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

03.02.2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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	3
Семестр	5

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

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

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
доцент кафедры кафедры ИиИБ, канд. техн. наук _____ У.В. Кузьмина

Рецензент:
начальник отдела информационной безопасности «КУБ» (АО) ,

_____ М.М. Близнецов

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 освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» являются: обучить обучающихся практическим навыкам работы с нормативно-правовой базой деятельности в области обеспечения безопасности информации. Знания и практические навыки, полученные в курсе «Организационное и правовое обеспечение информационной безопасности» используются обучаемыми при разработке курсовых и дипломных работ.

Задачи дисциплины:

• дать представление о законодательстве РФ в области информации;

• ознакомить с системой защиты государственной тайны;

• ознакомить с правилами лицензирования и сертификации в области защиты информации;

• ознакомить с организационными методами защиты информации;

• ознакомить с методами обеспечения информационной безопасности.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Организационное и правовое обеспечение информационной безопасности входит в обязательную часть учебного плана образовательной программы.

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

Основы информационной безопасности

Информатика

Основы безопасности цифрового общества

Организация ЭВМ и вычислительных систем

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

Защита электронного документооборота

Разработка эксплуатационной документации на системы защиты информации автоматизированных систем

Управление информационной безопасностью

Анализ рисков информационной безопасности

Защита программного обеспечения

Подготовка к сдаче и сдача государственного экзамена

Методы проектирования систем защиты распределенных информационных систем

Обеспечение информационной безопасности критической информационной инфраструктурой

Методы выявления нарушений информационной безопасности

Методы и стандарты оценки защищенности компьютерных систем

Безопасность сетей ЭВМ

Безопасность систем баз данных

Моделирование угроз информационной безопасности

Программно-аппаратные средства обеспечения информационной безопасности

Безопасность Интернета вещей

Защита информации от утечки по техническим каналам

Безопасность операционных систем

Технология построения защищенных распределенных приложений

Аттестация АИС

Методы и средства криптографической защиты информации

Разработка систем защиты информации автоматизированных систем

Производственная - практика по получению профессиональных умений и опыта профессиональной деятельности

Защита информационно-технологических ресурсов автоматизированных систем

Анализ безопасности информационных технологий

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Форензика

Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

Производственная - научно-исследовательская работа

Производственная - преддипломная практика

Моделирование систем защиты информации

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

В результате освоения дисциплины (модуля) «Организационное и правовое обеспечение информационной безопасности» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	
ОПК-5.1	Применяет основные нормативные правовые акты в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальной информации
ОПК-5.2	Применяет нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;

4. Структура, объём и содержание дисциплины (модуля)

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

– контактная работа – 55 акад. часов:

– аудиторная – 54 акад. часов;

– внеаудиторная – 1 акад. часов;

– самостоятельная работа – 53 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. Правовое обеспечение информационной безопасности								
1.1 Законодательство РФ в области информационной безопасности: Основы законодательства Российской федерации в области информационной безопасности. Понятие и виды защищаемой информации. Основы международного законодательства в области защиты информации.	5	1		2/1И	4	Самостоятельное изучение учебной и научной литературы, работа с материаламиобразовательного портала и ЭБС. Самостоятельная работа с интернет-источниками	Устный опрос, тестирование	ОПК-5.1, ОПК-5.2
1.2 Правовой режим защиты государственной тайны: Понятие государственной тайны. Государственная тайна как особый вид защищаемой информации. Система защиты государственной тайны. Система нормативных правовых актов, регламентиру-ющих обеспечение сохранности сведений, составляющих государственную тайну в РФ.		2		4/1И	5	Самостоятельное изучение учебной литературы и конспектов лекций, публикаций в периодических изданиях . Работа с Интернет-ресурсами. Изучение нормативной документации. Подготовка к аудиторным контрольным работам.	Аудиторная контрольная работа	ОПК-5.1, ОПК-5.2
1.3 Лицензирование в		4		4/3И	8	Самостоятельно	Индивидуальное	ОПК-5.1,

