МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

КГЭУ **«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»**
(ФГБОУ ВО «КГЭУ»)

«УТВЕРЖДАЮ»
Директор института
Цифровых технологий и экономики
_____ Торкунова Ю.В.

26 октября 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность объектов критической инфраструктуры

Направление подготовки 09.04.01 Информатика и вычислительная техника

Направленность(и) (профиль(и)) 09.04.01 Информационные технологии в топливно-энергетическом комплексе

Квалификация магистр

г. Казань, 2020

Рабочая программа дисциплины разработана в соответствии с ФГОС ВО - магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. № 918)

Программу разработал(и):

доцент,к.т.н. _____ Исмагилов И.Р.

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатика и информационно-управляющие системы, протокол №24 от 26.10.2020

Зав. кафедрой _____ Торкунова Ю.В.

Программа рассмотрена и одобрена на заседании выпускающей кафедры Информатика и информационно-управляющие системы, протокол №24 от 26.10.2020

Зав. кафедрой _____ Торкунова Ю.В.

Программа одобрена на заседании методического совета института Цифровых технологий и экономики, протокол № 2 от 26.10.2020

Зам. директора института
Цифровых технологий и экономики _____ Косулин В.В.

Программа принята решением Ученого совета института Цифровых технологий и экономики протокол №2 от 26.10.2020

1. Цель, задачи и планируемые результаты обучения по дисциплине

Целью освоения дисциплины является приобретение знаний обеспечения информационной безопасности на объектах критической информационной инфраструктуры (ОКИИ) и навыков, необходимых для разработки и реализации организационно-технических мер по обеспечению информационной безопасности на объектах КИИ

Задачи освоения дисциплины состоят в формировании способности:

- применять современные технические, программные и аппаратные средства защиты информации применительно к объектам критической информационной инфраструктуры (ОКИИ)
- классифицировать и оценивать угрозы и уязвимости информационной безопасности для информационных систем ОКИИ
- разрабатывать проекты нормативных и правовых актов предприятия, учреждения и организации, регламентирующих деятельность по обеспечению информационной безопасности на ОКИИ
- разрабатывать комплексную инфраструктуру защищенной информационной системы ОКИИ

Компетенции, формируемые у обучающихся, запланированные результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине (знать, уметь, владеть)

ПК-2 Способен к обеспечению соответствия проектируемых ИС принятым в топливно-энергетическом комплексе технологиям и стандартам	ПК-2.1 Понимает место и роль информационных систем в технологическом процессе производства, транспортировки и использования топливно-энергетических ресурсов	*Знать:* методы построения информационной инфраструктуры предприятия ТЭК, а также средств автоматизации и коммуникации с учетом требований по обеспечению информационной безопасности; основные виды угроз и рисков безопасности информации, возникающих при интеграции информационных систем для автоматизации технологических процессов производства, транспортировки и использования топливно-энергетических ресурсов; методы анализа рисков и расчета экономического ущерба для технологических процессов производства, транспортировки и использования топливно-энергетических ресурсов вследствие инцидентов информационной безопасности; *Уметь:* осуществлять анализ рисков и расчет экономического ущерба для технологических процессов производства, транспортировки и использования топливно-энергетических ресурсов вследствие инцидентов информационной безопасности; классифицировать угрозы безопасности информации и производить оценку их актуальности применительно информационным системам предприятий ТЭК; *Владеть:* навыками разработки модели нарушителя и угроз безопасности информации для информационной инфраструктуры объектов ТЭК с учетом требований законодательства в области защиты ОКИИ;

ПК-1 Способен к проектированию и управлению проектированием ИС в топливно-энергетическом комплексе	ПК-1.1 Кодирует на языках программирования в соответствии со стандартами обработки и передачи информации в топливно-энергетическом комплексе	*Знать:* современные методы разработки программного обеспечения, автоматизации и информатизации решения прикладных задач; основные принципы применения аппаратных и программных средств и платформ информационных технологий защиты информации: средств антивирусной защиты, межсетевых экранов, встроенных средств безопасности операционных систем; основные виды угроз и уязвимостей информационной безопасности для существующих стандартов обработки и передачи информации в топливно-энергетическом комплексе и способы их предотвращения на этапе проектирования информационных систем; *Уметь:* применять современные методы создания защищенных информационных систем для ТЭК, при решении прикладных задач автоматизации и информатизации; применять современные технические, программные и аппаратные средства защиты информации: средства антивирусной защиты, межсетевые экраны, встроенные средства безопасности операционных систем; *Владеть:* навыками использования сканеров безопасности для оценки уязвимостей информационной безопасности информационных систем предприятий ТЭК, являющихся объектами КИИ; подходами к базовой настройке и использования современных программных и аппаратных средств защиты информации: брандмауэров, детекторов вторжений;

ПК-2 Способен к обеспечению соответствия проектируемых ИС принятым в топливно-энергетическом комплексе технологиям и стандартам	ПК-2.2 Учитывает специфику стандартов и технологий ТЭК при проектировании ИС в топливно-энергетическом комплексе	*Знать:* теоретические подходы к проектированию архитектуры ИС предприятий и организаций в ТЭК типовые требования безопасности к защищенным информационным системам в ТЭК; методы безопасного использования коммуникационных сетей общего доступа при построении защищенных информационных систем ТЭК; модели нарушителей и политик безопасности при проектировании защищенных информационных систем в ТЭК; *Уметь:* проектировать архитектуру информационных систем предприятий и организаций ТЭК учитывая при этом требования заказчика; решать задачи проектирования защищенных информационных систем для ТЭК; *Владеть:* навыками разработки комплексной инфраструктуры защищенной информационной системы; навыками разработки проектов нормативных и правовых актов предприятий ТЭК, регламентирующих деятельность по обеспечению информационной безопасности согласно текущему законодательству в области защиты ОКИИ;

ПК-1 Способен к проектированию и управлению проектированием ИС в топливно-энергетическом комплексе	ПК-1.2 Управляет проектированием ИС в топливно-энергетическом комплексе	*Знать:* методологии и технологии проектирования и аудита прикладных информационных систем в ТЭК; методы оценки эффективности и качества проектов по проектированию ИС применительно к ТЭК; *Уметь:* обосновывать архитектуру информационных систем с учетом требований по обеспечению информационной безопасности на объектах КИИ; выбирать методологию и технологию проектирования защищенных информационных систем с учетом особенностей их внедрения и эксплуатации в ТЭК; *Владеть:* методами управления рисками информационной безопасности, связанных с проектами по информатизации прикладных процессов и систем в ТЭК; методами обеспечения безопасности информационных ресурсов и сервисов с использованием криптографических средств защиты информации;

2. Место дисциплины в структуре ОПОП

Дисциплина Информационная безопасность объектов критической инфраструктуры относится к части, формируемой участниками образовательных отношений учебного плана по направлению подготовки 09.04.01 Информатика и вычислительная техника.

