**МИНОБРНАУКИ РОССИИ**

**Федеральное государственное автономное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"**

**Кафедра информационных систем и математических методов в экономике**

Авторы-составители: **Ильин Вадим Владимирович**
**Радионова Марина Владимировна**

Рабочая программа дисциплины

# УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ И ЦИФРОВАЯ ГРАМОТНОСТЬ

Код УМК 98263

Утверждено
Протокол №9
от «06» июня 2022 г.

Пермь, 2022

## 1. Наименование дисциплины

Управление информационной безопасностью и цифровая грамотность

## 2. Место дисциплины в структуре образовательной программы

Дисциплина входит в вариативную часть Блока « М.1 » образовательной программы по направлениям подготовки (специальностям):

Направление: **38.04.04** Государственное и муниципальное управление
направленность Цифровое государство

## 3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Управление информационной безопасностью и цифровая грамотность** у обучающегося должны быть сформированы следующие компетенции:

**38.04.04** Государственное и муниципальное управление (направленность : Цифровое государство)

**ОПК.4** Способен организовывать внедрение современных информационно-коммуникационных технологий в соответствующей сфере профессиональной деятельности и обеспечивать информационную открытость деятельности органа власти

**Индикаторы**

**ОПК.4.1** Организует внедрение современных информационно-коммуникационных технологий в соответствующей сфере профессиональной деятельности

**ПК.2** Способен готовить экспертные заключения по проблемам государственного и муниципального управления

**Индикаторы**

**ПК.2.2** Проводит экспертизу нормативных документов и управленческих решений и дает рекомендации по ее итогам

## 4. Объем и содержание дисциплины

| | |
|---|---|
| **Направления подготовки** | 38.04.04 Государственное и муниципальное управление (направленность: Цифровое государство) |
| **форма обучения** | очная |
| **№№ триместров, выделенных для изучения дисциплины** | 2 |
| **Объем дисциплины (з.е.)** | 3 |
| **Объем дисциплины (ак.час.)** | 108 |
| **Контактная работа с преподавателем (ак.час.), в том числе:** | 36 |
| **Проведение лекционных занятий** | 12 |
| **Проведение практических занятий, семинаров** | 24 |
| **Самостоятельная работа (ак.час.)** | 72 |
| **Формы текущего контроля** | Входное тестирование (1)<br>Защищаемое контрольное мероприятие (2)<br>Итоговое контрольное мероприятие (1) |
| **Формы промежуточной аттестации** | Экзамен (2 триместр) |

## 5. Аннотированное описание содержания разделов и тем дисциплины

**Управление информационной безопасностью и цифровая грамотность**
Дисциплина направленна на приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, оценки рисков информационных ресурсов предприятия и аудита информационной безопасности, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность.

**Входной контроль**
Знание: основные положений информационных технологий и информационных систем.
Умение: осуществлять поиск и анализ информации с использование современных информационных технологий.
Владение: методами решения задач управления и прогнозирования, методикой моделирования деятельности организации.

**Тема-1 Базовые вопросы защиты информации и стандартизация в области управления информационной безопасности.**
Рассматриваются вопросы стандартизации в области информационной безопасности, рассматривается проблематика управления информационной безопасностью, анализируются средства обеспечения безопасности и системы информационной безопасности.

**Тема-2 Системы управления информационной безопасностью.**
Рассматривается управление информационной безопасностью организации, концепция, позволяющая комплексно управлять системой информационной безопасности. Анализируются решения, благодаря которым появляется возможность защищать информацию, передаваемую на внешнем и внутреннем уровне. Изучаются несколько подходов к управлению информационной безопасностью, а именно: организационный, кибернетический, процессный, теория принятия решений, оптимизационный.

**Тема-3 Основы правового обеспечения информационной безопасности. Техническая защита информации.**
Рассматриваются свойства информации как объекта защиты, определены закономерности создания защищённых информационных систем, раскрываются принципы обеспечения информационной безопасности государства, уделяется внимание информационным войнам и информационному противоборству. Дан краткий анализ моделей и политики безопасности (разграничения доступа), а также международных стандартов в области информационной безопасности.

**Тема-4 Основные понятия и критерии классификации угроз информационной безопасности. Криптографические методы защиты информации.**
Изложены основные понятия теории информационной безопасности, методология построения систем защиты автоматизированных информационных систем (АС), раскрывается понятие формальных политик безопасности. Дана классификация математических моделей информационной безопасности, рассмотрены основные дискреционные и мандатные модели, основные критерии защищенности АС, классы защищенности, включая международные стандарты, а также основные средства защиты информации, включая неформальные (законодательные, административные, процедурные) и формальные (программно-технические).