области защиты информации: Понятие лицензирования. Нормативные правовые акты РФ, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в области защиты информации.						е изучение учебной и научно литературы, работа с материалами образователь-ного портала.	домашнее задание	ОПК-5.2
1.4 Сертификация в области защиты информации: Понятие сертификации. Нормативные правовые акты РФ и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации.	5	2		4/3И	6	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала. Подготовка и выполнение ИДЗ	Индивидуальное домашнее задание	ОПК-5.1, ОПК-5.2
1.5 Законодательство РФ в области конфиденциальной информации и коммерческой тайны. Ответственность.		1		2/1И	1	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала.	Рубежный контроль: устная защита отчета по выполненным работам по разделу	ОПК-5.1, ОПК-5.2
Итого по разделу		10		16/9И	24			
2. Организационное обеспечение информационной безопасности								
2.1 Понятие организационной защиты информации. Сущность организационных методов защиты информации.	5	2		4/2И	8	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к практическим занятиям.	Устный опрос	ОПК-5.1, ОПК-5.2
2.2 Анализ и оценка угроз информационной безопасности объекта. Методы и способы анализа угроз безопасности информации. Порядок проведения оценки опасности угрозы.		2		6/1,6И	6	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС.	Устный опрос	ОПК-5.1, ОПК-5.2
2.3 Оценка ущерба:		1		2	3,5	Поиск	Индивидуальное	ОПК-5.1,

Понятие ущерба. Методы и способы оценки ущерба.						дополнительной информации по заданной теме.	домашнее задание	ОПК-5.2
2.4 Служба безопасности объекта: Место службы безопасности объекта в общей структуре системы защиты государственной тайны и государственной системы защиты информации. Задачи, решаемые службой безопасности объекта. Структура и состав службы безопасности объекта. Роль и место подразделения (штатного специалиста) по технической защите информации, решаемые задачи, права и обязанности.	5	1		2	1,5	Подготовка к компьютерному тестированию. Самостоятельная работа с интернет-источниками.	Компьютерное тестирование	ОПК-5.1, ОПК-5.2
2.5 Средства и методы физической защиты объекта: Объекты обеспечения физической без-опасности: сооружения, предметы, люди. Организация охраны, пропускного и внутриобъектового режима.		1		4	4	Поиск дополнительной информации по заданной теме.	Индивидуальное домашнее задание	ОПК-5.1, ОПК-5.2
2.6 Организация и обеспечение режима секретности: Допуск должностных лиц к государственной тайне и к информации ограниченного доступа, не отнесенной к государственной тайне. Требования к помещениям и хранилищам, в которых ведут-ся закрытые работы. Организация защиты информации при приеме посетителей, командированных лиц и иностранных представителей. Защита информации в экстремальных ситуациях.		1		2		Самостоятельное изучение учебной и научной литературы, работа с материаламиобразова-тельного портала и ЭБС. Самостоятельная работа с интернет-источниками	Рубежный контроль: устная защита отчета по выполненным работам по разделу	ОПК-5.1, ОПК-5.2
Итого по разделу		8		20/3,6 И	29			
Итого за семестр		18		36/12,6 И	47		зачёт	
Итого по дисциплине		18		36/12,6 И	53		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 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. 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 рефлексию. 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

а) Основная литература:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277 (дата обращения: 19.02.2026).

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844 (дата обращения: 26.04.2026).

3. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - URL: https://host.megaprolib.net/MP0109/Download/MObject/1858 (дата обращения: 26.04.2026). - ISBN 978-5-9967-1031-7. - Текст : электронный*.

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронной библиотеки МГТУ им. Г. И. Носова https://host.megaprolib.net/MP0109/Web.

2. Произвести авторизацию на портале (логин: Фамилия на русском языке, пароль: номер читательского билета)

3. Активизировать гиперссылку макрообъекта.

б) Дополнительная литература:

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».

3. Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне».

4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

5. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».

6. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

7. Доктрина информационной безопасности Российской Федерации (утв. Президен-том Российской Федерации 09.09.2000 № Пр-1895)

8. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утверждена за-местителем директора ФСТЭК России 14 февраля 2008 г.

9. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утверждена заместителем дирек-тора ФСТЭК России 15 февраля 2008 г.

10. ГОСТ Р 50922-2006 «Национальный стандарт российской федерации. Защита ин-формации. Основные термины и определения».

