



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
В.Р. Храмшин

03.03.2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

МОДЕЛИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки (специальность)

10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы

10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	5
Семестр	10

Магнитогорск
2021 год

Рабочая программа составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
19.02.2021, протокол № 9

Зав. кафедрой И.И. Баранкова И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
03.03.2021 г. протокол № 5

Председатель В.Р. Храмшин В.Р. Храмшин

Рабочая программа составлена:
зав. кафедрой ИиИБ, д-р техн. наук

И.И. Баранкова И.И. Баранкова

Рецензент:

Начальник отдела информационной безопасности "КУБ" (АО) ,
М.М. Блинецов М.М. Блинецов

Лист актуализации рабочей программы

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

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 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 2027 - 2028 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 «Моделирование систем защиты информации» является формирование у обучающихся знаний по основам организации, управления и обеспечения безопасности и целостности данных информационных систем и технологий, а также навыков и умений в области анализа потенциальных угроз информационной безопасности, выборе средств реализации защиты в информационных системах, ознакомление с принципами моделирования систем защиты информации.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Моделирование систем защиты информации входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

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

Основы информационной безопасности

Безопасность сетей ЭВМ

Безопасность систем баз данных

Разработка систем защиты информации автоматизированных систем

Методы проектирования систем защиты распределенных информационных систем

Математическое моделирование распределенных систем

Моделирование угроз информационной безопасности

Дискретная математика

Основы теории оптимизации

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

Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

Производственная - преддипломная практика

Производственная - научно-исследовательская работа

Подготовка к сдаче и сдача государственного экзамена

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Обеспечение информационной безопасности критической информационной инфраструктурой

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

В результате освоения дисциплины (модуля) «Моделирование систем защиты информации» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-6	Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем
ПК-6.1	Проводит анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем
ПК-6.2	Выявляет уязвимости информационно-технологических ресурсов автоматизированных систем

ПК-6.3	Выявляет основные угрозы безопасности информации в автоматизированных системах
ПК-6.4	Составляет протоколы тестирования систем защиты информации автоматизированных систем
ПК-7	Способен разрабатывать проектные решения по защите информации в автоматизированных системах
ПК-7.1	Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах
ПК-7.2	Выбирает меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы
ПК-7.3	Определяет виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации
ПК-7.4	Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетных единиц 180 акад. часов, в том числе:

- контактная работа – 86,8 акад. часов;
- аудиторная – 85 акад. часов;
- внеаудиторная – 1,8 акад. часов;
- самостоятельная работа – 93,2 акад. часов;
- в форме практической подготовки – 0 акад. час;

Форма аттестации - зачет с оценкой

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. Марковские модели процессов кибербезопасности								
1.1 Основные понятия марковских процессов. Применение марковских моделей при моделировании систем защиты информации	10	6	10/5,85И		20	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы;	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4, ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
1.2 Оценка уровня защищенности автоматизированных систем на основе стохастической марковской модели защиты информации		8	12/4И		15	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы;	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4, ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу		14	22/9,85И		35			
2. Имитационное моделирование систем защиты информации								

2.1 Методы и средства имитационного моделирования. Классификация средств имитационного моделирования. Агентное моделирование информационной безопасности	10	6	11/4И		20	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – индивидуальное задание;	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4, ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
2.2 Системно-динамическое моделирование угроз информационной безопасности		6	10/4И		20	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы;	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4, ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
2.3 Применение методов имитационного моделирования для исследования инфраструктурных атак и механизмов защиты от них		8	8		18,2	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы;	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4, ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу		20	29/8И		58,2			
Итого за семестр		34	51/17,85И		93,2		зао	
Итого по дисциплине		34	51/17,85И		93,2		зачет с оценкой	

5 Образовательные технологии

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

a) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям.

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

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

d) Проблемные лекции– для ведения диалога обучающихся с преподавателем по сложным темам, для более полного раскрытия содержания проблемы по некоторым темам, а так же для развития исследовательских навыков и изучения способов решения задач;

2) Лекции-визуализации – для наглядного представления материалов курса. Лекционные занятия проводятся с использованием презентационного оборудования (проектор, экран, ноутбук), в качестве наглядных материалов используются: Web-ориентированные программные учебные материалы, электронные плакаты, презентации к лекциям.

3) Модульно-компетентностная технология, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. Для формирования у обучающихся основных понятий дисциплины используются:

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.

4) Интерактивное обучение.. Все практические занятия проводятся в интерактивной форме. В рамках интерактивного обучения обучающихся применяются:

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 ИТ – для применения компьютеров в процессе освоения дисциплины и доступа к ЭОР кафедры и Интернет-ресурсам.

c) Проблемное обучение – для стимулирования к самостоятельной «добыче» знаний, необходимых для решения конкретной проблемы. Для этого каждому обучающемуся выдаётся индивидуальная тема, по которой он должен составить реферат.

