



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования

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

АКТУАЛИЗИРОВАНО
решением ученого совета ИТЭ
протокол №8 от 16.04.2024

УТВЕРЖДАЮ

Директор института Теплоэнергетики

_____ Чичирова Н.Д.

«21» июня 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Специальность: 14.05.02 Атомные станции: проектирование, эксплуатация
и инжиниринг

Специализация: Проектирование и эксплуатация атомных станций

Квалификация: Специалист

г. Казань, 2021

Рабочая программа дисциплины разработана в соответствии с ФГОС ВО 3++ - специалитет по специальности 14.05.02 Атомные станции: проектирование, эксплуатация и инжиниринг (приказ Минобрнауки России от 28.02.2018 г. № 154)

Программу разработал(и):
доцент, канд. техн. наук _____ Исмагилов И.Р.
ст. преподаватель Бикеева Н.Г.

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатика и информационно-управляющие системы, протокол № 9 от 17.06.2021 г.

Программа рассмотрена и одобрена на заседании выпускающей кафедры Атомные и тепловые электрические станции, протокол № 21-20/21 от 18.06.2021г.
Зав. кафедрой "7^-Чичирова Н.Д.

Программа одобрена на заседании методического совета института Теплоэнергетики, протокол № 05/21 от 21.06.2021 г.
Зам. директора института Теплоэнергетики

Программа принята решением Ученого совета института Теплоэнергетики протокол № 05/21 от 21.06.2021 г.

1. Цель, задачи и планируемые результаты обучения по дисциплине

Целью освоения дисциплины «Информационная безопасность» является получение базовых теоретических представлений о современных методах и средствах защиты информации и практических навыков использования этих средств при реализации программных и аппаратных средств информационных систем масштаба предприятия.

Задачами дисциплины является формирование у обучающихся:

1. знаний

- терминологии в области информационной безопасности и защиты информации
- основных нормативных и правовых актов, регламентирующих сферу информационной безопасности и защиты информации

- принципов организации защиты информации на предприятиях;

- мер и средств защиты информации

2. умений

- выявлять основные виды угроз и уязвимостей безопасности информации;
- разрабатывать нормативно-техническую документацию с учетом требований нормативных и правовых актов в области информационной безопасности и защиты информации

- криптографические методы обеспечения целостности и конфиденциальности информации

3. владения:

- навыками применения программно-аппаратных средств для обеспечения информационной безопасности

- навыками программной реализации криптографических алгоритмов

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине (знать, уметь, владеть)
Общепрофессиональные компетенции (ОПК)		
ОПК-3 Способен понимать принципы работы информационных технологий; осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий, соблюдать основные тре-	ОПК-3.2 Способен осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий	Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (31) Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований

<p>бования информационной безопасности, в том числе защиты государственной тайны</p>		<p>информационной безопасности (У1) Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности (В1)</p>
	<p>ОПК-3.3 Способен соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны</p>	<p>Знать: основные виды угроз безопасности информации, уязвимостей информационных систем, а также меры и средства противодействия атакам на информационные ресурсы при проектировании, разработке и внедрении программного обеспечения информационных систем (З1) Уметь: разрабатывать проектно-техническую документацию для информационных систем с учетом требований текущего законодательства, нормативно-правовых актов, стандартов и ведущих практик в области информационной безопасности (У1) Владеть: навыками применения программно-аппаратных средств для анализа защищенности информационных систем для выработки мер противодействия известным угрозам безопасности информации (В1)</p>

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность» относится к обязательной части образовательной программы подготовки специалистов 14.05.02 Атомные станции: проектирование, эксплуатация и инжиниринг, специализация «Проектирование и эксплуатация атомных станций».

Для освоения дисциплины обучающийся должен:

Знать:

1. основы математики, физики, вычислительной техники и программирования.
2. современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.
3. алгоритмические языки программирования, операционные системы и оболочки, современные среды разработки программного обеспечения.

Уметь:

1. решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования.
2. выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.
3. составлять алгоритмы, писать и отлаживать коды на языке программирования, тестировать работоспособность программы, интегрировать программные модули.

Владеть:

1. навыками применения современных информационных технологий и программных средств при решении задач профессиональной деятельности.

3. Структура и содержание дисциплины

3.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (ЗЕ), всего 108 часов, из которых 32 часа составляет контактная работа обучающегося с преподавателем (занятия лекционного типа 16 часов, практические работы 16 часов), самостоятельная работа обучающегося 76 часов.

Вид учебной работы	Всего зачетных единиц	Всего часов	семестр
			2
ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ, в т.ч. по РУП:	3	108	108
КОНТАКТНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ С ПРЕПОДАВАТЕЛЕМ		32	32
Лекции (Лк)		16	16
Практические занятия (ПР)		16	16
САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ		76	76
ВИД ПРОМЕЖУТОЧНОГО КОНТРОЛЯ	3	3а	3а

3.2. Содержание дисциплины, структурированное по разделам и видам занятий

Разделы дисциплины	Семестр	Распределение трудоемкости (в часах) по видам учебной работы, включая СРС							Итого	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	Лабораторные работы	Групповые консультации	Самостоятельная работа студента, в т.ч.	Контроль самостоятельной работы (КСР)	подготовка к промежуточной аттестации						
Раздел 1. Основные понятия и нормативно-правовая база информационной без опасности	2	2	2			10			14	ОПК-3.2- У1, ОПК-3.3- У1, ОПК-3.2- В1, ОПК-3.2- 31, ОПК-3.3-31	Л1.2, Л2.1, Л2.3	тест		14
Раздел 2. Управление информационной безопасностью	2	2	2			11			15	ОПК-3.2- 31, ОПК-3.2- У1	Л1.2, Л2.3, Л2.1	тест		14
Раздел 3. Меры и средства защиты информации. Криптографические средства защиты информации (КСЗИ)	2	4	2			11			17	ОПК-3.3- 31, ОПК-3.3- В1	Л1.2, Л2.1, Л2.3, Л1.1	тест		14
Раздел 4. Идентификация, аутентификация и управление доступом	2	2	4			11			17	ОПК-3.3- В1, ОПК-3.3-31	Л1.2, Л2.3	тест		14
Раздел 5. Обеспечение безопасности информации в операционных системах	2	2	2			11			15	ОПК-3.2- У1, ОПК-3.3- У1	Л1.1, Л1.2, Л2.3, Л2.1	тест		15
Раздел 6. Средства антивирусной защиты (САВЗ)	2	2	2			11			15	ОПК-3.2- У1, ОПК-3.2- В1	Л1.1, Л1.2, Л2.3	тест		15

Раздел 7. Обеспечение безопасности информации в компьютерных сетях	2	2	2			11				15	ОПК-3.3- 31, ОПК-3.3- В1	Л1.1, Л1.2, Л2.2, Л2.1	тест		14
ИТОГО	2	16	16	-	-	76	-	-	-	108	ОПК-3.2- ОПК3.3	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3			100

3.3. Тематический план лекционных занятий

№ п/п	Темы лекционных занятий	Трудоемкость, час.
1	Основные понятия информационной безопасности	1
2	Государственная политика в области информационной безопасности	1
3	Международные и российские стандарты информационной безопасности	1
4	Формирование политики информационной безопасности на предприятии	1
5	Симметричные криптосистемы шифрования. Стеганография	1
6	Ассиметричные криптосистемы шифрования и электронная подпись	1
7	Управление крипто ключами. Инфраструктура открытых ключей	1
8	Технологии аутентификации	1
9	Криптографические протоколы аутентификации. Биометрическая аутентификация	1
10	Модели разграничения доступа	1
11	Обеспечение безопасности информации в операционных системах семейства Windows	1
12	Средства антивирусной защиты информации	1
13	Классификация вредоносных программ	1
14	Классификация угроз безопасности информации и атак в компьютерных сетях	1
15	Технология виртуальных локальных сетей (VLAN)	1
16	Технологии межсетевого экранирования	1
	Всего	16

3.4. Тематический план практических занятий

№ п/п	Темы практических занятий	Трудоемкость, час.
1	Изучение видов информации, доступ к которым ограничен федеральными законами РФ	2
2	Программная реализация стеганографии в графических файлах	2
3	Программная реализация асимметричного алгоритма шифрования RSA	2
4	Защита информации в электронных документах путем	2

	шифрования и формирования электронной подписи	
5	Парольная аутентификация	2
6	Автоматизированное обнаружение уязвимостей программного обеспечения на рабочих станциях под управлением операционных систем семейства Microsoft Windows	2
7	Сравнительный анализ средств антивирусной защиты информации с использованием результатов независимых тестов	2
8	Изучение технологий межсетевого экранирования с помощью программы моделирования сетей Cisco Packet Tracer	2
Всего		16

3.5. Тематический план лабораторных работ

Данный вид занятий не предусмотрен в учебном плане.

3.6. Самостоятельная работа студента

№ п/п	Вид СРС	Содержание СРС	Трудоемкость, час.
1	подготовка к практическому занятию	Классификация информации, доступ к которой ограничен федеральными законами РФ. Виды юридической ответственности и правоприменительная практика в области информационной безопасности	2
2	изучение теоретического материала	Возникновение и история развития проблемы защиты информации. Понятие информационного общества. Актуальность проблемы обеспечения безопасности информации.	2
3	изучение теоретического материала	Стратегия национальной безопасности РФ. Доктрина информационной безопасности РФ	2
4	подготовка к практической работе	Моделирование и оценка угроз безопасности информации. Модель нарушителя. Методика определения актуальных угроз безопасности информации.	2
5	изучение теоретического материала	Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Отечественные стандарты безопасности информационных технологий	2
6	изучение теоретического материала	Структура политики безопасности организации. Разработка политики безопасности организации	2
7	подготовка к практической работе	Методика определения рисков информационной безопасности	2
8	изучение теоретического материала	Классификация симметричных криптосистем. Криптостойкость симметричных криптосистем.	4
9	подготовка к практической работе	Блочные и потоковые шифры. Шифр Цезаря. Шифр Виженера. Шифрование методом перестановки. Гаммирование.	2
10	подготовка к практической работе	Шифр playfair. Шифр Полибия. Афинный шифр. Виды криптоанализа. Установка языка программирования Python, изучение	4

	боте	базового синтаксиса. Работа с командной строкой Windows.	
11	подготовка к практическому занятию	Классификация стеганографических средств защиты информации	2
12	изучение теоретического материала	Генерация простых чисел для формирования ключей шифрования. Криптография на эллиптических кривых	2
13	подготовка к практическому занятию	Генерация простых чисел для формирования пары ключей для шифрования. Библиотеки Python для программной реализации асимметричных криптоалгоритмов.	4
14	подготовка к практической работе	PGP шифрование. Криптографические хеш-функции. Виды электронной подписи	2
15	изучение теоретического материала	Удостоверяющие центры и сертификаты.	2
16	изучение теоретического материала	Строгая аутентификация. Многофакторная аутентификация.	2
17	изучение теоретического материала	Виды биометрической идентификации	2
18	изучение теоретического материала	Классификация моделей разграничения доступа. Модель систем дискреционного разграничения доступа. Мандатное управление доступом. Ролевое разграничение. Сравнительный анализ моделей разграничения доступа.	4
19	изучение теоретического материала	Управление пользовательскими учетными записями (User Account Control - UAC). Брандмауэр.	2
20	подготовка к практическому занятию	Сканеры уязвимостей типа host-based. Система оценки уязвимостей - CVSS2.0 и CVSS3.0	2
21	подготовка к практической работе	Локальные и групповые политики ОС Microsoft Windows	2
22	изучение теоретического материала	Основные каналы распространения вредоносных программ. Антивирусные программы: основы работы антивирусных программ, особенности «облачной» антивирусной технологии, виды антивирусных программ, дополнительные модули антивирусных программ, режимы работы антивируса	4
23	изучение теоретического материала	Антивирусные программные комплексы: антивирус Касперского, антивирус Dr. Web, антивирус Norton AntiVirus от Symantec, антивирус McAfee, антивирус AntiVir Personal Edition	2
24	подготовка к практическому занятию	Методы обнаружения вредоносных программ. Режим "песочницы".	2
25	изучение теоретического материала	ARP-спуфинг. SYN-флуд. Smurf- атака. Атаки на беспроводные сети.	4
26	изучение теоретического материала	Сегментация сети с помощью технологии VLAN. Использование протокола 802.1Q	2
27	подготовка к лабораторной работе	Преимущества сегментирования локальных сетей. Настройка VLAN на коммутаторах фирмы Cisco.	2
28	изучение теоретического материала	Функции межсетевое экрана. Классификация МЭ.	2
29	подготовка к практическому занятию	Списки доступа (ACL). Демилитаризованная зона (DMZ)	2

30	изучение теоретического материала	VPN-туннелирование. VPN-сервер. VPN - клиент. Классификация VPN.	2
31	подготовка к лабораторной работе	Установка TCP соединения. Структура TCP-пакета. Флаги состояния. Применение фильтров для анализа трафика в Wireshark	2
32	подготовка к лабораторной работе	Разновидности сканеров безопасности сети. Виртуальные машины. ПО для работы с виртуальными машинами (Virtual Box)	2
Всего			76

4. Образовательные технологии

При проведении учебных занятий используются традиционные образовательные технологии (лекции в сочетании с практическими занятиями и лабораторными работами, 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.

5. Оценка результатов обучения

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

Текущий контроль успеваемости осуществляется в течение семестра, включает: отчет по лабораторной работе (ОЛР); проведение компьютерного тестирования.

Итоговой оценкой результатов освоения дисциплины является оценка, выставленная во время промежуточной аттестации обучающегося (зачет с оценкой) с учетом результатов текущего контроля успеваемости. На зачет с оценкой выносятся теоретические и практические задания, проработанные в течение семестра на учебных занятиях и в процессе самостоятельной работы обучающихся. Билеты содержат 2 теоретических задания и 1 задание практического характера.

Обобщенные критерии и шкала оценивания уровня сформированности компетенции (дескрипторы 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 незначительными 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	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 практических (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 практических (профессиональных) задач	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач
Уровень сформированности компетенции	Низкий	Ниже среднего	Средний	Высокий

Шкала оценки результатов обучения по дисциплине:

Код компетенции	Код индикатора достижения компетенции	Запланированные результаты обучения по дисциплине	Уровень сформированное™ компетенции (индикатора достижения компетенции)			
			Высокий	Средний	Ниже среднего	Низкий
			Шкала оценивания			
			отлично	хорошо	удовлетворительно	неудовлетворительно
			зачтено			не зачтено
ОПК-	ОПК-	Знать				
3	3.2	принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований 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				
		решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований 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
		Владеть				
		навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	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
ОПК-	ОПК-	Знать				

		основные виды угроз безопасности информации, уязвимостей информационных систем, а также меры и средства противодействия атакам на информационные ресурсы при проектировании, разработке и внедрении программного обеспечения 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				
	3.3	Разрабатывать проектно-техническую документацию для информационных систем с учетом требований текущего законодательства, нормативно-правовых актов, стандартов и ведущих практик в области 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
		Владеть				
		навыками применения программно-аппаратных средств для анализа защищенности информационных систем для выработки мер противодействия известным угрозам безопасности 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

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	Баранова Е. К., Бабаш А. В.	Криптографические методы защиты информации. Лабораторный практикум	Учебное пособие	М.: Кнорус	2017	https://www.book.ru/book/920017/	
2	Демушкин А. С., Кондрашова Т. В., Фабричнов А. Г., Куняев Н. Н.	Конфиденциальное делопроизводство и защищенный электронный документооборот	учебник для вузов	М.: Логос	2013	https://ibooks.ru/reading.php?productid=29403	

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	Крылов Г. О., Ларионова С. Л., Никитина В. Л.	Базовые понятия информационной безопасности	учебное пособие	М.: Русайнс	2021	https://book.ru/book/941862	
2	Шевченко В. П.	Вычислительные системы, сети и телекоммуникации	Учебник	М.: Кнорус	2021	https://book.ru/book/936930	

3	Мельников В. П., Куприянов А. И., Васильева Т. Ю.	Информационная безопасность	учебник	М.: Кнорус	2020	https://book.ru/book/932908	
---	---	-----------------------------	---------	------------	------	---	--

6.2. Информационное обеспечение

6.2.1. Электронные и интернет-ресурсы

№ п/п	Наименование электронных и интернет-ресурсов	Ссылка
1	Справочно-правовая система "Консультант Плюс"	http://www.consultant.ru/
2	Справочно-правовая система "Гарант"	http://www.garant.ru/
3	Банк данных угроз безопасности информации	https://bdu.fstec.ru/
4	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных	https://fstec.ru/component/attachments/download/289
5	ISO27000 - Искусство управления информационной безопасностью	http://www.iso27000.ru/standarty
6	Учебный курс на портале НОУ "ИНТУИТ" - Стандарты информационной безопасности	https://www.intuit.ru/studies/courses/30/30/info
7	Учебный курс на портале НОУ "ИНТУИТ" - Информационная безопасность. Технологии Microsoft	https://www.intuit.ru/studies/professional_retraining/952/courses/419/lecture/9577?page=2
8	Учебный курс на портале НОУ "ИНТУИТ" - Информационная безопасность. Технологии Microsoft: Анализ и управление рисками в информационных системах на базе операционных систем Microsoft	https://www.intuit.ru/studies/professional_retraining/952/courses/387/info
9	Anti-Malware Testing Standards Organization	https://www.amtso.org/
10	AV-TEST - The Independent IT-Security Institute	https://www.av-test.org/en/
11	AV-Comparatives - Independent Tests of Anti-Virus Software	https://www.av-comparatives.org/
12	Wireshark — программа-анализатор трафика для компьютерных сетей Ethernet	https://www.wireshark.org/
13	Справочное руководство Nmap на русском языке	https://nmap.org/man/ru/index.html
14	OpenVAS Russia. Русскоязычное сообщество пользователей сканера уязвимостей OpenVAS	https://openvas.ru/
15	Cisco Networking Academy	https://www.netacad.com/
16	Cisco Networking Academy - маршрутизация и коммутация	http://ccna.mpei.ac.ru/RoutingAndSwitching/

6.2.2. Профессиональные базы данных

№ п/п	Наименование профессиональных баз данных	Адрес	Режим доступа
1	Российская национальная библиотека	http://nlr.ru/	http://nlr.ru/
2	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	Браузер Chrome	Система поиска информации в сети интернет (включая русскоязычный интернет).	https://www.google.com/intl/ru/chrome/
2	Браузер Firefox	Свободный веб-браузер	https://www.mozilla.org/ru/firefox/new/
3	OpenOffice	Пакет офисных приложений. Одним из первых стал поддерживать новый открытый формат OpenDocument. Официально поддерживается на платформах Linux	https://www.openoffice.org/ru/download/index.html
4	Adobe Acrobat	Пакет программ	https://get.adobe.com/ru/reader/
5	LMS Moodle	Это современное программное обеспечение	https://download.moodle.org/releases/latest/
6	Windows 7 Профессиональная (Pro)	Пользовательская операционная система	№2011.25486 от 28.11.2011

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 опорнодвигательного 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 направлению 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.

