МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Директор филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске
_____ / Г.И. Заболотни
"_____" _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.02 «Кибербезопасность и криптография»

Код и направление подготовки (специальность)	13.04.02 Электроэнергетика и электротехника
Направленность (профиль)	Цифровая трансформация и управление проектами в электроэнергетике
Квалификация	Магистр
Форма обучения	Заочная
Год начала подготовки	2026
Институт / факультет	Кафедры филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске
Выпускающая кафедра	кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП)
Кафедра-разработчик	кафедра "Информатика и системы управления" (НФ-ИиСУ)
Объем дисциплины, ч. / з.е.	288 / 8
Форма контроля (промежуточная аттестация)	Зачет, Экзамен

Самара 2026

Б1.В.02 «Кибербезопасность и криптография»

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) **13.04.02 Электроэнергетика и электротехника**, утвержденного приказом Министерства образования и науки РФ от № 147 от 28.02.2018 и соответствующего учебного плана.

Разработчик РПД:

Доцент, кандидат технических наук	А.Н Лада
(должность, степень, ученое звание)	(ФИО)

Заведующий кафедрой	А.В. Волкодаева, кандидат экономических наук, доцент
	(ФИО, степень, ученое звание)

СОГЛАСОВАНО:

Председатель методического совета факультета / института (или учебно-методической комиссии)	Е.Т Демидова, кандидат юридических наук, доцент
	(ФИО, степень, ученое звание)
Руководитель образовательной программы	А.А. Складчиков, кандидат технических наук
	(ФИО, степень, ученое звание)
Заведующий выпускающей кафедрой	
	(ФИО, степень, ученое звание)

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Профессиональные компетенции			
Не предусмотрено	ПК-1 Способен участвовать в управлении проектами и цифровым развитием в сфере электроэнергетики	ПК-1.6 Использует методы обеспечения кибербезопасности	Владеть навыками использования методов обеспечения кибербезопасности и криптографии
			Знать методы обеспечения кибербезопасности и криптографии
			Уметь использовать методы обеспечения кибербезопасности и криптографии

2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины (модуля) в структуре образовательной программы: **часть, формируемая участниками образовательных отношений**

Код компетенции	Предшествующие дисциплины	Параллельно осваиваемые дисциплины	Последующие дисциплины

ПК-1		Машинное обучение в электроэнергетике; Микропроцессорные устройства релейной защиты и автоматики; Нейронные сети в среде R; Планирование электроэнергетических режимов электроэнергетических систем; Производственная практика: проектная практика; Стратегическое управление проектами цифровой трансформации; Управление информационной средой; Управление проектами в электроэнергетике; Управление ресурсами и сервисами информационных технологий; Управление рисками в проектах цифровой трансформации; Устройства телемеханики и телесигнализации; Элементы активно-адаптивной электрической сети	Подготовка к процедуре защиты и защита выпускной квалификационной работы; Производственная практика: преддипломная практика

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Вид учебной работы	Всего часов / часов в электронной форме	1 семестр часов / часов в электронной форме	2 семестр часов / часов в электронной форме	3 семестр часов / часов в электронной форме	4 семестр часов / часов в электронной форме
Аудиторная контактная работа (всего), в том числе:	12	4	2	4	2
Лекции	4	2	0	2	0
Практические занятия	8	2	2	2	2
Самостоятельная работа (всего), в том числе:	265	32	104	32	97
подготовка к практическим занятиям	265	32	104	32	97
Контроль	11	0	2	0	9
Итого: час	288	36	108	36	108
Итого: з.е.	8	1	3	1	3

4. Содержание дисциплины (модуля), структурированное по темам (разделам),

с указанием отведенного на них количества академических часов и видов учебных занятий

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	ЛР	ПЗ	СРС	Всего часов
1	Кибербезопасность в электроэнергетике	2	0	4	136	142
2	Основы криптографии	2	0	4	129	135
	Контроль	0	0	0	0	11
	Итого	4	0	8	265	288

4.1 Содержание лекционных занятий

№ занятия	Наименование раздела	Тема лекции	**Содержание лекции** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
1 семестр				
2	Кибербезопасность в электроэнергетике	1. Особенности организации кибербезопасности в электроэнергетике	Актуальность кибербезопасности в электроэнергетике. Компетенций в области кибербезопасности в электроэнергетике. Понятие данных, информации. Свойства информации. Операции с данными и информацией. Основные термины: защита информации, кибербезопасность, угроза, уязвимость, риск. Задачи обеспечения кибербезопасности. Базовые принципы кибербезопасности. Уязвимости в информационных системах в электроэнергетике. Классификация защищаемой информации. Базовые принципы кибербезопасности. Существующие российские и иностранные методики и стандарты обеспечения кибербезопасности. Применение моделирования для обеспечения кибербезопасности. Основные модели кибербезопасности. Модель ISO 27000.	1

3	Кибербезопасность в электроэнергетике	2. Организационное обеспечение и технические средства обеспечения кибербезопасности на объектах электроэнергетики	Виды законодательных мер обеспечения кибербезопасности. Виды информации по уровню доступа. Российское законодательство в области кибербезопасности. Российское законодательство в области кибербезопасности объектов электроэнергетики. Европейское законодательство в области кибербезопасности объектов электроэнергетики. Примеры противоправных действий. Организационные средства обеспечения кибербезопасности. Задачи организационные средств безопасности на объектах электроэнергетики. Классификация организационных мер. Политики безопасности организации. Регламенты и стандарты в области организационных мер обеспечения кибербезопасности. Оценка эффективности организационных мер. Роли и права доступа. Классификация технических средств защиты информации. Программные средства. Контроль доступа. Резервное копирование, архивирование, уничтожение. Шифрование, VPN, сетевой экран, сканер сети и портов. Антивирусы. Комплексные системы защиты. Обеспечение защиты объектов электроэнергетики при внедрении цифровых технологий. Технические меры: замки, устройства идентификация и аутентификация пользователей, защитная сигнализация, системы видеонаблюдения и т.д. Примеры на объектах электроэнергетики. Техническое обеспечение программных мер. Средства (модули) доверенной загрузки, электронный ключ, токен. Алгоритмические (криптографические меры), симметричные и асимметричные системы, хэш.	1
			Итого за семестр:	**2**
2 семестр				
6	Основы криптографии	3. Симметричное и асимметричное шифрование	Симметричное шифрование: принцип работы, преимущества, недостатки. Режимы работы блочных шифров (ECB, CBC, CTR, GCM). Асимметричное шифрование использует пару ключей: открытый (публичный) для шифрования и закрытый (приватный) для дешифрования (например, RSA, ECC, ElGamal). Гибридные криптосистемы (реальность современного мира). Основные атаки на симметричные и асимметричные системы.	1

8	Основы криптографии	4. Хеш-функции и электронная подпись	Криптографические хеш-функции, преобразующие входные данные произвольной длины в выходное значение фиксированной длины (хеш, дайджест сообщения). Основные требования: односторонность (необратимость): по хешу невозможно (вычислительно сложно) восстановить исходное сообщение; устойчивость к коллизиям: вычислительно сложно найти два разных сообщения с одинаковым хешем (второе свойство); лавинный эффект: малейшее изменение в исходных данных приводит к значительному изменению хеш-значения (не менее половины бит). Электронная подпись. Механизм, обеспечивающий подлинность и целостность электронного документа. Связь с асимметричной криптографией: подпись создается с использованием закрытого ключа отправителя, а проверяется с помощью его открытого ключа (обратный порядок по сравнению с шифрованием). Типичный процесс создания подписи. Процесс проверки подписи. Типы электронных подписей: простая, усиленная неквалифицированная, усиленная квалифицированная (юридическая сила, требования к сертификатам, ФСБ РФ). Примеры алгоритмов: RSA-PSS, DSA, ECDSA, ГОСТ Р 34.10-2012 (на эллиптических кривых).	1
			Итого за семестр:	**2**
			Итого:	**4**

4.2 Содержание лабораторных занятий

Учебные занятия не реализуются.

