



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. Храпшин

03.02.2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

**МЕТОДЫ И СТАНДАРТЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ
КОМПЬЮТЕРНЫХ СИСТЕМ**

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	4
Семестр	8

Магнитогорск
2026 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 22.01.2026, протокол № 5

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

Рабочая программа одобрена методической комиссией ИЭиАС 03.02.2026 г. протокол № 5

Председатель В.Р. Храмшин В.Р. Храмшин

Рабочая программа составлена:

ст. преподаватель кафедры ИиИБ, О.В.Пермякова О.В.Пермякова

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 2027 - 2028 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 2028 - 2029 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 2029 - 2030 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 2030 - 2031 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 2031 - 2032 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 2032 - 2033 учебном году на заседании кафедры Информатики и информационной безопасности

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

1 Цели освоения дисциплины (модуля)

Целями изучения дисциплины «Методы и стандарты оценки защищенности компьютерных систем» является формирование у обучающихся понятий о принципах и методах оценки безопасности компьютерных систем на основе комплексного подхода к определению актуальных угроз безопасности; критериях оценки безопасности информационных технологий; отечественных и международных стандартах оценки защищенности информационных систем; освоение методов качественной и количественных оценок систем информационной безопасности в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем».

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Методы и стандарты оценки защищенности компьютерных систем входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

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

Безопасность систем баз данных

Безопасность сетей ЭВМ

Безопасность операционных систем

Сети и системы передачи информации

Основы информационной безопасности

Организационное и правовое обеспечение информационной безопасности

Программно-аппаратные средства обеспечения информационной безопасности

Моделирование угроз информационной безопасности

Знания (умения, владения), полученные при изучении данной дисциплины

будут необходимы для изучения дисциплин/практик:

Подготовка к сдаче и сдача государственного экзамена

Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

Производственная - научно-исследовательская работа

Производственная - преддипломная практика

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

В результате освоения дисциплины (модуля) «Методы и стандарты оценки защищенности компьютерных систем» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-1	Способен проводить анализ безопасности компьютерных систем
ПК-1.1	Оценивает эффективность защиты информации
ПК-1.2	Применяет разработанные методики оценки защищенности программно-аппаратных средств защиты информации

4. Структура, объём и содержание дисциплины (модуля)

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

- контактная работа – 72 академических часов;
- аудиторная – 68 академических часов;
- внеаудиторная – 4 академических часов;
- самостоятельная работа – 36,3 академических часов;
- в форме практической подготовки – 0 академических часов;
- подготовка к экзамену – 35,7 академических часов

Форма аттестации - экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в академических часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Общие вопросы оценки безопасности компьютерных систем								
1.1 Стандарт ISO/IEC 15408 Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.	8	12		12/6И	1,5	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию; подготовка к практическому занятию	Рубежный контроль-тестирование	ПК-1.1, ПК-1.2
1.2 ГОСТ Р ИСОМЭК 15045-2013 методология оценки безопасности ИТ		6		3	1,3	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиям	Рубежный контроль-тестирование	ПК-1.1, ПК-1.2

						и);подготовка к тестированию; подготовка к практическому занятию		
1.3 Руководящие документы в области оценки защищенности	8	2		1	0,5	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	тестирование	ПК-1.1, ПК-1.2
Итого по разделу		20		16/БИ	3,3			
2. Методы оценки систем информационной безопасности								
2.1 Метод экспертных оценок	8	2		4	3	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	Компьютерное тестирование. Защита ИДЗ	ПК-1.1, ПК-1.2
2.2 Метод информационных потоков .		4		4	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию;	Компьютерное тестирование. Защита ИДЗ	ПК-1.1, ПК-1.2

						подготовка к практическому занятию		
2.3 Показатели ОУД	8	6		6/5,9И	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию; подготовка к практическому занятию	Компьютерное тестирование. Защита ИДЗ	ПК-1.1, ПК-1.2
Итого по разделу		12		14/5,9И	7			
3. Организация оценки безопасности компьютерных систем								
3.1 Оценки защищенности компьютерных систем	8	2		4	14	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию; подготовка к практическому занятию	Компьютерное тестирование, Рубежный контроль: Комплексная защита ИДЗ	ПК-1.1, ПК-1.2
Итого по разделу		2		4	14			
4. Экзамен								
4.1 Экзамен	8				12	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями,	Экзамен	ПК-1.1, ПК-1.2

					энциклопедиями);		
Итого по разделу				12			
Итого за семестр	34		34/11,9 И	36,3		экзамен	
Итого по дисциплине	34		34/11,9 И	36,3		экзамен	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Методы и стандарты оценки защищенности компьютерных систем» используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций, учета особенностей профессиональной деятельности выпускников и потребностей работодателей

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература:

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2025. — 349 с. — (Высшее образование). — ISBN 978-5-534-19762-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561077> (дата обращения: 12.03.2026).

2. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561313> (дата обращения: 12.03.2026).

3. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2024. — 400 с. — (Высшее образование). — DOI: <https://doi.org/10.12737/1759-3>. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2140566> (дата обращения: 12.03.2026). — Режим доступа: по подписке.

4. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2024. — 223 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016533-2. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2003474> (дата обращения: 12.03.2026). — Режим доступа: по подписке.

б) Дополнительная литература:

Гришина Наталия Васильевна (Российский государственный гуманитарный университет РГГУ).

1. Основы информационной безопасности предприятия : Учебное пособие / Гришина Наталия Васильевна ; Российский государственный гуманитарный университет РГГУ. - 1. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2024. - 216 с. - (Высшее образование: Специалитет). - ВО - Специалитет. - URL: <https://znanium.com/catalog/document?id=439186>. - URL:

<https://znanium.com/cover/2131/2131865.jpg>. - ISBN 978-5-16-016534-9. - ISBN 978-5-16-108800-5.

1. 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: 12.03.2026).

2. Душкин, А. В. Методологические основы построения защищенных автоматизированных систем: Монография / Душкин А.В. - Воронеж:Научная книга, 2016. - 76 с. ISBN 978-5-4446-0902-6. - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/923295> (дата обращения: 12.03.2026)

МАКРООБЪЕКТЫ:

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> (дата обращения 12.03.2026)

4. Баранков В. В. Развертывание и настройка виртуальных сетей [Электронный ресурс] : учебное пособие [для вузов] / В. В. Баранков, И. И. Баранкова, У. В. Михайлова, О. Б. Калугина ; МГТУ. - Магнитогорск : МГТУ, 2019. - 1 электрон. опт. диск (CD-ROM). - ISBN 978-5-9967-1305-9 URL:

<https://magtu.informsystema.ru/uploader/fileUpload?name=3813.pdf&show=dcatalogues/1/1529986/3813.pdf&view=true> (дата обращения 12.03.2026)

5. Архитектура и принципы работы вычислительных систем [Электронный ресурс] : учебное пособие [для вузов] / В.В. Баранков, И.И. Баранкова, М.В. Афанасьева, М.В. Коновалов; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - ISBN 978-5-9967-1306-6 URL :

<https://magtu.informsystema.ru/uploader/fileUpload?name=3924.pdf&show=dcatalogues/1/1530495/3924.pdf&view=true> (дата обращения 12.03.2026)

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронного каталога <https://magtu.informsystema.ru>

2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)

3. Активизировать гиперссылку макрообъекта

*При открытии макрообъектов учитывайте настройки антивирусной защиты

в) Методические указания:

1. Методические указания по выполнению практических работ по дисциплине «Методы и стандарты оценки защищенности компьютерных

систем» (Приложение 1) .

2. Методические указания по выполнению внеаудиторных самостоятельных работ по дисциплине «Методы и стандарты оценки защищенности компьютерных систем» (Приложение 2).

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
7Zip	свободно распространяемое ПО	бессрочно
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно
Calculate Linux Desktop Xfce	свободно распространяемое ПО	бессрочно
Ред ОС	Сертификат №01-04\22 от 06.05.2022	06.05.2025
Kaspersky Endpoint Security для бизнеса-Стандартный	Д-165-23 от 27.03.2023	27.03.2025
AdobeReader	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/?ysclid=lujkqy7cnw630508962
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/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi?ysclid=lujknksfy724757053
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	https://host.megaprolib.net/M P0109/Web
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Электронная база периодических изданий ООО «ИВИС»	https://eivis.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Учебные аудитории для проведения занятий лекционного типа
Мультимедийные средства хранения, передачи и представления информации.

Учебные аудитории для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации
Мультимедийные средства хранения, передачи и представления информации.