Код компетенции	Предшествующие дисциплины (модули), практики, НИР, др.	Последующие дисциплины (модули), практики, НИР, др.
УК-1		Производственная практика (преддипломная)
УК-6		Производственная практика (преддипломная)
ПК-1		Производственная практика (преддипломная)
ПК-1	Отраслевые стандарты передачи и хранения информации в топливно-энергетическом комплексе	
ПК-2		Производственная практика (преддипломная)
ПК-2	Отраслевые стандарты передачи и хранения информации в топливно-энергетическом комплексе	

Для освоения дисциплины обучающийся должен:

Знать:

– архитектуру информационных систем предприятий и организаций;

– основные законодательные акты РФ в информационной сфере;

– структуру локальных и глобальных компьютерных сетей, прикладные программы для использования ЭВМ;

– характеристики технических и программных средств реализации информационных технологий

Уметь:

– выбирать методологию и технологию проектирования информационных систем;

– проводить сравнительный анализ и выбор информационных технологий для решения прикладных задач;

– использовать ресурсы различных типов информационных систем для обработки информации

Владеть:

– навыками разработки технологической документации, использования функциональных и технологических стандартов;

– методами построения математических моделей типовых задач;

– методами поиска и обмена информацией в глобальных и локальных компьютерных сетях

3. Структура и содержание дисциплины

3.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) (ЗЕ), всего 108 часов, из которых 26 часов составляет контактная работа обучающегося с преподавателем (занятия лекционного типа 16 час., занятия семинарского типа (практические, семинарские занятия, лабораторные работы и т.п.) 8 час., зачета - 1 час., самостоятельная работа обучающегося 82 час, контроль самостоятельной работы (КСР) - 2 час. Практическая подготовка по виду профессиональной деятельности составляет 3 часа.

Вид учебной работы	Всего часов	Семестр
		3
ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ	108	108
КОНТАКТНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ С ПРЕПОДАВАТЕЛЕМ, в том числе:	26	26
Лекционные занятия (Лек)	16	16
Практические занятия (Пр)	8	8
Контроль самостоятельной работы и иная контактная работа (КСР)*	2	2
САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ (СРС):	82	82

Подготовка к промежуточной аттестации в форме: (зачет)		
ФОРМА ПРОМЕЖУТОЧНОЙАТТЕСТАЦИИ	За	За

3.2. Содержание дисциплины, структурированное по разделам и видам занятий

Разделы дисциплины	**Семестр**	**Распределение трудоемкости (в часах) по видам учебной работы, включая СРС**									**Формируемые результаты обучения (знания, умения, навыки)**	**Литература**	**Формы текущего контроля успеваемости**	**Формы промежуточной аттестации**	**Максимальное количество баллов по балльно - рейтинговой системе**
		Занятия лекционного типа	Занятия практического / семинарского типа	Лабораторные работы	Групповые консультации	Самостоятельная работа студента, в т.ч.	Контроль самостоятельной работы (КСР)	*подготовка к промежуточной аттестации*	Сдача зачета / экзамена	**Итого**					
Раздел 1. Основы информационной безопасности объектов критической информационной инфраструктуры (ОКИИ)															
1. Негативное воздействие компьютерных атак на критическую инфраструктуру государства	3	4				12				16	ПК-1.1 -З3, ПК-2.1 -З2, ПК-2.2 -З1, ПК-2.1 -З1, ПК-2.2 -У2	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3	Т, ДП	3	20

2. Субъекты и объекты КИИ. Классификация объектов КИИ	3	4				14				18	ПК-1.1-З3, ПК-2.1-З1, ПК-2.1-З2, ПК-2.2-З1, ПК-2.1-В1, ПК-2.2-У1, ПК-2.2-У2, ПК-1.2-З2, ПК-1.2-У1, ПК-1.2-У2, ПК-2.2-З3	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3	Т, ДП	3	20

3. Категорирование объектов КИИ	3	4								4	ПК-1.1-З3, ПК-1.2-З2, ПК-1.2-У1, ПК-1.2-У2, ПК-2.1-З1, ПК-2.1-З2, ПК-2.2-З1, ПК-2.2-У1, ПК-2.2-У2, ПК-2.2-В1, ПК-2.2-В2, ПК-2.1-В1	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3	Т	З	
Раздел 2. Разработка организационных и технических мер по обеспечению ИБ значимых ОКИИ															

4. Обеспечение информационной безопасности значимых объектов КИИ	3	2	8			56	2			68	ПК-1.1-З1, ПК-1.1-З2, ПК-1.1-З3, ПК-1.1-У1, ПК-1.1-У2, ПК-1.2-З1, ПК-1.2-З2, ПК-1.2-У1, ПК-1.2-У2, ПК-2.1-З1, ПК-2.1-З2, ПК-2.2-З1, ПК-2.2-З2, ПК-2.2-З3, ПК-2.2-У1, ПК-2.2-У2, ПК-1.1-В1, ПК-1.1-В2, ПК-1.2-В1, ПК-2.1-У1, ПК-2.2-В1, ПК-1.2-В2,	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3	Т, ДП, ОПР	З	60

