МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ С.И. Лукьянов

26.02.2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРОЙ

Направление подготовки (специальность)
10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ
Направленность (профиль/специализация) программы
10.05.03 специализация N 7 "Обеспечение информационной безопасности распределенных информационных систем";

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	5
Семестр	9

Магнитогорск
2020 год

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ (приказ Минобрнауки России от 01.12.2016 г. № 1509)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
18.02.2020, протокол № 6

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
26.02.2020 г. протокол № 5

Председатель _____ С.И. Лукьянов

Рабочая программа составлена:
доцент кафедры ИиИБ, канд. техн. наук _____ У.В. Михайлова

Рецензент:
Начальник отдела информационной безопасности АО "КУБ" _____ М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2022 - 2023 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целью освоения дисциплины "Обеспечение информационной безопасности критической информационной инфраструктуры" является получение компетенций, необходимых для осуществления профессиональной деятельности субъектов критической информационной инфраструктуры (КИИ), ответственных за обеспечение безопасности значимых объектов КИИ.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Обеспечение информационной безопасности критической информационной инфраструктурой входит в вариативную часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Организация ЭВМ и вычислительных систем

Введение в специальность

Теория информации

Основы безопасности цифрового общества

Информатика

Основы информационной безопасности

Сети и системы передачи информации

Правоведение

Физические основы передачи информации

Основы радиотехники

Моделирование угроз информационной безопасности

Математическая логика и теория алгоритмов

Технология построения защищенных распределенных приложений

Программно-аппаратные средства обеспечения информационной безопасности

Безопасность систем баз данных

Безопасность сетей ЭВМ

Безопасность Интернета вещей

Техническая защита информации

Тестирование систем защиты информации автоматизированных систем

Организационное и правовое обеспечение информационной безопасности

Методы выявления нарушений информационной безопасности

Информационная безопасность распределенных информационных систем

Безопасность операционных систем

Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Разработка и эксплуатация защищенных автоматизированных систем

Разработка эксплуатационной документации на системы защиты информации автоматизированных систем

Аттестация АИС

Методы и стандарты оценки защищенности компьютерных систем

Криптографические методы защиты информации

Иностранный язык в профессиональной деятельности

Анализ уязвимостей программного обеспечения

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Научно-исследовательская работа

Производственная-преддипломная практика

Управление информационной безопасностью

Подготовка к сдаче и сдача государственного экзамена

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Обеспечение информационной безопасности критической информационной инфраструктурой» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	
Знать	- нормативные и правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ; - основы функционирования ГосСОПКА; - понятия объектов и субъектов КИИ;
Уметь	- выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа уязвимостей значимого объекта КИИ; - способы реализации угроз безопасности и возможные последствия от их реализации; - определять требования по устранению возможных уязвимостей, приводящих к возникновению угроз безопасности информации;
Владеть	- навыками работы с нормативными и правовыми актами, методическими документами и национальными стандартами в области обеспечения безопасности значимых объектов КИИ; - навыками работы с информационными базами данных, содержащими информацию по угрозам безопасности информации и уязвимостями ПО значимых объектов КИИ; - навыками выявления и анализа угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа уязвимостей значимого объекта КИИ;
ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	
Знать	- понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ; - общие требования по обеспечения безопасности значимых объектов КИИ; - подходы категорирования значимости объектов КИИ;
Уметь	- определять категории значимых объектов КИИ и оформлять полученные результаты; - определять структуру системы безопасности значимого объекта КИИ; - определят требования по обеспечения безопасности значимых объектов КИИ; - определять требования к параметрам настройки программных и программно-аппаратных средств защиты информации (СЗИ);

Владеть	- навыками установки и настройки СЗИ, обрабатываемой объектами КИИ; - навыками подбора средств СЗИ с учетом совместимости с применяемым на значимом объекте КИИ ПО и категорированием значимого объекта КИИ;
ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	
Знать	-требования к организационным и техническим мерам для обеспечения безопасности значимых объектов КИИ; - основные принципы организации государственного контроля состояния защищенности значимых объектов КИИ; - процедуру категорирования объектов КИИ; - требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования;
Уметь	- осуществлять выбор СЗИ с учетом совместимости с применяемым на значимом объекте КИИ ПО и категорированием значимого объекта КИИ; - определять СЗИ для реализации технических мер обеспечения безопасности информации в рамках системы безопасности значимого объекта КИИ;
Владеть	- навыками участия в разработке организационных и технических мероприятий по защите объектов КИИ; - навыками разработки организационно-распорядительными документов по безопасности значимых объектов КИИ; - навыками проведения работ по контролю состояния безопасности объектов КИИ;