Помещения для самостоятельной работы обучающихся
Персональные компьютеры с выходом в Интернет и с доступом в электронную информационно-образовательную среду университета

ПРИЛОЖЕНИЕ 1

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

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

Практическая работа - познавательная учебная деятельность, когда последовательность мышления студента, его умственные и практические операции и действия зависят и определяются самим студентом. Работая практически, студент должен постепенно овладеть такими общими приёмами практической работы как ясное представление цели работы её выполнение, проверка, исправление ошибок. Выполнение практических работ студентами влияет на формирование и развитие информационных компетенций. Студенты овладевают способами работы с информацией:

- поиск в каталогах, поисковых системах, иерархических структурах;
- извлечение информации с различных носителей;
- систематизация, анализ и отбор информации (разные виды сортировки, фильтры, запросы, структурирование файловой системы, проектирование баз данных и т.д.);
- технические навыки сохранения, удаления, копирования информации и т.п. –
- преобразование информации (из графической – в текстовую, из аналоговой – в цифровую и т.п.)

Основными задачами практических работ являются: формирование умений подбирать материалы по их назначению, условиям эксплуатации, применять их при выполнении работ.

Содержание практической работы составляют:

- номер и тема практической работы;
- цель практической работы;
- рекомендации для выполнения практической работы;
- перечень используемых материалов, инструментов, оборудования;
- порядок выполнения работы;

- вывод о проделанной работе.

Перед тем как приступить к выполнению практической работы, студент должен пройти инструктаж по технике безопасности, усвоить краткие теоретические сведения по теме, методику выполнения работы, а также способы представления полученных данных.

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 и противопожарным мерам. После инструктажа каждый студент расписывается в журнале
2. Строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в кабинете.
3. Все практические работы проводятся за компьютерными столами учебного кабинета. Студентам не разрешается без уважительной причины отлучаться из кабинета до полного окончания практических работ.
4. На рабочем месте должны находиться только необходимые для работы оборудование и материалы. Класть сумки необходимо на специально отведенный для этого стол.
5. Бережно обращаться с оргтехникой. Входить в класс разрешается только после звонка на урок, спокойно, не торопясь, не задевая столы.
6. Занимать места в кабинете необходимо согласно «Схеме посадочных мест», начиная с первых парт.
7. Студент отвечает за состояние рабочего места и сохранность размещенного на нем оборудования.
8. Соблюдение всех вышеперечисленных рекомендаций по организации учебного процесса с использованием компьютеров и технических средств обучения должно способствовать сохранению оптимального уровня работоспособности и функционального состояния организма, на протяжении всех учебных занятий в колледже и полной безопасности для их жизни и здоровья.

Перед началом работы:

1. Проверить порядок на рабочем месте;
2. Отрегулировать положение монитора так, чтобы расстояние от глаз до экрана составляло не менее 50 см.

Во время работы:

1. Во время работы монитор является источником электромагнитного излучения, которое неблагоприятно действует на зрение. Поэтому надо работать на расстоянии 60-70 см, соблюдая правильную осанку (вертикально прямая спина, плечи опущены и расслаблены, ноги на полу не скрещены, стоят на подставке для ног, локти, запястья и кисти рук на одном уровне).
2. Непрерывное занятие студента за компьютером не должно превышать 30 минут. По истечении данного времени необходим перерыв длительностью 5 минут для снятия напряжения глаз. Для снятия усталости мышц используйте комплекс упражнений по

профилактике зрительного утомления, упражнения для рук и плечевого пояса, для туловища и ног.

3. При плохом самочувствии, появлении головной боли, головокружении и др. прекратить работу и сообщить об этом преподавателю.
4. Обо всех неисправностях немедленно сообщать преподавателю;
5. В случае аварийной ситуации выключить компьютер.

По окончании работы:

1. Собрать методические указания к практическим работам и сдать их преподавателю;
2. Выключить ЭВМ после разрешения преподавателя;
3. Навести порядок на рабочем месте.

При работе в компьютерном классе строго запрещается:

- 1) Находиться в верхней одежде и грязной обуви;
- 2) Принимать пищу на рабочем месте и в компьютерном кабинете.
- 3) Удалять и перемещать чужие файлы;
- 4) Приносить и запускать свое программное обеспечение (программы);
- 5) Работать на ЭВМ грязными или мокрыми руками;
- 6) Прикасаться пальцами к мониторам, стучать по ним;
- 7) Включать и выключать компьютер без разрешения преподавателя;
- 8) Класть диски, книги, тетради на составляющие компьютера;
- 9) Подключать к компьютеру свои устройства (сот. телефоны, плееры).
- 10) Работать на не исправном компьютере;
- 11) Оставлять вычислительную технику на длительное время без присмотра;
- 12) Прикасаться к электрическим вилкам, розеткам, проводам, разъемам, задним стенкам системного блока и монитора;
- 13) Вскрывать корпуса, вынимать и вставлять разъемы, платы

Правила выполнения практических работ

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 на занятии оценивает работу.