											ПК-2.1 -З3, ПК-2.2 -В2, ПК-2.1 -У2, ПК-2.1 -В1				
5. Взаимодействие с ГосСОПКА	3	2								2	ПК-1.1 -З1, ПК-1.1 -З2, ПК-1.1 -З3, ПК-1.1 -У1, ПК-1.1 -У2, ПК-1.2 -В2, ПК-2.1 -З1, ПК-2.2 -З1, ПК-2.2 -У1, ПК-2.2 -У2	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3	Т	З	
ИТОГО		16	8			82	2			108					

3.3. Тематический план лекционных занятий

Номер раздела дисциплины	Темы лекционных занятий	Трудоемкость, час.
1	Последствия негативного воздействия компьютерных атак на критическую инфраструктуру государства.	2
2	Предпосылки для разработки и принятия Федеральный закона «О безопасности критической информационной инфраструктуры РФ»	2
3	Федеральный закон "О безопасности КИИ РФ". Понятие субъекта и объекта КИИ	2
4	Определение принадлежности организации к субъектам КИИ. Классификация объектов КИИ	2
5	Правила категорирования объектов критической информационной инфраструктуры Российской Федерации (утв. Постановлением Правительства РФ от 8 февраля 2018 г. № 127)	2

6	Порядок и сроки категорирования объектов КИИ	2
7	Создание системы обеспечения информационной безопасности значимых объектов КИИ (СОИБ ЗОКИИ)	2
8	Структура ГосСОПКА. Схемы взаимодействия с ГосСОПКА.	2
	Всего	16

3.4. Тематический план практических занятий

Номер раздела дисциплины	Темы практических занятий	Трудоемкость, час.
1	Инструментальный анализ защищенности объектов КИИ	2
2	Разработка модели угроз безопасности информации объекта КИИ. Ознакомление с методическими документами ФСТЭК России по моделированию угроз безопасности информации	2
3	Оценка экономического ущерба от инцидентов кибербезопасности на объектах ТЭК	2
4	Обеспечение безопасности промышленных сетей посредством межсетевого экранирования	2
	Всего	8

3.5. Тематический план лабораторных работ

Данный вид работы не предусмотрен учебным планом

3.6. Самостоятельная работа студента

Номер раздела дисциплины	Вид СРС	Содержание СРС	Трудоемкость, час.
1	подготовка доклада с презентацией	Анализ нормативной правовой базы в области защиты критической информационной инфраструктуры	14
2	подготовка доклада с презентацией	Инциденты информационной безопасности в ТЭК: предпосылки и последствия	12
3	подготовка отчета по практической работе	Инструментальный анализ защищенности объектов КИИ	10
4	подготовка отчета по практической работе	Разработка модели угроз безопасности информации объекта КИИ. Ознакомление с методическими документами ФСТЭК России по моделированию угроз безопасности информации	10
5	подготовка отчета по практической работе	Оценка экономического ущерба от инцидентов кибербезопасности на объектах ТЭК	14
6	подготовка отчета по практической работе	Обеспечение безопасности промышленных сетей посредством межсетевого экранирования	10
7	подготовка доклада с презентацией	Перспективные технические меры обеспечения безопасности информации на объектах КИИ	12

Всего	82

4. Образовательные технологии

При проведении учебных занятий используются традиционные образовательные технологии (лекции в сочетании с практическими занятиями, самостоятельное изучение определённых разделов) и современные образовательные технологии, направленные на обеспечение развития у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств: интерактивные лекции, работа в команде, индивидуальное обучение, междисциплинарное обучение, преподавание дисциплины на основе результатов научных исследований с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей.

При реализации дисциплины «Информационная безопасность объектов критической инфраструктуры» по образовательной программе «Информационные технологии в топливно-энергетическом комплексе» направления подготовки бакалавров 09.04.01 "Информатика и вычислительная техника" применяются электронное обучение и дистанционные образовательные технологии.

В образовательном процессе используются:

- электронные образовательные ресурсы (ЭОР), размещенные в личных кабинетах студентов Электронного университета КГЭУ, URL: http://e.kgeu.ru/

5. Оценивание результатов обучения

Оценивание результатов обучения по дисциплине осуществляется в рамках текущего контроля успеваемости, проводимого по балльно-рейтинговой системе (БРС), и промежуточной аттестации.

Обобщенные критерии и шкала оценивания уровня сформированности компетенции (индикатора достижения компетенции) по итогам освоения дисциплины:

Планируемые результаты обучения	Обобщенные критерии и шкала оценивания результатов обучения			
	неудовлетворительно	удовлетворительно	хорошо	отлично
	не зачтено	зачтено		
Полнота знаний	Уровень знаний ниже минимальных требований, имеют место грубые ошибки	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок

Наличие умений	При решении стандартных задач не продемонстрированы основные умения, имеют место грубые ошибки	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме
Наличие навыков (владение опытом)	При решении стандартных задач не продемонстрированы базовые навыки, имеют место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов

Характеристика сформированности компетенции (индикатора достижения компетенции)	Компетенция в полной мере не сформирована. Имеющихся знаний, умений,навыков недостаточно для решения практических (профессиональных) задач	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практи-ческих (профессиональных) задач, но требуется дополнительная практика по большинству практических задач	Сформированность компетенции в целом соответствует требованиям. Имеющихся знаний, умений,навыков и мотивации в целом достаточно для решения стандартных практичес-ких (профессиональных) задач	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач
Уровень сформиро-ванности компетенции (индикатора достижения компетенции)	Низкий	Ниже среднего	Средний	Высокий

Шкала оценки результатов обучения по дисциплине:

Код компетенции	Код индикатора достижения компетенции	Запланированные результаты обучения по дисциплине	Уровень сформированности компетенции (индикатора достижения компетенции)			
			Высокий	Средний	Ниже среднего	Низкий
			Шкала оценивания			
			отлично	хорошо	удовлет-ворительно	неудовлет-ворительно
			зачтено			не зачтено
ПК-1	ПК-1.1	Знать				
		современные методы разработки программного обеспечения, автоматизации и информатизации решения прикладных задач;	Уровень знаний в объеме, соответствую щем программе подготовки, без ошибок	Уровень знаний в объеме, соответствую щем программе, имеет место несколько	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний ниже минимальных требований, имеют место грубые ошибки