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:

– контактная работа – 37 акад. часов:

– аудиторная – 36 акад. часов;

– внеаудиторная – 1 акад. часов

– самостоятельная работа – 107 акад. часов;

Форма аттестации - зачет

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Правовые основы обеспечение безопасности информации объектов КИИ РФ								
1.1 Понятия объекта и субъекта КИИ. 1.2 Законодательство РФ по обеспечение безопасности информации объектов КИИ. Нормативные методические документы ФСТЭК России по обеспечение безопасности информации объектов КИИ. 1.3 Угрозы безопасности информации, обрабатываемой на объектах КИИ	9	4	4		20	Изучение документов ФСТЭК России. Подготовка к практическим занятиям и тестированию.	Тестирование	ПК-4
1.4 Категорирование объектов КИИ 1.5 Организация работ по обеспечению безопасности объектов КИИ 1.6 ГосСОПКА		4	4		20	Изучение документов ФСТЭК России. Подготовка к практическим занятия и выполнение индивидуальног о домашнего задания (ИДЗ).	ИДЗ	ПК-4, ПК-24, ПК-25
Итого по разделу		8	8		40			
2. Обеспечение безопасности информации значимых объектов КИИ								

2.1 Требования по обеспечению безопасности значимых объектов КИИ 2.2 Система безопасности значимого объекта КИИ. Этапы разработки 2.3 Контроль за обеспечением безопасности значимого объекта КИИ.	9	5	5		25	Подготовка к практическим занятиям. Выполнение ИДЗ.	ИДЗ	ПК-24, ПК-25
2.4 Основные программно-технические подсистемы СОБИ КСИИ 2.5 Управление ОБИ КСИИ документирование и реализация основных процессов. 2.6 Этапы разработки СОБИ КИИ. Аналитическое обоснование необходимости создания СОБИ КИИ. 2.7 Техническое задание на разработку СОБИ КИИ. Основные проектные документы. Разработка комплекса внутренних организационно-распорядительных документов		5	5		25	Подготовка к практическим занятиям. Выполнение ИДЗ	ИДЗ	ПК-24, ПК-25
Итого по разделу		10	10		50			
3. Зачет								
3.1 Подготовка к зачету	9				10	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Самостоятельная работа с интернет-источниками.	Зачет	ПК-4, ПК-24, ПК-25
Итого по разделу					17			
Итого за семестр		18	18		100		зачёт	ПК-4,ПК-24,ПК-25
Итого по дисциплине		18	18		107		зачет	ПК-4,ПК-24,ПК-25

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. Формы учебных занятий с использованием традиционных технологий:

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. Формы учебных занятий с использованием традиционных технологий:

a) Вводная лекция – для целостного представления об учебном предмете и анализа учебно-методической литературы;

b) Обзорные лекции – для систематизации научных знаний на высоком уровне с использованием ассоциативных связей в процессе представления и осмысления информации;

c) Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя);

d) Семинар – беседа преподавателя и обучающихся, обсуждение заранее подготовленных сообщений по каждому вопросу плана занятия с единым для всех перечнем рекомендуемой обязательной и дополнительной литературы;

e) Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму;

f) Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2) Раздельно-компетентностная технология, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. Формы учебных занятий с использованием Раздельно-компетентностной технологии:

a) Кейс-методы – для овладения системой знаний и умений и творческого их использования в профессиональной деятельности и самообразовании; для квалифицированного и независимого решения профессиональных задач; для ориентации в многообразии учебных программ, пособий, литературы и выбора наиболее эффективных в применении к конкретной ситуации; для осуществления саморефлексии для дальнейшего профессионального, творческого роста и социализации личности.

3) Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отношения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды. Формы учебных занятий с использованием интерактивных технологий:

a) Case-study – для анализа реальных проблемных ситуаций и поиска лучших вариантов решений, разбор результатов тематических контрольных работ, анализ

ошибок, совместный поиск вариантов рационального решения проблемы.

b) Методы IT – для применения компьютеров в процессе освоения дисциплины и доступа к ЭОР кафедры и Интернет-ресурсам.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Перечень тем для тестирования

1.Объекты и субъекты КИИ. Права и обязанности субъектов КИИ.