9. Методические рекомендации для преподавателей по организации воспитательной работы с обучающимися

Методическое обеспечение процесса воспитания обучающихся выступает одним из определяющих факторов высокого качества образования. Преподаватель вуза, демонстрируя высокий профессионализм, эрудицию, четкую гражданскую позицию, самодисциплину, творческий подход в решении профессиональных задач, в ходе образовательного процесса способствует формированию гармоничной личности.

При реализации дисциплины преподаватель может использовать следующие методы воспитательной работы:

- методы формирования сознания личности (беседа, диспут, внушение, инструктаж, контроль, объяснение, пример, самоконтроль, рассказ, совет, убеждение и др.);

- методы организации деятельности и формирования опыта поведения (задание, общественное мнение, педагогическое требование, поручение, приучение, создание воспитывающих ситуаций, тренинг, упражнение, и др.);

- методы мотивации деятельности и поведения (одобрение, поощрение социальной активности, порицание, создание ситуаций успеха, создание ситуаций для эмоционально-нравственных переживаний, соревнование и др.)

При реализации дисциплины преподаватель должен учитывать следующие направления воспитательной деятельности:

Гражданское и патриотическое воспитание:

- формирование у обучающихся целостного мировоззрения, российской идентичности, формирование у обучающихся целостного мировоззрения, российской идентичности, уважения к своей семье, обществу, государству, принятым в семье и обществе духовнонравственным и социокультурным ценностям, к национальному, культурному и историческому наследию, формирование стремления к его сохранению и развитию;

- формирование у обучающихся активной гражданской позиции, основанной на традиционных культурных, духовных и нравственных ценностях российского общества, для повышения способности ответственно реализовывать свои конституционные права и обязанности;

- развитие правовой и политической культуры обучающихся, расширение кон-

структивного участия в принятии решений, затрагивающих их права и интересы, в том числе в различных формах самоорганизации, самоуправления, общественно-значимой деятельности;

- формирование мотивов, нравственных и смысловых установок личности, позволяющих противостоять экстремизму, ксенофобии, дискриминации по социальным, религиозным, расовым, национальным признакам, межэтнической и межконфессиональной нетерпимости, другим негативным социальным явлениям.

Духовно-нравственное воспитание:

- воспитание чувства достоинства, чести и честности, совестливости, уважения к родителям, учителям, людям старшего поколения;

- формирование принципов коллективизма и солидарности, духа милосердия и сострадания, привычки заботиться о людях, находящихся в трудной жизненной ситуации;

- формирование солидарности и чувства социальной ответственности по отношению к людям с ограниченными возможностями здоровья, преодоление психологических барьеров по отношению к людям с ограниченными возможностями;

- формирование эмоционально насыщенного и духовно возвышенного отношения к миру, способности и умения передавать другим свой эстетический опыт.

Культурно-просветительское воспитание:

- формирование уважения к культурным ценностям родного города, края, страны;

- формирование эстетической картины мира;

- повышение познавательной активности обучающихся.

Научно-образовательное воспитание:

- формирование у обучающихся научного мировоззрения;

- формирование умения получать знания;

- формирование навыков анализа и синтеза информации, в том числе в профессиональной области.

Лист регистрации изменений

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

В программу вносятся следующие изменения:

1..

2. _____

3. _____

Программа одобрена на заседании кафедры - разработчика « ____ »20_г.,
протокол №

Зав. кафедрой Торкунова Ю.В.

Программа одобрена методическим советом института Теплоэнергетики протокол
№ от 202 г.