4.3 Содержание практических занятий

№ занятия	**Наименование раздела**	**Тема практического занятия**	**Содержание практического занятия** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	**Количество часов / часов в электронной форме**
1 семестр				

4	Кибербезопасность в электроэнергетике	1. Особенности организации кибербезопасности в электроэнергетике	Актуальность кибербезопасности в электроэнергетике. Компетенций в области кибербезопасности в электроэнергетике. Понятие данных, информации. Свойства информации. Операции с данными и информацией. Основные термины: защита информации, кибербезопасность, угроза, уязвимость, риск. Задачи обеспечения кибербезопасности. Базовые принципы кибербезопасности. Уязвимости в информационных системах в электроэнергетике. Классификация защищаемой информации. Базовые принципы кибербезопасности. Существующие российские и иностранные методики и стандарты обеспечения кибербезопасности. Применение моделирования для обеспечения кибербезопасности. Основные модели кибербезопасности. Модель ISO 27000. Классификация кибер-угроз. Особенности кибер-угроз на объектах электроэнергетики. Техногенные угрозы. Внешние антропогенные угрозы. Внутренне антропогенные угрозы. Классификация способов обеспечения кибербезопасности. Правовые средства. Организационные средства. Программные, аппаратные и алгоритмические средства. Управление рисками. Управление рисками при обеспечении безопасности объектов электроэнергетики. Методики управления рисками. Расчет экономической эффективности мер кибербезопасности.	2

5	Кибербезопасность в электроэнергетике	2. Организационное обеспечение и технические средства обеспечения кибербезопасности на объектах электроэнергетики	Виды законодательных мер обеспечения кибербезопасности. Виды информации по уровню доступа. Российское законодательство в области кибербезопасности. Российское законодательство в области кибербезопасности объектов электроэнергетики. Европейское законодательство в области кибербезопасности объектов электроэнергетики. Примеры противоправных действий. Организационные средства обеспечения кибербезопасности. Задачи организационные средств безопасности на объектах электроэнергетики. Классификация организационных мер. Политики безопасности организации. Регламенты и стандарты в области организационных мер обеспечения кибербезопасности. Оценка эффективности организационных мер. Роли и права доступа. Классификация технических средств защиты информации. Программные средства. Контроль доступа. Резервное копирование, архивирование, уничтожение. Шифрование, VPN, сетевой экран, сканер сети и портов. Антивирусы. Комплексные системы защиты. Обеспечение защиты объектов электроэнергетики при внедрении цифровых технологий. Технические меры: замки, устройства идентификация и аутентификация пользователей, защитная сигнализация, системы видеонаблюдения и т.д. Примеры на объектах электроэнергетики. Техническое обеспечение программных мер. Средства (модули) доверенной загрузки, электронный ключ, токен. Алгоритмические (криптографические меры), симметричные и асимметричные системы, хэш.	2
			Итого за семестр:	**4**
2 семестр				
9	Основы криптографии	3. Симметричное и асимметричное шифрование	Симметричное шифрование: принцип работы, преимущества, недостатки. Режимы работы блочных шифров (ECB, CBC, CTR, GCM). Асимметричное шифрование использует пару ключей: открытый (публичный) для шифрования и закрытый (приватный) для дешифрования (например, RSA, ECC, ElGamal). Гибридные криптосистемы (реальность современного мира). Основные атаки на симметричные и асимметричные системы.	2

13	Основы криптографии	4. Хеш-функции и электронная подпись	Криптографические хеш-функции, преобразующие входные данные произвольной длины в выходное значение фиксированной длины (хеш, дайджест сообщения). Основные требования: односторонность (необратимость): по хешу невозможно (вычислительно сложно) восстановить исходное сообщение; устойчивость к коллизиям: вычислительно сложно найти два разных сообщения с одинаковым хешем (второе свойство); лавинный эффект: малейшее изменение в исходных данных приводит к значительному изменению хеш-значения (не менее половины бит). Электронная подпись. Механизм, обеспечивающий подлинность и целостность электронного документа. Связь с асимметричной криптографией: подпись создается с использованием закрытого ключа отправителя, а проверяется с помощью его открытого ключа (обратный порядок по сравнению с шифрованием). Типичный процесс создания подписи. Процесс проверки подписи. Типы электронных подписей: простая, усиленная неквалифицированная, усиленная квалифицированная (юридическая сила, требования к сертификатам, ФСБ РФ). Примеры алгоритмов: RSA-PSS, DSA, ECDSA, ГОСТ Р 34.10-2012 (на эллиптических кривых).	2
			Итого за семестр:	**4**
			Итого:	**8**

4.4. Содержание самостоятельной работы

Наименование раздела	**Вид самостоятельной работы**	**Содержание самостоятельной работы** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	**Количество часов**
1 семестр			

Кибербезопасность в электроэнергетике	Подготовка к практическим занятиям	Актуальность кибербезопасности в электроэнергетике. Компетенций в области кибербезопасности в электроэнергетике. Понятие данных, информации. Свойства информации. Операции с данными и информацией. Основные термины: защита информации, кибербезопасность, угроза, уязвимость, риск. Задачи обеспечения кибербезопасности. Базовые принципы кибербезопасности. Уязвимости в информационных системах в электроэнергетике. Классификация защищаемой информации. Базовые принципы кибербезопасности. Существующие российские и иностранные методики и стандарты обеспечения кибербезопасности. Применение моделирования для обеспечения кибербезопасности. Основные модели кибербезопасности. Модель ISO 27000. Классификация кибер-угроз. Особенности кибер-угроз на объектах электроэнергетики. Техногенные угрозы. Внешние антропогенные угрозы. Внутренне антропогенные угрозы. Классификация способов обеспечения кибербезопасности. Правовые средства. Организационные средства. Программные, аппаратные и алгоритмические средства. Управление рисками. Управление рисками при обеспечении безопасности объектов электроэнергетики. Методики управления рисками. Расчет экономической эффективности мер кибербезопасности.	32
		Итого за семестр:	**32**
2 семестр			

Кибербезопасность в электроэнергетике	1	Виды законодательных мер обеспечения кибербезопасности. Виды информации по уровню доступа. Российское законодательство в области кибербезопасности. Российское законодательство в области кибербезопасности объектов электроэнергетики. Европейское законодательство в области кибербезопасности объектов электроэнергетики. Примеры противоправных действий. Организационные средства обеспечения кибербезопасности. Задачи организационные средств безопасности на объектах электроэнергетики. Классификация организационных мер. Политики безопасности организации. Регламенты и стандарты в области организационных мер обеспечения кибербезопасности. Оценка эффективности организационных мер. Роли и права доступа. Классификация технических средств защиты информации. Программные средства. Контроль доступа. Резервное копирование, архивирование, уничтожение. Шифрование, VPN, сетевой экран, сканер сети и портов. Антивирусы. Комплексные системы защиты. Обеспечение защиты объектов электроэнергетики при внедрении цифровых технологий. Технические меры: замки, устройства идентификация и аутентификация пользователей, защитная сигнализация, системы видеонаблюдения и т.д. Примеры на объектах электроэнергетики. Техническое обеспечение программных мер. Средства (модули) доверенной загрузки, электронный ключ, токен. Алгоритмические (криптографические меры), симметричные и асимметричные системы, хэш.	104
		Итого за семестр:	**104**
3 семестр			

Основы криптографии	1	Симметричное шифрование: принцип работы, преимущества, недостатки. Режимы работы блочных шифров (ECB, CBC, CTR, GCM). Асимметричное шифрование использует пару ключей: открытый (публичный) для шифрования и закрытый (приватный) для дешифрования (например, RSA, ECC, ElGamal). Гибридные криптосистемы (реальность современного мира). Основные атаки на симметричные и асимметричные системы.	32
		Итого за семестр:	**32**
		4 семестр	
Основы криптографии	1	Криптографические хеш-функции, преобразующие входные данные произвольной длины в выходное значение фиксированной длины (хеш, дайджест сообщения). Основные требования: односторонность (необратимость): по хешу невозможно (вычислительно сложно) восстановить исходное сообщение; устойчивость к коллизиям: вычислительно сложно найти два разных сообщения с одинаковым хешем (второе свойство); лавинный эффект: малейшее изменение в исходных данных приводит к значительному изменению хеш-значения (не менее половины бит). Электронная подпись. Механизм, обеспечивающий подлинность и целостность электронного документа. Связь с асимметричной криптографией: подпись создается с использованием закрытого ключа отправителя, а проверяется с помощью его открытого ключа (обратный порядок по сравнению с шифрованием). Типичный процесс создания подписи. Процесс проверки подписи. Типы электронных подписей: простая, усиленная неквалифицированная, усиленная квалифицированная (юридическая сила, требования к сертификатам, ФСБ РФ). Примеры алгоритмов: RSA-PSS, DSA, ECDSA, ГОСТ Р 34.10-2012 (на эллиптических кривых).	97
		Итого за семестр:	**97**
		Итого:	**265**

5. Перечень учебной литературы и учебно-методического обеспечения по

дисциплине (модулю)

№ п/п	Библиографическое описание	Ресурс НТБ СамГТУ (ЭБС СамГТУ, IPRbooks и т.д.)
Основная литература		
1	Губарева, К.В. Системы мониторинга и управления инженерной инфраструктурой : учебное пособие / К. В. Губарева; Самарский государственный технический университет, Промышленная теплоэнергетика.- Самара, 2025.- 93 с..- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||elib||6465	Электронный ресурс
2	Криптография и безопасность сетей: учебное пособие / Фороузан Б.А., Профобразование, ред. Берлина А.Н.: 2024.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||139752	Электронный ресурс
3	Основы криптографии: учебное пособие / Басалова Г.В., Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа: 2024.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||133959	Электронный ресурс
4	Технологии искусственного интеллекта и кибербезопасность: монография / Менисов А.Б., Ай Пи Ар Медиа: 2022.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||123570	Электронный ресурс
Дополнительная литература		
5	Кибербезопасность: стратегии атак и обороны: монография / Диогенес Ю., Озкайя Э., ДМК Пресс, пер. Беликов Д.А.: 2020.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||124557	Электронный ресурс
6	Криптография – наука о тайнописи: учебное пособие / Фомичев В.М., Прометей: 2020.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||125666	Электронный ресурс
7	Основы криптографии: учебное пособие / Басалова Г.В., Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа: 2024.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||133959	Электронный ресурс
8	Современные методы криптографии и кодирования: учебное пособие / Данилов С.Н., Инфра-Инженерия: 2025.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||154449	Электронный ресурс

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование.