2.Полномочия органов гос. власти РФ в области обеспечения безопасности КИИ.

3.Информационные системы нормативно правовых актов в области обеспечения безопасности КИИ.

4.Система безопасности значимого объекта КИИ. Цели и задачи. Этапы разработки.

5.Основные понятия, термины и определения в области обеспечения безопасности КИИ.

6.Типовые угрозы безопасности информации ИС и автоматизированных систем управления.

Примерные индивидуальные задания

Задание 1. Составить майнд-карту угроз безопасности информации значимого объекта КИИ.

Задание 2. Составить майнд-карты оценки возможностей внешних и внутренних нарушителей для значимого объекта КИИ.

7 Оценочные средства для проведения промежуточной аттестации

Промежуточная аттестация имеет целью определить степень достижения запланированных результатов обучения по каждой дисциплине (модулю) за определенный период обучения (семестр) и может проводиться в форме зачета, экзамена, защиты курсовой работы.

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы		
Знать:	- нормативные и правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ; - основы функционирования ГосСОПКА; - понятия объектов и субъектов КИИ;	Теоретические вопросы: 1. Федеральный закон №187-ФЗ от 26.07.2017 г. «О безопасности критической информационной инфраструктуры РФ» 2. Положение о банке данных угроз безопасности информации. 3. Форма акта проверки, составляемого по итогам проведения гос. контроля в области обеспечения безопасности значимых объектов КИИ РФ. 4. Требования по обеспечению безопасности значимых объектов КИИ РФ. 5. Перечень объектов КИИ РФ подлежащих категорированию
Уметь:	- выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних	Задания: *1.* Составить майнд-карту угроз безопасности информации (УБИ) значимого объекта КИИ.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	и внутренних нарушителей, анализа уязвимостей значимого объекта КИИ; - способы реализации угроз безопасности и возможные последствия от их реализации; - определять требования по устранению возможных уязвимостей, приводящих к возникновению угроз безопасности информации;	*2.* Составить майнд-карты оценки возможностей внешних и внутренних нарушителей для значимого объекта КИИ.
Владеть:	- навыками работы с нормативными и правовыми актами, методическими документами и национальными стандартами в области обеспечения безопасности значимых объектов КИИ; - навыками работы с информационными базами данных, содержащими информацию по угрозам безопасности информации и уязвимостями ПО значимых объектов КИИ; - навыками выявления и анализа угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа уязвимостей значимого объекта КИИ;	Задания: 1. Составить перечень показателей критериев значимости объектов КИИ РФ. 2. Выбрать из информационной системы «Банк данных УБИ ФСТЭК России» УБИ по результатам оценки возможностей внешних и внутренних нарушителей значимого объекта КИИ. 3. Выбрать из информационной системы «Банк данных УБИ ФСТЭК России» УБИ по результатам анализа уязвимостей значимого объекта КИИ.
ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности		
Знать:	- понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ; - общие требования по обеспечения безопасности значимых объектов КИИ; - подходы категорирования значимости объектов КИИ;	Теоретические вопросы: 1. Требования к созданию систем безопасности значимых объектов КИИ РФ. 2. Обеспечение функционирования систем безопасности значимых объектов КИИ РФ. 3. Порядок определения масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ. 4. Правила и порядок категорирования объектов КИИ. 5. Реестр значимых объектов КИИ. 6. Правила формирования

