

**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 - программа специалитета  
по специальности  
23.05.04 Эксплуатация железных дорог,  
утвержденной первым проректором ФГАОУ ВО  
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: Заочная

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 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 №15 |
| Контактная работа при проведении учебных занятий (всего): | 16               | 16          |
| В том числе:                                              |                  |             |
| Занятия лекционного типа                                  | 8                | 8           |
| Занятия семинарского типа                                 | 8                | 8           |

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 56 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.

| №<br>п/п | Тематика лекционных занятий / краткое содержание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | <p><b>Цифровизация и цифровая трансформация экономики</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- концепции, цели и задачи;</li> <li>- цифровизация внутренних процессов компании (предоставление услуг, операционная деятельность, управление бизнес-процессами);</li> <li>- корпоративные информационные системы;</li> <li>- цифровые технологии как инструмент решения задач цифровой трансформации;</li> <li>- цифровые бизнес-процессы и цифровая культура;</li> <li>- прогресс и проблемы безопасности;</li> <li>- национальная программа «Цифровая экономика Российской Федерации 2024»;</li> <li>- проблемы информационной, компьютерной и кибербезопасности;</li> <li>- правовые основы информационной безопасности.</li> </ul>                                                                                       |
| 2        | <p><b>Информационная и кибербезопасность в цифровых технологиях и цифровой трансформации</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- интернет, мобильная связь, облака и облачные вычисления, дистанционное обучение, виртуальная и дополненная реальность, искусственный интеллект и машинное обучение, цифровой маркетинг;</li> <li>- интернет вещей;</li> <li>- цифровые трансформации и мировоззрение;</li> <li>- проблемы цифровизации, культуры, образования и безопасности;</li> <li>- человеческий фактор и проблемы информационной и кибербезопасности;</li> <li>- вирусы и программы-вымогатели;</li> <li>- основные тенденции информационной и кибербезопасности;</li> <li>- основные правила компьютерной «гигиены»: пароли и их обновление, отношение к непонятным ссылкам, работа в социальных сетях.</li> </ul> |
| 3        | <p><b>Информационная и кибербезопасность в корпоративных информационных системах.</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- цифровые технологии и трансформации в задачах управления финансами, персоналом, отношениями с поставщиками, транспортной деятельностью предприятия;</li> <li>- преимущества и выгоды, предоставляемые корпоративными информационными системами (КИС);</li> <li>- проблемы компьютерной и информационной безопасности в КИС;;</li> <li>- требования к защите информации, не составляющей государственной тайны, содержащейся в государственных информационных системах (Требования ФСТЭК России);</li> <li>- защита передаваемых электронных данных;</li> </ul>                                                                                                                                   |

| №<br>п/п | Тематика лекционных занятий / краткое содержание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <ul style="list-style-type: none"> <li>- электронная подпись;</li> <li>- классы безопасности электронных систем.</li> <li>- криптография и стеганография и их применение.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 4        | <b>Технологические и системные проблемы информационной и кибербезопасности</b><br>Рассматриваемые вопросы: <ul style="list-style-type: none"> <li>- цифровые технологии и проблемы уязвимости;</li> <li>- проблемы компьютерной и информационной безопасности в цифровой экономике;</li> <li>- комплексное решение проблемы информационной безопасности: защита Интернета, компьютеров, данных, телекоммуникационной инфраструктуры, канала передачи данных, удостоверений, основных услуг, приложений.</li> <li>- организационные методы решения проблем информационной и кибербезопасности</li> <li>- правовые методы решения проблем информационной и кибербезопасности</li> </ul> |

#### 4.2. Занятия семинарского типа.

##### Практические занятия

| №<br>п/п | Тематика практических занятий/краткое содержание                                                                                                                                                                                                                                                                                                                                 |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | <b>Законодательно-правовые методы обеспечения кибербезопасности технологических решений</b><br>В результате выполнения работы на практическом занятии студенты ознакомятся с нормативно-правовой базой обеспечения кибербезопасности технологических решений и ее применением                                                                                                    |
| 2        | <b>Нормативная база ФСТЭК для обеспечения информационной и кибербезопасности технологических решений</b><br>В результате выполнения работы на практическом занятии студенты ознакомятся с нормативными документами ФСТЭК для обеспечения кибербезопасности технологических решений                                                                                               |
| 3        | <b>Кибербезопасность в корпоративных информационных системах.</b><br>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        | <b>Организация системы менеджмента информационной безопасности (СМИБ)</b><br>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.