Организовано взаимодействие обучающегося и преподавателя с использованием электронной ин-формационной образовательной среды университета.

№ п/п	Наименование	Производитель	Способ распространения

1	Образовательная платформа «Юрайт»	ООО «ЭЛЕКТРОННОЕ ИЗДАТЕЛЬСТВО ЮРАЙТ» (Отечественный)	Лицензионное
2	Microsoft Office	Microsoft (Зарубежный)	Лицензионное
3	МойОфис Образование	ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ» (Отечественный)	Лицензионное

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

№ п/п	Наименование	Краткое описание	Режим доступа
1	Science online	http://www.sciencemag.org	Зарубежные базы данных ограниченного доступа
2	ВИНИТИ – Всероссийский Институт научной и технической информации		Российские базы данных ограниченного доступа
3	Электронная библиотека изданий СамГТУ	http://irbis.samgtu.local/cgi-bin/irbis64r_01/cgiirbis_64.exe	Российские базы данных ограниченного доступа
4	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/	Российские базы данных ограниченного доступа

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия

Аудитория для лекционных, семинарских и практических занятий, текущего контроля и промежуточной аттестации (с мультимедийным оборудованием) укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Практические занятия

Аудитория для практических и семинарских занятий, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (проектор, экран, компьютер/ноутбук), с выходом в сеть Интернет и доступом в электронную информационно-образовательную среду СамГТУ. Аудитория оборудована специализированной мебелью: столы и стулья для обучающихся; стол и стул для преподавателя, доска.

- компьютерные классы (ауд. 101, 102, 201, 401).

Самостоятельная работа

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде СамГТУ:

- Кабинет для текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций ауд. 212;
- Кабинет для самостоятельной работы, аудитория 304;
- компьютерные классы (ауд. 101, 102, 111, 201, 401, 404).

9. Методические материалы

Методические рекомендации при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции с тем, чтобы иметь представление о проблемах, которые будут разбираться в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т.е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплен в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т.п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

Конспектирование лекции позволяет обработать, систематизировать и лучше сохранить полученную информацию с тем, чтобы в будущем можно было восстановить в памяти основные, содержательные моменты. Типичная ошибка, совершаемая обучающимся, дословное конспектирование речи преподавателя. Как правило, при записи «слово в слово» не остается времени на обдумывание, анализ и синтез информации. Отбирая нужную информацию, главные мысли, проблемы, решения и выводы, необходимо сокращать текст, строить его таким образом, чтобы потом можно было легко в нем разобраться. Желательно оставить в рабочих конспектах поля, на которых можно будет делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С окончанием лекции работа над конспектом не может считаться завершенной. Нужно еще восстановить отдельные места, проверить, все ли понятно, уточнить что-то на консультации и т.п. с тем, чтобы конспект мог быть использован в процессе подготовки к практическим занятиям, зачету, экзамену. Конспект лекции – незаменимый учебный документ, необходимый для самостоятельной работы.

Методические рекомендации при подготовке и работе на практическом занятии

Практические занятия по дисциплине проводятся в целях выработки практических умений и приобретения навыков в решении профессиональных задач.

Рекомендуется следующая схема подготовки к практическому занятию:

1. ознакомление с планом практического занятия, который отражает содержание предложенной темы;
2. проработка конспекта лекции;
3. чтение рекомендованной литературы;
4. подготовка ответов на вопросы плана практического занятия;
5. выполнение тестовых заданий, задач и др.

Подготовка обучающегося к практическому занятию производится по вопросам, разработанным для каждой темы практических занятий и (или) лекций. В процессе подготовки к практическим

занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы.

Работа студентов во время практического занятия осуществляется на основе заданий, которые выдаются обучающимся в начале или во время занятия. На практических занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике занятий. Обучающимся необходимо обращать внимание на основные понятия, алгоритмы, определять практическую значимость рассматриваемых вопросов. На практических занятиях обучающиеся должны уметь выполнить расчет по заданным параметрам или выработать определенные решения по обозначенной проблеме. Задания могут быть групповые и индивидуальные. В зависимости от сложности предлагаемых заданий, целей занятия, общей подготовки обучающихся преподаватель может подсказать обучающимся алгоритм решения или первое действие, или указать общее направление рассуждений. Полученные результаты обсуждаются с позиций их адекватности или эффективности в рассмотренной ситуации.

Методические рекомендации по выполнению самостоятельной работы

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;
- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.;
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

10. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств представлен в приложении № 1.

Приложение 1 к рабочей программе дисциплины
Б1.В.02 «Кибербезопасность и криптография»

Фонд оценочных средств
по дисциплине
Б1.В.02 «Кибербезопасность и криптография»

Код и направление подготовки (специальность)	13.04.02 Электроэнергетика и электротехника
Направленность (профиль)	Цифровая трансформация и управление проектами в электроэнергетике
Квалификация	Магистр
Форма обучения	Заочная
Год начала подготовки	2026
Институт / факультет	Кафедры филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске
Выпускающая кафедра	кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП)
Кафедра-разработчик	кафедра "Информатика и системы управления" (НФ-ИиСУ)
Объем дисциплины, ч. / з.е.	288 / 8
Форма контроля (промежуточная аттестация)	Зачет, Экзамен

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Профессиональные компетенции			
Не предусмотрено	ПК-1 Способен участвовать в управлении проектами и цифровым развитием в сфере электроэнергетики	ПК-1.6 Использует методы обеспечения кибербезопасности	Владеть навыками использования методов обеспечения кибербезопасности и криптографии
			Знать методы обеспечения кибербезопасности и криптографии
			Уметь использовать методы обеспечения кибербезопасности и криптографии

Матрица соответствия оценочных средств запланированным результатам обучения

Код индикатора достижения компетенции	Результаты обучения	Оценочные средства	Текущий контроль успеваемости	Промежуточная аттестация
Кибербезопасность в электроэнергетике				
ПК-1.6 Использует методы обеспечения кибербезопасности	**Знать** методы обеспечения кибербезопасности и криптографии	оценочные средства промежуточного контроля	Нет	Да
	Владеть навыками использования методов обеспечения кибербезопасности и криптографии	оценочные средства промежуточного контроля	Нет	Да
	Уметь использовать методы обеспечения кибербезопасности и криптографии	оценочные средства промежуточного контроля	Нет	Да
	Знать методы обеспечения кибербезопасности и криптографии	тест	Да	Нет
	Владеть навыками использования методов обеспечения кибербезопасности и криптографии	практические задания	Да	Нет
	Уметь использовать методы обеспечения кибербезопасности и криптографии	практические задания	Да	Нет
Основы криптографии				

ПК-1.6 Использует методы обеспечения кибербезопасности	**Владеть** навыками использования методов обеспечения кибербезопасности и криптографии	практические задания	Да	Нет
	Знать методы обеспечения кибербезопасности и криптографии	тест	Да	Нет
	Уметь использовать методы обеспечения кибербезопасности и криптографии	практические задания	Да	Нет
	Владеть навыками использования методов обеспечения кибербезопасности и криптографии	оценочные средства промежуточного контроля	Нет	Да
	Знать методы обеспечения кибербезопасности и криптографии	оценочные средства промежуточного контроля	Нет	Да
	Уметь использовать методы обеспечения кибербезопасности и криптографии	оценочные средства промежуточного контроля	Нет	Да

Типовые задания для промежуточной аттестации по дисциплине
Б1.В.02 «Кибербезопасность и криптография»
(шифр и наименование дисциплины)

для направления подготовки 13.04.02 Электроэнергетика и электротехника
(шифр и наименование направления подготовки, специальности)

2026 ГОД ПРИЕМА
(год приема на образовательную программу)

Контролируемая (ые) компетенция(и):
ПК-1 *Способен участвовать в управлении проектами и цифровым развитием в сфере электроэнергетики*
(шифр и наименование компетенции(й))

Спецификация тестовых заданий

Содержание дисциплины (разделы / темы)	Число заданий									
	закрытые			открытые				комбинированные		всего
	однозначный выбор варианта ответа	многозначный выбор варианта ответа	задание на сопоставление	задание на установление правильной последовательности	задания на дополнение	задания с развернутым ответом	практико-ориентированные задания	Задания с выбором одного ответа и обоснованием выбора ответа	Задания с выбором нескольких ответов и обоснованием выбора ответов	
Раздел 1. Кибербезопасность в электроэнергетике	**6**	**9**	**6**	**7**	**7**	**7**				
Тема 1. Особенности организации кибербезопасности в электроэнергетике	2	4	3	4	3	3				19
Тема 2. Организационное обеспечение и технические средства обеспечения кибербезопасности на объектах электроэнергетики	4	5	3	3	4	4				23
Раздел 2. Основы криптографии	**5**	**8**	**5**	**6**	**7**	**5**				
Тема 3. Симметричное и асимметричное шифрование	2	3	2	3	3	2				15
Тема 4. Хеш-функции и электронная подпись	3	5	3	3	4	3				21
Итого	**11**	**17**	**11**	**13**	**14**	**12**				**78**

Количество заданий в комплекте оценочных материалов

Код компетенции	Наименование компетенции	Количество заданий
ПК-1	Способен участвовать в управлении проектами и цифровым развитием в сфере электроэнергетики	78

Сценарии выполнения диагностических заданий

Тип задания	Последовательность действий при выполнении задания
Задание закрытого типа с однозначным выбором варианта ответа	1. Внимательно прочитать текст задания. 2. Выбрать единственный вариант ответа из предложенных.

