



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
10.02.2023 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

***РАЗРАБОТКА ЭКСПЛУАТАЦИОННОЙ ДОКУМЕНТАЦИИ НА
СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ
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
2023 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
09.02.2023, протокол № 5

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

Рабочая программа одобрена методической комиссией ИЭиАС
10.02.2023 г. протокол № 7

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. Близицов

Лист актуализации рабочей программы

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

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

1. Цели освоения дисциплины (модуля)

Целями освоения дисциплины «Разработка эксплуатационной документации на системы защиты информации автоматизированных систем» является формирование у обучающихся понятий эксплуатационной документации, формировании требований и правил обслуживания систем защиты информации, разработки и ведения эксплуатационной документации на системы защиты информации автоматизированных систем и овладение обучающимися необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Разработка эксплуатационной документации на системы защиты информации автоматизированных 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:

Программно-аппаратные средства обеспечения информационной безопасности

Безопасность систем баз данных

Безопасность сетей ЭВМ

Сети и системы передачи информации

Безопасность операционных систем

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

Обеспечение информационной безопасности критической информационной инфраструктурой

Методы проектирования систем защиты распределенных информационных систем

Управление информационной безопасностью

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

В результате освоения дисциплины (модуля) «Разработка эксплуатационной документации на системы защиты информации автоматизированных систем» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ОПК-14	Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений;
ОПК-14.1	Осуществляет разработку защищенных автоматизированных систем
ОПК-14.2	Принимает участие во внедрении систем защиты информации автоматизированных систем
ОПК-14.3	Эксплуатирует системы защиты информации

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 2 зачетных единиц 72 акад. часов, в том числе:

- контактная работа – 34,95 акад. часов;
- аудиторная – 34 акад. часов;
- внеаудиторная – 0,95 акад. часов;
- самостоятельная работа – 37,05 акад. часов;
- в форме практической подготовки – 0 акад. час;

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. Техническая документация автоматизированных систем в защищенном исполнении								
1.1 Общие сведения. Назначение технической документации. Требования технической документации	8	2	1		2	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), подготовка к тестированию	Тестирование	ОПК-14.1, ОПК-14.2, ОПК-14.3
1.2 Стандарты в области информационных систем. Комплекс стандартов и руководящих документов на автоматизированные системы		2	2		3	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию.	Тестирование	ОПК-14.1, ОПК-14.2, ОПК-14.3

1.3 Содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении.		5	4		10	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию.	Тестирование	ОПК-14.1, ОПК-14.2, ОПК-14.3
Итого по разделу		9	7		15			
2. Разработка эксплуатационной документации								
2.1 Общие положения. Состав эксплуатационной документации. Виды и номенклатура эксплуатационных документов. Требования к эксплуатационной документации	8	4	4		10	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию.	Тестирование	ОПК-14.1, ОПК-14.2, ОПК-14.3
2.2 Составление руководства пользователя с выделением действий по обеспечению информационной безопасности.		2	2		2	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), выполнение ИДЗ	ИДЗ	ОПК-14.1, ОПК-14.2, ОПК-14.3
2.3 Составление программы и методики испытаний системы защиты автоматизированной системы.		2	4		10,05	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); выполнение ИДЗ; подготовка к зачету	ИДЗ	ОПК-14.1, ОПК-14.2, ОПК-14.3
Итого по разделу		8	10		22,05			
Итого за семестр		17	17		37,05		зачёт	
Итого по дисциплине		17	17		37,05		зачет	

5. Образовательные технологии

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

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. 2) Раздельно-компетентностная технология, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. 3) Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе лично 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. 4) Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности обучающихся. 5) Игровые технологии – организация образовательного процесса, основанная на реконструкции моделей поведения. Формы учебных занятий с использованием предложенных сценарных условий. 6) Технологии проектного обучения – организация образовательного процесса в соответствии с алгоритмом поэтапного решения проблемной задачи или выполнения учебного задания.

Проект предполагает совместную учебно-познавательную деятельность группы обучающихся, направленную на выработку концепции, установление целей и задач, формулировку ожидаемых результатов, определение принципов и методик решения поставленных задач, планирование хода работы, поиск доступных и оптимальных ресурсов, поэтапную реализацию плана работы, презентацию результатов работы, их осмысление и рефлексия. 7) Информационно-коммуникационные образовательные технологии – организация образовательного процесса, основанная на применении специализированных программных сред и технических средств работы с информацией.

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 (модуля)

а) Основная литература:

1. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/441287> (дата обращения: 24.02.2023).

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/437163> (дата обращения: 24.02.2023).

б) Дополнительная литература:

1. ГОСТ 2.610-2006 Единая система конструкторской документации (ЕСКД). Правила выполнения эксплуатационных документов. М.:Стандартинформ, 2008. – 39 с.
2. ГОСТ 34.601–90 Информационная технология. Комплекс стандартов на автоматизируемые системы. Стадии создания. – М.: Изд-во стандартов, 2003. – 6 с.
3. ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизируемые системы. Виды, комплектность и обозначение документов при создании автоматизированных систем М.: Переиздание Стандартинформ, 2008. –10с.
4. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000. – 34с.
5. 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 11.02.2023) - 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) Программное обеспечение и Интернет-ресурсы:**Программное обеспечение**

Наименование ПО	№ договора	Срок действия лицензии
7Zip	свободно распространяемое ПО	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
Calculate Linux Desktop Xfce	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.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/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/

9. Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционная аудитория:

- Мультимедийные средства хранения, передачи и представления информации

Компьютерный класс:

- Персональные компьютеры с ПО;

- Выход в Интернет и с доступ в электронную информационно-образовательную среду университета

Аудитории для самостоятельной работы:

- Персональные компьютеры с ПО;

