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)

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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	2
Семестр	3

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:
зав. кафедрой ИиИБ, д-р техн. наук _____ И.И. Баранкова

Рецензент:
Начальник отдела информационной безопасности "КУБ" (АО) .
_____ 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 дисциплины «Основы информационной безопасности» является понимание социальной значимости своей будущей профессии в соответствии с доктриной информационной безопасности Российской Федерации. Формирование у студентов навыков их практического применения в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем». Дисциплина «Основы информационной безопасности» рассматривает основные принципы и основные направления обеспечения информационной безопасности Российской Федерации.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Основы информационной безопасности входит в базовую часть учебного плана образовательной программы.

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

Физика

Информатика

Введение в специальность

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

Организационное и правовое обеспечение информационной безопасности

Информационная безопасность распределенных информационных систем

Методы и стандарты оценки защищенности компьютерных систем

Методы мониторинга информационной безопасности АС

Информационная безопасность систем организационного управления

Методы проектирования систем защиты распределенных информационных систем

Обеспечение информационной безопасности критической информационной инфраструктурой

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

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

Структурный элемент компетенции	Планируемые результаты обучения
ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	
Знать	Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации. Системы регулирования возникающих общественных отношений в информационной сферы. Составляющие информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации. Влияние информационной сферы на состояние политической, экономической, оборонной и других составляющих безопасности РФ.

Уметь	Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем. Использовать инфраструктуру единого информационного пространства РФ в личных целях. Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем.
Владеть	Методами разработки проектов нормативных документов, регламентирующих работу по защите информации. Способами использования информационной инфраструктуры в интересах общественного развития. Методами разработки проектов нормативных документов, регламентирующих работу по защите информации.
ПК-3 способностью проводить анализ защищенности автоматизированных систем	
Знать	Основы методологии научных исследований. Технические средства контроля эффективности мер защиты информации. Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем Классификацию современных компьютерных систем. Современные способы использования компьютерных технологий для проведения исследований. Технические средства контроля эффективности мер защиты информации. Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.
Уметь	Пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет. Анализировать основные узлы и устройства современных автоматизированных систем. Пользоваться сетевыми информационными ресурсами для подбора необходимых современных компьютерных систем и правил работы в этих системах. Эффективно использовать современные компьютерные технологии для изучения предмета исследования.
Владеть	Представлением о возможности использования информационных технологий для решения профессиональных задач. Представлением использования информационных технологий для проведения исследовательской работы в профессиональной деятельности. Навыками пользования библиотеками прикладных программ для проведения исследовательской работы в профессиональной деятельности. Представлением о способах и методах анализа защищенности информационной инфраструктуры автоматизированной системы.

ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	
Знать	Основные информационные технологии, используемые в автоматизированных системах. Сущность и понятие информационной безопасности и характеристику ее составляющих. Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах.
Уметь	Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам. Принимать участие в исследованиях и анализе современной научно-технической информации по информационной безопасности. Анализировать современную научно-техническую информацию по информационной безопасности. Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе
Владеть	Основными методами научного познания в области защиты информации. Навыками участия в проведении исследовательских работ по информационной безопасности. Профессиональной терминологией в области информационной безопасности. Разрабатывать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах
ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	
Знать	Основные меры по защите информации в автоматизированных системах. Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. Принципы организации работы малых коллективов исполнителей.
Уметь	Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации.
Владеть	Профессиональной терминологией в области информационной безопасности. Навыками участия в проведении исследовательских работ по информационной безопасности. Методами синтеза структурных и функциональных схем защищенных автоматизированных систем.