Задание закрытого типа с многозначным выбором вариантов ответа	1. Внимательно прочитать текст задания. 2. Выбрать несколько вариантов ответа из предложенных.
Задание закрытого типа на установление соответствия	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 - вопросы, утверждения, факты, понятия и т.д.; список 2 - утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать буквы вариантов ответа (например, АБВГ)
Задание закрытого типа на установление последовательности	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. 2. Внимательно прочитать предложенные варианты ответа. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы вариантов ответа в нужной последовательности без пробелов и знаков препинания (например, БВА)
Задание открытого типа на дополнение	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается недостающее дополнение. 2. Определить какой информации не хватает. 3. Внесение пропущенного слова. 4. Записать в ответ только дополнение.
Задание открытого типа с развернутым ответом	1. Внимательно прочитать текст задания и понять суть вопроса. 2. Продумать логику и полноту ответа. 3. Записать ответ, используя четкие компактные формулировки. 4. В случае расчетной задачи записать решение и ответ.
Задание комбинированного типа: практико-ориентированные задания	1. Внимательно прочитать текст задания. 2. Выполните указанные в задания действия
Задание комбинированного типа с выбором одного ответа и обоснованием выбора ответа	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один ответ, наиболее верный. 4. Записать только букву выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа
Задание комбинированного типа с выбором нескольких ответов и обоснованием выборов ответов	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать несколько верных вариантов ответов. 4. Записать последовательно буквы выбранных вариантов без пробелов и знаков препинания (например, АБВ). 5. Записать аргументы, обосновывающие выбор каждого из ответов

Система оценивания заданий

Указания по оцениванию	**Результат оценивания (баллы, полученные за выполнение задания / характеристика правильности ответа)**
Задание закрытого типа с однозначным выбором варианта ответа считается верным, если правильно определен вариант ответа	За правильный вариант ответа начисляется 1 балл
Задание закрытого типа с многозначным выбором вариантов ответа считается верным, если правильно определены все варианты ответа	За правильный вариант ответа начисляется 1 балл
Задание закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Количество баллов определяется числом пар для сопоставления. За каждое правильно установленное соответствие начисляется 1 балл.
Задание закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Максимальный балл определяется количеством элементов в последовательности. В случае ошибки в одном месте - снижение на один балл. За каждое правильно указанное место элемента в последовательности начисляется 1 балл.
Задание открытого типа на дополнение, где предоставляется предложение или фрагмент текста, в котором пропущено одно или несколько слов или фраз. Задача состоит в том, чтобы заполнить пропуски, восстановив тем самым исходный смысл предложения.	2 балла засчитывается, если студент вписал правильный ответ в соответствии с ключом. 1 балл может быть засчитан за близкий к правильному ответ, если он демонстрирует частичное понимание.
Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте	Максимальный балл - 4. Студент может получить 4 балла за полный и правильный ответ, логично изложенный и с корректной терминологией, или

	меньше за неполные или неточно сформулированные ответы. Полнота (1 балл), Правильность (1 балл), Логичность (1 балл), Терминология (1 балл).
Задание комбинированного типа с выбором одного ответа и обоснованием выбора ответа считается верным, если правильно указана цифра и приведены корректные аргументы, используемые при выборе ответа	За правильный выбор ответа начисляется 1 балл. За качественное обоснование - еще 2-3 балла. Критерии оценивания обоснования должны быть четко определены (например, логичность, полнота, использование фактов). Неправильный выбор ответа - 0 баллов, даже если обоснование частично верное.
Задание комбинированного типа с выбором нескольких вариантов ответа и обоснованием выбора ответа считается верным, если правильно указана цифра и приведены корректные аргументы, используемые при выборе ответа	За правильный выбор ответа начисляется 1 балл. За качественное обоснование - еще 2-3 балла. Критерии оценивания обоснования должны быть четко определены (например, логичность, полнота, использование фактов). Неправильный выбор ответа - 0 баллов, даже если обоснование частично верное.

Тестовые задания с ключами ответов

№ задания	*Содержание задания*	*Ответ на задание*	*Тип задания*	*Уровень сложности (балл)*	*№ Темы*
***ПК-1** Способен участвовать в управлении проектами и цифровым развитием в сфере электроэнергетики*					
1.	**Прочитайте и дополните фразу:** Слабая сторона (недостаток) в информационной системе или её компонентах, которая может быть использована для реализации угрозы, называется _____ .	уязвимостью	Задание открытого типа на дополнение	2	1
2.	**Прочитайте и дополните фразу:** Категория киберугроз, источником которых являются действия человека (умышленные или неумышленные), называется _____.	антропогенными угрозами	Задание открытого типа на дополнение	2	1
3.	**Прочитайте и дополните фразу:** Классификация способов обеспечения кибербезопасности включает правовые, организационные, программные, _____ и алгоритмические средства.	аппаратные	Задание открытого типа на дополнение	2	1
4.	**Прочитайте вопрос и дайте развернутый ответ.** Укажите три основные задачи обеспечения кибербезопасности применительно к объектам электроэнергетики.	1) Обеспечение бесперебойной работы технологических систем управления (АСУ ТП). 2) Защита критической информации от утечки. 3) Обеспечение целостности и достоверности управляющих команд.	Задание открытого типа с развернутым ответом	4	1
5.	**Прочитайте вопрос и дайте развернутый ответ.** Назовите три специфических особенности киберугроз для объектов электроэнергетики (в отличие от обычных корпоративных сетей).	1) Приоритет безопасности (Safety) над информационной безопасностью (Security). 2) Длительный жизненный цикл оборудования (10-25 лет). 3) Связь с физическими процессами (кибер-физические системы)..	Задание открытого типа с развернутым ответом	4	1
6.	**Прочитайте вопрос и дайте развернутый ответ.**	1) Конфиденциальность	Задание открытого типа с	4	1

№ задания	*Содержание задания*	*Ответ на задание*	*Тип задания*	*Уровень сложности (балл)*	*№ Темы*
	Назовите три базовых принципа кибербезопасности (модель CIA)	2) Целостность 3) Доступность	развернутым ответом		
7.	**Упорядочите этапы процесса управления рисками (согласно общему подходу) в их логической последовательности:** 1. Обработка рисков (выбор и внедрение мер). 2. Идентификация рисков (активы, угрозы, уязвимости). 3. Оценка и анализ рисков (вероятность, ущерб). 4. Мониторинг и пересмотр рисков. Ответ запишите в виде последовательности цифр через запятую слева направо.	2,3,1,4	Задание закрытого типа на установление последовательности	1	1
8.	**Упорядочите стадии развития кибератаки на объект электроэнергетики (модель «киллчейн»):** 1. Нарушение физического процесса (срабатывание нештатных режимов, отключение). 2. Разведка и сбор информации о конфигурации. 3. Проникновение в сегмент АСУ ТП через шлюз (промышленный периметр). 4. Закрепление в системе и изучение логики технологического процесса. Ответ запишите в виде последовательности цифр через запятую слева направо.	2,3,4,1	Задание закрытого типа на установление последовательности	1	1
9.	**Упорядочите иерархию информации по степени критичности (от наиболее защищаемой к наименее):** 1. Параметры оперативного режима энергосистемы (current, P, Q). 2. Технологические данные открытых источников (типы оборудования). 3. Пароли и ключи шифрования АСУ ТП. 4. Регламентные (плановые) отчёты о работе оборудования. Ответ запишите в виде последовательности цифр через запятую слева направо.	3,1,4,2	Задание закрытого типа на установление последовательности	1	1
10.	**Упорядочите классы уязвимостей по их происхождению (от проектных до эксплуатационных):** 1. Ошибки конфигурации, оставшиеся пароли по умолчанию. 2. Отсутствие обновлений безопасности (незакрытые бэкдоры). 3. Архитектурные недостатки протоколов (например, Modbus без аутентификации). Ответ запишите в виде последовательности цифр через запятую слева направо.	3,1,2	Задание закрытого типа на установление последовательности	1	1
11.	**Прочитайте текст вопроса и соотнесите классификации угроз с их источниками:** <u>Классификации:</u> 1) Техногенные угрозы; 2) Внешние антропогенные угрозы;	<table><tr><td>1</td><td>2</td><td>3</td></tr><tr><td>Б</td><td>В</td><td>А</td></tr></table>	Задание закрытого типа на установление соответствия	1	1