- Выход в Интернет и с доступ в электронную информационно-образовательную среду университета

Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Разработка эксплуатационной документации на системы защиты информации автоматизированных систем» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

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 и вопросы по темам:

Перечень контрольных вопросов:

1. Жизненный цикл системы информационной безопасности
2. Стадии и этапы создания автоматизированной системы
3. Понятие эксплуатационной документации на автоматизированную систему
4. Виды документов, относящихся к эксплуатационной документации
5. Требования к управлению документами проекта
6. Основные понятия проектного менеджмента и их взаимосвязь
7. Требования при создании (модернизации) автоматизированной системы в защищенном исполнении
8. Национальные стандарты, рекомендуемые к применению при создании автоматизированных систем в защищенном исполнении
9. Содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении
10. Содержание эксплуатационной документации на систему защиты автоматизированной системы
11. Содержание документа «Руководство по эксплуатации»
12. Содержание документа «Формуляр»
13. Виды испытаний автоматизированных систем
14. Виды программных документов
15. Назначение документа «Программа и методика испытаний» на систему защиты автоматизированной системы
16. Перечень проверок, подлежащих включению в программу испытаний
17. Основные разделы программы испытаний
18. Содержание документа «Общее описание системы»
19. Состав приемочных испытаний
20. Руководство пользователя системы защиты автоматизированной системы
21. Основные моменты в описании технологического процесса обработки данных в системе защиты автоматизированной системы
22. Инструкция по формированию и ведению базы данных (набора данных)
23. Составление инструкции о мерах по обеспечению информационной безопасности
24. Инструкция администратору безопасности информации автоматизированной системы

Оценочные средства для проведения промежуточной аттестации

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

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОПК-14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений;		
Знать	<ul style="list-style-type: none"> – руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; – нормативные правовые акты в области защиты информации; – основные методы управления проектами в области информационной безопасности. 	<ol style="list-style-type: none"> 1. Перечислить национальные стандарты, рекомендуемые к применению при создании автоматизированных систем в защищенном исполнении 2. Рассказать порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении 3. Перечислить документы, относящиеся к эксплуатационной документации на систему защиты автоматизированной системы 4. Перечислить виды испытаний автоматизированных систем 5. Перечислить виды программных документов 6. Перечислить требования к управлению документами проекта 7. Рассказать об основных понятиях проектного менеджмента и установить их взаимосвязь 8. Дать определение эксплуатационной документации на автоматизированную систему
Уметь	<ul style="list-style-type: none"> – разрабатывать эксплуатационную документацию на систему защиты автоматизированных систем; – анализировать программные, архитектурно-технические и схмотехнические решения 	<ol style="list-style-type: none"> 1. Составить перечень необходимой документации стадии «Рабочая документация», относящейся к эксплуатационной 2. Составить технологическую инструкцию для системы защиты автоматизированной системы 3. Составить руководство по эксплуатации системы защиты автоматизированной системы 4. Составить программу опытной эксплуатации для системы защиты автоматизированной системы 5. Составить схему организационной структуры управления проектами и определить взаимосвязи основных понятий проектного менеджмента

	<p>компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем;</p> <p>— проводить технико-экономическое обоснование и исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности.</p>	
Владеть	<p>— методами анализа технической документации информационной инфраструктуры автоматизированной системы;</p> <p>— навыком документирования программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации.</p>	<ol style="list-style-type: none"> 1. Составить руководство по эксплуатации комплекса технических средств системы защиты автоматизированной системы 2. На основании технического задания определить требования к составу и содержанию работ по подготовке системы защиты к вводу в действие; 3. Составить инструкцию для администратора безопасности информации автоматизированной системы; 4. Разработать инструкцию по формированию и ведению базы данных (набора данных)
Знать	— основные	1. Описать технологический процесс обработки и

	<p>меры по защите информации в автоматизированных системах;</p> <ul style="list-style-type: none"> – особенность и защиты информации в автоматизированных системах управления технологическим и процессами; – угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах. 	<p>хранения конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации средств ВТ.</p> <ol style="list-style-type: none"> 2. Проверить выполнение требований по защите информации от утечки за счет ПЭМИ СВТ. 3. Перечислить испытания на соответствие требованиям по ЗИ от НСД. 4. Перечислить требования при создании (модернизации) автоматизированной системы в защищенном исполнении 5. Дать понятие политики информационной безопасности организации
<p>Уметь</p>	<ul style="list-style-type: none"> – определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах; – Оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите. 	<ol style="list-style-type: none"> 1. Выполнить описание технологического процесса обработки и хранения конфиденциальной информации; 2. Составить инструкцию по антивирусному контролю; 3. Разработать организационно-распорядительную документацию разрешительной системы доступа персонала к защищаемым ресурсам автоматизированной системы; 4. Составить предписание на эксплуатацию СВТ; 5. Составить инструкцию по эксплуатации СЗИ (по выбору) в соответствии с ГОСТ 2.610-2006
<p>Владеть</p>	<ul style="list-style-type: none"> – методами анализа защищенности информационной инфраструктуры автоматизированных 	<ol style="list-style-type: none"> 1. Составить инструкцию о мерах по обеспечению информационной безопасности 2. Составить технический паспорт на систему защиты автоматизированной системы с приложениями: <ol style="list-style-type: none"> а) состав технических и программных средств, входящих в систему защиты АС;

<p>ой системы; — навыками формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач;</p>	<p>b) места установки СЗИ и технических средств; c) параметры и порядок настройки средств защиты информации, программного обеспечения и технических средств.</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

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

Показатели и критерии оценивания зачета:

- на оценку «**зачтено**» – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач;
- на оценку «**не зачтено**» – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки решения типовых задач.