МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
специализированного высшего образования
по направлению подготовки
23.04.01 Технология транспортных процессов,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Кибербезопасность технологий в условиях цифровой трансформации

Направление подготовки: 23.04.01 Технология транспортных процессов

Направленность (профиль): Цифровые транспортно-логистические системы

Форма обучения: Очная

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.

Основными задачами 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-2 - Способен оперативно выбирать методы и инструменты управления выявленными логистическими рисками.

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

Знать:

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

Уметь:

- самостоятельно разрабатывать программы и планы для обеспечения кибербезопасности современных технологических решений и информационных систем в соответствии с требованиями российского законодательства и нормативной документации;
- организовывать и управлять средствами обеспечения кибербезопасности при цифровизации внутренних процессов компании (предоставление услуг, операционная деятельность и пр.), внедрении решений в области современных цифровых технологий.

Владеть:

- навыками разработки программ, планов, организационно-распорядительной документации для практического обеспечения требований к кибербезопасности технологических решений и информационных систем в соответствии с требованиями российского законодательства и нормативной документации;
- 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 5 з.е. (180 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 №3
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	32	32

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 132 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	Цифровизация и цифровая трансформация экономики Рассматриваемые вопросы: - концепции, цели и задачи цифровой трансформации экономики; цифровизация внутренних процессов компании (предоставление услуг, - операционная деятельность, управление бизнес-процессами); - корпоративные информационные системы и их кибербезопасность; - 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	Кибербезопасность в цифровых технологиях и цифровой трансформации Рассматриваемые вопросы: - интернет, мобильная связь, облака и облачные вычисления, дистанционное обучение, виртуальная и дополненная реальность, искусственный интеллект и машинное обучение, цифровой маркетинг; - интернет вещей и проблемы кибербезопасности; цифровые трансформации и мировоззрение; - проблемы цифровизации, культуры, образования и безопасности; человеческий фактор и проблемы кибербезопасности; - вирусы и программы-вымогатели, современные тенденции в киберпреступности; основные правила компьютерной «гигиены»: - пароли и их обновление, отношение к непонятным ссылкам, фишингу, работа в социальных сетях.
3	Кибербезопасность в корпоративных информационных системах Рассматриваемые вопросы: - цифровые технологии и трансформации в задачах управления финансами, персоналом, отношениями с поставщиками, транспортной деятельностью предприятия; - преимущества и выгоды, предоставляемые корпоративными информационными системами (КИС);

№ п/п	Тематика лекционных занятий / краткое содержание
	- 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; электронная подпись и ее применение; классы безопасности электронных систем.
4	Кибербезопасность в системах искусственного интеллекта (СИИ) и машинного обучения Рассматриваемые вопросы: - цифровой мир и его многообразие; разработка интеллектуальных систем и проблемы кибербезопасности; основные подсистемы интеллектуальных систем и их уязвимости; признаковое пространство и его метрики; - решающие правила и методы их построения, проблемы помехозащищенности; - основные проблемы в обеспечении кибербезопасности СИИ, защита целостности, доступности и конфиденциальности; - методы и средства защиты информации; - классификация методов защиты информации: управление, препятствие, маскировка, регламентация, принуждение, убеждение; - классификация средств защиты информации: физические, аппаратные, программные, организационные, законодательные, морально-этические (психологичестие).
5	Кибербезопасность в нейронных логических сетях Рассматриваемые вопросы: - цифровизация и нейронные логические сети; проблема моделирования работы мозга и принятия решений; - персептрон и его применение в цифровых технологиях; - обучение персептронов и проблемы помехоустойчивости; - применение нейронных логических сетей в технике, экономике, управлении и проблемы обеспечения кибербезопасности ; - кибербезопасность в нейронных логических сетях; идентификация, аутентификация и авторизация и их роль в задачах обеспечения кибербезопасности; - методы аутентификации: пароли, электронные карточки, биометрические параметры, координаты, многофакторная аутентификация; - идентификаторы доступа: механические, магнитные, оптические, электронные контактные, электронные радиочастотные, акустические, биометрические, комбинированные и их применение.
6	Кибербезопасность в системах виртуальной и дополненной реальности Рассматриваемые вопросы: - многообразие мира и методов его цифровизации и трансформации; виртуальный мир и его особенности; - виртуальная реальность и задачи математического и имитационного моделирования; - имитационное моделирование транспортных процессов и систем и проблемы кибербезопасности; - дополненная реальность, ее перспективы в задачах цифровизации и проблемы кибербезопасности; - виртуальная реальность в обучении, управлении и экономике и проблемы кибербезопасности; - методы и средства обеспечения кибербезопасности в системах виртуальной и дополненной реальности; - криптография и стеганография и их применение; - симметричное и асимметричное шифрование и их применение; - асимметричное шифрование открытым и закрытым ключами; - криптографическое ПО, алгоритмы и стандарты и их применение для обеспечения кибербезопасности в цифровых технологиях.
7	Кибербезопасность в социальных сетях и цифровом маркетинге Рассматриваемые вопросы: - социальные сети и их «жители», проблемы информационной и кибербезопасности;