№ задания	*Содержание задания*	*Ответ на задание*	*Тип задания*	*Уровень сложности (балл)*	*№ Темы*
	3) Внутренние антропогенные угрозы. Источники: А) Ошибки собственных сотрудников (операторов АСУ ТП, неосторожные действия электромонтёров). Б) Отказы оборудования, ошибки ПО, наводки, помехи. В) Хакерские атаки из интернета, атаки конкурентов, промышленный шпионаж. Запишите выбранные буквы под соответствующими цифрами: 1 2 3 _ _ _				
12.	**Прочитайте текст вопроса и соотнесите категории средств защиты с формами их реализации:** Категории: 1) Организационные средства; 2) Программно-аппаратные средства (технические); 3) Правовые средства. Реализация: А) Регламенты доступа, должностные инструкции, обучение персонала, физическая охрана. Б) Федеральные законы («О безопасности КИИ РФ» — 187-ФЗ), постановления правительства. В) Межсетевые экраны (NGFW), системы обнаружения вторжений (IDS/IPS), антивирусы. Запишите выбранные буквы под соответствующими цифрами: 1 2 3 _ _ _	1 2 3 А В Б	Задание закрытого типа на установление соответствия	1	1
13.	**Прочитайте текст вопроса и соотнесите понятия с их определениями:** Понятия: 1) Защита информации; 2) Кибербезопасность; 3) Риск. Определения: А) Сочетание вероятности наступления события (угрозы) и его последствий (ущерба). Б) Деятельность по предотвращению утечки, хищения, утраты, искажения, подделки, несанкционированного доступа (широкое понятие). В) Более узкое понятие, охватывающее защиту только киберпространства (каналов связи, сетей, ПО) от кибератак. Запишите выбранные буквы под соответствующими цифрами: 1 2 3 _ _ _	1 2 3 Б В А	Задание закрытого типа на установление соответствия	1	1
14.	**Прочитайте вопрос и выберите верный ответ:** Укажите какое свойство информации в энергетике является наиболее приоритетным (в отличие от банковской сферы): А) Конфиденциальность;	Б	Задание закрытого типа с однозначным выбором варианта ответа	1	1

№ задания	*Содержание задания*	*Ответ на задание*	*Тип задания*	*Уровень сложности (балл)*	*№ Темы*
	Б) Доступность (безотказность управляющих систем); В) Полнота; Г) Актуальность.				
15.	**Прочитайте вопрос и выберите верный ответ:** «Уязвимость нулевого дня» (zero-day vulnerability) – это: А) Уязвимость, которая не требует никаких усилий для эксплуатации; Б) Уязвимость, обнаруженная до того, как для неё выпущено обновление (патч); В) Уязвимость, существующая только при выключенном питании; Г) Уязвимость, характерная только для старых операционных систем.	Б	Задание закрытого типа с однозначным выбором варианта ответа	1	1
16.	**Прочитайте и выберите два верных ответа:** Укажите какие из перечисленных факторов отличают обеспечение кибербезопасности АСУ ТП электростанции от обычного офисного сегмента сети: А) Реальный приоритет безопасности Людей и отсутствия аварий (Safety) над информационной безопасностью (Security); Б) Долгий жизненный цикл оборудования (10–20 лет) без процедуры обновления ПО; В) Отсутствие требований к электромагнитной совместимости оборудования; Г) Все операторы имеют неограниченный доступ в интернет.	А, Б	Задание закрытого типа с многозначным выбором варианта ответа	1	1
17.	**Прочитайте и выберите два верных ответа:** К внешним антропогенным киберугрозам в электроэнергетике относятся: А) DDoS-атака на публичный портал компании с целью информационной блокады; Б) Заражение компьютера в технологической сети через инфицированную флешку, занесённую незаметно (физическое проникновение); В) Ложное срабатывание релейной защиты из-за грозового разряда; Г) Ошибка диспетчера при ручном вводе команды.	А, Б	Задание закрытого типа с многозначным выбором варианта ответа	1	1
18.	**Прочитайте и выберите два верных ответа:** Идентификация рисков кибербезопасности включает стадии: А) Определение информационных активов (что защищаем); Б) Оценка экономической эффективности мер защиты; В) Выявление актуальных угроз и уязвимостей для конкретного объекта; Г) Разработка политики управления паролями.	А, В	Задание закрытого типа с многозначным выбором варианта ответа	1	1

№ задания	*Содержание задания*	*Ответ на задание*	*Тип задания*	*Уровень сложности (балл)*	*№ Темы*
19.	**Прочитайте и выберите два верных ответа:** К организационно-распорядительным мерам кибербезопасности относятся средства: А) Инструкция о действиях персонала при обнаружении подозрительного ПО; Б) Межсетевой экран (Firewall); В) Допуск персонала к коммерческой тайне и контроль доступа в ЦОД; Г) Система резервного копирования.	А, В	Задание закрытого типа с многозначным выбором варианта ответа	1	1
20.	**Прочитайте и дополните фразу:** Совокупность законодательных актов, нормативных документов, регламентов и организационных мер, направленных на защиту информации, называется _____	организационным обеспечением кибербезопасности.	Задание открытого типа на дополнение	2	2
21.	**Прочитайте и дополните фразу:** Устройство (программное или программно-аппаратное), осуществляющее фильтрацию сетевого трафика в соответствии с заданными правилами, называется _____	сетевым экраном	Задание открытого типа на дополнение	2	2
22.	**Прочитайте и дополните фразу:** Программно-аппаратное средство для защищённого хранения ключей, сертификатов и выполнения криптографических операций, имеющее форму USB-брелока, называется _____ (токен).	электронным ключом	Задание открытого типа на дополнение	2	2
23.	**Прочитайте и дополните фразу:** Процесс создания резервных копий данных для их последующего восстановления при сбое или атаке называется _____	резервным копированием.	Задание открытого типа на дополнение	2	2
24.	**Прочитайте вопрос и дайте развернутый ответ.** Назовите три основные категории технических средств защиты информации (ТСЗИ) на объектах электроэнергетики по их функциональному назначению.	1) Средства контроля доступа и идентификации. 2) Средства защиты от вторжений и разграничения трафика. 3) Средства антивирусной защиты и контроля целостности.	Задание открытого типа с развернутым ответом	4	2
25.	**Прочитайте вопрос и дайте развернутый ответ.** Назовите четыре уровня (или категории) информации по уровню доступа, которые защищаются в электроэнергетике.	1) Информация ограниченного доступа. 2) Персональные данные сотрудников и клиентов 3) Государственная тайна. 4) Общедоступная (открытая) информация.	Задание открытого типа с развернутым ответом	4	2
26.	**Прочитайте вопрос и дайте развернутый ответ.** Назовите три основные задачи организационных мер безопасности на объектах электроэнергетики.	1) Разграничение доступа и определение ролей. 2) Регламентация действий в нештатных ситуациях. 3) Контроль и отчётность.	Задание открытого типа с развернутым ответом	4	2
27.	**Прочитайте вопрос и дайте развернутый ответ.** Укажите три алгоритмических (криптографических) средства,	1) Симметричное шифрование 2) Асимметричное шифрование 3) Хеш-функции	Задание открытого типа с развернутым ответом	4	2

№ задания	Содержание задания	Ответ на задание	Тип задания	Уровень сложности (балл)	№ Темы
	которые используются для обеспечения кибербезопасности				
28.	**Упорядочите классификацию организационных мер безопасности в электроэнергетике по степени их иерархии (от наиболее общего документа к частным):** 1. Инструкция для оператора АСУ ТП по реагированию на угрозы. 2. Федеральный закон (187-ФЗ). 3. Политика информационной безопасности организации. 4. Регламент использования VPN и удалённого доступа. Ответ запишите в виде последовательности цифр через запятую слева направо.	2,3,4,1	Задание закрытого типа на установление последовательности	1	2
29.	**Упорядочите этапы внедрения политики информационной безопасности на объекте в логической последовательности:** 1. Назначение ответственных за ИБ и разграничение ролей (DBA, администратор безопасности). 2. Внедрение средств защиты (брандмауэры, антивирусы). 3. Разработка и утверждение «Политики ИБ» и сопутствующих регламентов. 4. Анализ рисков и категорирование информационной системы. Ответ запишите в виде последовательности цифр через запятую слева направо.	4,3,1,2	Задание закрытого типа на установление последовательности	1	2
30.	**Упорядочите виды технических средств защиты по «уровню» модели OSI (от физического к прикладному):** 1. Межсетевой экран (L3-L4). 2. Шлюз с функцией шифрования (VPN, L3). 3. Биометрический замок СКУД (физический уровень). 4. Антивирус на почтовом шлюзе (L7). Ответ запишите в виде последовательности цифр через запятую слева направо.	3,2,1,4	Задание закрытого типа на установление последовательности	1	2
31.	**Прочитайте текст вопроса и соотнесите виды средств защиты с их примерами:** <u>Виды средств защиты:</u> 1) Программные средства; 2) Аппаратные средства; 3) Алгоритмические (криптографические). <u>Примеры:</u> А) Хеширование файлов конфигурации, сквозное шифрование (шифрование по алгоритму RSA). Б) Антивирус Касперского для АСУ ТП, SIEM-система (MaxPatrol). В) Токен Rutoken для двухфакторной аутентификации, аппаратный модуль доверенной загрузки (TPM). Запишите выбранные буквы под соответствующими цифрами:	<table><tr><td>1</td><td>2</td><td>3</td></tr><tr><td>Б</td><td>В</td><td>А</td></tr></table>	Задание закрытого типа на установление соответствия	1	2