Зам. директора по УМР

//



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
КГЭУ «КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КГЭУ»)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ по дисциплине
Информационная безопасность

Специальность: 14.05.02 Атомные станции: проектирование, эксплуатация и инжиниринг

Специализация: Проектирование и эксплуатация атомных станций

Квалификация: Специалист

РЕЦЕНЗИЯ

на оценочные материалы для проведения текущей аттестации по дисциплине «**Информационная безопасность**»

Содержание ОМ соответствует требованиям федерального государственного стандарта высшего образования по специальности 14.05.02 «Атомные станции: проектирование, эксплуатация и инжиниринг» и учебному плану.

Перечень формируемых компетенций: ОПК-3.2; ОПК-3.3, которыми должен овладеть обучающийся в результате освоения дисциплины, соответствует ФГОС ВО.

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

Контрольные задания оценки результатов освоения разработаны на основе принципов оценивания: валидности, определённости, однозначности, надёжности, позволяют объективно оценить уровни сформированности компетенций.

Заключение. Учебно-методический совет делает вывод о том, что представленные материалы соответствуют требованиям ФГОС ВО по специальности 14.05.02 «Атомные станции: проектирование, эксплуатация и инжиниринг» и рекомендуются для использования в учебном процессе.

Рассмотрено на заседании учебно-методического совета института теплоэнергетики 21.06.2021 г. протокол № 05/21

Председатель УМС

Н.Д. Чичирова

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

ОПК-3 Способен понимать принципы работы информационных технологий; осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны

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:

Промежуточная аттестация имеет целью определить уровень достижения запланированных результатов обучения по дисциплине за 2 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 2

Номер раздела/ темы дисциплины	Вид СРС	Наименование оценочного средства	Код индикатора достижения компетенций	Уровень освоения дисциплины, баллы				
				удов-но	удов-но	хорошо	отлично	
				не зачтено	зачтено			
				низкий	ниже среднего	средний	высокий	
Текущий контроль успеваемости								
1	Изучение теоретического материала	тест	ОПК-3.2	менее 7	7 - 9	9 - 12	12-14	
2	Изучение теоретического материала	тест	ОПК-3.2, ОПК-3.3	менее 8	8 - 10	10 - 12	12-14	
3	Изучение теоретического материала	тест	ОПК-3.2	менее 8	8 - 10	10 - 12	12-14	
4	Изучение теоретического материала	тест	ОПК-3 .1	менее 8	8- 10	10 - 12	12-14	
5	Изучение теоретического материала	тест	ОПК-3.2, ОПК-3 .2	менее 8	8- 10	11- 12	12-15	

6	Изучение теоретического материала	тест	ОПК-3.2, ОПК-3.2	менее 8	8- 10	10 - 12	13-15
7	Изучение теоретического материала	тест	ОПК-3.2, ОПК-3.3	менее 8	8 - 10	10 - 12	12-14
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
Тест по теме раздела	Тест из 10 вопросов для закрепления лекционного материала	Тест из 10 вопросов разного типа

3. Оценочные материалы текущего контроля успеваемости обучающихся

Наименование оценочного средства	Тест по теме лекции (Тест)
Представление и содержание оценочных материалов	Тест из 10 вопросов разного типа по определенному разделу дисциплины Примеры тестов из раздела дисциплины «Основные понятия и нормативно-правовая база информационной безопасности»: 1.2 Возможность за приемлемое время получить требуемую информационную услугу — это _____ а) доступность б) конфиденциальность с) целостность d) адекватность е) неотказуемость 1.8 Совокупность условий или действий, создающих потенциальную или реально существующую опасность нарушения безопасности информации а)угроза безопасности информации b) риск безопасности информации с) уязвимость безопасности информации d) атака на информационные ресурсы
Критерии оценки и шкала оценивания в баллах	При количестве правильных ответов: 8-15 - зачтено, менее 8 - не зачтено

4. Оценочные материалы промежуточной аттестации

Промежуточная аттестация не предусмотрена учебным планом