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 специалитета
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: 19.06.2024

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

- Формирование знаний об рганизации 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	Тема 1. Цифровизация и цифровая трансформация экономики Рассматриваемые вопросы: - 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. Тема 2. Информационная и 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; - 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. Тема 3. Информационная и 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); - 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; - классы безопасности электронных систем.

№ п/п	Тематика лекционных занятий / краткое содержание
	- криптография и стеганография и их применение. Тема 4. Информационная и кибербезопасность в системах искусственного интеллекта (СИИ) и машинного обучения Рассматриваемые вопросы: - цифровой мир и его многообразие; - разработка интеллектуальных систем; - основные подсистемы интеллектуальных систем; - признаковое пространство и его метрики; - решающие правила и методы их построения; - основные проблемы в обеспечении информационной и кибербезопасности СИИ; - методы и средства защиты информации; - классификация методов: управление, препятствие, маскировка, регламентация, принуждение, понуждение; - классификация средств: физические, аппаратные, программные, организационные, законодательные, морально-этические. Тема 5. Информационная и 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; - применение нейронных логических сетей в экономике и управлении; - информационная и кибербезопасность в нейронных логических сетях; - идентификация, аутентификация и авторизация; - методы аутентификации: пароли, электронные карточки, биометрические параметры, координаты; - идентификаторы доступа: механические, магнитные, оптические, электронные контактные, электронные радиочастотные, акустические, биометрические, комбинированные. Тема 6. Информацинная и 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; - дополненная реальность и ее перспективы в задачах цифровизации; - виртуальная реальность в обучении, управлении и экономике; - информационная и кибербезопасность в системах виртуальной и дополненной реальности; - криптография и стеганография; - симметричное и асимметричное шифрование; - асимметричное шифрование открытым и закрытым ключами; - криптографическое ПО, алгоритмы и стандарты. Тема 7 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

№ п/п	Тематика лекционных занятий / краткое содержание
	- правовые методы решения проблем информационной и кибербезопасности

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	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 (часть 1). 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 получат навыки в разработке и организации СМИБ для современных цифровых технологии в области управления, связи, информационного обеспечения. 5. Кибербезопасность в системах искусственного интеллекта (СИИ) и машинного обучения 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). 6. Технологические и системные проблемы кибербезопасности (часть 1). 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. 7. Защита персональных данных. ФЗ №152 и ГОСТы РФ В результате выполнения практического задания студент получает навыки в применении организационно-правовых методов защиты персональных данных.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом

№ п/п	Вид самостоятельной работы
2	Подготовка к практическим занятиям
3	Подготовка к промежуточной аттестации.

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: 19.06.2024).- Текст электронный.
2	Сэрра Э. Кибербезопасность: правила игры. Как руководители и сотрудники влияют на культуру безопасности в компании. Издательство "Альпина Паблишер", 2022 - 192с. – ISBN 978-5-907534-38-4	https://e.lanbook.com/book/213989 (дата обращения: 19.06.2024).- Текст электронный.
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: 19.06.2024).- Текст электронный.
4	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: 19.06.2024).- 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: 19.06.2024).- 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	https://e.lanbook.com/book/130184 (дата обращения: 19.06.2024).- Текст электронный.
7	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: 19.06.2024).- Текст электронный.
8	Никифоров С. Н. Методы защиты информации. Защищенные сети, 2021 - 96с. – ISBN 978-5-8114-7907-8	https://e.lanbook.com/book/167186 (дата обращения: 19.06.2024.- 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).

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 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, 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