МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы магистратуры
по направлению подготовки
10.04.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Нормативно-правовое обеспечение информационной безопасности на транспорте

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины (модуля) является

- формирование компетенций по основным разделам теоретических и практических основ применения законодательных актов РФ при разработке и эксплуатации систем обеспечения информационной безопасности на транспорте.

Задачами дисциплины (модуля) являются:

- ознакомление с законодательными актами и нормативно-правовым обеспечением информационной безопасности на транспорте;
- изучение особенностей практического применения законодательных актов и нормативно-правового обеспечения информационной безопасности на транспорте.
- изучение технических и организационных методов практического применения законодательных актов и нормативно-правового обеспечения информационной безопасности на транспорте.
- изучение методов построения систем обеспечения информационной безопасности с учетом законодательных актов и нормативно-правового обеспечения.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-3 - Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

ПК-6 - Способность организовать работу по созданию, модернизации и сертификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

УК-6 - Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- основные законодательные акты и нормативно-правовое обеспечение информационной безопасности на транспорте;

- средства и технологии обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России .

Уметь:

- разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;
- организовать работу по созданию, модернизации и сертификации систем, средств и технологий обеспечения информационной безопасности.

Владеть:

- навыками разработки и оформления документов, регламентирующих деятельность служб обеспечения информационной безопасности предприятия;
- навыками проектирования политик информационной безопасности предприятия с учетом требований российского законодательства и ведомственных нормативно-правовых актов.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №4
Контактная работа при проведении учебных занятий (всего):	36	36
В том числе:		
Занятия лекционного типа	18	18
Занятия семинарского типа	18	18

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 108 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при

ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Информационная безопасность: сущность и содержание Рассматриваемые вопросы: -Информация как один из наиболее важных ресурсов современности. -Информационная безопасность в системе национальной безопасности. -Понятие информационной безопасности как состояния защищенности жизненно важных интересов личности, общества и государства в информационной сфере. - Разграничение понятий «информационная безопасность», «компьютерная безопасность» и «защита информации». -Правовой, организационный и программно-технический уровни обеспечения информационной безопасности. -Проблемы разработки и внедрения методов и средств обеспечения информационной безопасности в государственных организациях и коммерческих предприятиях России.
2	Государственная политика в сфере обеспечения информационной безопасности Рассматриваемые вопросы: -Понятие государственной политики в информационной сфере. -Основные положения государственной политики в сфере информационной безопасности. -Обеспечение равенства участников процесса информационного взаимодействия. - Совершенствование нормативно-правовой базы регулирования информационных отношений. - Контроль за соблюдением и исполнением законодательства в информационной сфере. -Развитие современных информационных и телекоммуникационных технологий как одна из приоритетных задач государственной политики в сфере информационной безопасности. -Государственная политика в сфере обеспечения информационной безопасности на транспорте. - Национальная Программа "Цифровая экономика Российской Федерации". -Национальные проекты в сфере цифровизации.
3	Основные задачи обеспечения информационной безопасности Рассматриваемые вопросы: -Обеспечение информационной безопасности как комплексная задача. -Создание системы органов, ответственных за информационную безопасность. -Разработка теоретико-методологической основы обеспечения безопасности информации. -Создание нормативно-правовой базы, регламентирующей решение всех задач обеспечения информационной безопасности. -Организация подготовки специалистов по защите информации. -Решение проблемы управления защитой информации и ее автоматизация. -Общие задачи обеспечения информационной безопасности. - Режим государственной, коммерческой, личной (семейной) тайны. -Частные задачи обеспечения информационной безопасности.