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		комиссии по категорирования объектов КИИ.
Уметь:	- определять категории значимых объектов КИИ и оформлять полученные результаты; - определять структуру системы безопасности значимого объекта КИИ; - определят требования по обеспечения безопасности значимых объектов КИИ; - определять требования к параметрам настройки программных и программно-аппаратных средств защиты информации (СЗИ);	Задания: 1. Для выбранного предприятия/организации определить перечень объектов КИИ с обоснованием. 2. Для выбранного предприятия/организации сформировать сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения одной из таких категорий. 3. Для выбранного объекта КИИ сформировать требования к параметрам настройки программных и программно-аппаратных СЗИ.
Владеть:	- навыками установки и настройки СЗИ, обрабатываемой объектами КИИ; - навыками подбора средств СЗИ с учетом совместимости с применяемым на значимом объекте КИИ ПО и категорированием значимого объекта КИИ;	Задания: 1. Провести тестирование работоспособности СЗИ «Страж NT» с учетом сформированных требований к объекту КИИ. 2. Для выбранного объекта КИИ сформировать перечень необходимых программных и программно-аппаратных СЗИ с учетом их стоимости.
ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций		
Знать:	-требования к организационным и техническим мерам для обеспечения безопасности значимых объектов КИИ; - основные принципы организации государственного контроля состояния защищенности значимых объектов КИИ; - процедуру категорирования объектов КИИ; - требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования;	Теоретические вопросы: 1. Понятие ГосСОПКА 2. Понятие СОБИ КСИИ 3. Основные подсистемы СОБИ КСИИ 4. Этапы разработки СОБИ КИИ 5. Требования к организационным и техническим мерам для обеспечения безопасности объектов КИИ 6. Ответственность за нарушение законодательства в области обеспечения безопасности КИИ РФ.
Уметь:	- осуществлять выбор СЗИ с учетом совместимости с	Задания: 1. Для выбранного объекта КИИ

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	применяемым на значимом объекте КИИ ПО и категорированием значимого объекта КИИ; - определять СЗИ для реализации технических мер обеспечения безопасности информации в рамках системы безопасности значимого объекта КИИ;	сформировать перечень необходимых технических СЗИ с учетом их стоимости и категории значимости объекта КИИ. 2. Проанализировать этапы жизненного цикла системы безопасности значимого объекта КИИ и выявить слабые места.
Владеть:	- навыками участия в разработке организационных и технических мероприятий по защите объектов КИИ; - навыками разработки организационно-распорядительными документов по безопасности значимых объектов КИИ; - навыками проведения работ по контролю состояния безопасности объектов КИИ;	Задания: 1. Составить майнд-карту мероприятий по реагированию на компьютерные инциденты для выбранного значимого объекта КИИ в ходе его эксплуатации. 2. Разработать необходимые документы для обеспечения функционирования выбранного значимого объекта КИИ в рамках созданной системы безопасности.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Показатели и критерии оценивания зачета:

– на оценку **«зачтено»** – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации;

– на оценку **«не зачтено»** – обучающийся не может показать знания на уровне воспроизведения и объяснения информации.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Душкин, А. В. Методологические основы построения защищенных автоматизированных систем: Монография / Душкин А.В. - Воронеж:Научная книга, 2016. - 76 с. ISBN 978-5-4446-0902-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/923295 (дата обращения: 26.02.2020)

2. Зашита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1018901 (дата обращения: 26.02.2020)

б) Дополнительная литература:

1. Баранкова И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности [Электронный ресурс] : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true . - Макрообъект*. - ISBN 978-5-9967-1031-7.

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/441287 (дата обращения: 24.02.2020).

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронного каталога https://magtu.informsystema.ru .
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта.

Примечание: при открытии макрообъектов учитывать особенности настройки антивирусной защиты.

в) Методические указания:

1. Методические указания по выполнению лабораторных работ. (Приложение 1.)
2. Методические указания по выполнению внеаудиторных самостоятельных работ. (Приложение 2.)

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия
MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
MS Office Visio Prof 2016(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2019(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
LibreOffice	свободно распространяемое ПО	бессрочно
MS Windows 10 Professional (для классов)	Д-1227-18 от 08.10.2018	11.10.2021
СЗИ Страж NT в.3	К-271-12 от 16.10.2012	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно

Linux Calculate	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	http://window.edu.ru /
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/
Российская Государственная библиотека. Каталоги	ers/catalogues/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	web2/Default.asp
Международная наукометрическая реферативная и полнотекстовая база данных научных изданий «Web of science»	http://webofscience.com
Международная реферативная и полнотекстовая справочная база данных научных изданий «Scopus»	http://scopus.com
Международная база полнотекстовых журналов Springer Journals	http://link.springer.com/
Международная база справочных изданий по всем отраслям знаний SpringerReference	ferences

Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации ФСТЭК России	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:
Материально-техническое обеспечение дисциплины включает:

Лекционные аудитории:

- Мультимедийные средства хранения, передачи и представления информации.