4. Структура, объём и содержание дисциплины (модуля)

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

– контактная работа – 73,9 акад. часов:

– аудиторная – 72 акад. часов;

– внеаудиторная – 1,9 акад. часов

– самостоятельная работа – 70,1 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. Место и роль информационной безопасности в системе национальной безопасности РФ								
1.1 Сущность и понятие информации. Понятие национальной безопасности. Основы государственной информационной политики	3	4	4		10	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательног о портала и ЭБС. Подготовка к контрольному тестированию	Контрольное тестирование	ОПК-6
1.2 Угрозы национальной безопасности страны во всех сферах деятельности государства все осуществляемые через информационную среду		4	4		10	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательног о портала и ЭБС. Подготовка к контрольному тестированию	Контрольное тестирование	ОПК-6
Итого по разделу		8	8		20			
2. Классификация защищаемой информации и угроз информационной безопасности								

2.1 Классификация защищаемой информации по видам тайны и степеням конфиденциальности	3	4	4		10	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к индивидуальному домашнему заданию (ИДЗ)	ИДЗ	ОПК-6, ПК-3
2.2 Источники и классификация угроз информационной безопасности для объектов информатизации		4	4		7,9	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к ИДЗ.	ИДЗ	ОПК-6, ПК-3
Итого по разделу		8	8		17,9			
3. Способы обеспечения информационной безопасности автоматизированных систем								
3.1 Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации	3	6	6		8	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к аудиторной контрольной работе (АКР)	АКР	ПК-6
3.2 Классификация средств и способов обеспечения информационной безопасности, принципы построения систем защиты информации		6	6		4	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР	АКР	ПК-3, ПК-6
Итого по разделу		12	12		12			
4. Методы формирования требований по защите информации								

4.1 Анализ существующих методов и средств, применяемых для защиты информации	3	4	4		11,2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к ИДЗ.	ИДЗ	ПК-6
4.2 Разработка предложений по совершенствованию существующих методов и средств, применяемых для контроля и защиты информации и повышению их эффективности		4	4		3	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к ИДЗ.	ИДЗ	ПК-18
4.3 Подготовка к зачету					6	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к зачету.	Зачет	ОПК-6, ПК-3, ПК-6, ПК-18
Итого по разделу		8	8		20,2			
Итого за семестр		36	36		70,1		зачёт	
Итого по дисциплине		36	36		70,1		зачет	ОПК-6,ПК-3,ПК-6,ПК-18

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:

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.

c) Лекция «обратной связи» – лекция–провокация (изложение материала с заранее запланированными ошибками), лекция-беседа, лекция-дискуссия, лекция-прессконференция.

d) Семинар-дискуссия – коллективное обсуждение какого-либо спорного вопроса, проблемы, выявление мнений в группе (межгрупповой диалог, дискуссия как спор-диалог).

e) Контекстное обучение – для мотивации обучающихся к усвоению знаний путем выявления связей между конкретным знанием и его применение. Овладев в рамках изучения дисциплины навыками обеспечения безопасности информации с помощью типовых программных средств, обучающийся приобретет способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности;

f) Междисциплинарное обучение – для использования знаний из различных областей, их группировки и концентрации в контексте решаемой задачи. Для реализации данного метола обучения обучающимся выдаются задания по решения задач из другой предметной области.

4) Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности обучающихся. Формы учебных занятий с использованием технологий проблемного обучения:

a) Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала.

b) Лекция «вдвоем» (бинарная лекция) – изложение материала в форме диалогического общения двух преподавателей (например, реконструкция диалога представителей различных научных школ, «ученого» и «практика» и т.п.).

c) Практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от обучающегося применения как научно-теоретических знаний, так и практических навыков.

d) Практическое занятие на основе кейс-метода – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации. разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.

5) Игровые технологии – организация образовательного процесса, основанная на реконструкции моделей поведения Формы учебных занятий с использованием предложенных сценарных условий. Формы учебных занятий с использованием игровых технологий:

a) Учебная игра – форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем отношений, которые характерны для этой деятельности как целого.

b) Деловая игра – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», реконструкцией функционального взаимодействия в коллективе и т.п.

c) Ролевая игра – имитация или реконструкция моделей ролевого поведения в предложенных сценарных условиях.

6) Технологии проектного обучения – организация образовательного процесса в соответствии с алгоритмом поэтапного решения проблемной задачи или выполнения учебного задания.

