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)

АНАЛИЗ РИСКОВ 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	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:
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)

Целями освоения дисциплины (модуля) «Анализ рисков информационной безопасности» являются: выявление источников и способов реализации угроз информационной безопасности, фиксация параметров безопасности и анализа безопасности АС, изучение основных понятий и принципов анализа и оценки рисков информационной безопасности.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Анализ рисков информационной безопасности входит в вариативную часть учебного плана образовательной программы.

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

Моделирование угроз информационной безопасности

Организационное и правовое обеспечение информационной безопасности

Разработка и эксплуатация защищенных автоматизированных систем

Безопасность операционных систем

Техническая защита информации

Безопасность Интернета вещей

Безопасность сетей ЭВМ

Безопасность систем баз данных

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

Научно-исследовательская работа

Производственная-преддипломная практика

Подготовка к сдаче и сдача государственного экзамена

Подготовка к защите и защита выпускной квалификационной работы

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

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

Структурный элемент компетенции	Планируемые результаты обучения
ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	
Знать	- методологию анализа рисков информационной безопасности; - методики определения информационно-технологических ресурсов, подлежащих защите; - способы применения анализа рисков информационной безопасности при работе над междисциплинарными проектами; - перечень информационно-технологических ресурсов, подлежащих защите способы применения анализа рисков в информационной безопасности при работе над инновационными проектами.

Уметь	- применять терминологию анализа рисков информационной безопасности при работе над междисциплинарными и инновационными проектами; - выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите.
Владеть	- терминологией, используемой при анализе особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно- технологических ресурсов, подлежащих защите; - навыками анализа особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите.
ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	
Знать	- Порядок разработки политик безопасности; - методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах;
Уметь	- разрабатывать политики безопасности; - использовать методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах; - анализировать и оценивать угрозы информационной безопасности объекта, выполнять анализ рисков информационной безопасности в распределенных информационных системах.
Владеть	- методиками проведения анализа рисков информационной безопасности распределенных информационных систем; - методами оценки информационных рисков; - навыками разработки политики информационной безопасности автоматизированных систем.

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 акад. часов, в том числе:

– контактная работа – 73,9 акад. часов:

– аудиторная – 72 акад. часов;

– внеаудиторная – 1,9 акад. часов

– самостоятельная работа – 34,1 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. Методики и технологии управления рисками информационной безопасности и их оценки								
1.1 Оценочные стандарты в информационной безопасности. Роль стандартов информационной безопасности. «Критерии определения безопасности компьютерных систем» как оценочный стандарт. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.	9	6		10/2И	10	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме.	– устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий.	ПК-5, ПСК-7.2
1.2 Методика оценки рисков информационной безопасности предприятия. Управление рисками. Основные понятия. Метод оценки рисков на основе модели угроз и уязвимостей		6		10/4И	10	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ПК-5, ПСК-7.2

1.3 Методика оценки рисков информационной организации. Метод оценки рисков на основе модели информационных потоков. Расчет рисков по угрозе конфиденциальность		6		6/4И	10	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ПК-5, ПСК-7.2
1.4 Методики и технологии управления рисками. Качественные методики управления рисками. Количественные методики управления рисками. Метод CRAMM		6		3/4И	1	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ПК-5, ПСК-7.2
1.5 Тема 5. Разработка корпоративной методики анализа рисков. Постановка задачи. Методы оценивания информационных рисков. Табличные методы оценки рисков. Оценка рисков по двум факторам. Разделение рисков на приемлемые и неприемлемые. Оценка рисков по трем факторам. Методика анализа рисков Microsoft		6		3/4И	2	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ПК-5, ПСК-7.2
1.6 Современные методы и средства анализа и управление рисками информационных систем. Методика FRAP. Методика OCTAVE. Методика RiskWatch		6		4/4И	1,1	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ПК-5, ПСК-7.2
Итого по разделу		36		36/22И	34,1			
Итого за семестр		36		36/22И	34,1		зачёт	
Итого по дисциплине		36		36/22И	34,1		зачет	ПК-5,ПСК-7.2

5 Образовательные технологии

Согласно п. 34 Порядка организации и осуществления деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом МОиН РФ от 05.04.2017 г. № 301) при проведении учебных занятий организация обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

1. Традиционные образовательные технологии ориентируются на организацию образовательного процесса, предполагающую прямую трансляцию знаний от преподавателя к студенту (преимущественно на основе объяснительно-иллюстративных методов обучения). Учебная деятельность студента носит в таких условиях, как правило, репродуктивный характер.