Компьютерные классы:

- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Лаборатория программно-аппаратных средств обеспечения информационной безопасности:

- Система защиты информации от несанкционированного доступа СТРАЖ NT(версия 3.0)

Лаборатория технической защиты информации:

1. АКС-1301 Анализатор спектра
2. Комплекс радиомониторинга "Касандра К6" с диапазоном рабочих частот 0,009-6000Мгц
3. Комплекс радиомониторинга "Касандра К21" с диапазоном рабочих частот 0,009-21000Мгц
4. Генератор шума стационарный "ГШ-1000-М"
5. Система виброакустической и акустической защиты "Соната-АВ"
6. Устройство защиты телефонных переговоров от прослушивания и записи "Прокруст-200"
7. Портативный поисковый комплекс амплитудной пеленгации «Касандра С6»
8. Система оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН) Сигурд

Помещения для самостоятельной работы обучающихся:

- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета

ПРИЛОЖЕНИЕ 1

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Рекомендации направлены на оказание методической помощи студентам при выполнении лабораторных занятий.

Лабораторное занятие – это занятие, проводимое под руководством преподавателя в учебной аудитории (компьютерном классе университета или учебной специализированной лаборатории университета), направленное на углубление научно-теоретических знаний и получение лабораторных навыков решения типовых и прикладных задач.

Целью лабораторных занятий является формирование и отработка лабораторных умений и навыков, необходимых в последующей деятельности обучающихся.

Основными задачами лабораторных занятий являются:

- углубление уровня освоения общекультурных и профессиональных компетенций;
- обобщение, систематизация, углубление, закрепление полученных лабораторных знаний по конкретным темам дисциплин различных циклов;
- приобретение студентами умений и навыков использования современных теоретических знаний в решении конкретных прикладных задач;
- развитие профессионального мышления, профессиональной и познавательной мотивации.

Перечень тем лабораторных работ определяется рабочей программой дисциплины. План лабораторных занятий отвечает общей направленности лекционного курса и соотнесен с ним в последовательности тем.

Структура лабораторного занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущей лабораторной работы, ставится ее цели и задачи, проводиться инструктаж по технике безопасности выполнения работы, проверяется исходный уровень готовности студентов к лабораторной работе (выполнение тестов, контрольные вопросы и т.п.), выдается порядок и условия выполнения лабораторной работы.

На лабораторном занятии преподаватель может использовать разнообразные образовательные технологии (методы IT, работа в команде, case-study, проблемное обучение, учебные дискуссии и т.п.) по своему выбору для достижения качественного уровня обучения.

Правила по технике безопасности для обучающихся при проведении лабораторных работ

Общие правила:

1. Лабораторные работы проводятся под наблюдением преподавателя. К выполнению лабораторных работ студенты допускаются только после прослушивания инструктажа по технике безопасности, правилам поведения, противопожарным мерам в компьютерном классе и специализированных лабораториях.

2. Обучаемый должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах и специализированных лабораториях университета.

Порядок выполнения лабораторных работ

При подготовке к выполнению лабораторных работ студент должен повторить теоретический материал, необходимый для выполнения заданий по текущей теме.

Лабораторная работа выполняется каждым студентом самостоятельно, согласно индивидуальному заданию.

Студенты, пропустившие занятия, выполняют лабораторные работы во внеурочное

время.

После выполнения каждой лабораторной работы студент демонстрирует результат выполнения преподавателю в виде отчета по лабораторной работе и отвечает на вопросы. Преподаватель оценивает работу в соответствии с заданными критериями оценки лабораторных работ.

Правила оформления результатов и оценивания лабораторной работы

Результаты выполненной лабораторной работы оформляются в соответствии с требованиями к выполнению конкретной работы.

Практическая работа считается выполненной, если студент набрал балл, который составляет половину максимального количества баллов.

Для оценивания работы прилагаются следующие критерии.

Оценка «отлично» – работа выполнена в полном объеме и без замечаний.

Оценка «хорошо» – работа выполнена правильно с учетом 2-3 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

Оценка «неудовлетворительно» – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя, или работа не выполнена.

ПРИЛОЖЕНИЕ 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы студентов и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
   a) предоставляемыми преподавателем на лекционных занятиях;
   b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
   c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.
2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.
3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.
4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы со студентами группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: индивидуальные задания, аудиторные контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

- выполняет индивидуальные задания в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.