Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Директор по образовательной деятельности

_____ С.Т. Князев
«12» октября 2021 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля
М.1.8.

Модуль
Кибербезопасность в энергетике

Екатеринбург, 2021

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа Искусственный интеллект в электроэнергетике	**Код ОП**
Направление подготовки Прикладная математика	**Код направления и уровня подготовки** 01.04.04

Области образования, в рамках которых реализуется модуль образовательной программы по СУОС УрФУ:

№ п/п	Перечень областей образования, для которых разработан СУОС УрФУ	Уровень подготовки
1	Математические и естественные науки	магистратура

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Хальясмаа Александра Ильмаровна	Канд. техн. наук, доцент	Доцент	Кафедра электротехники, Уральский энергетический институт

Руководитель модуля А.И. Хальясмаа

Рекомендовано учебно-методическим советом Уральского энергетического института

Протокол № 114 от 08.10.2021 г.

ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ КИБЕРБЕЗОПАСНОСТЬ В ЭНЕРГЕТИКЕ

1.1. Аннотация содержания модуля

Модуль состоит из одноименной дисциплины. Дисциплина «Кибербезопасность в энергетике» изучает основные принципы обеспечения защиты информации и защиты от кибернетических угроз объектов электроэнергетики, правовые, организационные, программные, технические и алгоритмические способы защиты, используемые для оценки угроз и мер защиты модели, существующую законодательную базу в области защиты информации и отраслевые стандарты. Дисциплина формирует представление о видах защищаемой информации, классификации кибернетических угроз на объектах электроэнергетики, различных способах защиты, принципах их действия и методиках выбора средств защиты в соответствии с угрозами, рисками и их последствиями.

При реализации модуля используются проектная технология обучения, проблемное обучение, информационно-коммуникационные технологии, исследовательские методы. В процессе изучения разделов дисциплин активно применяется проблемное обучение, основанное на разборе реальных производственных проблем и поиске их решений.

Дисциплина модуля может быть реализована в смешанной и традиционной технологии. Реализация модуля с использованием смешанной технологии обучения предполагает применение разработанных электронных ресурсов, имеющих статус ЭОР УрФУ и размещенных на образовательной платформе УрФУ, включая учебные пособия, презентации, задания и тесты.

1.2. Структура и объем модуля

Таблица 1

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах и часах
1	Кибербезопасность в энергетике	3/108
	ИТОГО по модулю:	**3/108**

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	Отсутствуют
Постреквизиты и кореквизиты модуля	Отсутствуют

1.4. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения (индикаторы) по модулю

Таблица 2

Перечень дисциплин модуля	Код и наименование компетенции	Планируемые результаты обучения (индикаторы)
1	2	3
Кибербезопасность	УК-7 - Способен обрабатывать, анализировать, передавать данные и информацию с использованием цифровых средств для эффективного решения поставленных задач с учетом требований информационной безопасности	УК-7. З-1. Сделать обзор угроз информационной безопасности, основных принципов организации безопасной работы в информационных системах и в сети интернет УК-7. З-2. Описать способы и средства защиты персональных данных и данных в организации в соответствии с действующим законодательством УК-7. З-3. Сделать обзор современных цифровых средств и технологий, используемых для обработки, анализа и передачи данных при решении поставленных задач У-1 - Определять основные угрозы безопасности при использовании информационных технологий и выбирать оптимальные способы и средства защиты персональных данных и данных организации от мошенников и вредоносного ПО УК-7. У-2. Выбирать современные цифровые средства и технологии для обработки, анализа и передачи данных с учетом поставленных задач УК-7. П-1. Обосновать выбор технических и программных средств защиты персональных данных и данных организации при работе с информационными системами на основе анализа потенциальных и реальных угроз безопасности информации УК-7. П-1. Решать поставленные задачи, используя эффективные цифровые средства и средства информационной безопасности
	ПК-2. Способен исследовать и разрабатывать архитектуры систем искусственного интеллекта для различных предметных областей на основе комплексов методов и инструментальных средств систем искусственного интеллекта	ПК-2. Способен исследовать и разрабатывать архитектуры систем искусственного интеллекта для различных предметных областей на основе комплексов методов и инструментальных средств систем искусственного интеллекта ПК-2.1. Разрабатывает единые стандарты в области безопасности (в том числе отказоустойчивости) и совместимости программного обеспечения, эталонных архитектур вычислительных систем и программного обеспечения, а также определяет критерии эталонных открытых тестовых сред (условий) в целях улучшения качества и эффективности программного обеспечения

