

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
23.05.04 Эксплуатация железных дорог,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная и кибербезопасность

Специальность: 23.05.04 Эксплуатация железных дорог

Специализация: Цифровые технологии управления
транспортными процессами

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 РУТ (МИИТ)
ID подписи: 4196
Подписал: заведующий кафедрой Желенков Борис
Владимирович
Дата: 16.06.2026

1. Общие сведения о дисциплине (модуле).

Целью освоения дисциплины является формирование у обучающихся систематизированных теоретических и практических знаний в области основ кибербезопасности цифровых технологий и цифровой трансформации экономики, применения методов и средств защиты информации в корпоративных информационных системах, системах распознавания образов, машинного обучения, имитационного моделирования, Интернета вещей, в логических нейронных сетях для систем распознавания, управления и принятия решений.

Задачами освоения дисциплины являются:

- Формирование у обучающихся знаний и навыков в области разработки методов и средств кибербезопасности при реализации технологических решений в области цифровизации управленческой и производственной деятельности компании, современного электронного документооборота и архивирования;

- Формирование у обучающихся знаний и навыков в области разработки методов и средств кибербезопасности при реализации технологических решений в области современных систем принятия решений, имитационного моделирования систем и процессов;

- Формирование знаний об организации и управлении кибербезопасностью при цифровизации внутренних процессов компании (предоставление услуг, операционная деятельность и пр.), внедрении решений в области современных цифровых технологий;

- Формирование знаний об организации и управлении кибербезопасностью деятельности подразделений, использующих современные цифровые технологии в области управления, связи, информационного обеспечения.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-20 - Способен использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности с учётом требований информационной безопасности.

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

Знать:

- основные методы и средства обеспечения информационной и кибербезопасности информационных технологий и систем в условиях цифровой трансформации

Уметь:

- организовывать и управлять средствами обеспечения информационной и кибербезопасности при цифровизации внутренних процессов компании (предоставление услуг, операционная деятельность и пр.), внедрении решений в области современных цифровых технологий.

Владеть:

- навыками практической организации и управления средствами обеспечения кибербезопасности при цифровизации внутренних процессов компании (предоставление услуг, операционная деятельность и пр.), внедрении решений в области современных цифровых технологий.

3. Объем дисциплины (модуля).**3.1. Общая трудоемкость дисциплины (модуля).**

Общая трудоемкость дисциплины (модуля) составляет 2 з.е. (72 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 №8
Контактная работа при проведении учебных занятий (всего):	28	28
В том числе:		
Занятия лекционного типа	14	14
Занятия семинарского типа	14	14

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 44 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	<p>Цифровизация и цифровая трансформация экономики</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - концепции, цели и задачи; - цифровизация внутренних процессов компании (предоставление услуг, операционная деятельность, управление бизнес-процессами); - корпоративные информационные системы; - цифровые технологии как инструмент решения задач цифровой трансформации; - цифровые бизнес-процессы и цифровая культура; - прогресс и проблемы безопасности; - национальная программа «Цифровая экономика Российской Федерации 2024»; - проблемы информационной, компьютерной и кибербезопасности; - правовые основы информационной безопасности.
2	<p>Информационная и кибербезопасность в цифровых технологиях и цифровой трансформации</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - интернет, мобильная связь, облака и облачные вычисления, дистанционное обучение, виртуальная и дополненная реальность, искусственный интеллект и машинное обучение, цифровой маркетинг; - интернет вещей; - цифровые трансформации и мировоззрение; - проблемы цифровизации, культуры, образования и безопасности; - человеческий фактор и проблемы информационной и кибербезопасности; - вирусы и программы-вымогатели; - основные тенденции информационной и кибербезопасности; - основные правила компьютерной «гигиены»: пароли и их обновление, отношение к непонятным ссылкам, работа в социальных сетях.
3	<p>Информационная и кибербезопасность в корпоративных информационных системах.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - цифровые технологии и трансформации в задачах управления финансами, персоналом, отношениями с поставщиками, транспортной деятельностью предприятия; - преимущества и выгоды, предоставляемые корпоративными информационными системами (КИС); - проблемы компьютерной и информационной безопасности в КИС;: - требования к защите информации, не составляющей государственной тайны, содержащейся в государственных информационных системах (Требования ФСТЭК России); - защита передаваемых электронных данных;