		основные принципы применения аппаратных и программных средств и платформ информационных технологий защиты информации: средств антивирусной защиты, межсетевых экранов, встроенных средств безопасности операционных систем;	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок	Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний ниже минимальных требований, имеют место грубые ошибки
		основные виды угроз и уязвимостей информационной безопасности для существующих стандартов обработки и передачи информации в топливно-энергетическом комплексе и способы их предотвращения на этапе проектирования информационных систем;	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок	Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний ниже минимальных требований, имеют место грубые ошибки
		Уметь				
		применять современные методы создания защищенных информационных систем для ТЭК, при решении прикладных задач автоматизации и информатизации;	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	При решении стандартных задач не продемонстрированы основные умения, имеют место грубые ошибки

		применять современные технические, программные и аппаратные средства защиты информации: средства антивирусной защиты, межсетевые экраны, встроенные средства безопасности операционных систем;	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	При решении стандартных задач не продемонстрированы основные умения, имеют место грубые ошибки
		Владеть				
		навыками использования сканеров безопасности для оценки уязвимостей информационной безопасности информационных систем предприятий ТЭК, являющихся объектами КИИ;	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	При решении стандартных задач не продемонстрированы базовые навыки, имеют место грубые ошибки
		подходами к базовой настройке и использования современных программных и аппаратных средств защиты информации: брандмауэров, детекторов вторжений;	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	При решении стандартных задач не продемонстрированы базовые навыки, имеют место грубые ошибки
	ПК-1.2	Знать				
		методологии и технологии проектирования и аудита прикладных информационных систем в ТЭК;	Уровень знаний в объеме, соответствующем программе подготовки, без	Уровень знаний в объеме, соответствующем программе,	Минимально допустимый уровень знаний, имеет место много	Уровень знаний ниже минимальных требований, имеют место
		методы оценки эффективности и качества проектов по проектированию ИС применительно к ТЭК;	Уровень знаний в объеме, соответствующем программе подготовки, без	Уровень знаний в объеме, соответствующем программе,	Минимально допустимый уровень знаний, имеет место много	Уровень знаний ниже минимальных требований, имеют место
		Уметь				

		обосновывать архитектуру информационных систем с учетом требований по обеспечению информационной безопасности на объектах КИИ;	Продемонстрированы все основные умения, решены все основные задачи с отдельными	Продемонстрированы все основные умения, решены все основные задачи с негрубыми	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками,	При решении стандартных задач не продемонстрированы основные умения, имеют место грубые
		выбирать методологию и технологию проектирования защищенных информационных систем с учетом особенностей их внедрения и эксплуатации в ТЭК;	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественн	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками,	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все	При решении стандартных задач не продемонстрированы основные умения, имеют место грубые ошибки
		Владеть				
		методами управления рисками информационной безопасности, связанных с проектами по информатизации прикладных процессов и систем в ТЭК;	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	При решении стандартных задач не продемонстрированы базовые навыки, имеют место грубые ошибки
		методами обеспечения безопасности информационных ресурсов и сервисов с использованием криптографических средств защиты информации;	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	При решении стандартных задач не продемонстрированы базовые навыки, имеют место грубые ошибки
ПК-2	ПК-2.1	Знать				
		методы построения информационной инфраструктуры предприятия ТЭК, а также средств автоматизации и коммуникации с учетом требований по обеспечению информационной безопасности;	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок	Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний ниже минимальных требований, имеют место грубые ошибки

		основные виды угроз и рисков безопасности информации, возникающих при интеграции информационных систем для автоматизации технологических процессов производства, транспортировки и использования топливно-энергетических ресурсов;	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок	Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний ниже минимальных требований, имеют место грубые ошибки
		методы анализа рисков и расчета экономического ущерба для технологических процессов производства, транспортировки и использования топливно-энергетических ресурсов вследствие инцидентов информационной безопасности;	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок	Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний ниже минимальных требований, имеют место грубые ошибки
		Уметь				
		осуществлять анализ рисков и расчет экономического ущерба для технологических процессов производства, транспортировки и использования топливно-энергетических ресурсов вследствие инцидентов информационной безопасности;	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	При решении стандартных задач не продемонстрированы основные умения, имеют место грубые ошибки

		классифицировать угрозы безопасности информации и производить оценку их актуальности применительно информационным системам предприятий ТЭК;	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	При решении стандартных задач не продемонстрированы основные умения, имеют место грубые ошибки
		Владеть				
		навыками разработки модели нарушителя и угроз безопасности информации для информационной инфраструктуры объектов ТЭК с учетом требований законодательства в области защиты ОКИИ;	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	При решении стандартных задач не продемонстрированы базовые навыки, имеют место грубые ошибки
	ПК-2.2	Знать				
		теоретические подходы к проектированию архитектуры ИС предприятий и организаций в ТЭК типовые требования безопасности к защищенным информационным системам в ТЭК;	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок	Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний ниже минимальных требований, имеют место грубые ошибки
		методы безопасного использования коммуникационных сетей общего доступа при построении защищенных информационных систем ТЭК;	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок	Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний ниже минимальных требований, имеют место грубые ошибки

		модели нарушителей и политик безопасности при проектировании защищенных информационных систем в ТЭК;	Уровень знаний в объеме, соответствую щем программе подготовки, без ошибок	Уровень знаний в объеме, соответствую щем программе, имеет место несколько	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний ниже минимальных требований, имеют место грубые ошибки
		Уметь				