		технологий и систем искусственного интеллекта ПК-2.1. З-1. Знает единый стандарты в области безопасности (в том числе отказоустойчивости) и совместимости программного обеспечения, эталонных архитектур вычислительных сисетм и программного обеспечения технологий и систем искусственного интеллекта ПК-2.1. З-2. Знает методики определения критериев сопоставления программного обеспечения и критериев эталонных открытых тестовых сред (условий) ПК-2.1. У-1. Умеет применять и разрабатывать единые стандарты в области безопасности (в том числе отказоустойчивости) и совместимости программного обеспечения, эталонных архитектур вычислительных систем и программного обеспечения технологий и систем искусственного интеллекта ПК-2.1. У-2. Умеет определять критерии сопоставления программного обеспечения и критерии эталонных открытых тестовых сред (условий) в целях определения качества и эффективности программного обеспечения технологий и систем искусственного интеллекта
	ПК-8. Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях	ПК-8.1. Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях ПК-8.1. З-1. Знает новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ПК-8.1. У-1. Умеет разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной, очно-заочной и заочной формах.

2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

ПРОГРАММА МОДУЛЯ
КИБЕРБЕЗОПАСНОСТЬ В ЭНЕРГЕТИКЕ

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1 КИБЕРБЕЗОПАСНОСТЬ В ЭНЕРГЕТИКЕ

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Хальясмаа Александра Ильмаровна	Канд. техн. наук, доцент	Доцент	Кафедра электротехники, Уральский энергетический институт

Рекомендовано учебно-методическим советом Уральского энергетического института

Протокол № 114 от 08.10.2021 г.

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 1 (майнор) КИБЕРБЕЗОПАСНОСТЬ В ЭНЕРГЕТИКЕ

2.1. Технологии обучения, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Смешанная модель обучения с использованием онлайн-курса УрФУ;
- Исключительно электронного обучения с использованием внутреннего онлайн-курса УрФУ.

2.2. Содержание дисциплины 1

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины	Содержание
Р1	Особенности обеспечения 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.
Р2	Особенности организации кибербезопасности 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.
Р3	Виды угроз на объектах электроэнергетики	Классификация кибер-угроз. Особенности кибер-угроз на объектах электроэнергетики. Техногенные угрозы. Внешние антропогенные угрозы. Внутренне антропогенные угрозы.
Р4	Способы обеспечения кибербезопасности	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.
Р5	Правовое обеспечение кибербезопасности	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.
Р6	Организационное обеспечение кибербезопасности на объектах электроэнергетики	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.
Р7	Технические средства обеспечения кибербезопасности на объектах электроэнергетики	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.

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации /полностью на иностранном языке

2.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 1 КИБЕРБЕЗОПАСНОСТЬ В ЭНЕРГЕТИКЕ

Электронные ресурсы (издания)

1. Applied Cybersecurity Handbook. Enhancement of cyber educational system of Montenegro; 2015; https://ecesm.net/sites/default/files/Dev.2.4-v1_new.pdf
2. Синадский, Н. В. Учебно-методический комплекс дисциплины "Защита информации в компьютерных сетях"; Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность"; Екатеринбург; 2008. https://elar.urfu.ru/handle/10995/1654
3. What Is Cybersecurity? Cisco. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Профессиональные базы данных, информационно-справочные системы

1. Oxford University Press
2. ProQuest Digital Dissertations and Theses Global
3. Computers & Applied Sciences Complete
4. eLibrary Научная электронная библиотека
5. IEEE Xplore
6. Scopus
7. EndNote Web

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

1. Научная электронная библиотека eLibrary https://www.elibrary.ru/
2. Реферативная БД Scopus https://www.scopus.com/

