели оценки***
3	получены правильные ответы на три вопроса
4	получены правильные ответы на четыре вопроса
5	получены правильные ответы на все вопросы

Дидактическая единица для контроля:
1.3 состав, функции и возможности использования информационных и телекоммуникационных технологий в профессиональной деятельности;
Задание №1 (из текущего контроля)

1. Перечислить задачи, решаемые САПР на стадиях проектирования и подготовки производства.
2. Перечислить программы, используемые при машиностроительном проектировании.
3. Перечислить функции CAD-систем.

Оценка	***Показатели оценки***

3	Получен ответ на один вопрос из трех представленных: 1. Перечислить задачи, решаемые САПР на стадиях проектирования и подготовки производства. 2. Перечислить современные системы автоматизированного проектирования. 3. Основная цель создания САПР — повышение эффективности труда инженеров, включая: • сокращения трудоемкости проектирования и планирования; • сокращения сроков проектирования; • сокращения себестоимости проектирования; • повышения качества и технико-экономического уровня результатов проектирования; • сокращения затрат на натурное моделирование и испытания. В России и странах СНГ наиболее широко распространены: • программный пакет **AutoCAD** • **КОМПАС** - система автоматизированного проектирования, разработанная российской компанией <АСКОН> с возможностями оформления проектной и конструкторской документации согласно стандартам серии ЕСКД и СПДС. Существует в двух версиях: КОМПАС-График и КОМПАС-3D, соответственно предназначенных для плоского черчения и трехмерного проектирования. • **Autodesk Inventor** — система трехмерного твердотельного проектирования для разработки сложных машиностроительных изделий. Функции CAD-систем в машиностроении подразделяют на функции двухмерного*(2D)* и трехмерного *(3D)* проектирования. К функциям *2D* относятся черчение, оформление конструкторской документации; к функциям *3D* — получение трехмерных моделей, метрические расчеты, реалистичная визуализация, взаимное преобразование*2D* и *3D* моделей.

4	Получен ответ на два вопроса из трех представленных: 1. Перечислить задачи, решаемые САПР на стадиях проектирования и подготовки производства. 2. Перечислить современные системы автоматизированного проектирования. 3. Основная цель создания САПР — повышение эффективности труда инженеров, включая: • сокращения трудоемкости проектирования и планирования; • сокращения сроков проектирования; • сокращения себестоимости проектирования; • повышения качества и технико-экономического уровня результатов проектирования; • сокращения затрат на натурное моделирование и испытания. В России и странах СНГ наиболее широко распространены: • программный пакет **AutoCAD** • **КОМПАС** - система автоматизированного проектирования, разработанная российской компанией <АСКОН> с возможностями оформления проектной и конструкторской документации согласно стандартам серии ЕСКД и СПДС. Существует в двух версиях: КОМПАС-График и КОМПАС-3D, соответственно предназначенных для плоского черчения и трехмерного проектирования. • **Autodesk Inventor** — система трехмерного твердотельного проектирования для разработки сложных машиностроительных изделий. Функции CAD-систем в машиностроении подразделяют на функции двухмерного*(2D)* и трехмерного *(3D)* проектирования. К функциям *2D* относятся черчение, оформление конструкторской документации; к функциям *3D* — получение трехмерных моделей, метрические расчеты, реалистичная визуализация, взаимное преобразование*2D* и *3D* моделей.

5	Получен ответ на три вопроса из трех представленных: 1. Перечислить задачи, решаемые САПР на стадиях проектирования и подготовки производства. 2. Перечислить современные системы автоматизированного проектирования. 3. Основная цель создания САПР — повышение эффективности труда инженеров, включая: • сокращения трудоемкости проектирования и планирования; • сокращения сроков проектирования; • сокращения себестоимости проектирования; • повышения качества и технико-экономического уровня результатов проектирования; • сокращения затрат на натурное моделирование и испытания. В России и странах СНГ наиболее широко распространены: • программный пакет **AutoCAD** • **КОМПАС** - система автоматизированного проектирования, разработанная российской компанией <АСКОН> с возможностями оформления проектной и конструкторской документации согласно стандартам серии ЕСКД и СПДС. Существует в двух версиях: КОМПАС-График и КОМПАС-3D, соответственно предназначенных для плоского черчения и трехмерного проектирования. • **Autodesk Inventor** — система трехмерного твердотельного проектирования для разработки сложных машиностроительных изделий. Функции CAD-систем в машиностроении подразделяют на функции двухмерного*(2D)* и трехмерного *(3D)* проектирования. К функциям *2D* относятся черчение, оформление конструкторской документации; к функциям *3D* — получение трехмерных моделей, метрические расчеты, реалистичная визуализация, взаимное преобразование*2D* и *3D* моделей.