| №<br>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 проектов

Курсовой проект на тему "Организационные и программно-аппаратные методы обеспечения кибербезопасности технологических решений" состоит в разработке методики обеспечения кибербезопасности технологического решения, разрабатываемого каждым обучающимся в рамках своей диссертационной работы. В соответствии с учебным планом работа выполняется вне сетки расписания учебных занятий. Индивидуальными заданиями предусмотрена разработка комплекса мер, обеспечивающих кибербезопасность конкретного технологического решения:

- идентификация и аутентификация пользователей,
- меры антивирусной защиты, обеспечения сохранности программ и данных,
- управления идентификаторами,
- разделение полномочий между пользователями и лицами, обеспечивающими функционирование технологического решения,
- ограничение неуспешных попыток входа в систему,
- реализация защищенного удаленного доступа,
- управление инсталляцией компонентов ПО,
- контроль установки обновлений ПО,
- управление доступом к машинным носителям информации,
- уничтожение (стирание) информации на машинных носителях при их передаче между пользователями или в сторонние организации,
- определение событий безопасности, подлежащих регистрации, и сроков их хранения
- защита информации о событиях безопасности
- резервирование технических средств, ПО, каналов передачи информации
- защита технических средств от внешних воздействий.

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 | <a href="https://e.lanbook.com/book/131717">https://e.lanbook.com/book/131717</a><br>(дата обращения: 19.06.2024).-<br>Текст электронный. |
| 2     | Сэрра Э. Кибербезопасность: правила игры. Как руководители и сотрудники влияют на культуру                                          | <a href="https://e.lanbook.com/book/213989">https://e.lanbook.com/book/213989</a><br>(дата обращения: 19.06.2024).-<br>Текст электронный. |

|   |                                                                                                                                                              |                                                                                                                                           |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
|   | безопасности в компании. Издательство "Альпина Паблишер", 2022 - 192с. – ISBN 978-5-907534-38-4                                                              |                                                                                                                                           |
| 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 | <a href="https://e.lanbook.com/book/183115">https://e.lanbook.com/book/183115</a><br>(дата обращения: 19.06.2024).-<br>Текст электронный. |
| 4 | Петров А. А. Компьютерная безопасность. Криптографические методы защиты. Издательство "ДМК Пресс", 2008 - 448с. – ISBN 5-89818-064-8                         | <a href="https://e.lanbook.com/book/3027">https://e.lanbook.com/book/3027</a><br>(дата обращения: 19.06.2024).-<br>Текст электронный.     |
| 5 | Краковский Ю. М. Методы защиты информации. Издательство "Лань", 2021 - 236с. – ISBN 978-5-8114-5632-1                                                        | <a href="https://e.lanbook.com/book/156401">https://e.lanbook.com/book/156401</a><br>(дата обращения: 19.06.2024).-<br>Текст электронный. |
| 6 | Тумбинская М.В., Петровский М.В. Защита информации на предприятии: учебное пособие. Издательство "Лань", 2020 - 184с. – ISBN 978-5-8114-4291-1               | <a href="https://e.lanbook.com/book/130184">https://e.lanbook.com/book/130184</a><br>(дата обращения: 19.06.2024).-<br>Текст электронный. |
| 7 | Прохорова О. В. Информационная безопасность и защита информации. Издательство "Лань", 2022 - 124с. – ISBN 978-5-8114-8924-4                                  | <a href="https://e.lanbook.com/book/185333">https://e.lanbook.com/book/185333</a><br>(дата обращения: 19.06.2024).-<br>Текст электронный. |
| 8 | Никифоров С. Н. Методы защиты информации. Защищенные сети, 2021 - 96с. – ISBN 978-5-8114-7907-8                                                              | <a href="https://e.lanbook.com/book/167186">https://e.lanbook.com/book/167186</a><br>(дата обращения: 19.06.2024).-<br>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 с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

9. Форма промежуточной аттестации:

Зачет в 15 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 ЦТУТП

В.Е. Нутович

Заведующий кафедрой ВССиИБ

Б.В. Желенков

Председатель учебно-методической  
комиссии

Н.А. Андриянова