Проект предполагает совместную учебно-познавательную деятельность группы обучающихся, направленную на выработку концепции, установление целей и задач, формулировку ожидаемых результатов, определение принципов и методик решения поставленных задач, планирование хода работы, поиск доступных и оптимальных ресурсов, поэтапную реализацию плана работы, презентацию результатов работы, их осмысление и рефлексию. Основные типы проектов:

a) Исследовательский проект – структура приближена к формату научного исследования (доказательство актуальности темы, определение научной проблемы, предмета и объекта исследования, целей и задач, методов, источников, выдвижение гипотезы, обобщение результатов, выводы, обозначение новых проблем).

b) Творческий проект, как правило, не имеет детально проработанной структуры; учебно-познавательная деятельность обучающихся осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия и т.п.).

c) Информационный проект – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).

7) Информационно-коммуникационные образовательные технологии – организация образовательного процесса, основанная на применении специализированных программных сред и технических средств работы с информацией. Формы учебных занятий с использованием информационно-коммуникационных технологий:

a) Лекция-визуализация – изложение содержания сопровождается презентацией (демонстрацией учебных материалов, представленных в различных знаковых системах, в т.ч. иллюстративных, графических, аудио- и видеоматериалов).

Практическое занятие в форме презентации – представление результатов проектной или исследовательской деятельности с использованием специализированных программных сред.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для студента с использованием *методов IT* .

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде чтения литературы по соответствующему разделу с проработкой материала и выполнения домашних заданий с консультациями преподавателя, а также с применением *кейс-технологий*.

Контрольные вопросы и задания для проведения текущего контроля

Темы для ИДЗ:

1. Стратегия развития информационного общества в России
2. Правовая охрана программ и данных. Защита информации.
3. Методы защиты информации
4. Системы защиты информации
5. Защита баз данных
6. Угрозы национальной безопасности страны в экономической сфере, осуществляемые через информационную среду.
7. Угрозы национальной безопасности страны в политической сфере, осуществляемые через информационную среду.

8. Угрозы национальной безопасности страны в военной сфере, осуществляемые через информационную среду.
9. Угрозы национальной безопасности страны в духовной сфере, осуществляемые через информационную среду.

Задания и вопросы по разделам

Раздел 1-4

Вопросы:

1. Понятие информационной безопасности государства.
2. Источники угроз информационной безопасности для объекта информатизации.
3. Классификация угроз информационной безопасности для объекта информатизации.
4. Требования защиты информации.
5. Угрозы национальной безопасности страны в экономической сфере, осуществляемые через информационную среду.
6. Угрозы национальной безопасности страны в политической сфере, осуществляемые через информационную среду.
7. Угрозы национальной безопасности страны в военной сфере, осуществляемые через информационную среду.
8. Угрозы национальной безопасности страны в духовной сфере, осуществляемые через информационную среду.
9. Классификация защищаемой информации по видам тайны.

Классификация защищаемой информации по степеням конфиденциальности.

7 Оценочные средства для проведения промежуточной аттестации

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

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности		
Знать	Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации. Системы регулирования возникающих общественных отношений в информационной сферы. Составляющие информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации. Влияние информационной сферы на	Вопросы для зачета: 1. Понятие информационной безопасности государства. 2. Источники угроз информационной безопасности для объекта информатизации. 3. Классификация угроз информационной безопасности для объекта информатизации. 4. Требования защиты информации. 5. Стратегия развития информационного общества в России.

	состояние политической, экономической, оборонной и других составляющих безопасности РФ.	
Уметь	Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем. Использовать инфраструктуру единого информационного пространства РФ в личных целях. Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем.	1. Найти перечень нормативно-правовых документов в области защиты информации автоматизированных систем. 2. Провести анализ нормативно-правовых документов в области защиты информации автоматизированных систем.
Владеть	Методами разработки проектов нормативных документов, регламентирующих работу по защите информации. Способами использования информационной инфраструктуры в интересах общественного развития. Методами разработки проектов нормативных документов, регламентирующих работу по защите информации	1. На основе проведенного анализа нормативно-правовых документов в области защиты информации автоматизированных систем найти слабые места в системе управления безопасностью информации в автоматизированных системах на современном уровне развития общества.
ПК-3 способностью проводить анализ защищенности автоматизированных систем		
Знать	Основы методологии научных исследований. Технические средства контроля эффективности мер защиты информации. Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. Классификацию современных компьютерных систем. Современные способы использования компьютерных технологий для проведения исследований. Технические средства контроля эффективности мер защиты информации. Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.	1. Понятие информационной безопасности государства. 2. Источники угроз информационной безопасности для объекта информатизации. 3. Классификация угроз информационной безопасности для объекта информатизации. 4. Требования защиты информации.

Уметь	Пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет. Анализировать основные узлы и устройства современных автоматизированных систем. Пользоваться сетевыми информационными ресурсами для подбора необходимых современных компьютерных систем и правил работы в этих системах. Эффективно использовать современные компьютерные технологии для изучения предмета исследования.	1. Определить угрозы национальной безопасности страны в экономической сфере, осуществляемые через информационную среду. 2. Определить угрозы национальной безопасности страны в политической сфере, осуществляемые через информационную среду.
Владеть	Представлением о возможности использования информационных технологий для решения профессиональных задач. Представлением использования информационных технологий для проведения исследовательской работы в профессиональной деятельности. Навыками пользования библиотеками прикладных программ для проведения исследовательской работы в профессиональной деятельности. Представлением о способах и методах анализа защищенности информационной инфраструктуры автоматизированной системы.	1. Составить перечень программного обеспечения, позволяющего автоматизировать работу в области ИБ. 2. Составить перечень сертифицированных средств ЗИ от НСД. 3. Составить перечень средств СКЗИ.
ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности		
Знать	Основные информационные технологии, используемые в автоматизированных системах. Сущность и понятие информационной безопасности и характеристику ее составляющих. Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах.	Вопросы для зачета 8. Угрозы национальной безопасности страны в духовной сфере, осуществляемые через информационную среду. 9. Классификация защищаемой информации по видам тайны. 10. Классификация защищаемой информации по степеням конфиденциальности. 11. Стратегия развития информационного общества в России.
Уметь	Пользоваться современной научно-технической информацией по рассматриваемым в рамках	1. Определить угрозы национальной безопасности страны в духовной сфере,

	дисциплины проблемам и задачам. Принимать участие в исследованиях и анализе современной научно-технической информации по информационной безопасности. Анализировать современную научно-техническую информацию по информационной безопасности. Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе	осуществляемые через информационную среду. 2. Определить угрозы национальной безопасности страны в военной сфере, осуществляемые через информационную среду.
Владеть	Основными методами научного познания в области защиты информации. Навыками участия в проведении исследовательских работ по информационной безопасности. Профессиональной терминологией в области информационной безопасности. Разрабатывать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах	1. На основе проведенного анализа нормативно-правовых документов в области защиты информации автоматизированных систем разработать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах на современном уровне развития общества.
ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности		
Знать	Основные меры по защите информации в автоматизированных системах. Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. Принципы организации работы малых коллективов исполнителей.	Вопросы для зачета 4. Требования защиты информации. 5. Угрозы национальной безопасности страны в экономической сфере, осуществляемые через информационную среду. 6. Угрозы национальной безопасности страны в политической сфере, осуществляемые через информационную среду. 7. Угрозы национальной безопасности страны в военной сфере, осуществляемые через информационную среду.
Уметь	Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. Классифицировать и оценивать угрозы информационной безопасности для объекта	1. Классифицировать защищаемую информацию по видам тайны. 2. Классифицировать защищаемую информацию по степеням конфиденциальности.

	информатизации. Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации.	3. Составить перечень средств ЗИ для обеспечения защиты от утечки по акустическому каналу.
Владеть	Профессиональной терминологией в области информационной безопасности. Навыками участия в проведении исследовательских работ по информационной безопасности. Методами синтеза структурных и функциональных схем защищенных автоматизированных систем.	1. Составить глоссарий по терминологии в области информационной безопасности. 2. Исследовать угрозы национальной безопасности страны в военной сфере. 3. Исследовать стратегия развития информационного общества в России.

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

Показатели и критерии оценивания зачета:

«зачтено» – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач.