№ задания	Содержание задания	Ответ на задание	Тип задания	Уровень сложности (балл)	№ Темы
	1 2 3 _ _ _				
32.	**Прочитайте текст вопроса и соотнесите организационные меры с их содержанием:** Меры: 1) Ролевая модель доступа (RBAC); 2) Реагирование на инциденты (IR); 3) Обучение персонала. Содержание: А) Инструкции, тестирование, тренинги по распознаванию фишинга. Б) Права доступа задаются не для человека, а для роли («Инженер АСУ ТП»), затем человек получает роль. В) Алгоритм действий (команда реагирования, локализация, изоляция сегмента). Запишите выбранные буквы под соответствующими цифрами: 1 2 3 _ _ _	1 2 3 Б В А	Задание закрытого типа на установление соответствия	1	2
33.	**Прочитайте текст вопроса и соотнесите законы РФ с их сферой регулирования:** Законы: 1) ФЗ № 187-ФЗ «О безопасности КИИ»; 2) ФЗ № 152-ФЗ «О персональных данных»; 3) ФЗ № 149-ФЗ «Об информации...» (базовый). Сфера регулирования: А) Определяет правовые основы работы с персональными данными. Б) Категорирование и защита объектов критической инфраструктуры. В) Основы получения, хранения, передачи информации. Запишите выбранные буквы под соответствующими цифрами: 1 2 3 _ _ _	1 2 3 Б А В	Задание закрытого типа на установление соответствия	1	2
34.	**Прочитайте вопрос и выберите верный ответ:** Укажите какой стандарт описывает международный подход к системам менеджмента информационной безопасности (СМИБ), который часто внедряется на энергообъектах для соответствия требованиям А) ISO 50001; Б) ISO 27001; В) ГОСТ Р 34.10; Г) IEEE 802.1X.	Б	Задание закрытого типа с однозначным выбором варианта ответа	1	2
35.	**Прочитайте вопрос и выберите верный ответ:** Программным средством класса IDS (Intrusion Detection System) является: А) СИИ (система индикации износа); Б) Система обнаружения атак (Snort, Suricata); В) Система управления базами данных; Г) Система контроля версий.	Б	Задание закрытого типа с однозначным выбором варианта ответа	1	2

№ задания	*Содержание задания*	*Ответ на задание*	*Тип задания*	*Уровень сложности (балл)*	*№ Темы*
36.	**Прочитайте вопрос и выберите верный ответ:** Модуль доверенной загрузки (Trusted Boot) предназначен: А) Для ускорения загрузки операционной системы; Б) Для проверки цифровой подписи загрузчика и ядра ОС (предотвращение загрузки руткита); В) Для создания резервных копий баз данных; Г) Для управления энергопотреблением.	Б	Задание закрытого типа с однозначным выбором варианта ответа	1	2
37.	**Прочитайте вопрос и выберите верный ответ:** Как называется комплексная система, централизованно собирающая и коррелирующая события безопасности со всех устройств (АСУ ТП, Active Directory, сетевые экраны)? А) ERP; Б) SIEM (Security Information and Event Management); В) SCADA; Г) MES.	Б	Задание закрытого типа с однозначным выбором варианта ответа	1	2
38.	**Прочитайте и выберите два верных ответа:** **К техническим средствам выявления нарушителей** на объектах электроэнергетики (физическая защита) относятся меры: А) Видеонаблюдение (CCTV) с записью и системой аналитики (обнаружение движения); Б) Магнитные контакты на дверях в серверную (датчик открытия); В) Антивирус Касперского; Г) Политика паролей (сложность пароля).	А, Б	Задание закрытого типа с многозначным выбором варианта ответа	1	2
39.	**Прочитайте и выберите два верных ответа:** С помощью систем резервного копирования (Backup) на объектах электроэнергетики решаются задачи: А) Восстановление данных после атаки программы-вымогателя (Ransomware); Б) Защита от сбоя жёсткого диска на сервере SCADA; В) Шифрование трафика между диспетчерским пунктом и подстанцией; Г) Фильтрация спама.	А, Б	Задание закрытого типа с многозначным выбором варианта ответа	1	2
40.	**Прочитайте и выберите два верных ответа:** Укажите какие из перечисленных технических решений обеспечивают защиту от атак типа «человек посередине» (MITM) на сети передачи данных: А) Использование протоколов с шифрованием (TLS/SSL, IPsec); Б) Внедрение сертификатов открытых ключей (PKI) для аутентификации узлов;	А, Б	Задание закрытого типа с многозначным выбором варианта ответа	1	2

№ задания	*Содержание задания*	*Ответ на задание*	*Тип задания*	*Уровень сложности (балл)*	*№ Темы*
	В) Применение DLP-системы; Г) Установка системы резервного копирования.				
41.	**Прочитайте и выберите два верных ответа:** К защите конечных точек (Endpoint Protection) в промышленных сетях относятся решения: А) Установка списка разрешённого ПО (Application whitelisting); Б) Специализированный антивирус для АСУ ТП (с ручным обновлением баз); В) Резервирование канала связи по радиоканалу; Г) Установка замка в стойке.	А, Б	Задание закрытого типа с многозначным выбором варианта ответа	1	2
42.	**Прочитайте и выберите два верных ответа:** Примерами неправомерных (противоправных) действий в киберпространстве, которые наказываются законодательством РФ являются: А) Создание, использование и распространение вредоносных программ (вирусов); Б) Несанкционированный доступ к компьютерной информации (подбор пароля, взлом); В) Настройка файервола (Firewall) штатным администратором; Г) Пинг (ping) своего сервера.	А, Б	Задание закрытого типа с многозначным выбором варианта ответа	1	2
43.	**Прочитайте и дополните фразу:** При симметричном шифровании для зашифрования и расшифрования данных используется один и тот же _____.	секретный ключ	Задание открытого типа на дополнение	2	33
44.	**Прочитайте и дополните фразу:** Схема, сочетающая в себе быстродействие симметричного шифрования и удобство управления ключами асимметричного шифрования, называется _____.	гибридной криптосистемой	Задание открытого типа на дополнение	2	3
45.	**Прочитайте и дополните фразу:** Атака на асимметричные алгоритмы, основанная на разложении большого числа на простые множители (для RSA), называется атакой _____	на факторизацию	Задание открытого типа на дополнение	2	3
46.	**Прочитайте вопрос и дайте развернутый ответ.** Опишите **гибридную криптосистему**.	Гибридная криптосистема – это комбинация асимметричного и симметричного шифрования, использующая преимущества каждого подхода.	Задание открытого типа с развернутым ответом	4	3
47.	**Прочитайте вопрос и дайте развернутый ответ.** Назовите три **режима работы блочных шифров** и кратко опишите их особенности.	1) ECB (Electronic Code Book): 2) CBC (Cipher Block Chaining): 3) CTR (Counter Mode):	Задание открытого типа с развернутым ответом	4	3
48.	**Упорядочите этапы гибридной криптосистемы в процессе установления защищённого**	3,1,2,5,4	Задание закрытого типа на установление	1	3

№ задания	Содержание задания	Ответ на задание	Тип задания	Уровень сложности (балл)	№ Темы
	соединения (TLS): 1. Клиент генерирует случайный сеансовый ключ. 2. Клиент шифрует сеансовый ключ открытым ключом сервера. 3. Клиент получает сертификат с открытым ключом сервера. 4. Клиент и сервер обмениваются данными, зашифрованными симметричным сеансовым ключом. 5. Сервер расшифровывает сеансовый ключ своим закрытым ключом. Ответ запишите в виде последовательности цифр через запятую слева направо.		последовательности		
49.	**Упорядочите режимы работы блочного шифра по степени их безопасности (от наименее безопасного к наиболее безопасному в типовых сценариях):** 1. GCM (Galois/Counter Mode). 2. ECB (Electronic Code Book). 3. CBC (Cipher Block Chaining). 4. CTR (Counter Mode). Ответ запишите в виде последовательности цифр через запятую слева направо.	2,3,4,1	Задание закрытого типа на установление последовательности	1	3
50.	**Упорядочите этапы процесса шифрования в режиме CBC:** 1. Шифрование результата XOR с использованием блочного шифра. 2. XOR текущего блока открытого текста с предыдущим блоком шифротекста (или IV для первого блока). 3. Получение блока шифротекста. Ответ запишите в виде последовательности цифр через запятую слева направо.	2,1,3	Задание закрытого типа на установление последовательности	1	3
51.	**Прочитайте текст вопроса и соотнесите режимы блочных шифров с их характеристиками:** Режимы: 1) ECB; 2) CBC; 3) CTR. Характеристики: А) Превращает блочный шифр в поточный; позволяет произвольный доступ к блокам. Б) Требует вектор инициализации (IV); шифрование последовательное (не параллелится). В) Самый простой, но при шифровании повторяющихся блоков возникают паттерны. Запишите выбранные буквы под соответствующими цифрами: 1 | 2 | 3 | |	1 | 2 | 3 В | Б | А	Задание закрытого типа на установление соответствия	1	3
52.	**Прочитайте текст вопроса и соотнесите понятия с их описанием:** Понятия:	1 | 2 | 3 Б | А | В	Задание закрытого типа на установление соответствия	13	