5) 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;

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

b) Для приобретения новых фактических знаний и практических умений используются практические занятия:

- a) компьютерный практикум;
- b) разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Моделирование систем защиты информации» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает решение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающегося.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Примерные задания:

1. Составить граф состояний и переходов системы при воздействии на нее независимых угроз и устранении уязвимостей.
2. Составить имитационную модель системно-динамической модели угроз информационной безопасности в среде AnyLogic. Провести имитационный эксперимент: определить оптимальное значение среднегодового количества инцидентов информационной безопасности при заданном ограничении на количество угроз с недопустимым уровнем риска

7 Оценочные средства для проведения промежуточной аттестации

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

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ПК-6 Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем		
ПК-6.1	Проводит анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	Исследовать структуру одной из автоматизированных систем предприятия. Провести моделирование автоматизированной системы с использованием цепей Маркова.
ПК-6.2	Выявляет уязвимости информационно-технологических ресурсов автоматизированных систем	Составить имитационную модель DDOS-атаки ботнет-сети на сервер
ПК-6.3	Выявляет основные угрозы безопасности информации в автоматизированных системах	Составить имитационную модель системно-динамической модели угроз информационной безопасности в среде AnyLogic. Провести имитационный эксперимент: исследовать динамику множеств угроз с

		допустимыми и недопустимыми уровнями риска. Выявить зависимости величин множества угроз с допустимыми и недопустимыми уровнями риска при фиксированных значениях других параметров модели.
ПК-6.4	Составляет протоколы тестирования систем защиты информации автоматизированных систем	Составить граф состояния субъекта в модели PSIDR. Составить имитационную модель распространения вредоносного ПО при помощи среды AnyLogic и протестировать PSIDR-модель.
ПК-7 Способен разрабатывать проектные решения по защите информации в автоматизированных системах		
ПК-7.1	Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах	Составить имитационную модель системно-динамической модели угроз информационной безопасности в среде AnyLogic. Провести имитационный эксперимент по вариации факторов, определяющих информационную безопасность. Выявить степень влияния различных значений потенциала нарушителя на величину множества угроз с допустимыми и недопустимыми уровнями риска.
ПК-7.2	Выбирает меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы	Составить имитационную модель зависимости применения мер безопасности от атак со стороны инсайдеров.
ПК-7.3	Определяет виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации	Подготовьте описание угроз для АСУ ТП типового объекта Разработайте имитационную модель системы защиты информации
ПК-7.4	Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем	Описать методику моделирования систем защиты информации с помощью теории графов Провести классификацию нарушителей в зависимости от имеющихся возможностей определить возможные киберфизические последствия от реализации заданной угрозы

--	--	--

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

Показатели и критерии оценивания зачета с оценкой:

– на оценку «отлично» – обучающийся должен показать высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку «хорошо» – обучающийся должен показать средний уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач;

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

– на оценку «неудовлетворительно» – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки решения типовых задач.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. 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* (дата обращения 11.02.2021)

2. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: <https://doi.org/10.29039/01848-4>. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1232287> (дата обращения: 31.05.2021). – Режим доступа: по подписке.

***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

б) Дополнительная литература:

1. Баранова, Е. К. Моделирование системы защиты информации. Практикум : учеб. пособие / Е.К. Баранова, А.В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2018. — 224 с. + Доп. материалы [Электронный ресурс; Режим доступа: <http://new.znanium.com>]. — (Высшее образование: Бакалавриат). — DOI: <https://doi.org/10.12737/18877>. - ISBN 978-5-16-102078-4. - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/916068> (дата обращения: 19.03.2021)

2. 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: 26.02.2021)

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
7Zip	свободно	бессрочно
LibreOffice	свободно	бессрочно
Браузер Mozilla Firefox	свободно распространяе	бессрочно
Браузер	свободно	бессрочно
AnyLogic University	Д-895-14 от 14.07.2014	бессрочно
Calculate Linux Desktop	свободно распространяе	бессрочно
FAR Manager	свободно	бессрочно
Linux	свободно	бессрочно
MS Visual Studio 2017 Community	свободно распространяе мое ПО	бессрочно
MS Visual Studio Code	свободно распространяе	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
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
Электронная база периодических изданий East	https://dlib.eastview.com/
Федеральное государственное бюджетное учреждение «Федеральный институт	URL: http://www1.fips.ru/

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.

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 выполнившему 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.

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ
САМОСТОЯТЕЛЬНЫХ РАБОТ****Общие положения**

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы обучающихся 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):
 - а) предоставляемыми преподавателем на лекционных занятиях;
 - б) предоставляемыми преподавателем в рамках электронных образовательных курсов;
 - с) 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 обучающимися 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, аудиторские 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 7.6) «Оценочные средства для проведения промежуточной аттестации» данной РПД.