Формы учебных занятий с использованием традиционных технологий:

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

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

Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

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

2. Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности студентов.

Формы учебных занятий с использованием технологий проблемного обучения:

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

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.).

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

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.

3. Игровые технологии – организация образовательного процесса, основанная на реконструкции моделей поведения в рамках предложенных сценарных условий.

Формы учебных занятий с использованием игровых технологий:

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

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.

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

4. 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 студентов, 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:

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).

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

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).

5. 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 специализированных интерактивных технологий:

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

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

6. 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:

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

Тема 1. Основные понятия информационной безопасности

– Понятие информационной безопасности.

– Основные составляющие информационной безопасности.

– Управление информационной безопасностью.

– Важность и сложность проблемы информационной безопасности.

Тема 2. Оценочные стандарты в информационной безопасности.

– Роль стандартов информационной безопасности.

– «Критерии определения безопасности компьютерных систем» как оценочный стандарт.

– Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.

Тема 3. Стандарты управления информационной безопасностью.

–Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799.

–Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования".

–Сертификация СУИБ на соответствие ISO 27001.

Тема 4. Создание СУИБ на предприятии.

–Этапы разработки и внедрения системы управления ИБ.

–Содержание этапов разработки и внедрения системы управления ИБ.

Тема 5. Методика оценки рисков информационной безопасности предприятия.

–Управление рисками. Основные понятия.

–Метод оценки рисков на основе модели угроз и уязвимостей.

Тема 6. Методика оценки рисков информационной организации.

– Метод оценки рисков на основе модели информационных потоков.

– Расчет рисков по угрозе конфиденциальность.

Тема 7. Методики и технологии управления рисками.

– Качественные методики управления рисками.

– Количественные методики управления рисками. Метод CRAMM.

Тема 8. Разработка корпоративной методики анализа рисков.

– Методы оценивания информационных рисков.

– Табличные методы оценки рисков.

– Оценка рисков по двум факторам.

– Разделение рисков на приемлемые и неприемлемые.

– Оценка рисков по трем факторам.

– Методика анализа рисков Microsoft.

Тема 9 Современные методы и средства анализа и управление рисками информационных систем.

– Методика FRAP.

– Методика OCTAVE.

– Методика RiskWatch.

Перечень контрольных вопросов по терминологии:

Угроза (Threat)

Уязвимость (Vulnerability)

- *Анализ рисков.*

Базовый уровень безопасности .

Базовый (Baseline) анализ рисков .
Полный (Full) анализ рисков.
Риск нарушения ИБ (Security Risk).
Оценка рисков (Risk Assessment).
Управление рисками (Risk Management).
Система управления ИБ (Information Security Management System).
Класс рисков.
Терминология COBIT

- *Риски*

Типы рисков.
Приемлемый уровень риска
Стандарт управления рисками.
Матрица ИТ рисков.

- *Руководство рисками*

Владелец процессов оценки рисков.
План работ по снижению рисков.
Политики и процедуры.
Обновление величин рисков.
Глобальный и системный уровни оценки ИТ- рисков.
Резюме для руководителя.
Стратегия управления ИТ

- *Идентификация*

Определение компонентов риска.
Области рисков.
Обновление матрицы рисков.
Меры оценки
Количественная оценка.
Качественная оценка.

- *Способы управления*

Независимое мнение.
Возврат инвестиций.
Баланс способов управления
Управление конфликтами.

- *Мониторинг*

Мониторинг используемых способов управления.
Процедура реагирования на инциденты.
Согласование плана работ по снижению рисков.

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
ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы		
Знать	– методологию анализа рисков информационной безопасности – методики определения информационно-технологических ресурсов, подлежащих	1. Назвать угрозы информационной безопасности в информационных системах. 2. Перечислить оценочные стандарты в информационной безопасности.