№ задания	*Содержание задания*	*Ответ на задание*	*Тип задания*	*Уровень сложности (балл)*	*№ Темы*
	1) Квантовая атака (алгоритм Шора); 2) Атака «грубой силы» (brute force); 3) Атака «человек посередине» (MITM) на этапе обмена ключами. Описание: А) Перебор всех возможных ключей; стойкость зависит от длины ключа. Б) Потенциально взламывает RSA и ECC за полиномиальное время. В) Злоумышленник перехватывает открытые ключи сторон и подменяет их своими. Запишите выбранные буквы под соответствующими цифрами: 1 | 2 | 3 | |				
53.	**Прочитайте вопрос и выберите верный ответ:** Основная проблема режима ECB в блочных шифрах заключается в: А) Невозможность расшифрования; Б) Одинаковые блоки открытого текста превращаются в одинаковые блоки шифротекста, что позволяет анализировать структуру данных; В) Слишком медленная работа; Г) Требуется вектор инициализации (IV).	Б	Задание закрытого типа с однозначным выбором варианта ответа	1	3
54.	**Прочитайте вопрос и выберите верный ответ:** Математический аппарат **эллиптических кривых** использует алгоритм асимметричного шифрования: А) RSA; Б) ECC; В) DES; Г) Blowfish.	Б	Задание закрытого типа с однозначным выбором варианта ответа	1	3
55.	**Прочитайте и выберите два верных ответа:** Асимметричному шифрованию присущи недостатки: А) Низкая скорость работы (в 100-000 раз медленнее симметричного); Б) Уязвимость к квантовым атакам (алгоритм Шора) для RSA и ECC; В) Проблема безопасной передачи ключей (требуется защищённый канал); Г) Невозможность реализации цифровой подписи.	А, Б	Задание закрытого типа с многозначным выбором варианта ответа	1	3
56.	**Прочитайте и выберите два верных ответа:** Симметричному шифрованию присущи преимущества**:** А) Высокая скорость шифрования (подходит для больших объёмов данных); Б) Простота аппаратной реализации (можно встроить в чип); В) Решает проблему распространения ключей (можно публиковать ключ); Г) Не требует хранить секретный ключ в тайне.	А, Б	Задание закрытого типа с многозначным выбором варианта ответа	1	3

№ задания	*Содержание задания*	*Ответ на задание*	*Тип задания*	*Уровень сложности (балл)*	*№ Темы*
57.	**Прочитайте и выберите два верных ответа:** Для симметричного шифрования актуальны угрозы: А) Перехват секретного ключа при передаче по незащищённому каналу; Б) Brute force attack (перебор всех возможных ключей); В) Квантовая атака (алгоритм Шора) на факторизацию; Г) Подмена открытого ключа злоумышленником.	А, Б	Задание закрытого типа с многозначным выбором варианта ответа	1	3
58.	**Прочитайте и дополните фразу:** Свойство хеш-функции, означающее, что по хешу вычислительно сложно восстановить исходное сообщение, называется _____ .	односторонностью	Задание открытого типа на дополнение	2	4
59.	**Прочитайте и дополните фразу:** Эффект, при котором малейшее изменение в исходных данных приводит к значительному изменению хеш-значения (не менее половины бит), называется _____.	лавинным эффектом	Задание открытого типа на дополнение	2	4
60.	**Прочитайте и дополните фразу:** Электронная подпись создаётся с использованием _____ ключа отправителя, а проверяется с помощью его _____ ключа.	закрытого открытого	Задание открытого типа на дополнение	2	4
61.	**Прочитайте и дополните фразу:** Тип электронной подписи, который имеет юридическую силу, приравненную к собственноручной подписи, и требует сертификат ключа проверки, выданный аккредитованным удостоверяющим центром, называется _____ электронной подписью.	усиленной квалифицированной	Задание открытого типа на дополнение	2	4
62.	**Прочитайте вопрос и дайте развернутый ответ.** Перечислите три основных требования, предъявляемых к криптографическим хеш-функциям.	1) Односторонность (необратимость) 2) Устойчивость к коллизиям (второе свойство) 3) Лавинный эффект	Задание открытого типа с развернутым ответом	4	4
63.	**Прочитайте вопрос и дайте развернутый ответ.** Опишите процесс проверки электронной подписи**.**	Процесс проверки электронной подписи: 1) Расшифровка подписи открытым ключом 2) Вычисление хеша полученного документа 3) Сравнение хешей	Задание открытого типа с развернутым ответом	4	4
64.	**Прочитайте вопрос и дайте развернутый ответ.** Перечислите три типа электронных подписей по российскому законодательству (ФЗ №63).	1) Простая электронная подпись 2) Усиленная неквалифицированная электронная подпись 3) Усиленная квалифицированная электронная подпись	Задание открытого типа с развернутым ответом	4	4
65.	**Упорядочите этапы создания и проверки электронной подписи в их логической последовательности (с точки зрения отправителя и получателя):** 1. Отправитель вычисляет хеш	1,2,4,5,3,6	Задание закрытого типа на установление последовательности	1	4

№ задания	Содержание задания	Ответ на задание	Тип задания	Уровень сложности (балл)	№ Темы
	документа. 2. Отправитель шифрует хеш своим закрытым ключом. 3. Получатель вычисляет хеш полученного документа. 4. Отправитель отправляет документ вместе с подписью. 5. Получатель расшифровывает подпись открытым ключом отправителя. 6. Получатель сравнивает хеши. Ответ запишите в виде последовательности цифр через запятую слева направо.				
66.	**Упорядочите типы электронных подписей по возрастанию их юридической силы (от наименее юридически значимой к наиболее значимой):** 1. Усиленная квалифицированная подпись (УКЭП). 2. Простая подпись (ПЭП). 3. Усиленная неквалифицированная подпись (НЭП). Ответ запишите в виде последовательности цифр через запятую слева направо.	2,3,1	Задание закрытого типа на установление последовательности	1	4
67.	**Упорядочите известные криптографические алгоритмы хеширования в порядке их разработки (от устаревших к современным):** 1. SHA-256 (Secure Hash Algorithm). 2. MD5 (Message Digest 5). 3. ГОСТ Р 34.11-2012 («Стрибог»). 4. SHA-1. Ответ запишите в виде последовательности цифр через запятую слева направо.	2,4,1,3	Задание закрытого типа на установление последовательности	1	4
68.	**Прочитайте текст вопроса и соотнесите требования к хеш-функциям с их описанием:** <u>Требования:</u> 1) Односторонность; 2) Устойчивость к коллизиям; 3) Лавинный эффект. <u>Описание:</u> А) Изменение одного бита на входе приводит к изменению ~50% бит на выходе. Б) Невозможность восстановить исходное сообщение по его хешу. В) Невозможность найти два разных сообщения с одинаковым хешем. Запишите выбранные буквы под соответствующими цифрами: 1 2 3 _ _ _	1 2 3 Б В А	Задание закрытого типа на установление соответствия	1	4
69.	**Прочитайте текст вопроса и соотнесите алгоритмы с их назначением:** Алгоритмы: 1) RSA-PSS; 2) SHA-256; 3) ГОСТ Р 34.10-2012. Назначение:	1 2 3 В А Б	Задание закрытого типа на установление соответствия	1	4

№ задания	Содержание задания	Ответ на задание	Тип задания	Уровень сложности (балл)	№ Темы
	А) Алгоритм хеширования (standard hash). Б) Алгоритм электронной подписи (на эллиптических кривых). В) Алгоритм электронной подписи (RSA). Запишите выбранные буквы под соответствующими цифрами: 1 2 3 _ _ _				
70.	**Прочитайте текст вопроса и соотнесите понятия с их описанием:** Понятия: 1) Коллизия хеш-функции; 2) Квалифицированный сертификат ключа проверки ЭП; 3) Хеш-сумма. Описание: А) Документ, подтверждающий принадлежность открытого ключа определённому лицу, выданный аккредитованным удостоверяющим центром. Б) Ситуация, когда два разных входных сообщения дают одинаковый хеш. В) Результат работы хеш-функции фиксированной длины. Запишите выбранные буквы под соответствующими цифрами: 1 2 3 _ _ _	1 2 3 Б А В	Задание закрытого типа на установление соответствия	1	4
71.	**Прочитайте вопрос и выберите верный ответ:** Устаревшей и небезопасной из-за обнаруженных коллизий считается хеш-функция: А) SHA-256; Б) MD5; В) SHA-3 (Keccak); Г) ГОСТ «Стрибог».	Б	Задание закрытого типа с однозначным выбором варианта ответа	1	4
72.	**Прочитайте вопрос и выберите верный ответ:** Хранение паролей с помощью хеш-функций используется для: А) Для шифрования пароля, чтобы его можно было расшифровать; Б) Для контроля целостности файлов; В) Для создания электронной подписи; Г) Для того, чтобы не хранить пароль в открытом виде (при аутентификации сравниваются хеши).	Г	Задание закрытого типа с однозначным выбором варианта ответа	1	4
73.	**Прочитайте вопрос и выберите верный ответ:** Укажите какой тип электронной подписи требует использования сертифицированных ФСБ РФ средств криптографической защиты информации (СКЗИ) А) Простая подпись (ПЭП); Б) Усиленная неквалифицированная подпись (НЭП);	В	Задание закрытого типа с однозначным выбором варианта ответа	1	4