№ п/п	Тематика лекционных занятий / краткое содержание
	- проблемы сбора, хранения и обработки больших данных и их решение, проблемы кибербезопасности; - цифровой маркетинг в социальных сетях и проблемы манипуляции мнением человека; - виртуальный мир и управление его трансформацией, угрозы, уязвимости и проблемы кибербезопасности; - компьютерные вредоносные программы и методы защиты от них; - способы распространения компьютерных вредоносных программ, - проблемы лояльности сотрудников и их влияние на кибербезопасность; - классификация компьютерных вредоносных программ, история развития и применения в компьютерных сетях; - макровирусы; - защита от компьютерных вредоносных программ: профилактика, диагностика, лечение. Антивирусные программы.
8	Технологические и системные проблемы кибербезопасности Рассматриваемые вопросы: - цифровые технологии и проблемы уязвимости; - проблемы компьютерной и информационной безопасности в цифровой экономике, угрозы и уязвимости, возможные атаки и их последствия; - комплексное решение проблемы кибербезопасности: защита Интернета, компьютеров, данных, телекоммуникационной инфраструктуры, канала передачи данных, удостоверений, основных услуг, приложений.

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 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 (часть 1). В результате выполнения работы на практическом занятии студенты изучат административные (организационные) методы обеспечения кибербезопасности цифровых технологий в задачах управления транспортной деятельности предприятия.
4	Кибербезопасность в корпоративных информационных системах (часть 2). 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).
5	Организация системы менеджмента информационной безопасности (СМИБ) В результате выполнения работы на практическом занятии студенты получат навыки в разработке и организации СМИБ для современных цифровых технологии в области управления, связи, информационного обеспечения.

№ п/п	Тематика практических занятий/краткое содержание
6	Кибербезопасность в системах искусственного интеллекта (СИИ) и машинного обучения (часть 1). В результате выполнения работы на практическом занятии студенты изучат и получат навыки в применении программно- технических методов обеспечения кибербезопасности (методы и средства защиты информации; классификация методов защиты информации).
7	Кибербезопасность в системах искусственного интеллекта (СИИ) и машинного обучения (часть 2). В результате выполнения работы на практическом занятии студенты изучат и получат навыки в применении технологических решений для обеспечения кибербезопасности (защита целостности, доступности и конфиденциальности).
8	Кибербезопасность в нейронных логических сетях (часть 1). В результате выполнения работы на практическом занятии студенты изучат и получат навыки в применении криптографических методов обеспечения кибербезопасности.
9	Кибербезопасность в нейронных логических сетях (часть 2). В результате выполнения работы на практическом занятии студенты изучат и получат навыки в применении методов идентификации, аутентификации и авторизации.
10	Кибербезопасность в системах виртуальной и дополненной реальности (часть 1). В результате выполнения работы на практическом занятии студенты изучат и получат навыки в применении стеганографических методов обеспечения кибербезопасности систем виртуальной и дополненной реальности.
11	Кибербезопасность в системах виртуальной и дополненной реальности (часть 2). В результате выполнения работы на практическом занятии студенты изучат и получат навыки в применении криптографического ПО, алгоритмов и стандартов для обеспечения кибербезопасности в цифровых технологиях, в системах виртуальной и дополненной реальности.
12	Технологические и системные проблемы кибербезопасности (часть 1). В результате выполнения работы на практическом занятии студенты изучат и получат навыки в разработке комплексных методик обеспечения кибербезопасности.
13	Технологические и системные проблемы кибербезопасности (часть 2). В результате выполнения работы на практическом занятии студенты изучат и получат навыки в разработке технологических решений для реализации комплексных методик обеспечения кибербезопасности и их применение.
14	Антивирусная защита домашнего компьютера В результате выполнения практического задания студент получает навыки в настройке для защиты домашнего компьютера Microsoft Defender, а также навыки в настройке для защиты домашнего компьютера двух популярных антивирусов и содержательном сравнительном анализе их работы. Анализируются методы искусственного интеллекта применяемые в антивирусных программах.
15	Антивирусная защита компьютерной сети В результате выполнения практического задания студент получает навыки в настройке для защиты компьютерной сети Microsoft Defender, а также навыки в настройке для защиты компьютерной сети двух популярных антивирусов и содержательном сравнительном анализе их работы. Анализируются методы искусственного интеллекта применяемые в антивирусных программах.
16	Применение методов искусственного интеллекта в СКУД В результате выполнения практического задания студент получает навыки в применении методов искусственного интеллекта в системах контроля и управления доступом (СКУД).