		проектировать архитектуру информационных систем предприятий и организаций ТЭК учитывая при этом требования заказчика;	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок	Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний ниже минимальных требований, имеют место грубые ошибки
		решать задачи проектирования защищенных информационных систем для ТЭК;	Уровень знаний в объеме, соответствующем программе	Уровень знаний в объеме, соответствующем	Минимально допустимый уровень знаний, имеет место	Уровень знаний ниже минимальных требований,
		Владеть				
		навыками разработки комплексной инфраструктуры защищенной информационной системы;	Продемонстрированы навыки при решении нестандартных задач без ошибок и	Продемонстрированы базовые навыки при решении стандартных задач с	Имеется минимальный набор навыков для решения стандартных задач с	При решении стандартных задач не продемонстрированы базовые навыки, имеют
		навыками разработки проектов нормативных и правовых актов предприятий ТЭК, регламентирующих деятельность по обеспечению информационной безопасности согласно текущему законодательству в области защиты ОКИИ;	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	При решении стандартных задач не продемонстрированы базовые навыки, имеют место грубые ошибки

Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации приведены в Приложении к рабочей программе дисциплины. Полный комплект заданий и материалов, необходимых для оценивания результатов обучения по дисциплине, хранится на кафедре-разработчике в бумажном и электронном виде.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Учебно-методическое обеспечение

Основная литература

№ п/п	Автор(ы)	Наименование	Вид издания (учебник, учебное пособие, др.)	Место издания, издательство	Год издания	Адрес электронного ресурса	Кол-во экземпляров в библиотеке КГЭУ

1	Шаньгин В. Ф.	Информационная безопасность		М.: ДМК Пресс	2014	https://ibooks.ru/reading.php?productid=344097	1
2	Стрельцов А.А.	Организационно-правовое обеспечение информационной безопасности	учебное пособие для вузов	М.: Академия	2008		25
3	Нестеров С. А.	Основы информационной безопасности	учебное пособие	СПб.: Лань	2019	https://e.lanbook.com/book/114688	1

Дополнительная литература

№ п/п	Автор(ы)	Наименование	Вид издания (учебник, учебное пособие, др.)	Место издания, издательство	Год издания	Адрес электронного ресурса	Кол-во экземпляров в библиотеке КГЭУ
1	Коваленко Ю. И., Москвитин Г. И., Тараскин М. М.	Методика защиты информации в организациях	монография	М.: Русайнс	2016	https://www.book.ru/book/920134	1
2	Сотов А. И.	Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации	монография	М.: Русайнс	2015	https://www.book.ru/book/917131	1

3	Тараскин М. М., Захаров А. Г., Коваленко Ю. И., Москвитин Г. И.	Комплексная защита информации в организации	монография	М.: Русайнс	2016	https://www.book.ru/book/920774	1

6.2. Информационное обеспечение

6.2.1. Электронные и интернет-ресурсы

№ п/п	Наименование электронных и интернет-ресурсов	Ссылка
1	Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/threat
2	ФСТЭК России. Документы по обеспечению безопасности критической информационной инфраструктуры	https://fstec.ru/normotvorcheskaya/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury
3	Kaspersky Industrial Control Systems Cyber Emergency Response Team	https://ics-cert.kaspersky.ru/
4	Безопасность объектов КИИ	https://www.ptsecurity.com/ru-ru/solutions/bezopasnost-kii/
5	Стандарты информационной безопасности. Курс на площадке НОУ "ИНТУИТ"	https://www.intuit.ru/studies/courses/30/30/info
6	RUSCADASEC - независимая некоммерческая инициатива по развитию открытого русскоязычного международного сообщества специалистов по промышленной кибербезопасности / кибербезопасности АСУ ТП	https://www.youtube.com/channel/UCLGBGUsWM9zjPIQbSmfzG1w/about

6.2.2. Профессиональные базы данных

№ п/п	Наименование профессиональных баз данных	Адрес	Режим доступа
1	Официальный сайт Правительства Российской Федерации	http://government.ru/	http://government.ru/
2	Официальный сайт Министерства энергетики Российской Федерации	https://minenergo.gov.ru/opendata	https://minenergo.gov.ru/opendata
3	Научная электронная библиотека eLIBRARY.RU	http://elibrary.ru	http://elibrary.ru

6.2.3. Информационно-справочные системы

№ п/п	Наименование информационно-справочных систем	Адрес	Режим доступа
1	ИСС «Кодекс» / «Техэксперт»	http://app.kgeu.local/Home/Apps	http://app.kgeu.local/Home/Apps
2	«Гарант»	http://www.garant.ru/	http://www.garant.ru/
3	«Консультант плюс»	http://www.consultant.ru/	http://www.consultant.ru/

6.2.4. Лицензионное и свободно распространяемое программное обеспечение дисциплины

№ п/п	Наименование программного обеспечения	Описание	Реквизиты подтверждающих документов
1	Office 365 ProPlus	Пакет программных продуктов содержащий в себе необходимые офисные программы	ООО "Софтлайн трейд" № Tr096148 от 29.09.2020 Неискл. право. До 14.09.2021
2	Windows 10	Пользовательская операционная система	ООО "Софтлайн трейд" № Tr096148 от 29.09.2020 Неискл. право. До 14.09.2021
3	Adobe Acrobat	Пакет программ для создания и просмотра файлов формата PDF	Свободная лицензия Неискл. право. Бессрочно
4	Браузер Chrome	Система поиска информации в сети интернет	Свободная лицензия Неискл. право. Бессрочно

7. Материально-техническое обеспечение дисциплины

№ п/п	Вид учебной работы	Наименование специальных помещений и помещений для СРС	Оснащенность специальных помещений и помещений для СРС
1	Лекционные занятия	Учебная аудитория для проведения занятий лекционного типа	180 посадочных мест, доска аудиторная, акустическая система, проектор, усилитель-микшер для систем громкой связи, экран, микрофон, миникомпьютер, монитор, подключение к сети "Интернет", доступ в электронную информационно-образовательную среду
2	Самостоятельная работа обучающегося	Компьютерный класс с выходом в Интернет	30 посадочных мест, моноблок (30шт.), экран (1 шт.), камера (6 шт.), подключение к сети "Интернет", доступ в электронную информационно-образовательную среду
		Читальный зал библиотеки	30 посадочных мест, моноблок (30шт.), экран (1 шт.), камера (6 шт.), подключение к сети "Интернет", доступ в электронную информационно-образовательную среду
3	Практические занятия	Компьютерный класс с выходом в Интернет	50 посадочных, персональный компьютер (26 шт.), интерактивная доска, мультимедийный проектор., подключение к сети «Интернет», доступ в электронную информационно-образовательную среду

8. Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья и инвалидов

Лица с ограниченными возможностями здоровья (ОВЗ) и инвалиды имеют возможность беспрепятственно перемещаться из одного учебно-лабораторного корпуса в другой, подняться на все этажи учебно-лабораторных корпусов, заниматься в учебных и иных помещениях с учетом особенностей психофизического развития и состояния здоровья.