Дидактическая единица для контроля:
1.4 методы и средства сбора, обработки, хранения, передачи и накопления информации;
Задание №1 (из текущего контроля)

1. Что относится к аппаратным средствам создания и обработки графических изображений?
2. Что относится к программным средствам создания и обработки графических изображений?
3. В каком виде может быть представлено ПО?

Оценка	***Показатели оценки***
3	Получен ответ на один вопроса из трех представленных: 1. К аппаратным средствам создания и обработки графических изображений относятся: • монитор и видеокарта, поддерживающая графический режим отображения; • видеоадаптеры (видеоускорители), ускоряющие выполнение графических операций и тем самым «разгружающие» центральный процессор; • манипуляторы «мышь», без которых не мыслится работа большинства современных программных средств работы с графикой; • сканеры как устройства оцифровки графических изображений; • дигитайзеры (совместно со световым пером и графическим планшетом), преобразующие в векторный формат изображение, полученное в результате передвижения руки оператора; • принтеры и графопостроители (плоттеры) в качестве основных устройств вывода графических изображений. 2.К программным средствам создания и обработки графических изображений относятся:

	• графические редакторы; • аниматоры; • программные средства для работы с трехмерной графикой; • средства деловой графики; • средства для создания презентаций, функции которых часто совмещаются с функциями вышеперечисленных средств. 3. ПО может быть представлено в виде: • отдельных самостоятельных программ (чаще всего это графические редакторы); • отдельных модулей, входящих в состав других программных средств (например, «Мастер диаграмм» как составная часть текстового процессора или электронных таблиц); • сложного комплекса программных модулей (большинство ПО для работы с трехмерной графикой, средства автоматизированного проектирования и т.п.).
4	Получен ответ на два вопроса из трех представленных: К аппаратным средствам создания и обработки графических изображений относятся: • монитор и видеокарта, поддерживающая графический режим отображения; • видеоадаптеры (видеоускорители), ускоряющие выполнение графических операций и тем самым «разгружающие» центральный процессор; • манипуляторы «мышь», без которых не мыслится работа большинства современных программных средств работы с графикой; • сканеры как устройства оцифровки графических изображений; • дигитайзеры (совместно со световым пером и графическим планшетом), преобразующие в векторный формат изображение, полученное в результате передвижения руки оператора; • принтеры и графопостроители (плоттеры) в качестве

	основных устройств вывода графических изображений. К программным средствам создания и обработки графических изображений относятся: - графические редакторы; - аниматоры; - программные средства для работы с трехмерной графикой; - средства деловой графики; - средства для создания презентаций, функции которых часто совмещаются с функциями вышеперечисленных средств. 3. ПО может быть представлено в виде: • отдельных самостоятельных программ (чаще всего это графические редакторы); • отдельных модулей, входящих в состав других программных средств (например, «Мастер диаграмм» как составная часть текстового процессора или электронных таблиц); • сложного комплекса программных модулей (большинство ПС для работы с трехмерной графикой, средства автоматизированного проектирования и т.п.).
5	Получен ответ на три вопроса из трех представленных: К аппаратным средствам создания и обработки графических изображений относятся: • монитор и видеокарта, поддерживающая графический режим отображения; • видеоадаптеры (видеоускорители), ускоряющие выполнение графических операций и тем самым «разгружающие» центральный процессор; • манипуляторы «мышь», без которых не мыслится работа большинства современных программных средств работы с графикой; • сканеры как устройства оцифровки графических изображений; • дигитайзеры (совместно со световым пером и графическим планшетом), преобразующие в векторный формат изображение, полученное в результате передвижения руки оператора;

	• принтеры и графопостроители (плоттеры) в качестве основных устройств вывода графических изображений. К программным средствам создания и обработки графических изображений относятся: - графические редакторы; - аниматоры; - программные средства для работы с трехмерной графикой; - средства деловой графики; - средства для создания презентаций, функции которых часто совмещаются с функциями вышеперечисленных средств. 3. ПО может быть представлено в виде: • отдельных самостоятельных программ (чаще всего это графические редакторы); • отдельных модулей, входящих в состав других программных средств (например, «Мастер диаграмм» как составная часть текстового процессора или электронных таблиц); • сложного комплекса программных модулей (большинство ПС для работы с трехмерной графикой, средства автоматизированного проектирования и т.п.).

Дидактическая единица для контроля:

1.5 базовые системные программные продукты и пакеты прикладных программ в области профессиональной деятельности;

Задание №1 (из текущего контроля)

Что такое профиль эскиза?

Что такое траектория эскиза?

На что влияют зависимости в эскизе?