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к практическим занятиям
3	Выполнение курсового проекта.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых проектов

Курсовой проект на тему "Кибербезопасность технологий в условиях цифровой трансформации" состоит в разработке методики обеспечения кибербезопасности технологического решения, разрабатываемого каждым обучающимся в рамках своей магистерской 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.

Примерный перечень тем курсовых проектов:

- Обеспечение кибербезопасности информационных потоков TMS системы
- Обеспечение кибербезопасности информационных потоков при интеграции цепей поставок
- Разработка и внедрение системы информационной безопасности в транспортной компании
- Разработка методики защиты информации от целевого фишинга в автоматизированной системе предприятия
- Обеспечение безопасности информации при попытке доступа в удаленную систему
- Разработка организационно-технических мер по защите информации, составляющей служебную тайну предприятия (на конкретном примере)
- Выявление киберугрозы информационным системам предприятия (на конкретном примере)
- Обеспечение безопасности при распределении ресурсов сети в мобильной спутниковой системе связи
- Средства автоматизации тестирования на проникновения веб-приложений
- Исследование основных криптографических методов защиты информационных систем
- Методы защиты конфиденциальной информации при проведении переговоров в неспециализированных помещениях.
- Настройка антивирусного программного обеспечения для защиты веб-сайта с использованием методов искусственного интеллекта.
- Методы защиты новостных порталов от вирусных атак с использованием методов искусственного интеллекта.
- Методы защиты от атак, связанных с системными структурами жёстких дисков, с использованием методов искусственного интеллекта.
- Антивирусная защита ИСПДн на основе отечественной аппаратно-программной платформы с использованием методов искусственного интеллекта.
- Обеспечение антивирусной защиты цифровых систем управления запасами в логистике терминально-складских комплексов с использованием методов искусственного интеллекта.
- Обеспечение антивирусной защиты Департамента Логистики и Планирования компании Z с использованием методов искусственного интеллекта.

- Обеспечение антивирусной защиты мультимодальных транспортно-логистических центров с использованием методов искусственного интеллекта.

- Обеспечение антивирусной защиты персонального компьютера при разработке платформы имитационной модели складского процесса с использованием методов искусственного интеллекта.

- Обеспечение антивирусной защиты цифровой платформы «Личные диаметры» с использованием методов искусственного интеллекта.

- Обеспечение антивирусной защиты в бизнес-процессах закупочной логистики с использованием методов искусственного интеллекта.

- Обеспечение антивирусной защиты при работе оператора, использующего технологию «Физический интернет».

- Обеспечение антивирусной защиты при работе оператора, использующего цифровую платформу ЭТП ГП.

- Обеспечение антивирусной защиты контейнерного терминала компании Z с использованием методов искусственного интеллекта.

- Обеспечение антивирусной защиты Департамента управления персоналом компании Z с использованием методов искусственного интеллекта.

- Организация антивирусной защиты от автоматизированных методов сбора информации из открытых интернет-ресурсов с использованием методов искусственного интеллекта.

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: 31.10.2025).- 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: 31.10.2025).- Текст электронный
3	Мосолов А. С., Акинин Н. И. Компьютерные технологии и методы проектирования в сфере	https://e.lanbook.com/book/183115 (дата обращения:30.10.2025).- Текст электронный.

	безопасности. Издательство "Лань", 2021 - 444с. – ISBN 978-5-8114-8034-0	
4	Прохорова О. В. Информационная безопасность и защита информации: Учебник для вузов	https://e.lanbook.com/book/462293 (дата обращения: 31.10.2025).- Текст электронный.
5	Краковский Ю. М. Методы защиты информации. Издательство "Лань", 2021 - 236с. – ISBN 978-5-8114-5632-1	https://e.lanbook.com/book/156401 (дата обращения: 31.10.2025).- Текст электронный.
6	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: 31.10.2025).- Текст электронный.
7	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: 31.10.2025).- 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 3 семестре.

Курсовой проект в 3 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