Для обучения лиц с ОВЗ и инвалидов, имеющих нарушения опорно- двигательного аппарата, обеспечены условия беспрепятственного доступа во все учебные помещения. Информация о специальных условиях, созданных для обучающихся с ОВЗ и инвалидов, размещена на сайте университета www//kgeu.ru. Имеется возможность оказания технической помощи ассистентом, а также услуг сурдопереводчиков и тифлосурдопереводчиков.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушенным слухом справочного, учебного материала по дисциплине обеспечиваются следующие условия:

- для лучшей ориентации в аудитории, применяются сигналы оповещения о начале и конце занятия (слово «звонок» пишется на доске);
- внимание слабослышащего обучающегося привлекается педагогом жестом (на плечо кладется рука, осуществляется нерезкое похлопывание);
- разговаривая с обучающимся, педагогический работник смотрит на него, говорит ясно, короткими предложениями, обеспечивая возможность чтения по губам.

Компенсация затруднений речевого и интеллектуального развития слабослышащих обучающихся проводится путем:

- использования схем, диаграмм, рисунков, компьютерных презентаций с гиперссылками, комментирующими отдельные компоненты изображения;
- регулярного применения упражнений на графическое выделение существенных признаков предметов и явлений;
- обеспечения возможности для обучающегося получить адресную консультацию по электронной почте по мере необходимости.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой по выбранному направле-нию подготовки, обеспечиваются следующие условия:

- ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;
- педагогический работник, его собеседник (при необходимости), присутствующие на занятии, представляются обучающимся, при этом каждый раз называется тот, к кому педагогический работник обращается;
- действия, жесты, перемещения педагогического работника коротко и ясно комментируются;
- печатная информация предоставляется крупным шрифтом (от 18 пунктов), тотально озвучивается;
- обеспечивается необходимый уровень освещенности помещений;
- предоставляется возможность использовать компьютеры во время занятий и право записи объяснений на диктофон (по желанию обучающихся).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ и инвалидов определяется педагогическим работником в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ, инвалиду с учетом их индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.

Структура дисциплины по заочной форме обучения

Вид учебной работы	Всего часов	Курс
		2
ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ	108	108
КОНТАКТНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ С ПРЕПОДАВАТЕЛЕМ, в том числе:	12,5	12,5
Лекционные занятия (Лек)	4	4
Практические занятия (Пр)	4	4
Контроль самостоятельной работы и иная контактная работа (КСР)*	4	4
Контактные часы во время аттестации (КПА)	0,5	0,5
САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ (СРС):	91,5	91,5
Подготовка к промежуточной аттестации в форме: (зачет)	4	4
ФОРМА ПРОМЕЖУТОЧНОЙАТТЕСТАЦИИ	3	3

Лист регистрации изменений

Дополнения и изменения в рабочей программе дисциплины на 20___ /20____ учебный год

В программу вносятся следующие изменения:

1. _____

2. _____

3. _____

Указываются номера страниц, на которых внесены изменения, и кратко дается характеристика этих изменений

Программа одобрена на заседании кафедры –разработчика «__» _____ 20_г., протокол № _____

Зав. кафедрой _____ Торкунова Ю.В.

Программа одобрена методическим советом института _____ «___»_____ 20____г., протокол № _____

Зам. директора по УМР_____ /_____/

Подпись, дата

Согласовано:

Руководитель ОПОП _____ /_____/

Подпись, дата

Приложение к рабочей программе дисциплины

КГЭУ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КГЭУ»)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
по дисциплине

Информационная безопасность объектов критической инфраструктуры

Направление подготовки 09.04.01 Информатика и вычислительная техника

Направленность(и) (профиль(и)) 09.04.01 Информационные технологии в топливно-энергетическом комплексе

Квалификация магистр

г. Казань, 2020

Оценочные материалы для проведения промежуточной аттестации обучающихся по дисциплине
«Информационная безопасность объектов критической инфраструктуры»
(наименование дисциплины, практики)

Содержание ОМ соответствует требованиям федерального государственного стандарта высшего образования по направлению подготовки 09.04.01 Информатика и вычислительная техника и учебному плану.
код и наименование направления подготовки

ОМ соответствует требованиям, предъявляемым к структуре, содержанию ОМ по дисциплине, а именно:

1 Перечень формируемых компетенций, которыми должен овладеть обучающийся в результате освоения дисциплины, соответствует ФГОС ВО и профстандарту, будущей профессиональной деятельности выпускника.

2 Показатели и критерии оценивания компетенций, а также шкалы оценивания обеспечивают возможность проведения всесторонней оценки результаты обучения, уровней сформированности компетенций.

3 Контрольные задания и иные материалы оценки результатов освоения разработаны на основе принципов оценивания: валидности, определённости, однозначности, надёжности, а также соответствуют требованиям к составу и взаимосвязи оценочных средств, полноте по количественному составу оценочных средств и позволяют объективно оценить результаты обучения, уровни сформированности компетенций.

4 Методические материалы ОМ содержат чётко сформулированные рекомендации по проведению процедуры оценивания результатов обучения и сформированности компетенций.

2. Направленность ОМ по дисциплине соответствует целям ОПОП ВО по направлению 09.04.01 «Информатика и вычислительная техника», профстандартам.

3. Объём ОМ соответствует учебному плану подготовки.

4. Качество ОМ в целом обеспечивают объективность и достоверность результатов при проведении оценивания с различными целями.

Заключение. На основании проведенной экспертизы можно сделать заключение, что ОМ по дисциплине соответствует требованиям ФГОС ВО, профессионального стандарта, современным требованиям рынка труда и рекомендуются для использования в учебном процессе.