Оценка	***Показатели оценки***

3	Получен ответ на один из трех представленных вопросов. 1. Профиль эскиза — это замкнутый контур, определенный эскизной или ссылочной геометрией, которая представляет поперечное сечение элемента. 2. Траектория эскиза — это траектория элемента сдвига. Траекторией может являться замкнутый или разомкнутый контур, состоящий из линий, дуг, эллипсов и окружностей с указанной начальной точкой. 3. Зависимости влияют на следующие факторы: • ориентацию геометрии в системе координат эскиза. (при построении практически вертикальной линии Inventor автоматически создает ее по вертикали); • связь между геометрией эскиза.(зависимости можно добавлять для создания перпендикулярных, параллельных, касательных или концентрических форм или линий). Можно также задавать пропорциональные связи между кривыми эскиза. Либо использовать размерные зависимости для стабилизации эскизов. Параметрические размеры определяют размер и положение геометрии эскиза и помогают предотвратить искажение при изменении размера элементов эскиза.

4	Получены два ответа из трех представленных вопросов. 1. Профиль эскиза — это замкнутый контур, определенный эскизной или ссылочной геометрией, которая представляет поперечное сечение элемента. 2. Траектория эскиза — это траектория элемента сдвига. Траекторией может являться замкнутый или разомкнутый контур, состоящий из линий, дуг, эллипсов и окружностей с указанной начальной точкой. 3. Зависимости влияют на следующие факторы: • ориентацию геометрии в системе координат эскиза. (при построении практически вертикальной линии Inventor автоматически создает ее по вертикали); • связь между геометрией эскиза.(зависимости можно добавлять для создания перпендикулярных, параллельных, касательных или концентрических форм или линий). Можно также задавать пропорциональные связи между кривыми эскиза. Либо использовать размерные зависимости для стабилизации эскизов. Параметрические размеры определяют размер и положение геометрии эскиза и помогают предотвратить искажение при изменении размера элементов эскиза.

5	Получены три ответа из трех представленных вопросов. Профиль эскиза — это замкнутый контур, определенный эскизной или ссылочной геометрией, которая представляет поперечное сечение элемента. Траектория эскиза — это траектория элемента сдвига. Траекторией может являться замкнутый или разомкнутый контур, состоящий из линий, дуг, эллипсов и окружностей с указанной начальной точкой. Зависимости влияют на следующие факторы: • ориентацию геометрии в системе координат эскиза. (при построении практически вертикальной линии Inventor автоматически создает ее по вертикали); • связь между геометрией эскиза.(зависимости можно добавлять для создания перпендикулярных, параллельных, касательных или концентрических форм или линий). Можно также задавать пропорциональные связи между кривыми эскиза. Либо использовать размерные зависимости для стабилизации эскизов. Параметрические размеры определяют размер и положение геометрии эскиза и помогают предотвратить искажение при изменении размера элементов эскиза.

Дидактическая единица для контроля:

1.6 основные методы и приемы обеспечения информационной безопасности

Задание №1 (из текущего контроля)

1. Что такое информационная безопасность?
2. Перечислить основные методы информационной безопасности. Перечислить основные организационно технические методы обеспечения информационной безопасности.
3. На какие классы можно разделить методы обеспечения информационной безопасности

Оценка	***Показатели оценки***

3	Получен ответ на один вопрос из трех представленных: 1. Информационная безопасность это совокупность деятельности по недопущению вреда свойствам объекта безопасности обусловливаемым информацией и информационной инфраструктурой и субъектов а также средств этой деятельности. 2. Методы обеспечения информационной безопасности: • организационно правовые методы,(документы, регламентирующие все аспекты обеспечения информационной безопасности) • организационно технические методы.(Этот процесс никогда не закончится, так как совершенствуются методы нарушения информационной безопасности.) Перечислены основные организационно технические методы обеспечения информационной безопасности: 1. Авторизация. (позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.) 2. Иденификация и аутентификация.(Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам. Аутентификация-проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д.) 3. Экранирование – разделение информационных потоков между различными информационными системами. 4. Физическая защита. 1. Физические устройства доступности к сетевым узлам и линиям связи. 2. Противопожарные меры 3. Защита поддержки инфраструктуры (электропитание, кондиционирование…) 4. Защита мобильных и радио систем.

5. Защита от перехвата данных.

5. Поддержка текущей работоспособности.
    1. Резервное копирование.
    2. Управление носителями.
    3. Регламентированные работы.

В международных стандартах выделяют 7 классов безопасности систем, которые объединены в 4 уровня:
D — нулевой уровень безопасности;
C — системы с произвольным доступом;
B — системы с принудительным доступом;
A — системы с верифицируемой безопасностью.
Уровню D соответствуют системы, в которых слабо развита технология защиты. При такой ситуации любое постороннее лицо имеет возможность получить доступ к сведениям. Использование слаборазвитой технологии защиты чревато потерей или утратой сведений.
В уровне C есть следующие классы — C1 и C2. Класс безопасности C1 предполагает разделение данных и пользователей. Определенная группа пользователей имеет доступ только к определенным данным, для получения сведений необходима аутентификация — проверка подлинности пользователя путем запроса пароля. При классе безопасности C1 в системе имеются аппаратные и программные средства защиты. Системы с классом C2 дополнены мерами, гарантирующими ответственность пользователей: создается и поддерживается журнал регистрации доступа.
Уровень B включает технологии обеспечения безопасности, которые имеют классы уровня C, плюс несколько дополнительных. Класс B1 предполагает наличие политики безопасности, При классе B1 специалисты осуществляют тщательный анализ и тестирование исходного кода и архитектуры. Класс безопасности B2 характерен для многих современных систем и предполагает: Снабжение метками секретности всех ресурсов системы; Формальную политику безопасности; Высокую устойчивость систем к внешним атакам. Класс B3 предполагает, в дополнение к классу B1, оповещение администратора о попытках нарушения политики безопасности, анализ появления тайных каналов, наличие механизмов для восстановления данных после сбоя в работе аппаратуры или

программного обеспечения.
Уровень А включает один, наивысший класс безопасности — А. К данному классу относятся системы, прошедшие тестирование и получившие подтверждение соответствия формальным спецификациям верхнего уровня.

- Экранирование – разделение информационных потоков между различными информационными системами.
- Физическая защита.
    1. Физические устройства доступности к сетевым узлам и линиям связи.
    2. Противопожарные меры
    3. Защита поддержки инфраструктуры (электропитание, кондиционирование…)
    4. Защита мобильных и радио систем.
    5. Защита от перехвата данных.
- Поддержка текущей работоспособности.
    1. Резервное копирование.
    2. Управление носителями.
    3. Регламентированные работы.

Перечислены основные методы обеспечения информационной безопасности:

1. Авторизация. (позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.)
2. Иденификация и аутентификация.(Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам. Аутентификация-проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д.)
3. Информационная безопасность это совокупность деятельности по недопущению вреда свойствам объекта безопасности обусловливаемым информацией и информационной инфраструктурой и субъектов а также средств этой деятельности.

	Методы обеспечения информационной безопасности 4. организационно правовые методы,(документы, регламентирующие все аспекты обеспечения информационной безопасности) 5. организационно технические методы.(Этот процесс никогда не закончится, так как совершенствуются методы нарушения информационной безопасности.)
4	Получен ответ на два вопроса из трех представленных: 1. Информационная безопасность это совокупность деятельности по недопущению вреда свойствам объекта безопасности обусловливаемым информацией и информационной инфраструктурой и субъектов а также средств этой деятельности. Методы обеспечения информационной безопасности 2. организационно правовые методы,(документы, регламентирующие все аспекты обеспечения информационной безопасности) 3. организационно технические методы.(Этот процесс никогда не закончится, так как совершенствуются методы нарушения информационной безопасности.) 4. Перечислены основные методы обеспечения информационной безопасности: 5. Авторизация. (позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.) 6. Иденификация и аутентификация.(Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам. Аутентификация-проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д.) 7. Экранирование – разделение информационных потоков между различными информационными системами. 8. Физическая защита.

1. Физические устройства доступности к сетевым узлам и линиям связи.
2. Противопожарные меры
3. Защита поддержки инфраструктуры (электропитание, кондиционирование…)
4. Защита мобильных и радио систем.
5. Защита от перехвата данных.

9. Поддержка текущей работоспособности.
    1. Резервное копирование.
    2. Управление носителями.
    3. Регламентированные работы

Перечислены основные методы обеспечения информационной безопасности:

1. В международных стандартах выделяют 7 классов безопасности систем, которые объединены в 4 уровня:
   D — нулевой уровень безопасности;
   C — системы с произвольным доступом;
   B — системы с принудительным доступом;
   A — системы с верифицируемой безопасностью.
   Уровню D соответствуют системы, в которых слабо развита технология защиты. При такой ситуации любое постороннее лицо имеет возможность получить доступ к сведениям. Использование слаборазвитой технологии защиты чревато потерей или утратой сведений.
   В уровне C есть следующие классы — C1 и C2. Класс безопасности C1 предполагает разделение данных и пользователей. Определенная группа пользователей имеет доступ только к определенным данным, для получения сведений необходима аутентификация — проверка подлинности пользователя путем запроса пароля. При классе безопасности C1 в системе имеются аппаратные и программные средства защиты. Системы с классом C2 дополнены мерами, гарантирующими ответственность пользователей: создается и поддерживается журнал регистрации доступа.
   Уровень B включает технологии обеспечения

безопасности, которые имеют классы уровня С, плюс несколько дополнительных. Класс В1 предполагает наличие политики безопасности, При классе В1 специалисты осуществляют тщательный анализ и тестирование исходного кода и архитектуры. Класс безопасности В2 характерен для многих современных систем и предполагает: Снабжение метками секретности всех ресурсов системы; Формальную политику безопасности; Высокую устойчивость систем к внешним атакам. Класс В3 предполагает, в дополнение к классу В1, оповещение администратора о попытках нарушения политики безопасности, анализ появления тайных каналов, наличие механизмов для восстановления данных после сбоя в работе аппаратуры или программного обеспечения.

Уровень А включает один, наивысший класс безопасности — А. К данному классу относятся системы, прошедшие тестирование и получившие подтверждение соответствия формальным спецификациям верхнего уровня.

2. Экранирование – разделение информационных потоков между различными информационными системами.
3. Физическая защита.
    1. Физические устройства доступности к сетевым узлам и линиям связи.
    2. Противопожарные меры
    3. Защита поддержки инфраструктуры (электропитание, кондиционирование…)
    4. Защита мобильных и радио систем.
    5. Защита от перехвата данных.
4. Поддержка текущей работоспособности.
    1. Резервное копирование.
    2. Управление носителями.
    3. Регламентированные работы.
5. Авторизация. (позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.)
6. Иденификация и аутентификация.(Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и

	другим признакам. Аутентификация-проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д.) 7. Информационная безопасность это совокупность деятельности по недопущению вреда свойствам объекта безопасности обусловливаемым информацией и информационной инфраструктурой и субъектов а также средств этой деятельности. Методы обеспечения информационной безопасности 8. организационно правовые методы,(документы, регламентирующие все аспекты обеспечения информационной безопасности) 9. организационно технические методы.(Этот процесс никогда не закончится, так как совершенствуются методы нарушения информационной безопасности.)
5	Получен ответ на три вопроса из трех представленных: 1. Информационная безопасность это совокупность деятельности по недопущению вреда свойствам объекта безопасности обусловливаемым информацией и информационной инфраструктурой и субъектов а также средств этой деятельности. Методы обеспечения информационной безопасности 2. организационно правовые методы,(документы, регламентирующие все аспекты обеспечения информационной безопасности) 3. организационно технические методы.(Этот процесс никогда не закончится, так как совершенствуются методы нарушения информационной безопасности.) 4. Перечислены основные методы обеспечения информационной безопасности: 5. Авторизация. (позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.) 6. Иденификация и аутентификация.(Идентификация

позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам. Аутентификация-проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д.)

7. Экранирование – разделение информационных потоков между различными информационными системами.
8. Физическая защита.
    1. Физические устройства доступности к сетевым узлам и линиям связи.
    2. Противопожарные меры
    3. Защита поддержки инфраструктуры (электропитание, кондиционирование…)
    4. Защита мобильных и радио систем.
    5. Защита от перехвата данных.
9. Поддержка текущей работоспособности.
    1. Резервное копирование.
    2. Управление носителями.
    3. Регламентированные работы.

Информационная безопасность это совокупность деятельности по недопущению вреда свойствам объекта безопасности обусловливаемым информацией и информационной инфраструктурой и субъектов а также средств этой деятельности.
Методы обеспечения информационной безопасности

1. организационно правовые методы,(документы, регламентирующие все аспекты обеспечения информационной безопасности)
2. организационно технические методы.(Этот процесс никогда не закончится, так как совершенствуются методы нарушения информационной безопасности.)

Перечислены основные методы обеспечения информационной безопасности:

- Авторизация. (позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать

доступ пользователя к этим ресурсам.)

- Иденификация и аутентификация.(Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам. Аутентификация-проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д.)
- Экранирование – разделение информационных потоков между различными информационными системами.
- Физическая защита.
    1. Физические устройства доступности к сетевым узлам и линиям связи.
    2. Противопожарные меры
    3. Защита поддержки инфраструктуры (электропитание, кондиционирование…)
    4. Защита мобильных и радио систем.
    5. Защита от перехвата данных.
- Поддержка текущей работоспособности.
    1. Резервное копирование.
    2. Управление носителями.
    3. Регламентированные работы.

В международных стандартах выделяют 7 классов безопасности систем, которые объединены в 4 уровня:
D — нулевой уровень безопасности;
C — системы с произвольным доступом;
B — системы с принудительным доступом;
A — системы с верифицируемой безопасностью.
Уровню D соответствуют системы, в которых слабо развита технология защиты. При такой ситуации любое постороннее лицо имеет возможность получить доступ к сведениям. Использование слаборазвитой технологии защиты чревато потерей или утратой сведений.
В уровне C есть следующие классы — C1 и C2. Класс безопасности C1 предполагает разделение данных и пользователей. Определенная группа пользователей имеет доступ только к определенным данным, для получения сведений необходима аутентификация — проверка подлинности пользователя путем запроса пароля. При классе безопасности C1 в системе имеются аппаратные и программные средства защиты.