«не зачтено» – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Защита 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: 26.02.2019)

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772 (дата обращения: 24.02.2020)

б) Дополнительная литература:

1. Ковалев, Д. В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/997105 (дата обращения: 26.02.2019)

2. Внуков, А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/414083 (дата обращения: 24.02.2020) .

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

*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 лицензии
MS Windows 7 Professional(д	Д-1227-18 от 08.10.2018	11.10.2021
7Zip	свободно	бессрочно
MS Office 2007	№ 135 от 17.09.2007	бессрочно
LibreOffice	свободно	бессрочно
MS Windows 10 Professional	Д-1227-18 от 08.10.2018	11.10.2021
Браузер Mozilla	свободно распространяем	бессрочно
Браузер	свободно	бессрочно
MS Windows XP Professional(д	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2003	№ 135 от 17.09.2007	бессрочно
FAR Manager	свободно	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East	https://dlib.eastview.com/
Федеральное государственное бюджетное учреждение «Федеральный институт	URL: http://www1.fips.ru/
Информационная система - Единое окно доступа к	URL: http://window.edu.ru/
Информационная система - Банк данных угроз	https://bdu.fstec.ru/
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii

9 Материально-техническое обеспечение дисциплины (модуля)

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.

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

Лабораторные работы проводятся в компьютерных классах или специализированных лабораториях с целью получения практических умений для формирования и развития профессиональных навыков и соответствующих компетенций по дисциплине. При подготовке к выполнению заданий лабораторной работы используйте лекции, справочный материал программного обеспечения, рекомендованную литературу и цифровые образовательные ресурсы соответствующих методических материалов, размещенных в сети Интернет или локальной сети университета. Перед выполнением лабораторной работы необходимо получить свой вариант индивидуального задания у преподавателя. Прежде чем приступить к выполнению лабораторной работы, внимательно прочтите рекомендации к ее выполнению. Ознакомьтесь с перечнем рекомендуемой литературы, повторите теоретический материал, относящийся к теме работы. Ответьте на контрольные вопросы, выполните задания для самостоятельного выполнения. По результатам лабораторной работы предоставляется отчет. Отчет к лабораторным работам должен содержать:

- название лабораторной работы;
- цель и задачи работы;
- краткие теоретические сведения;
- задания по лабораторной работе;
- ход работы - описание последовательности действий при выполнении работы;
- выводы или результаты.

Результаты выполнения лабораторной работы могут быть представлены в электронном варианте или распечатанные. Результаты выполнения заданий лабораторной работы можно сохранить на образовательном портале в личном кабинете и использовать при подготовке к экзамену.

Защита работы и результаты оценивания.

Защита проводится в два этапа:

1. Демонстрируются результаты выполнения задания. В случае выполнения лабораторной работы, предусматривающей разработку программы, при помощи тестового примера доказывается, что результат, получаемый при выполнении программы, является правильным.

2. Для защиты работы студенту необходимо ответить на дополнительные вопросы преподавателя. Каждая лабораторная работа оценивается определенным количеством баллов исходя из 5-бальной системы оценок.

Лабораторная работа считается выполненной и защищенной, если выполнены все задания и даны правильные ответы преподавателю на заданные вопросы. Лабораторная работа считается выполненной и незащищенной, если выполнены все задания, но полученные результаты являются неверными или не даны правильные ответы преподавателю на заданные вопросы и ответы были не полные. Обучающемуся, не выполнившим в полном объеме все задания лабораторной работы, или пропустившим по уважительной причине лабораторную работу, необходимо выполнить ее самостоятельно в компьютерном классе или специализированной лаборатории, результаты выполненной работы сохранить на съемном накопителе или на образовательном портале. Результаты предоставить в сроки, указанные преподавателем вместе с отчетом, демонстрацией

полученных результатов в компьютерном классе (или специализированной лаборатории) или предоставлением материалов на электронном образовательном ресурсе.

Правила по технике безопасности для обучающихся при проведении лабораторных работ:

1. Лабораторные работы проводятся под наблюдением преподавателя. К выполнению лабораторных работ студенты допускаются только после прослушивания инструктажа по технике безопасности и противопожарным мерам.

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

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.