№ п/п	Тематика лекционных занятий / краткое содержание
	-Обеспечение безопасности функционирования информационных систем. -Разработка стратегии обеспечения информационной безопасности России. -Обоснование государственной политики в условиях глобализации информационных процессов, формирования геоинформационных сетей. -Разработка научно-практических основ формирования и проведения государственной политики в области обеспечения информационной безопасности. -Обоснование приоритетов национальной безопасности, соответствующих долговременных интересам общественного развития. -Реализация национальных проектов в сфере цифровизации в проекте Минтранса «Цифровой транспорт и логистика».
4	Основные законы, регламентирующие организационно-правовую базу в области информационной безопасности. Рассматриваемые вопросы: • Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и защите информации» • Федеральный закон № 152-ФЗ «О персональных данных». • Доктрина информационной безопасности Российской Федерации • Федеральный закон N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации". • Федеральный закон Российской Федерации N 98-ФЗ "О коммерческой тайне" -Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации. -Обладатель информации, его права и обязанности. -Конфиденциальность персональных данных. - Согласие субъекта персональных данных на обработку его персональных данных. -Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных. -Угрозы информационной безопасности РФ. - Угрозы информационному обеспечению государственной политики РФ. -Угрозы развитию отечественной индустрии информации. - Угрозы безопасности информационных и телекоммуникационных средств и систем. - Принципы Государственная политика обеспечения информационной безопасности. -Принципы обеспечения безопасности критической информационной инфраструктуры. - Полномочия Президента РФ и органов государственной власти РФ в области обеспечения безопасности критической информационной инфраструктуры. -Категорирование объектов критической информационной инфраструктуры. - Система безопасности значимого объекта критической информационной инфраструктуры
5	Основные задачи обеспечения информационной безопасности. Рассматриваемые вопросы: -Организационно-технические, экономические и правовые методы. -Этапы обеспечения ИБ на предприятии. Создание режима охраны информации; разработка правил взаимоотношений между сотрудниками; регламентация работы с документами; правила использования технических средств в рамках существующего правового поля РФ; аналитическая работа по оценке угроз информационной безопасности. -Обязанности руководства организации по обеспечению ИБ (ISO 27001)

№ п/п	Тематика лекционных занятий / краткое содержание
	-Создание нормативно-правовой базы, регламентирующей решение всех задач обеспечения информационной безопасности. -Организация подготовки специалистов по защите информации. -Решение проблемы управления защитой информации и ее автоматизации.
6	Угрозы информационной безопасности -Рассматриваемые вопросы: -Понятие угрозы информационной безопасности. Виды угроз информационной безопасности. -Информационное оружие и направления его применения. -Информационные войны. -Внешние и внутренние угрозы информационной безопасности. -Компьютерные сети и информационная безопасность. -Понятие и виды атак на компьютерную систему. -Классификация атак на компьютерную систему. -Вредоносные программы, их виды и направления применения -Понятие и виды антивирусного программного обеспечения. -Правовой, организационный и программно-технический способы нейтрализации угроз информационной безопасности. -Программно-Технические средства защиты информации А-утентификация и идентификация. - Организационные средства защиты информации. -Электронная подпись. -Простая, усиленная неквалифицированная, усиленная квалифицированная электронные подписи.
7	Формирование нормативно-правовой базы обеспечения информационной безопасности. Рассматриваемые вопросы: -Разработка нормативно-правовых и организационно-методических документов, регламентирующих деятельность органов государственной власти в области информационной безопасности; взаимоотношения субъектов информационной деятельности в части обеспечения информационной безопасности. -Государственная регламентация процессов функционирования и развития рынка средств информации, информационных продуктов и услуг. -Разработка концепции информационной безопасности. -Регулирование правового статуса субъектов системы информационной безопасности, пользователей информационных и телекоммуникационных систем. -Силы обеспечения информационной безопасности
8	Развитие современных методов обеспечения информационной безопасности Рассматриваемые вопросы: -Разработка методов комплексного исследования деятельности персонала информационных систем. - Разработка практических рекомендаций по сохранению и укреплению политической стабильности в обществе; обеспечению прав и свобод граждан; укреплению законности и правопорядка методами информационной безопасности. -Формирование подходов и способов обеспечения органов государственной власти и управления, граждан и их объединений достоверной, полной и своевременной информацией. -Выработка основных направлений деятельности по предотвращению негативных информационных воздействий на индивидуальное, групповое и общественное сознание.
9	ГОСТы РФ в области информационной безопасности Рассматриваемые вопросы: - ГОСТ Р 50922, ГОСТ Р 51275, ГОСТ Р ИСО/МЭК 15408, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 13335, ГОСТ Р ИСО/ТО 13569, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 18044, ГОСТ Р ИСО/МЭК 18045, ГОСТ Р ИСО/МЭК 19794, ГОСТ Р 50739, ГОСТ Р 51188, ГОСТ Р 51725.6, ГОСТ Р 51898, ГОСТ Р 52069, ГОСТ Р 52447, ГОСТ 28147, ГОСТ Р 34.10,

№ п/п	Тематика лекционных занятий / краткое содержание
	ГОСТ Р 34.11 - Стандарты в области ИБ организаций банковской системы РФ: СТО БР ИББС-1.0/1.1, РС БР ИББС-2.0/2.1/2.2 - ГОСТы серии ГОСТ Р ИСО/МЭК 2700 «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности».