3. Электронный научный архив УрФУ https://elar.urfu.ru/
4. Зональная научная библиотека (УрФУ) - http://lib.urfu.ru/

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 1 КИБЕРБЕЗОПАСНОСТЬ В ЭНЕРГЕТИКЕ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мультимедийная аудитория. Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов. Рабочее место преподавателя. Доска аудиторная. Периферийное устройство.	Microsoft Office (Word, Excel, Power Point)
2	Практические занятия	Терминальный класс. Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов. Рабочее место преподавателя. Персональные компьютеры по количеству обучающихся.	Microsoft Office (Word, Excel, Power Point)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Код модуля	**Модуль**
М.1.8	Кибербезопасность в энергетике

Екатеринбург, 2021

Оценочные материалы по модулю составлены авторами:

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Хальясмаа Александра Ильмаровна	Канд. техн. наук, доцент	Доцент	Кафедра электротехники, Уральский энергетический институт

1. СТРУКТУРА И ОБЪЕМ МОДУЛЯ КИБЕРБЕЗОПАСНОСТЬ В ЭНЕРГЕТИКЕ

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах и часах	Форма итоговой промежуточной аттестации по дисциплинам модуля и в целом по модулю
1	Кибербезопасность в энергетике	3 /108	Зачет
	ИТОГО по модулю:	**3 /108**	

2. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО МОДУЛЮ

Не предусмотрено

Раздел 3. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ
КИБЕРБЕЗОПАСНОСТЬ В ЭНЕРГЕТИКЕ

Модуль КИБЕРБЕЗОПАСНОСТЬ В ЭНЕРГЕТИКЕ

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Хальясмаа Александра Ильмаровна	Канд. техн. наук, доцент	Доцент	Кафедра электротехники, Уральский энергетический институт

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ КИБЕРБЕЗОПАСНОСТЬ В ЭНЕРГЕТИКЕ

Таблица 1.1

Код и наименование компетенций, формируемые с участием дисциплины	**Индикаторы достижения компетенции**	**Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине**
1	**2**	**3**
УК-7. Способен обрабатывать, анализировать, передавать данные и информацию с использованием цифровых средств для эффективного решения поставленных задач с учетом требований информационной безопасности	УК-7. З-1 - Сделать обзор угроз информационной безопасности, основных принципов организации безопасной работы в информационных системах и в сети интернет УК-7. З-2 - Описать способы и средства защиты персональных данных и данных в организации в соответствии с действующим законодательством УК-7. З-3 - Сделать обзор современных цифровых средств и технологий, используемых для обработки, анализа и передачи данных при решении поставленных задач УК-7. У-1 - Определять основные угрозы безопасности при использовании информационных технологий и выбирать оптимальные способы и средства защиты персональных данных и данных организации от мошенников и вредоносного ПО УК-7. У-2. Выбирать современные цифровые средства и технологии для обработки, анализа и передачи данных с учетом поставленных задач УК-7. П-1 - Обосновать выбор технических и программных средств	Практические занятия № 1, 2, 3, 5, 9 Круглый стол Зачет

	защиты персональных данных и данных организации при работе с информационными системами на основе анализа потенциальных и реальных угроз безопасности информации УК-7. П-1 – Решать поставленные задачи, используя эффективные цифровые средства и средства информационной безопасности	

Таблица 1.2

Код и наименование компетенций, формируемые с участием дисциплины	**Индикаторы достижения компетенции**	**Планируемые результаты обучения**	**Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине**
1	**2**	**3**	**4**
ПК-2. Способен исследовать и разрабатывать архитектуры систем искусственного интеллекта для различных предметных областей на основе комплексов методов и инструментальных средств систем искусственного интеллекта	ПК-2. Способен исследовать и разрабатывать архитектуры систем искусственного интеллекта для различных предметных областей на основе комплексов методов и инструментальных средств систем искусственного интеллекта	ПК-2.1. Разрабатывает единые стандарты в области безопасности (в том числе отказоустойчивости) и совместимости программного обеспечения, эталонных архитектур вычислительных систем и программного обеспечения, а также определяет критерии эталонных открытых тестовых сред (условий) в целях улучшения качества и эффективности программного обеспечения технологий и систем искусственного интеллекта ПК-2.1. З-1. Знает единый стандарты в области безопасности (в том числе отказоустойчивости) и совместимости программного обеспечения, эталонных	Практические занятия № 3, 4, 6, 8, 9 Круглый стол Зачет

		архитектур вычислительных сисетм и программного обеспечения технологий и систем искусственного интеллекта ПК-2.1. З-2. Знает методики определения критериев сопоставления программного обеспечения и критериев эталонных открытых тестовых сред (условий) ПК-2.1. У-1. Умеет применять и разрабатывать единые стандарты в области безопасности (в том числе отказоустойчивости) и совместимости программного обеспечения, эталонных архитектур вычислительных систем и программного обеспечения технологий и систем искусственного интеллекта ПК-2.1. У-2. Умеет определять критерии сопоставления программного обеспечения и критерии эталонных открытых тестовых сред (условий) в целях определения качества и эффективности программного обеспечения технологий и систем искусственного интеллекта	
ПК-8. Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с	ПК-8.1. Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	ПК-8.1. З-1. Знает новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях	Практические занятия № 1, 7, 8, 9 Круглый стол Зачет

учетом требований информационной безопасности в различных предметных областях		ПК-8.1. У-1. Умеет разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях	

2. ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ, ВКЛЮЧАЯ МЕРОПРИЯТИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ

2.1. Распределение объема времени по видам учебной работы

Таблица 2

№ п/п	Наименование дисциплины модуля Кибербезопасность в энергетике	Объем времени, отведенный на освоение дисциплины модуля								
		Аудиторные занятия, час.				Промежуточная аттестация (форма итогового контроля)	Контактная работа (час.)	Самостоятельная работа студента, включая текущую аттестацию (час.)	Всего по дисциплине	
		Занятия лекционного типа	Практические работы	Лабораторные работы	Всего				Час.	Зач. ед.
1	2	3	4	5	6	7	8	9	10	11
1	Кибербезопасность в энергетике	18	18	0	36	Зачет	41,65	66,35	108	3
Всего на освоение дисциплины модуля (час.)									108	3
								Итого по модулю:	**108**	**3**

2.2. Виды СРС, количество и объем времени на контрольно-оценочные мероприятия СРС по дисциплине

Контрольно-оценочные мероприятия СРС включают самостоятельное изучение материала, подготовку к аудиторным занятиям и мероприятиям текущего контроля, выполнение и оформление внеаудиторных мероприятий текущего контроля и подготовку к мероприятиям промежуточного контроля.

Таблица 3

№ п/п	Вид самостоятельной работы студента по дисциплине модуля	Количество контрольно-оценочных мероприятий СРС	Объем контрольно-оценочных мероприятий СРС (час.)
1	Подготовка к аудиторным занятиям и мероприятиям текущего контроля: лекционным, практическим занятиям.		23,5
2	Подготовка к круглому столу	1	12
3	Подготовка к зачету	1	4
4	Самостоятельное изучение материала		26,85
	Итого на СРС по дисциплине:		66,35

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

3.1. Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,6		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Самостоятельное изучение материала	2 семестр, 3, 11, 15 уч. н.	40
Круглый стол	2 семестр, 5, 7 уч. н.	60
Весовой коэффициент значимости результатов текущей аттестации по лекциям–0,4		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические занятия: коэффициент значимости совокупных результатов практических занятий – 0,4		

Текущая аттестация на практических занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Самостоятельное изучение материала	2 семестр, 5, 9 уч. н.	40
Выполнение практических работ	2 семестр, 2, 4, 6, 8, 10, 12, 14, 16 уч. н.	60
Весовой коэффициент значимости результатов текущей аттестации по практическим занятиям–1		
Промежуточная аттестация по практическим/семинарским занятиям–не предусмотрена **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторных занятиям– 0**		

3.3. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	**Коэффициент значимости результатов освоения дисциплины в семестре**
2	**1**

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	**Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам**
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Личностные качества	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и

	формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2. Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	**Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)**	**Шкала оценивания**		
		Традиционная характеристика уровня		**Качественная характеристика уровня**
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

Задания по контрольно-оценочным мероприятиям в рамках текущей и промежуточной аттестации должны обеспечивать освоение и достижение результатов обучения (индикаторов) и предметного содержания дисциплины на соответствующем уровне.

5.1. Описание контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля

5.1.1. Практические занятия

Номер занятия	Примерный перечень тем практических занятий
1	Актуальность кибербезопасности в электроэнергетике
2	Анализ существующих моделей кибербезопасности
3	Анализ примеров кибер-угроз
4	Методики управления рисками. Расчет экономической эффективности мер кибербезопасности
5	Российское и европейское законодательство в области кибербезопасности
6	Настройка прав доступа к облачным хранилищам данных при совместной работе
7	Алгоритмы шифрации сообщений
8	Средства электронной цифровой подписи, обеспечение подлинности и целостности файлов
9	Программные средства защиты информации

5.1.2. Лабораторные занятия

Не предусмотрено

5.1.3. Курсовая работа / Курсовой проект

Не предусмотрено

5.1.4. Контрольная работа

Не предусмотрено

5.1.5. Домашняя работа

Не предусмотрено

5.1.6. Расчетная работа / Расчетно-графическая работа

Не предусмотрено

5.1.7. Реферат / эссе / творческая работа *[оставить нужное]*

Не предусмотрено

5.1.8. Проектная работа

Не предусмотрено

5.1.9. Круглый стол

Примерные задания для подготовки к круглому столу

Подготовить презентацию и краткий доклад по теме

1. Особенности цифровых сигналов с точки зрения защиты информации от перехвата
2. Особенности цифровых сигналов с точки зрения защиты информации от искажения, принципы контрольной суммы.
3. Применение средств анализа данных в системах обеспечения кибербезопасности.
4. Технические средства повышения защиты каналов передачи данных.
5. Выбор программного обеспечения для использования технологии VPN.
6. Примеры и последствия кибератак на объекты энергетики.
7. Примеры и последствия утечек больших данных
8. Надежность и защищенность функционирования системы, основанных на знаниях.
9. Безопасная интеграция программных компонентов систем, основанных на знаниях.
10. Применение методов искусственного интеллекта в обеспечении кибербезопасности.

5.1.10. Кейс-анализ

Не предусмотрено

5.2. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля

5.2.1. Зачет в форме независимого тестового контроля (НТК)

НТК по дисциплине модуля не проводится.

Для проведения промежуточной аттестации используется
Не предусмотрено

Спецификация теста в системе СМУДС УрФУ / ФЭПО /Интернет-тренажера:
Не предусмотрено

5.2.2. Зачет в традиционной форме – устные ответы на вопросы билетов

Список примерных вопросов

1. Свойства информации. Операции с данными и информацией.
2. Классификация защищаемой информации.
3. Современные цифровые средства и технологии, используемые для обработки, анализа и передачи данных.
4. Большие данные, построение и защита информационных систем, использующих большие данные.
5. Особенности защиты информации в рекомендательных системах и системах поддержки принятия решений.
6. Основные модели кибербезопасности. Модель ISO 27000.
7. Классификация кибер-угроз. Особенности кибер-угроз на объектах электроэнергетики.
8. Критерии эффективности и качества функционирования систем, основанной на знаниях с точки зрения кибербезопасности, выбор программные платформ для их реализации.
9. Техногенные угрозы.
10. Внешние антропогенные угрозы. Внутренне антропогенные угрозы.
11. Классификация способов обеспечения кибербезопасности.
12. Правовые средства обеспечения кибербезопасности.
13. Организационные средства обеспечения кибербезопасности.
14. Программные, аппаратные и алгоритмические средства обеспечения кибербезопасности.

15. Управление рисками. Управление рисками при обеспечении безопасности объектов электроэнергетики. Методики управления рисками.

16. Расчет экономической эффективности мер кибербезопасности.

17. Виды законодательных мер обеспечения кибербезопасности. Виды информации по уровню доступа.

18. Организационные средства обеспечения кибербезопасности.

19. Классификация технических средств защиты информации. Программные средства.

20. Криптографические средства защиты информации.