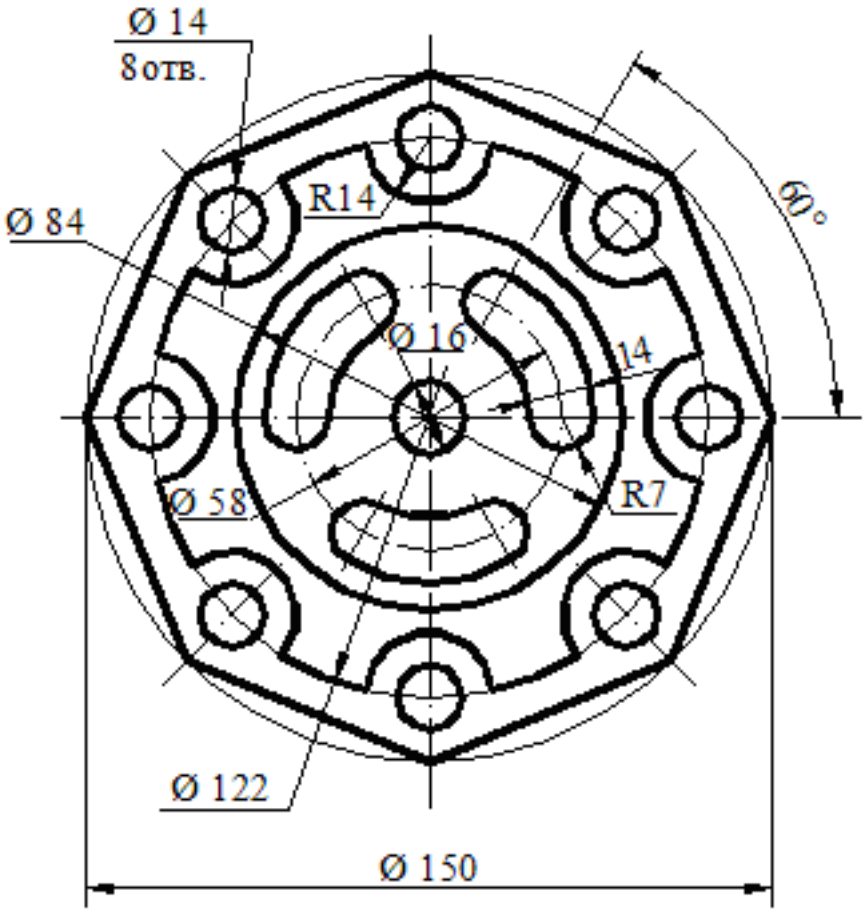
	Системы с классом C2 дополнены мерами, гарантирующими ответственность пользователей: создается и поддерживается журнал регистрации доступа. Уровень B включает технологии обеспечения безопасности, которые имеют классы уровня C, плюс несколько дополнительных. Класс B1 предполагает наличие политики безопасности, При классе B1 специалисты осуществляют тщательный анализ и тестирование исходного кода и архитектуры. Класс безопасности B2 характерен для многих современных систем и предполагает: Снабжение метками секретности всех ресурсов системы; Формальную политику безопасности; Высокую устойчивость систем к внешним атакам. Класс B3 предполагает, в дополнение к классу B1, оповещение администратора о попытках нарушения политики безопасности, анализ появления тайных каналов, наличие механизмов для восстановления данных после сбоя в работе аппаратуры или программного обеспечения. Уровень A включает один, наивысший класс безопасности — A. К данному классу относятся системы, прошедшие тестирование и получившие подтверждение соответствия формальным спецификациям верхнего уровня.

Дидактическая единица для контроля:

2.1 использовать технологии сбора, размещения, хранения, накопления, преобразования и передачи данных в профессионально ориентированных информационных системах;

Задание №1 (из текущего контроля)

Вычертить контур плоской детали с элементами деления окружности, сопряжений, нанесением размеров (Задания выдаются по вариантам).



Оценка	*Показатели оценки*
3	1. На созданном по умолчанию формате листа построены элементы чертежа не требующие дополнительных построений. 2. Построены сопряжения, и выполнено деление окружности на равные части используя соответствующие инструменты САПР. 3. Нанесены размеры согласно ГОСТ 2.307-2011. 4. Заполнена основная надпись.
4	1. Выбран масштаб детали. 2. Выбран формат листа в зависимости от масштаба детали. 3. Построены элементы чертежа не требующие дополнительных построений. 4. Построены сопряжения, и выполнено деление окружности на равные части используя соответствующие инструменты САПР. 5. Построены центровые линии. 6. Нанесены размеры согласно ГОСТ 2.307-2011. 7. Заполнена основная надпись

5	1. Выбран масштаб детали. 2. Измен формат листа в зависимости от масштаба детали с помощью инструмента Редактировать лист выбранного из контекстного меню Раскладка. 3. Построены элементы чертежа не требующие дополнительных построений. 4. Построены сопряжения, и выполнено деление окружности на равные части используя соответствующие инструменты САПР. 5. Построены центровые и осевые линии используя соответствующие инструменты САПР. 6. Нанесены размеры согласно ГОСТ 2.307-2011. 7. Заполнена основная надпись.