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Защита персональных данных. ФЗ №152 и ГОСТы РФ В результате выполнения практического задания студент получает навыки в применении организационно-правовых методов защиты персональных данных.
2	Способы защиты коммерческой тайны. ФЗ №98 и ГОСТы РФ В результате выполнения практического задания студент получает навыки в применении организационно-правовых методов защиты коммерческой тайны.
3	Методы и средства защиты информации. Российские и международные стандарты В результате выполнения практического задания студент получает навыки в применении методов и средств защиты информации.
4	Организация службы информационной безопасности на предприятии В результате выполнения практического задания студент получает навыки в организации и реорганизации службы информационной безопасности на предприятии.
5	Организационные каналы утечки конфиденциальной информации В результате выполнения практического задания студент получает навыки в определении и классификации организационных каналов утечки конфиденциальной информации.
6	Оценка угроз безопасности информации В результате выполнения практического задания студент получает навыки в оценке угроз безопасности информации в соответствии с методикой ФСТЭК.
7	Стандартизация и сертификация систем искусственного интеллекта В результате выполнения практического задания студент получает навыки внедрения требований ГОСТов в разрабатываемые или эксплуатируемые системы искусственного интеллекта.
8	Стандартизация кибербезопасности вычислительного комплекса В результате выполнения практического задания студент получает навыки разработки методов и средств обеспечения кибербезопасности вычислительного комплекса в соответствии с требованиями ГОСТов.
9	Система контроля и управления доступом (СКУД): задачи и методы проектирования В результате выполнения практического задания студент получает навыки разработки систем контроля и управления доступом (СКУД) на предприятие.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	1 Работа с лекционным материалом 2 Подготовка к практическим занятиям 3 Изучение вопросов для самостоятельной дополнительной проработки

2	Подготовка к промежуточной аттестации.
3	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Диогенес Ю., Озкайя Э. Кибербезопасность. Стратегия атак и обороны. Издательство "ДМК Пресс", 2020 - 326с. – ISBN 978-5-97060-709-1	https://e.lanbook.com/book/131717 (дата обращения: 19.04.2024).- Текст электронный.
2	Мосолов А. С., Акинин Н. И. Компьютерные технологии и методы проектирования в сфере безопасности. Издательство "Лань", 2021 - 444с. – ISBN 978-5-8114-8034-0	https://e.lanbook.com/book/183115 (дата обращения: 19.04.2024).- Текст электронный.
3	Петров А. А., Компьютерная безопасность. Криптографические методы защиты. Издательство "ДМК Пресс", 2008 - 448с. – ISBN 5-89818-064-8	https://e.lanbook.com/book/3027 (дата обращения: 19.04.2024).- Текст электронный.
4	Краковский Ю. М., Методы защиты информации. Издательство "Лань", 2021 - 236с. – ISBN 978-5-8114-5632-1	https://e.lanbook.com/book/156401 (дата обращения: 19.04.2024).- Текст электронный.
5	Тумбинская М.В., Петровский М.В. Защита информации на предприятии: учебное пособие. Издательство "Лань", 2020 - 184с. – ISBN 978-5-8114-4291-1	https://e.lanbook.com/book/130184 (дата обращения: 19.04.2024).- Текст электронный.
6	Прохорова О. В., Информационная безопасность и защита информации. Издательство "Лань", 2022 - 124с. – ISBN 978-5-8114-8924-4	https://e.lanbook.com/book/185333 (дата обращения: 19.04.2024).- Текст электронный.
7	Никифоров С. Н., Методы защиты информации. Защищенные сети, 2021 - 96с. – ISBN 978-5-8114-7907-8	https://e.lanbook.com/book/167186 (дата обращения: 19.04.2024).- Текст электронный.
8	Ермакова А.Ю., Методы и средства защиты компьютерной информации: учебное пособие. МИРЭА - Российский технологический университет, 2020.-223с	https://e.lanbook.com/book/163844 (дата обращения: 19.04.2024).- Текст электронный.
9	Пугин В. В., Голубничая Е. Ю., Лабада С. А. Защита информации в компьютерных информационных системах: учебное пособие. Поволжский государственный университет телекоммуникаций и информатики, 2018.-119с	https://e.lanbook.com/book/182299 (дата обращения: 19.04.2024).- Текст электронный.
10	Леонтьев А. С., Защита информации: учебное пособие. МИРЭА - Российский технологический университет 2021.-79с	https://e.lanbook.com/book/182491 (дата обращения: 19.04.2024).- Текст электронный.

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

- Официальный сайт РУТ (МИИТ) https://www.miit.ru/
- Образовательная платформа «Юрайт» https://urait.ru/
- ЭБС ibooks.ru http://ibooks.ru/
- ЭБС "Лань" https://e.lanbook.com/book/

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

- Microsoft Windows
- Microsoft Office

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Экзамен в 4 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

доцент, доцент, к.н. кафедры
«Вычислительные системы, сети и
информационная безопасность» С.В. Малинский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова