

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ))



Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором ФГАОУ ВО
РУТ (МИИТ) Тимониним В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

**Организационное и правовое обеспечение информационной
безопасности**

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей
(в сфере связи, информационных и
коммуникационных технологий)

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде
электронного документа выгружена из единой
корпоративной информационной системы управления
университетом и соответствует оригиналу

Простая электронная подпись, выданная ФГАОУ ВО РУТ
(МИИТ)

ID подписи: 4196

Подписал: заведующий кафедрой Желенков Борис
Владимирович

Дата: 01.09.2026

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.

Задачами дисциплины (модуля) являются:

- ознакомление с законодательными актами и нормативно-правовым обеспечением информационной безопасности;
- изучение особенностей практического применения законодательных актов и нормативно-правового обеспечения информационной безопасности;
- изучение технических и организационных методов практического применения законодательных актов и нормативно-правового обеспечения информационной безопасности;
- 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-4 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

ПК-4 - Способность применять аналитические и правовые подходы в расследовании компьютерных инцидентов.

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

Знать:

- основные законодательные акты и нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;
- средства и технологии обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России.

Уметь:

- применять на практике нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

- организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Владеть:

- навыками применения на практике нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации;

- навыками организации технологических процессов, регламентирующих защиту информации в сфере профессиональной деятельности, в соответствии с нормативными правовыми актами, нормативными и методическими документами.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 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 №7
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	16	16

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 60 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 законодательства в информационной сфере; -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; -Разработка стратегии обеспечения информационной безопасности России.
4	Основные законы, регламентирующие организационно-правовую базу в области информационной безопасности

№ п/п	Тематика лекционных занятий / краткое содержание
	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"
5	Основные законы, регламентирующие организационно-правовую базу в области информационной безопасности(продолжение) Рассматриваемые вопросы: -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 развитию отечественной индустрии информации; -Принципы обеспечения безопасности критической информационной инфраструктуры; -Категорирование объектов критической информационной инфраструктуры;
6	Основные задачи обеспечения информационной безопасности. Организационно-технические, экономические и правовые методы Рассматриваемые вопросы: -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) -Создание нормативно-правовой базы, регламентирующей решение всех задач обеспечения информационной безопасности.
7	Угрозы информационной безопасности Рассматриваемые вопросы: -Понятие угрозы информационной безопасности; -Виды угроз информационной безопасности; -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;
8	Угрозы информационной безопасности(продолжение) Рассматриваемые вопросы: -Понятие угрозы информационной безопасности; -Виды угроз информационной безопасности; -Внешние и внутренние угрозы информационной безопасности; -Компьютерные сети и информационная безопасность;

№ п/п	Тематика лекционных занятий / краткое содержание
9	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.
10	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.
11	Стандартизация в области информационной безопасности Рассматриваемые вопросы: -Проблема стандартизации в области информационной безопасности в международных и национальных стандартах; -ГОСТы серии 27000; -Стандартизация терминологии в ISO/IEC 27000; -Стандартизация базовых требований в ISO/IEC 27001/27002; -Стандартизация порядка внедрения СМИБ в ISO/IEC 27003;
12	Стандартизация в области информационной(продолжение) Рассматриваемые вопросы: -Стандартизация основных процессов в ISO/IEC 27004/27005/27007/27008; -Стандартизация корпоративного управления СМИБ в ISO/IEC 27014/27016; -Стандартизация кибербезопасности в ISO/IEC 27103.
13	Стандартизация и сертификация в области защиты информации Рассматриваемые вопросы: -Система ГОСТов в области защиты информации: ГОСТ Р 52069;0-2013; -Общие технические требования к защите от несанкционированного доступа к информации в ГОСТ Р 50739; -Основные требования и определения в ГОСТ Р 50922; -Порядок создания автоматизированных систем в защищенном исполнении в ГОСТ Р 51583; -Стандартизация номенклатуры качества защиты информации в ГОСТ Р 52447; -Стандартизация требований к средствам высоконадежной биометрической аутентификации в ГОСТ Р 52633.
14	Стандартизация и сертификация в условиях цифровой информации Рассматриваемые вопросы: -Национальная Программа "Цифровая экономика Российской Федерации" и ее Федеральные проекты «Цифровое государственное управление», «Цифровые технологии», «Информационная безопасность», «Кадры для цифровой экономики», «Информационная инфраструктура», «Нормативное регулирование цифровой среды», «Искусственный интеллект», «Развитие кадрового потенциала ИТ-отрасли», «Обеспечение доступа в Интернет за счет развития спутниковой связи»; -Проблемы стандартизации и сертификации в Федеральных проектах.

№ п/п	Тематика лекционных занятий / краткое содержание
15	Стандартизация и сертификация систем искусственного интеллекта Рассматриваемые вопросы: -Федеральный проект «Искусственный интеллект» и проблемы стандартизации и сертификации; -Стандартизация и унификация представления правовой информации для цифровой платформы «Государственная система правовой информации»; -ПНСТ «Умное производство»; -Двойники цифровые производства» (части 1-4); -ПНСТ «Информационные технологии»; -Умный город; -Функциональная совместимость»; -ПНСТ «Информационные технологии»; -Умный город; -Руководства по обмену и совместному использованию данных; - ПНСТ «Информационные технологии»; -Интернет вещей; Протокол обмена для высокоскоростных сетей с большим радиусом действия и низким энергопотреблением».
16	Проблемы повышения эффективности обеспечения информационной безопасности на современном этапе Рассматриваемые вопросы: -Обеспечение согласованности решений органов, ответственных за реализацию государственной политики в сфере обеспечения информационной безопасности в рамках единого информационного пространства; -Политика протекционизма, направленная на поддержку деятельности отечественных производителей средств информатизации и защиты информации; -Защита внутреннего рынка от проникновения некачественных средств информатизации и информационных продуктов.

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.

№ п/п	Тематика практических занятий/краткое содержание
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.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к практическим занятиям
3	Подготовка к тестированию
4	Подготовка к промежуточной аттестации.
5	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: 28.05.2026).- Текст электронный.
2	Ермакова А.Ю. Методы и средства защиты компьютерной информации: учебное пособие. МИРЭА - Российский технологический университет, 2020.-223с,ISBN 978-5-8114-8034-0	https://e.lanbook.com/book/163844
3	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: 28.05.2026).- 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: 28.05.2026).- Текст электронный
5	Тумбинская М.В., Петровский М.В. Защита информации на предприятии: учебное пособие.	https://e.lanbook.com/book/130184 (дата обращения: 28.05.2026).- Текст электронный

	Издательство "Лань", 2020 - 184с. – ISBN 978-5-8114-4291-1	
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: 28.05.2026).- 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: 28.05.2026).- Текст электронный.
8	Путин 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
9	Леонтьев А. С. Защита информации: учебное пособие. МИРЭА - Российский технологический университет 2021.-79с	https://e.lanbook.com/book/182491

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).

Учебная аудитория для проведения учебных занятий (занятий лекционного типа, лабораторных работ):

- компьютер преподавателя, рабочие станции студентов, мультимедийное оборудование, доска.

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Зачет в 7 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 и
квантовые коммуникации»

С.В. Малинский

Согласовано:

Заведующий кафедрой ВССиИБ

Б.В. Желенков

Председатель учебно-методической
комиссии

Н.А. Андриянова