Дидактическая единица для контроля:

2.2 использовать в профессиональной деятельности различные виды программного обеспечения, в т.ч. специального;

Задание №1 (из текущего контроля)

Дана сборка реального производства (например штуцер). Произвести обмер каждой детали. Построить ассоциативный чертеж, Оформить чертеж согласно ГОСТ 2.305-2008. Размеры нанести согласно ГОСТ 2.307-2011

Оценка	***Показатели оценки***
3	Проанализирован состав сборки (каждя деталь мысленно разбита на элементарные составляющие элементы). Произведен обмер каждой детали с помощью штангенциркуля. Согласно размерам построены 3 D модели каждой детали и собраны в сборку. Согласно размерам сборки произведено оформление чертежа согласно ГОСТ 2.103-68, 2.104-2006, 2.302-68, 2.303-68, 2.304-81 Оформление чертежа произведено согласно ГОСТ 2.305-2008
4	Проанализирован состав сборки (каждя деталь мысленно разбита на элементарные составляющие элементы). Произведен обмер каждой детали с помощью штангенциркуля. Согласно размерам построены 3 D модели каждой детали и собраны в сборку. Согласно размерам сборки произведено оформление чертежа согласно ГОСТ 2.103-68, 2.104-2006, 2.302-68, 2.303-68, 2.304-81 Оформление чертежа произведено согласно ГОСТ 2.305-2008

5	Проанализирован состав сборки (каждя деталь мысленно разбита на элементарные составляющие элементы). Произведен обмер каждой детали с помощью штангенциркуля. Согласно размерам построены 3 D модели каждой детали и собраны в сборку. Согласно размерам сборки произведено оформление чертежа согласно ГОСТ 2.103-68, 2.104-2006, 2.302-68, 2.303-68, 2.304-81 Оформление чертежа произведено согласно ГОСТ 2.305-2008 Размеры нанесены согласно ГОСТ 2.307-2011

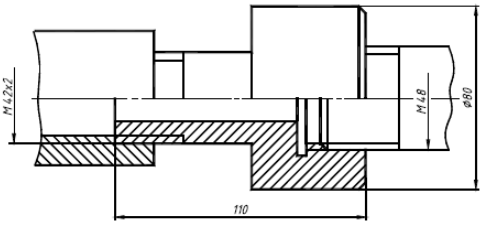
Дидактическая единица для контроля:

2.3 применять компьютерные и коммуникационные средства;

Задание №1 (из текущего контроля)

1. Ответить на вопрос: что такое *компьютерные коммуникации*
2. Начертить резьбовое соединение в по приведенному описанию, нанести размеры резьбы, габаритные размеры и оформить изображение в виде рабочего чертежа на формате А4.

Деталь цилиндрической формы расположена горизонтально. Левая часть детали – цилиндр 42 мм, длиной 60 мм. На нем с левой стороны на длину 35 мм нарезана метрическая резьба с мелким шагом 2 мм. Правая часть – цилиндр 80 мм, длиной 60 мм. Слева направо в детали проходит цилиндрическое отверстие 16 мм. Справа налево в детали просверлено отверстие 48 мм и глубиной 30 мм, в котором нарезана метрическая резьба с круп-ным шагом. Отверстие заканчивается канавкой 52 мм и шири-ной 5 мм. На цилиндр 42 мм навернута на глубину 15 мм втул-ка 60 мм, в которой на всю длину нарезана резьба. Длина втул-ки не задается, и она показывается на чертеже с обрывом. В от-верстие 48 мм с правой стороны ввернут на глубину 20 мм стержень, на котором нарезана резьба на длину 30 мм. Длина са-мого стержня не задается, и он показывается на чертеже с обры-вом. Цилиндр 80 мм с правой стороны имеет фаску размером 3 мм под углом 45о. Стержень 48 мм с левой стороны имеет фас-ку размером 2 мм под углом 45о.



Оценка	*Показатели оценки*
3	Начерчено резьбовое соединение в по приведенному описанию
4	Начерчено резьбовое соединение в по приведенному описанию нанесены размеры
5	Начерчено резьбовое соединение по приведенному описанию правильно нанесены размеры, получен правильный ответ на вопрос

1. Пример выполнения задания показан на рис.

Дидактическая единица для контроля:

2.4 уметь выполнять ассоциативные чертежи на основе созданных 3D моделей с необходимым числом видов, разрезов, сечений.

Задание №1 (из текущего контроля)

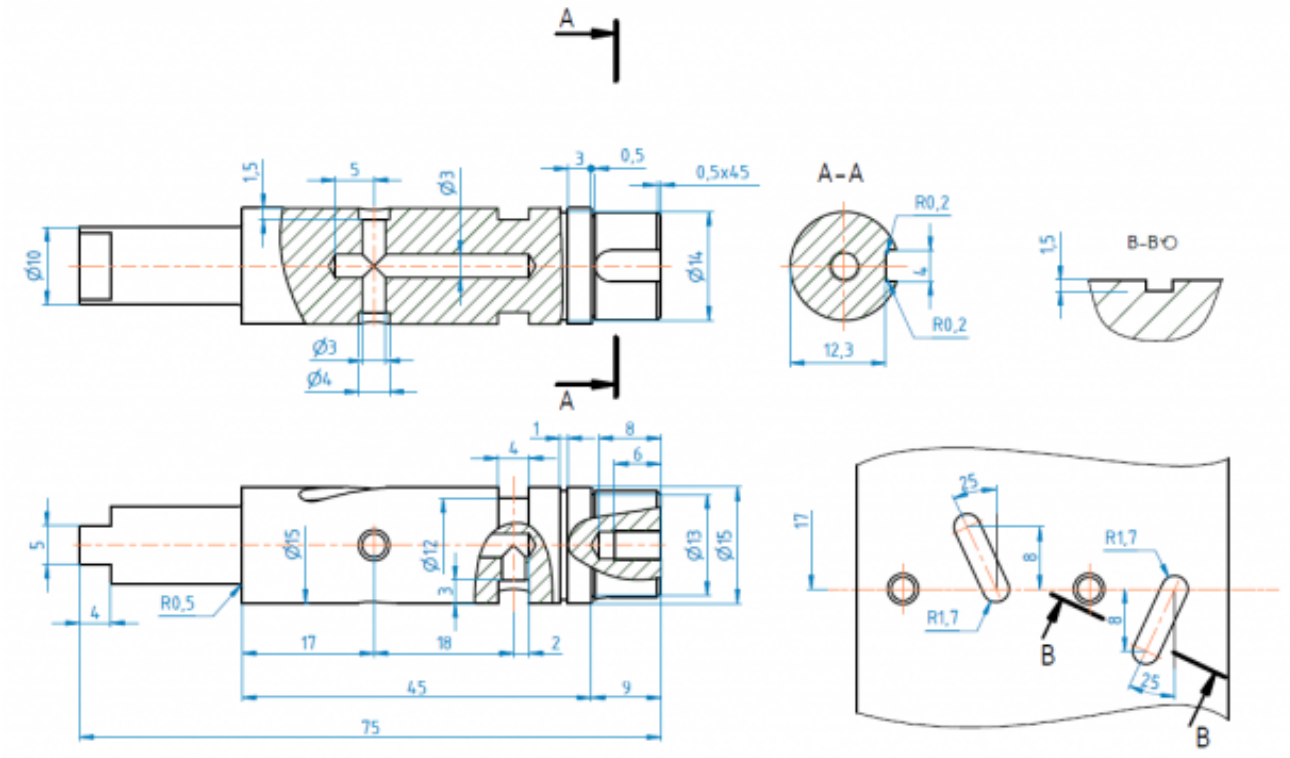
Создать ассоциативный чертеж детали Шатун с необходимым числом видов, разрезов, сечений. Нанести размеры

Оценка	*Показатели оценки*
3	Создан ассоциативный чертеж детали Шатун. Нанесено 30% размеров.
4	Создан ассоциативный чертеж детали Шатун с необходимым числом видов, разрезов, сечений. Нанесено 70% размеров.
5	Создан ассоциативный чертеж детали Шатун с необходимым числом видов, разрезов, сечений. Нанесены все размеры.

Дидактическая единица для контроля:

2.5 оформлять ассоциативные чертежи, наносить размеры, заполнять технические требования

Задание №1 (из текущего контроля)



Создать ассоциативный чертеж вала, нанести размеры, заполнить технические требования

Оценка	*Показатели оценки*
3	Создан ассоциативный чертеж вала
4	Создан ассоциативный чертеж вала, правильно нанесены размеры.
5	Создать ассоциативный чертеж вала, правильно нанести размеры, заполнены технические требования

Дидактическая единица для контроля:

2.6 уметь создавать компоненты сборки, накладывать зависимости совмещения, проводить анализ на пространственное пересечение компонентов

Задание №1 (из текущего контроля)

В сборке Редуктор построить компанент "Прокладка" , нанести необходимые зависимости

Оценка	*Показатели оценки*
3	В сборке Редуктор построен компанент "Прокладка"
4	В сборке Редуктор построен компанент "Прокладка" , нанесены зависимости

5	В сборке Редуктор построен компанент "Прокладка" , нанесены все необходимые зависимости