№ задания	*Содержание задания*	*Ответ на задание*	*Тип задания*	*Уровень сложности (балл)*	*№ Темы*
	В) Усиленная квалифицированная подпись (УКЭП); Г) Все типы подписей.				
74.	**Прочитайте и выберите два верных ответа:** Укажите какие из перечисленных алгоритмов электронной подписи поддерживаются российским законодательством и стандартами (актуальные): А) ГОСТ Р 34.10-2012 (на эллиптических кривых); Б) MD5 (как алгоритм хеширования для подписи); В) RSA (с определёнными длинами ключей допускается); Г) CRC32.	А, В	Задание закрытого типа с многозначным выбором варианта ответа	1	4
75.	**Прочитайте и выберите два верных ответа:** На преодоление защиты, обеспечиваемой хеш-функциями направлены атаки: А) Поиск коллизий (нахождение двух сообщений с одинаковым хешем); Б) Атака «дня рождения» (birthday attack) для поиска коллизий; В) Атака грубой силы (brute force) на ключ шифрования; Г) Атака «человек посередине» (MITM) на сессию TLS.	А, Б	Задание закрытого типа с многозначным выбором варианта ответа	1	4
76.	**Прочитайте и выберите два верных ответа:** С помощью электронной подписи решаются задачи: А) Удостоверение авторства документа (неотказуемость – невозможность отказаться от подписи); Б) Обеспечение целостности документа (обнаружение любых изменений после подписания); В) Шифрование содержимого документа (скрытие от посторонних); Г) Ускорение передачи документа по сети.	А, Б	Задание закрытого типа с многозначным выбором варианта ответа	1	4
77.	**Прочитайте и выберите два верных ответа:** Какие из перечисленных алгоритмов являются криптографическими хеш-функциями (актуальные на сегодня)? А) SHA-256 (и SHA-3); Б) ГОСТ Р 34.11-2012 («Стрибог»); В) AES-256; Г) RSA-2048.	А, Б	Задание закрытого типа с многозначным выбором варианта ответа	1	4
78.	**Прочитайте и выберите два верных ответа:** Алгоритму MD5 присущи недостатки: А) Обнаружена возможность подбора коллизий (два разных файла дают одинаковый хеш); Б) Высокая скорость вычислений (позволяет проводить атаки перебором); В) Является алгоритмом асимметричного шифрования;	А, Б	Задание закрытого типа с многозначным выбором варианта ответа	1	4

№ задания	*Содержание задания*	*Ответ на задание*	*Тип задания*	*Уровень сложности (балл)*	*№ Темы*
	Г) Требует лицензии для использования.				

Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процессы формирования компетенций

Характеристика процедуры текущего контроля успеваемости и промежуточной аттестации по дисциплине

Оценивание знаний, умений, навыков и опыта деятельности проводятся на основе сведений, приводимых в матрице соответствия оценочных средств запланированным результатам обучения.

Цель текущего контроля успеваемости и промежуточной аттестации по учебным дисциплинам в семестре – проверка приобретаемых обучающимися знаний, умений, навыков в контексте формирования установленных образовательной программой компетенций в течение семестра.

Шкала оценивания:

«Отлично» – выставляется, если сформированность заявленных образовательных результатов компетенций оценивается критериями «хорошо» и «отлично», при условии отсутствия оценки «неудовлетворительно»: студент показал прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи повышенной сложности, свободно использовать справочную литературу, делать обоснованные выводы из результатов анализа конкретных ситуаций;

«Хорошо» – выставляется, если сформированность заявленных образовательных результатов компетенций оценивается критериями «хорошо» и «отлично», при условии отсутствия оценки

«неудовлетворительно», допускается оценка «удовлетворительно»: обучающийся показал прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи, предусмотренные рабочей программой, ориентироваться в рекомендованной справочной литературе, умеет правильно оценить полученные результаты анализа конкретных ситуаций;

«Удовлетворительно» – выставляется, если сформированность заявленных образовательных результатов компетенций оценивается критериями «удовлетворительно», «хорошо» и «отлично»: обучающийся показал знание основных положений фактического материала, умение получить с помощью преподавателя правильное решение конкретной практической задачи из числа предусмотренных рабочей программой, знакомство с рекомендованной справочной литературой;

«Неудовлетворительно» – выставляется, если при ответе обучающегося выявились существенные пробелы в знаниях основных положений фактического материала, неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой учебной дисциплины.

Ответы и решения, обучающихся оцениваются по следующим общим критериям: распознавание проблем; определение значимой информации; анализ проблем; аргументированность; использование стратегий; творческий подход; выводы; общая грамотность.

Обучающиеся обязаны сдавать все задания в сроки, установленные преподавателем. Оценка

«Удовлетворительно» по дисциплине, может выставляться и при неполной сформированности компетенций в ходе освоения отдельной учебной дисциплины, если их формирование предполагается продолжить на более поздних этапах обучения, в ходе изучения других учебных дисциплин.

Текущий контроль осуществляется через систему оценки преподавателем всех видов работ обучающихся, предусмотренных рабочей программой дисциплины и учебным планом.

Критерии оценки теста.

Количество верных ответов:

80-100% -оценка «отлично»: обучаюшийся демонстрирует глубокое знание учебно-программного материала, умение свободно выполнять задания, усвоивший взаимосвязь основных понятий дисциплины; способный самостоятельно приобретать новые знания и умения; способный самостоятельно использовать углубленные знания;

71-85% -оценка «хорошо»: обучающийся демонстрирует полное знание учебно-программного материала, успешно выполняющий предусмотренные программой задания, показывающий систематический характер знаний по дисциплине и способный к их самостоятельному пополнению и обновлению в ходе дальнейшего обучения в вузе и в будущей профессиональной деятельности;

50-70% -оценка «удовлетворительно»: обучающийся обнаруживает знание основного учебного программного материала в объеме, необходимом для дальнейшего обучения, выполняющего задания, предусмотренные программой, допустившим неточности в ответе, но обладающим необходимыми знаниями для их устранения;

менее 50% -оценка «неудовлетворительно»: обучающийся демонстрирует пробелы в знаниях основного учебного программного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий.

На этапе промежуточной аттестации используется система оценки успеваемости обучающихся, которая позволяет преподавателю оценить сформированность планируемых результатов обучения, а также уровень освоения материала обучающимися.

Форма оценки знаний: оценка - 5 «отлично»; 4 «хорошо»; 3 «удовлетворительно»; 2 «неудовлетворительно». возможно использовать балльно-рейтинговые оценки.

Основанием для определения оценки на зачете служит уровень освоения обучающимся материала и формирования компетенция, предусмотренных учебным планом.

Успеваемость на зачете определяется оценками: «зачтено»; «не зачтено».

Оценка	Критерии оценивания	Балльно-рейтинговая оценка
«Зачтено»	Обучающийся освоил компетенции дисциплины на 51-100 % и показал хорошие знания изученного учебного материала, логично и последовательно изложил и полностью раскрыл смысл предлагаемого вопроса; продемонстрировал умение применить теоретические знания для решения практической задачи; выполнил все контрольные задания, предусмотренные рабочей программой дисциплины	51-100
«Не зачтено»	Обучающийся освоил компетенции дисциплины менее чем на 51% и при ответе на предлагаемый вопрос выявились существенные пробелы в знаниях учебного материала, неумение с помощью преподавателя получить правильное решение практической задачи; не в полном объеме выполнил все контрольные задания, предусмотренные рабочей программой дисциплины	0- 50

Основанием для определения оценки на экзамене служит уровень освоения обучающимся учебного материала, умение решать практические задачи и формирования компетенция, предусмотренных учебным планом.

Успеваемость на экзамене определяется оценками: «отлично»; «хорошо; «удовлетворительно»; «не удовлетворительно».

Оценка	Критерии оценивания	Балльно-рейтинговая оценка
«Отлично»	Обучающийся освоил компетенции дисциплины на всех этапах их формирования на 86-100 %, показал глубокие знания учебного материала, логично и последовательно изложил содержание ответов на вопросы билета; продемонстрировал умение иллюстрировать теоретические положения конкретными примерами и свободно выполнять экзаменационные задания; усвоил основную и ознакомился с дополнительной литературой; выполнил все контрольные задания, предусмотренные рабочей программой дисциплины	86-100
«Хорошо»	Обучающийся освоил компетенции дисциплины на всех этапах их формирования на 61-85 %, показал глубокие знания учебного материала, логично и последовательно изложил содержание ответов на вопросы билета, но допустил несущественные неточности; продемонстрировал умение иллюстрировать теоретические положения конкретными примерами и выполнять экзаменационные задания; усвоил основную и ознакомился с дополнительной литературой; выполнил все контрольные задания, предусмотренные рабочей программой дисциплины	61-85
«Удовлетворительно»	Обучающийся освоил компетенции дисциплины на всех этапах их формирования на 51-60 %, показал знания учебного материала в объеме, необходимом для дальнейшего освоения учебных программ, но допустил погрешности в изложении ответов на вопросы билета и при выполнении экзаменационных заданий; ознакомился с основной литературой, рекомендованной программой; справился с контрольными заданиями, предусмотренными рабочей программой дисциплины	51-60
«Не удовлетворительно»	Обучающийся освоил компетенции дисциплины на всех этапах их формирования менее чем на 51 %, обнаружил пробелы в знаниях учебного материала, допустил принципиальные ошибки в	0-50

	выполнении контрольных заданий, предусмотренных рабочей программой дисциплины	

Интегральная оценка

Критерии	Традиционная оценка	Балльно-рейтинговая оценка
5	5	86 - 100
4	4	61-85
3	3	51-60
2 и 1	2, Незачет	0-50
5, 4, 3	Зачет	51-100