Следует отметить, что созданы условия для максимального приближения системы оценки и контроля компетенций обучающихся к условиям их будущей профессиональной деятельности.

Рассмотрено на заседании учебно-методического совета
«_26_» __октября___2020__ г., протокол № _2__
Председатель УМС_____ Торкунова Ю.В.

Рецензент__Петрова А.С., ООО «ДжиДиСи Сервисез», инженер поддержки программно-аппаратных комплексов, к.ф.-м.н._____
(Фамилия И.О., место работы, должность, ученая степень) личная подпись

Дата 26.10.2020

Оценочные материалы по дисциплине «Информационная безопасность объектов критической инфраструктуры» - комплект контрольно-измерительных материалов, предназначенных для оценивания результатов обучения на соответствие индикаторам достижения компетенции(й):

ПК-1.1 Кодирует на языках программирования в соответствии со стандартами обработки и передачи информации в топливно- энергетическом комплексе

ПК-1.2 Управляет проектированием ИС в топливно-энергетическом комплексе

ПК-2.1 Понимает место и роль информационных систем в технологическом процессе производства, транспортировки и использования топливно- энергетических ресурсов

ПК-2.2 Учитывает специфику стандартов и технологий ТЭК при проектировании ИС в топливно-энергетическом комплексе

Оценивание результатов обучения по дисциплине осуществляется в рамках текущего контроля успеваемости, проводимого по балльно-рейтинговой системе (БРС), и промежуточной аттестации.

Текущий контроль успеваемости обеспечивает оценивание процесса обучения по дисциплине. При текущем контроле успеваемости используются следующие оценочные средства: отчет по практической работе, тест, подготовка доклада с презентацией, зачет.

Промежуточная аттестация имеет целью определить уровень достижения запланированных результатов обучения по дисциплине за 3 семестр. Форма промежуточной аттестации зачёт.

Оценочные материалы включают задания для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся, разработанные в соответствии с рабочей программой дисциплины.

1.Технологическая карта

Семестр 3

Номер раздела/ темы дисциплины	Вид СРС	Наименование оценочного средства	Код индикатора достижения компетенций	Уровень освоения дисциплины, баллы			
				неудов-но	удов-но	хорошо	отлично
				не зачтено	зачтено		
				низкий	ниже среднего	средний	высокий
Текущий контроль успеваемости							
1	подготовка доклада с презентацией	Т, ДП	ПК-1, ПК-2, ПК-2	менее 12	12 - 15	15 - 17	18 - 20
2	подготовка доклада с презентацией	Т, ДП	ПК-1, ПК-2, ПК-2	менее 12	12 - 15	16 - 18	18 - 20
4	подготовка отчета по практической работе	Т, ОПР	ПК-1, ПК-1, ПК-2, ПК-2	менее 4	4 - 6	6 - 8	7 - 10
4	подготовка отчета по практической работе	Т, ОПР	ПК-1, ПК-1, ПК-2, ПК-2	менее 4	5 - 6	6 - 8	8 - 10

4	подготовка отчета по практической работе	Т, ОПР	ПК-1, ПК-1, ПК-2, ПК-2	менее 5	5 - 6	6 - 8	8 - 10
4	подготовка отчета по практической работе	Т, ОПР	ПК-1, ПК-1, ПК-2, ПК-2	менее 5	5 - 6	6 - 8	8 - 10
4	подготовка доклада с презентацией	Т, ДП	ПК-1, ПК-1, ПК-2, ПК-2	менее 12	12 - 15	15 - 18	18 - 20
			Всего баллов	0 - 54	55-69	70-84	85-100

2. Перечень оценочных средств

Краткая характеристика оценочных средств, используемых при текущем контроле успеваемости и промежуточной аттестации обучающегося по дисциплине:

Наименование оценочного средства	Краткая характеристика оценочного средства	Оценочные материалы
Отчет по практической работе (ОПР)	Отчет по практической работе выполняется индивидуально каждым из студентов согласно Методическим указаниям, выданным на занятии. Отчет загружается в электронном виде в соответствующее задание на курсе в LMS Moodle. Преподаватель после проверки проставляет оценку по шкале "зачтено/не зачтено" с указанием замечаний, при необходимости отправляет отчет на доработку.	Задание к практической работе
Тест (Т)	Тест для закрепления теоретического материала	Тест из вопросов разного типа
Подготовка доклада с презентацией (ДП)	Доклад выполняется группой студентов (или индивидуально), оформляется в виде реферата, представляется на практическом занятии и сопровождается демонстрацией слайдов презентации. Предполагает ответы на вопросы аудитории и преподавателя. Оценивается качество - содержания доклада на соответствие заданной теме, - оформления презентации, - ответов на вопросы	Реферат, презентация
Зачет (З)	Зачет по результатам сдачи работ в течение семестра	Отсутствуют

3. Оценочные материалы текущего контроля успеваемости обучающихся

Наименование оценочного средства	**Подготовка доклада с презентацией (ДП)**
Представление и содержание оценочных материалов	Студентам необходимо подготовить доклад с презентацией, в котором будут рассмотрены принцип работы, характеристики, особенности применения одного из современных протоколов или интерфейсов, используемых для передачи информации в промышленных сетях предприятий топливно-энергетического комплекса. При подготовке и презентации доклада студенты могут работать как в индивидуальном порядке, так в команде. Темы докладов по разделу «Нормативная правовая база в области защиты КИИ» 1. Доктрина информационной безопасности Российской Федерации 2. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ 3. Федеральный закон от 26 июля 2017 г. N 193-ФЗ О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" 4. Постановление Правительства № 127 от 08.02.2018 г. «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» 5. Постановление Правительства № 162 от 17.02.2018 г. «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» 6. Приказ ФСТЭК России № 235 от 21.12.2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» 7. Приказ ФСТЭК России № 239 от 25.12.2017 г. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (далее — Требования по безопасности КИИ). 8. Приказ ФСБ РФ от 06.05.2019 № 196 «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» 9. Методика моделирования угроз безопасности информации. Методический документ ФСТЭК России 10. Юридическая ответственность должностных лиц субъекта КИИ за несоблюдение установленных правил эксплуатации технических средств объекта КИИ Темы докладов по разделу «Технические меры обеспечения безопасности информации на значимых объектах КИИ»: 1. Комплекс встроенных средств защиты ОС серверов и АРМ 2. Комплекс встроенных средств защиты ППО серверов и АРМ 3. Комплекс средств защиты среды виртуализации 4. Комплекс антивирусной защиты 5. Комплекс межсетевого экранирования и обнаружения вторжений 6. Комплекс контроля безопасности конфигураций активного сетевого оборудования 7. Комплекс встроенных средств защиты АСО 8. Комплекс резервного копирования 9. Комплекс анализа защищенности инфраструктуры 10. Комплекс сбора, анализа и корреляции событий безопасности (SIEM)