**Тема-5 Менеджмент и аудит систем информационной безопасности. Комплексная защита объектов информатизации.**
Дано описание системы менеджмента и аудита информационной безопасности. Рассмотрены меры

безопасности в контексте ISO. Представлен порядок использования политик, стандартов, руководств. Представлена типовая модель безопасности информационной сети предприятия, методы и средства аудита безопасности информационных систем, рассмотрены методы и средства аудита безопасности информационных систем.

**Тема-6 Проблемы безопасности современных цифровых технологий.**
Рассматриваются проблемные вопросы, связанные с обеспечением безопасности цифровых технологий в РФ, а также проведены разграничения понятий «компьютерные», «информационные» и «цифровые» технологии. Анализируется ответственность за противоправные деяния, посягающие на общественные отношения в сфере обеспечения безопасности цифровых сведений, технологий, систем и устройств.

## 6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

## 7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

## 8. Перечень основной и дополнительной учебной литературы

**Основная:**

1. Основы информационной безопасности:учебный курс

2. Информационная безопасность и защита информации : учебно-методический комплекс / составители С. А. Омарова, К. А. Искакова, Н. А. Тойганбаева. — Алматы : Нур-Принт, 2012. — 98 c. — ISBN 9965-756-05-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/67055.html

3. Безопасность ИТ:[Криптографические основы безопасности. Основы информационной безопасности. Протоколы безопасного сетевого взаимодействия. Стандарты информационной безопасности]/Интернет-Университет информационных технологий.-Москва:Новый диск,2006.-1.

**Дополнительная:**

1. Основы информационной безопасности:учебное пособие для студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности/Е. Б. Белов [и др.].-Москва:Горячая линия-Телеком,2006, ISBN 5-93517-292-5.-544.-Библиогр.: с. 268-270

## 9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

При освоении дисциплины использование ресурсов сети Интернет не предусмотрено.

## 10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Управление информационной безопасностью и цифровая грамотность** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине предполагает:
- презентационные материалы (слайды по темам лекционных и практических занятий);
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательную среду университета.

Перечень необходимого лицензионного и (или) свободно распространяемого программного обеспечения:
пакет MS Office, "Консультант Плюс" (свободно распространяемая версия с официального сайта).

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).

система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (https://indigotech.ru/).

## 11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

В учебном процессе для изучения дисциплины для проведения лекционных занятий требуется аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для проведения лабораторных занятий требуется компьютерный класс, оснащенный персональными ЭВМ и соответствующим программным обеспечением. Состав оборудования определен в Паспорте компьютерного класса.
Для самостоятельной работы требуется аудитория, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченный доступом в электронную информационно-образовательную среду университета, а так же помещения Научной библиотеки ПГНИУ.
Индивидуальные и групповые консультации - аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программный обеспечением, меловой (и) или маркерной доской или аудитория, оснащенная меловой (и) или маркерной доской.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.
2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными

компьютерами с доступом к  локальной и глобальной компьютерным сетям.

3. Читальный зал естественной литературы,  корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к  локальной и глобальной компьютерным сетям.

4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к  локальной и глобальной компьютерным сетям.

5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к  локальной и глобальной компьютерным сетям.

6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к  локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

**Фонды оценочных средств для аттестации по дисциплине**
**Управление информационной безопасностью и цифровая грамотность**

**Планируемые результаты обучения по дисциплине для формирования компетенции. Индикаторы и критерии их оценивания**

**ОПК.4**

**Способен организовывать внедрение современных информационно-коммуникационных технологий в соответствующей сфере профессиональной деятельности и обеспечивать информационную открытость деятельности органа власти**

| Индикатор | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| **ОПК.4.1**<br>Организует внедрение современных информационно-коммуникационных технологий в соответствующей сфере профессиональной деятельности | Знать:<br>современные подходы к управлению информационной безопасностью и направлениях их развития, основные стандарты, регламентирующие управление ИБ.<br>Уметь:<br>использовать современные методы и средства, разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность.<br>Владеть:<br>Методикой внедрения современных информационно-коммуникационных технологий в соответствующей сфере профессиональной деятельности | **Неудовлетворител**<br>выставляется студенту, который не знает общие положения основного материала, не овладел навыками работы с программным обеспечением, допускает неточности в основных определениях, нарушение последовательности в изложении материала и испытывает трудности в выполнении практических заданий<br>**Удовлетворительн**<br>выставляется студенту, который знает общие положения основного материала, но не усвоил его деталей, допускает неточности в определениях и испытывает трудности в выполнении практических заданий<br>**Хорошо**<br>выставляется за твердое знание материала, способен применять программное обеспечение и информационные технологии по защите информации в информационных системах, правильное применение теоретических сведений, положений при решении практических задач и вопросов, владение практическими навыками решения задач<br>**Отлично**<br>оценивается знания студента, глубоко и прочно усвоившего программный материал данной темы, исчерпывающе, последовательно, грамотно и логически стройно его излагающего; при этом студент не затрудняется с ответом на видоизмененное задание, свободно справляется с задачами, вопросами и другими видами применения знаний, |

| Индикатор | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| | | **Отлично**<br>показывает знакомство с учебной литературой, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических работ на компьютере |

**ПК.2**

**Способен готовить экспертные заключения по проблемам государственного и муниципального управления**

| Индикатор | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| **ПК.2.2**<br>Проводит экспертизу нормативных документов и управленческих решений и дает рекомендации по ее итогам | Знать:<br>взаимосвязи отдельных процессов управления ИБ в рамках общей системы управления информационной безопасностью.<br>Уметь:<br>проводит экспертизу нормативных документов и управленческих решений и дает рекомендации по ее итогам.<br>Владеть:<br>навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом. | **Неудовлетворител**<br>выставляется студенту, который не знает общие положения основного материала, не овладел навыками работы с программным обеспечением, допускает неточности в основных определениях, нарушение последовательности в изложении материала и испытывает трудности в выполнении практических заданий<br>**Удовлетворительн**<br>выставляется студенту, который знает общие положения основного материала, но не усвоил его деталей, допускает неточности в определениях и испытывает трудности в выполнении практических заданий<br>**Хорошо**<br>выставляется за твердое знание материала, способен применять программное обеспечение и информационные технологии по защите информации в информационных системах, правильное применение теоретических сведений, положений при решении практических задач и вопросов, владение практическими навыками решения задач<br>**Отлично**<br>оценивается знания студента, глубоко и прочно усвоившего программный материал данной темы, исчерпывающе, последовательно, грамотно и логически стройно его излагающего; при этом студент не затрудняется с ответом на |

| Индикатор | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| | | **Отлично**<br>видоизмененное задание, свободно справляется с задачами, вопросами и другими видами применения знаний, показывает знакомство с учебной литературой, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических работ на компьютере |

## Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

**Вид мероприятия промежуточной аттестации :** Экзамен
**Способ проведения мероприятия промежуточной аттестации :** Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
**Максимальное количество баллов :** 100

**Конвертация баллов в отметки**

**«отлично» -** от 81 до 100
**«хорошо» -** от 61 до 80
**«удовлетворительно» -** от 50 до 60
**«неудовлетворительно» / «незачтено»** менее 50 балла

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|---|---|
| **Входной контроль** | Входной контроль<br>**Входное тестирование** | Знание: основные положений информационных технологий и информационных систем.Умение: осуществлять поиск и анализ информации с использование современных информационных технологий.Владение: методами решения задач управления и прогнозирования, методикой моделирования деятельности организации. |
| **ПК.2.2**<br>Проводит экспертизу нормативных документов и управленческих решений и дает рекомендации по ее итогам<br>**ОПК.4.1**<br>Организует внедрение современных информационно-коммуникационных технологий в соответствующей сфере профессиональной деятельности | Тема-3 Основы правового обеспечения информационной безопасности. Техническая защита информации.<br>**Защищаемое контрольное мероприятие** | Знать:современные подходы к управлению ИБ и направлениях их развития.Уметь:анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ.Владеть:навыками построения как отдельных процессов управления ИБ, так и системыпроцессов в целом. |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|---|---|
| **ПК.2.2** Проводит экспертизу нормативных документов и управленческих решений и дает рекомендации по ее итогам **ОПК.4.1** Организует внедрение современных информационно-коммуникационных технологий в соответствующей сфере профессиональной деятельности | Тема-5 Менеджмент и аудит систем информационной безопасности. Комплексная защита объектов информатизации. **Защищаемое контрольное мероприятие** | Знать: принципы разработки процессов управления ИБ.Уметь:разрабатывать и внедрять СУИБ и оценивать ее эффективность.Владеть:навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ. |
| **ПК.2.2** Проводит экспертизу нормативных документов и управленческих решений и дает рекомендации по ее итогам **ОПК.4.1** Организует внедрение современных информационно-коммуникационных технологий в соответствующей сфере профессиональной деятельности | Тема-6 Проблемы безопасности современных цифровых технологий. **Итоговое контрольное мероприятие** | Знать: государственную политику РФ в информационной сфере и информационной безопасности, содержание государственной системы и концепции правового обеспечения информационной деятельности и информационной безопасности предприятия.Уметь:используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность.Владеть: терминологией и процессным подходом построения систем управления ИБ, методами защиты информации и коммерческой тайны; |

## Спецификация мероприятий текущего контроля

### Входной контроль

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**
Проходной балл: **0**

| Показатели оценивания | Баллы |
|---|---|
| оценивается знания студента, глубоко и прочно усвоившего программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающего, в ответе тесно увязывающего теорию с практикой; при этом студент не затрудняется с ответом на видоизмененное задание, свободно справляется с задачами, вопросами и другими видами | 10 |

| | |
|---|---|
| применения знаний, показывает знакомство с учебной литературой, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических работ. | |
| выставляется за твердое знание материала, грамотное и конкретное его изложение, без существенных неточностей, правильное применение теоретических сведений, положений при решении практических задач и вопросов, владение практическими навыками и приемами. | 7 |
| выставляется студенту, который знает общие положения основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушение последовательности в изложении материала и испытывает трудности в выполнении практических заданий. | 5 |

**Тема-3 Основы правового обеспечения информационной безопасности. Техническая защита информации.**

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **15**

| Показатели оценивания | Баллы |
|---|---|
| На «30 баллов» оценивается знания студента, глубоко и прочно усвоившего программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающего, в ответе тесно увязывающего теорию с практикой; при этом студент не затрудняется с ответом на видоизмененное задание, свободно справляется с задачами, вопросами и другими видами применения знаний, показывает знакомство с учебной литературой, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических работ; | 30 |
| «20 баллов» выставляется за твердое знание материала, грамотное и конкретное его изложение, без существенных неточностей, правильное применение теоретических сведений, положений при решении практических задач и вопросов, владение практическими навыками и приемами; | 20 |
| «15 баллов» выставляется студенту, который знает общие положения основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушение последовательности в изложении материала и испытывает трудности в выполнении практических заданий. | 15 |

**Тема-5 Менеджмент и аудит систем информационной безопасности. Комплексная защита объектов информатизации.**

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **15**

| Показатели оценивания | Баллы |
|---|---|
| На «30 баллов» оценивается знания студента, глубоко и прочно усвоившего программный | 30 |

| | |
|---|---|
| материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающего, в ответе тесно увязывающего теорию с практикой; при этом студент не затрудняется с ответом на видоизмененное задание, свободно справляется с задачами, вопросами и другими видами применения знаний, показывает знакомство с учебной литературой, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических работ; | |
| «20 баллов» выставляется за твердое знание материала, грамотное и конкретное его изложение, без существенных неточностей, правильное применение теоретических сведений, положений при решении практических задач и вопросов, владение практическими навыками и приемами; | 20 |
| «15 баллов» выставляется студенту, который знает общие положения основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушение последовательности в изложении материала и испытывает трудности в выполнении практических заданий. | 15 |

**Тема-6 Проблемы безопасности современных цифровых технологий.**

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **20**

| **Показатели оценивания** | **Баллы** |
|---|---|
| На «40 баллов» оценивается знания студента, глубоко и прочно усвоившего программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающего, в ответе тесно увязывающего теорию с практикой; при этом студент не затрудняется с ответом на видоизмененное задание, свободно справляется с задачами, вопросами и другими видами применения знаний, показывает знакомство с учебной литературой, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических работ. | 40 |
| «30 баллов» выставляется за твердое знание материала, грамотное и конкретное его изложение, без существенных неточностей, правильное применение теоретических сведений, положений при решении практических задач и вопросов, владение практическими навыками и приемами. | 30 |
| «20 баллов» выставляется студенту, который знает общие положения основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушение последовательности в изложении материала и испытывает трудности в выполнении практических заданий. | 20 |