	защите – способы применения анализа рисков информационной безопасности при работе над междисциплинарными проектами – перечень информационно-технологических ресурсов, подлежащих защите способы применения анализа рисков в информационной безопасности при работе над инновационными проектами	3. Описать «Оранжевую книгу» как оценочный стандарт. 4. Международный стандарт ISO/IEC 15408. Описать критерии оценки безопасности информационных систем. 5. Перечислить стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения. 6. Международный стандарт ISO/IEC 27001:2005 Назвать требования к системам управления информационной безопасностью. 7. Сертификация СУИБ на соответствие ISO 27001.
Уметь	– применять терминологию анализа рисков информационной безопасности при работе над междисциплинарными и инновационными проектами – выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите	Провести расчеты оценки рисков информационной безопасности компании по методу оценки рисков на основе частной модели угроз.
Владеть	– терминологией, используемой при анализе особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите – навыками анализа особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите	***Задание:*** Для заданного предприятия определить: информационные активы компании; ценность активов; какие угрозы могут повлиять на информационные активы; с помощью каких механизмов можно защитить ключевые активы; уровень риска и предполагаемых потерь. провести оценку рисков ИБ (по выбранной методике): инвентаризацию информационных активов и их стоимости; определение методологии, необходимой для проведения оценки рисков и ее применение в конкретной компании; анализ возможных угроз и уязвимостей;

		определение мер, направленных на осуществление ИБ; создать матрицу рисков; осуществить количественную и качественную оценку рисков; подготовить отчет о выполненной работе по оценке рисков; подготовить плана оптимизации рисков.
ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах		
Знать	- Порядок разработки политик безопасности; - методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах;	1. Методика оценки рисков информационной безопасности компании. 2. Управление рисками. Перечислить основные понятия. 3. Метод оценки рисков на основе модели угроз и уязвимостей. 4. Расчет рисков по угрозе информационной безопасности. 5. Метод оценки рисков на основе модели информационных потоков. 6. Методики и технологии управления рисками. Качественные методики управления рисками. Количественные методики управления рисками. Метод CRAMM. 7. Разработка корпоративной методики анализа рисков. 8. Современные методы и средства анализа и управление рисками информационных систем компаний. 9. Обоснование необходимости инвестиций в информационную безопасность компании.
Уметь	- Разрабатывать политики безопасности; - использовать методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах; - анализировать и оценивать угрозы информационной безопасности объекта, выполнять анализ рисков информационной безопасности в распределенных информационных системах.	Провести расчеты оценки рисков информационной безопасности компании на основе модели информационных потоков.

Владеть	- методиками проведения анализа рисков информационной безопасности распределенных информационных систем; - методами оценки информационных рисков; - навыками разработки политики информационной безопасности автоматизированных систем.	***Задание*** Для заданного предприятия разработать: – карту информационных активов фирмы; – карты уязвимостей и угроз; – отчет о результатах оценки рисков; – план по обработке рисков; – частные политики безопасности.

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

– 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. Веселов, Г. Е. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог:Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/997108 (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. 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. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2019. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-106148-0. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/996789 (дата обращения: 20.03.2020)

3. Баранкова И. И. Сетевая защита информации. Лабораторный практикум [Электронный ресурс] : учебное пособие [для вузов] / И. И., Баранкова, Д.Н. Мазнин, У.В. Михайлова, М.В. Афанасьева ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - ISBN 978-5-9967-1605-0 URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3824.pdf&show=dcatalogues/1/1530260/3824.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 практических 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(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
7Zip	свободно распространяемое ПО	бессрочно
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
MS Office 2003 Professional	№ 135 от 17.09.2007	бессрочно
MS Windows XP Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
Adobe Reader	свободно распространяемое ПО	бессрочно
MS Windows 10 Professional (для классов)	Д-1227-18 от 08.10.2018	11.10.2021
Calculate Linux Desktop Xfce	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
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/

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.

Учебные аудитории для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации:

- 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 ПРАКТИЧЕСКИХ РАБОТ

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

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

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

Основными задачами практических занятий являются:

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

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

Структура практического занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущего практического занятия, ставится его цели и задачи, проверяется исходный уровень готовности студентов к практическому занятию (выполнение тестов, контрольные вопросы и т.п.)

На практическом 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 практических работ

Общие правила:

1. Практические работы проводятся под наблюдением преподавателя. К выполнению практических 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 практических работ

При подготовке к выполнению практических работ студент должен повторить

теоретический материал, необходимый для выполнения заданий по текущей теме.

Практическая работа выполняется каждым студентом самостоятельно, согласно индивидуальному заданию.

Студенты, пропустившие занятия, выполняют практические работы во внеурочное время.

После выполнения каждой практической работы студент демонстрирует результат выполнения преподавателю, отвечает на вопросы. Преподаватель оценивает работу в соответствии с заданными критериями оценки практических работ.

Правила оформления результатов и оценивания практической работы

Результаты выполненной практической 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 прилагается 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.