Критерии оценки и шкала оценивания в баллах	Оцениваются следующие аспекты работы студента: 1. качество оформления презентации для доклада (требования по оформлению презентации указаны ниже в разделе «Практические занятия»): - оформление презентации полностью соответствует требованиям – 4 балла; - требования по оформлению презентации частично не выполнены – 1-3 балла; - оформление презентации не соответствует требованиям – 0 баллов; 2. знание материала: - содержание материала раскрыто в полном объеме, предусмотренном программой дисциплины – 4 балла; - содержание материала раскрыто неполно, показано общее понимание вопроса, достаточное для дальнейшего изучения программного материала – 1-3 балла; - не раскрыто основное содержание учебного материала – 0 баллов; 3. Последовательность изложения: - содержание материала раскрыто последовательно, достаточно хорошо продумано – 4 балла; - последовательность изложения материала недостаточно продумана – 1-3 балла; - путаница в изложении материала – 0 баллов; 4. Владение речью и терминологией: - материал изложен грамотным языком, с точным использованием терминологии – 4 балла; - в изложении материала имелись затруднения и допущены ошибки в определении понятий и в использовании терминологии – 1-3 балла; - допущены ошибки в определении понятий – 0 баллов; 5. Применение конкретных примеров: - показано умение иллюстрировать материал конкретными примерами – 4 балла; - приведение примеров вызывает затруднение – 1-3 балла; - неумение приводить примеры при объяснении материала – 0 баллов.

Наименование оценочного средства	**Тест (Т)**
	1. Угроза информационной безопасности _____ a) потенциальное нарушение свойств информации b) все перечисленное c) то же самое, что компьютерная атака d) является причиной уязвимости 2. Наиболее опасные угрозы ИБ, с которыми сталкиваются специалисты информационной безопасности промышленных предприятий: a) утечка конфиденциальной информации b) типовое вредоносное ПО c) кибероружие d) целевые и сложные атаки 3. Какое из следующих утверждений верно для промышленных систем: * a) Большинство атак на промышленные системы являются ненаправленными, случайными атаками b) Большинство атак на промышленные системы являются целевыми атаками c) Случайный или направленный характер атаки зависит от географического расположения промышленного объекта d) Случайный или ненаправленный характер атаки зависит от принадлежности промышленного объекта к критической инфраструктуре 4. Вредонос Industroyer направлен на a) реализацию DoS-атак на сайты энергетических компаний b) шифрования данных на компьютерах инженерных работников с целью вымогания денег c) кражу критической информации из информационных систем промышленных предприятий d) нарушение критических процессов в промышленных системах управления 5. Угрозы ИБ по отношению к промышленным системам реализуются чаще всего вследствие a) некорректных механизмов аутентификации b) недостаточного контроля доступа c) некорректного контроля доступа d) наличия уязвимостей при работе с памятью 6. Наиболее распространенным подходом к обеспечению ИБ на предприятиях топливно-энергетического комплекса в настоящее время является a) подход, основанный на решениях для безопасности от разработчика b) подход, основанный на комплексном обеспечении c) игнорирование требований ИБ d) «выжидающий» подход 7. Комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами a) межсетевой экран b) система обнаружения вторжений c) DLP-система d) система предотвращения вторжений 8. Хакерская атака на вычислительную систему с целью довести её до отказа a) XML- инъекция b) DoS-атака c) SQL-инъекция d) XSS-атака 9. Федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры РФ является: * a) Ростехнадзор b) Роскомнадзор c) ФСТЭК d) ФСБ 10. Какой из перечисленных объектов вы бы не отнесли к объектам КИИ a) информационная система частной логистической компании b) информационно-телекоммуникационная сеть федерального оператора мобильной связи c) система дистанционного банковского обслуживания d) автоматизированная система оперативного управления диспетчерской службой скорой медицинской помощи e) автоматизированная система управления технологическими процессами АЭС 11. Согласно статистике наиболее уязвимым компонентом промышленных систем по отношению к угрозам ИБ является a) SCADA-системы b) Программируемые логические контроллеры c) Программное обеспечение АСУТП d) Промышленное сетевое оборудование
	При количестве правильных ответов: 8-10 – 4 балла, 5-7 – 2 балл, 0-4 – 0 баллов.

Наименование оценочного средства	**Отчет по практической работе (ОПР)**
Представление и содержание оценочных материалов	Задания представлены в методических указаниях к практическим работам.
Критерии оценки и шкала оценивания в баллах	Работа оценивается по следующим критериям: 1. Оформления отчета по практической работе согласно требованиям, установленным в методических указаниях (0-3 балла) 2. Описания результатов выполнения поставленных задач с прикреплением подтверждающих скриншотов, расчетов, таблиц, диаграмм, файлов (0-4 балла) 3. Наличия ответов на контрольные вопросы по тематике практической работы (0-3 балла)

4. Оценочные материалы промежуточной аттестации

Наименование оценочного средства	**Зачет**
Представление и содержание оценочных материалов	Отсутствуют
Критерии оценки и шкала оценивания в баллах	Студент, своевременно и качественно выполнивший в течение семестра все практические работы и тесты, набирает проходные 55 баллов и получает оценку «зачтено». В противном случае для добора баллов студент сдает необходимое количество работ и тестов.