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

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

Linux Calculate	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Calculate Linux Desktop Xfce	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Международная реферативная и полнотекстовая справочная база данных научных изданий «Springer Nature»	https://www.nature.com/siteindex
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/MP0109/Web
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:

1. Аудитории для самостоятельной работы (ауд. 132а): компьютерные классы; читальные залы библиотеки.

2. Компьютерные классы с выходом в Интернет и с доступом в электронную информационно-образовательную среду университета

3. Мультимедийные поточные аудитории университета с мультимедийными средствами хранения, передачи и представления информации

ПРИЛОЖЕНИЕ 1

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Организационное и правовое обеспечение информационной безопасности» 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 индивидуальные домашние задания (ИДЗ):

Тема 1.1. Задание 1. Выбрать, вид и область деятельности, название фирмы. Составить план мероприятий по защите коммерческой тайны (в соответствии с законом РФ «О коммерческой тайне»). Указать перечень внутрифирменных документов, которые будут использоваться в целях правовой защиты секретов фирмы. Составить перечень сведений, составляющих коммерческую тайну фирмы. Описать методы конкурентной разведки, которые будут использоваться информационно-аналитической службой.

Тема 1.4. Задание 2. Обосновать необходимость проведения лицензирования выбранного вида деятельности. Указать порядок и необходимость (обязательная или добровольная) сертификации средств, используемых в выбранном виде деятельности. Указать перечень сертификационных документов, необходимых для выбранной деятельности фирмы. Составить для фирмы документы, необходимые для осуществления заданного вида деятельности.

ПРИЛОЖЕНИЕ 2

7. Оценочные средства для проведения промежуточной аттестации

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

Компетенция / Индикатор достижения компетенции	**Оценочные средства**
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	
ОПК-5.1 Применяет основные нормативные правовые акты в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальной информации	Теоретические вопросы 1. Основы законодательства Российской федерации в области информационной безопасности. 2. Понятие и виды защищаемой информации. 3. Основы международного законодательства в области защиты информации. 4. Понятие государственной тайны. Государственная тайна как особый вид защищаемой информации. Система защиты государственной тайны. 5. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. 6. Понятие лицензирования. Нормативные правовые акты Российской Федерации, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в области защиты информации. 7. Понятие сертификации. Нормативные правовые акты Российской Федерации и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации. 8. Регуляторы в области информационной безопасности. 9. Сущность организационных методов защиты информации. 10. Лицензионные требования ФСТЭК России на деятельность по технической защите конфиденциальной информации. 11. Лицензионные требования ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации.
ОПК-5.2 Применяет нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;	1. Определить регуляторы и мероприятия по контролю и надзору за деятельностью аккредитованных испытательных лабораторий и органов по сертификации средств защиты информации в системе сертификации средств защиты информации по требованиям безопасности информации.

Компетенция / Индикатор достижения компетенции	**Оценочные средства**
	2. Обосновать необходимость проведения лицензирования выбранного вида деятельности по защите информации. Указать порядок и необходимость (обязательная или добровольная) аккредитации выбранного вида деятельности по защите информации. 3. Подготовить инструкции по конфиденциальному делопроизводству выбранной организации. 4. Составить перечень нормативно правовых документов для обеспечения режима гос. тайны. 5. Составить перечень нормативно правовых документов для обеспечения режима конфиденциальности 6. Указать мероприятия, проводимые при создании системы защиты информации в корпоративной инфраструктуре. 7. Составьте перечень РД ФСТЭК, учитываемых при разработке «Политики безопасности» на промышленном предприятии. 8. Разработать требования к организации работы режимного помещения предприятия. 9. Написать регламент организации защиты информации при приеме посетителей, командированных лиц и иностранных представителей. 10. Написать инструкцию по защита информации в экстремальных ситуациях. 11. Разработать проект документа «Допуск должностных лиц к информации ограниченного доступа, не отнесенной к государственной тайне». 12. Разработать проект документа «Оценка соответствия помещения требованиям к помещениям и хранилищам, в которых ведутся закрытые работы.

Критерии оценки

– на оценку **«зачтено»** – обучающийся должен успешно пройти запланированные рубежные контроли и показать пороговый уровень знаний на уровне воспроизведения и объяснения информации;

– на оценку **«не зачтено»** – обучающийся не прошел запланированные рубежные контроли и не может показать знания на уровне воспроизведения и объяснения информации.