№ п/п	Тематика лекционных занятий / краткое содержание
	- электронная подпись; - классы безопасности электронных систем. - криптография и стеганография и их применение.
4	Технологические и системные проблемы информационной и кибербезопасности Рассматриваемые вопросы: - цифровые технологии и проблемы уязвимости; - проблемы компьютерной и информационной безопасности в цифровой экономике; - комплексное решение проблемы информационной безопасности: защита Интернета, компьютеров, данных, телекоммуникационной инфраструктуры, канала передачи данных, удостоверений, основных услуг, приложений. - организационные методы решения проблем информационной и кибербезопасности - правовые методы решения проблем информационной и кибербезопасности

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Законодательно-правовые методы обеспечения кибербезопасности технологических решений В результате выполнения работы на практическом занятии студенты ознакомятся с нормативно-правовой базой обеспечения кибербезопасности технологических решений и ее применением
2	Нормативная база ФСТЭК для обеспечения информационной и кибербезопасности технологических решений В результате выполнения работы на практическом занятии студенты ознакомятся с нормативными документами ФСТЭК для обеспечения кибербезопасности технологических решений
3	Кибербезопасность в корпоративных информационных системах. В результате выполнения работы на практическом занятии студенты изучат технологические решения обеспечения кибербезопасности в корпоративных информационных системах и их применение (защита передаваемых электронных данных; электронная подпись и ее применение; классы безопасности электронных систем).
4	Организация системы менеджмента информационной безопасности (СМИБ) В результате выполнения работы на практическом занятии студенты получают навыки в разработке и организации СМИБ для современных цифровых технологий в области управления, связи, информационного обеспечения.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к практическим занятиям
3	Подготовка к промежуточной аттестации.

4.4. Примерный перечень тем курсовых работ

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: 03.02.2026).- Текст электронный.
2	Нефедов В.С. Безопасность прикладных информационных технологий и систем: учебное пособие. МИРЭА - Российский технологический университет, 2025 - 113с. – ISBN 978-5-7339-2570-7	https://e.lanbook.com/book/504831 (дата обращения: 03.02.2026).- Текст электронный.
3	Лозовецкий В. В., Комаров Е. Г., Лебедев В.В. Защита автоматизированных систем обработки информации и телекоммуникационных сетей: Учебное пособие для вузов. Издательство "Лань", 2024 - 488с. – ISBN 978-5-507-47615-2	https://e.lanbook.com/book/397355 (дата обращения: 03.02.2026).- Текст электронный.
4	Тумбинская М.В., Петровский М.В. Защита информации на предприятии: Учебное пособие для вузов. Издательство "Лань", 2025 - 184с. – ISBN 978-5-507-52967-4	https://e.lanbook.com/book/463043 (дата обращения: 03.02.2026).- Текст электронный.
5	Краковский Ю. М. Методы защиты информации. Издательство "Лань", 2025 - 272с. – ISBN 978-5-507-52958-2	https://e.lanbook.com/book/463013 (дата обращения: 03.02.2026).- Текст электронный.
6	Баланов А.Н. Защита информационных систем. Кибербезопасность: Учебное пособие для вузов. Издательство "Лань", 2025 - 280с. – ISBN 978-5-507-50467-1	https://e.lanbook.com/book/438971 (дата обращения: 03.02.2026).- Текст электронный.
7	Вавилин Я.А., Солдатов В.Г., Манкевич И.Г. Информационные технологии в управлении качеством и защита информации: Учебное пособие для вузов. Издательство "Лань", 2025 - 196с. – ISBN 978-5-507-51437-3	https://e.lanbook.com/book/447242 (дата обращения: 03.02.2026).- Текст электронный.
8	Богатенков С. А., Гельруд Я.Д. Проектирование системы обеспечения безопасности профессиональной деятельности в информационном обществе: Учебное пособие для вузов. Издательство "Лань", 2025 – 152с. – ISBN 978-5-507-53215-5	https://e.lanbook.com/book/506690 (дата обращения: 03.02.2026).- 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).

Для проведения аудиторных занятий и самостоятельной работы требуется:

1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET
2. Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.
3. Компьютерный класс с кондиционером. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET
4. Для проведения практических занятий: компьютерный класс; кондиционер; компьютеры.

9. Форма промежуточной аттестации:

Зачет в 8 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 ЦТУТП

В.Е. Нутович

Заведующий кафедрой ВССиИБ

Б.В. Желенков

Председатель учебно-методической
комиссии

Н.А. Андриянова