Правила оформления результатов практической работы

Результаты выполненной практической работы оформляются в виде отчета.

Критерии оценки практических работ

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

Для оценивания работы прилагается эталон и шкала оценок.

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.

Во всех случаях оценка снижается, если студент не соблюдает требования безопасности труда.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ ПО ДИСЦИПЛИНЕ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы студентов по дисциплине «Информатика» 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.

Особенностью изучения дисциплины «Информатика» является освоение теоретического материала и получение практических умений, направленных на использование современных информационных технологий.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины (модуля)» 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 и к решению олимпиадных заданий.
- 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: защита реферата, индивидуальные домашние задания, аудиторные контрольные работы, компьютерное тестирование, участие в конкурсах и олимпиадах.

Максимальное количество баллов обучающийся получает, если:

- выполняет ИДЗ 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.

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-1 Способен проводить анализ безопасности компьютерных систем		
ПК-1.1	Оценивает эффективность защиты информации	<p>Перечень вопросов:</p> <ol style="list-style-type: none"> 1. Что такое уровень гарантированности? 2. Какие виды гарантированности бывают? 3. Что такое классы безопасности и уровни доверия? 4. Перечислите классы функциональных требований в ISO 15408. 5. Перечислите классы требований доверия в ISO 15408. 6. Перечислите оценочные уровни доверия в стандарте ISO 15408. 7. Перечислите группы элементов управления в стандарте ISO 17799. 8. Перечислите ключевые элементы управления в ISO 17799. 9. Средства защиты в компьютерных системах 10. Теоретико-вероятностный метод оценки защищенности в компьютерных системах 11. Экспертный метод оценки в компьютерных системах 12. Статистический метод оценки в компьютерных системах 13. Вероятностно-статистический метод оценки рисков в компьютерных системах 14. Взаимосвязь угроз, уязвимостей и рисков 15. Оценки защищенности на основе модели комплекса механизмов защиты 16. Семантические показатели защищенности компьютерных систем 17. Нечеткие оценки защищенности компьютерных систем 18. Комплексные оценки защищенности компьютерных систем 19. Типовая архитектура системы выявления атак. Методы тестирования системы защиты <p>Рубежный контроль: Защита разработанного задания по безопасности объекта оценки ИТ по требованиям стандарта ГОСТ ИСОМЭК 15408</p>
ПК-	Применяет	Задание:

1.2	разработанные методики оценки защищенности программно-аппаратных средств защиты информации	<p>Оценить показатели защиты информации для заданной системы</p> <p>Виды систем:</p> <ol style="list-style-type: none"> 1. Информационно-поисковые системы 2. Электронный документооборот и делопроизводство 3. Электронные архивы 4. Системы управления ресурсами организации 5. Системы автоматизации проектирования 6. Информационно-аналитические системы 7. Системы поддержки принятия решений 8. Системы видеоконференцсвязи и цифровой телефонии 9. Ситуационные и управляющие центры <p>Используя метод оценки защищенности на основе модели комплекса механизмов защиты определить защищенность, обеспечиваемой отдельным механизмом и СЗИ в целом. Определить эффективность применяемых методов обеспечения безопасности компьютерной системы.</p> <p>Используя онлайн-калькулятор банка данных угроз ФСТЭК определить базовые, временные и контекстные метрики угроз информационной безопасности компьютерных систем</p> <p>Рубежный контроль:</p> <p>Тестовый контроль знаний по терминам стандартов серии ГОСТ ИСОМЭК 15408</p> <p>Тестовый контроль знаний по процедуре проведения оценки согласно критериям оценки безопасности ИТ ГОСТ ИСОМЭК 15408</p>
-----	--	---

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

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме экзамена.

Критерии оценки (в соответствии с формируемыми компетенциями и планируемыми результатами обучения):

Показатели и критерии оценивания экзамена:

– на оценку «отлично» (5 баллов) – обучающийся успешно прошел запланированные рубежные контроли и в ходе промежуточной аттестации демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку «хорошо» (4 балла) – обучающийся успешно прошел запланированные рубежные контроли и в ходе промежуточной аттестации демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку «удовлетворительно» (3 балла) – обучающийся прошел запланированные рубежные контроли и в ходе промежуточной аттестации демонстрирует пороговый

уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

– на оценку «неудовлетворительно» (2 балла) – обучающийся прошел запланированные рубежные контроли, но в ходе промежуточной аттестации демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

– на оценку «неудовлетворительно» (1 балл) – не прошел запланированные рубежные контроли, обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.