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: Заочная

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 принципы алгоритмизации;
- методы программирования на языке С++.

Уметь:

- самостоятельно разрабатывать алгоритмы решения задач, описывать их в виде блок-схем;
- реализовывать разработанные алгоритмы на языке С++;
- выполнять отладку написанных программ.

Владеть:

- владеть навыками разработки алгоритмов и программ на языке С++.

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	Сем. №14
Контактная работа при проведении учебных занятий (всего):	12	12
В том числе:		
Занятия лекционного типа	6	6
Занятия семинарского типа	6	6

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	Тема 1Цифровизация 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.
2	Тема 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; - цифровые трансформации и мировоззрение; - проблемы цифровизации, культуры, образования и безопасности; - человеческий фактор и проблемы кибербезопасности; - вирусы и программы-вымогатели; - основные правила компьютерной «гигиены»: пароли и их обновление, отношение к непонятным ссылкам, работа в социальных сетях.
3	Тема 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); - 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.
4	Тема 4 Кибербезопасность в системах искусственного интеллекта (СИИ) и машинного обучения Рассматриваемые вопросы: - цифровой мир и его многообразие;

№ п/п	Тематика лекционных занятий / краткое содержание
	- разработка интеллектуальных систем; - основные подсистемы интеллектуальных систем; - признаковое пространство и его метрики; - решающие правила и методы их построения; - основные проблемы в обеспечении кибербезопасности СИИ; - методы и средства защиты информации; - классификация методов: управление, препятствие, маскировка, регламентация, принуждение, понуждение; - классификация средств: физические, аппаратные, программные, организационные, законодательные, морально-этические.
5	Тема 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; - применение нейронных логических сетей в экономике и управлении; - 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.
6	Тема 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; - дополненная реальность и ее перспективы в задачах цифровизации; - виртуальная реальность в обучении, управлении и экономике; - 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.
7	Тема 7 Кибербезопасность в социальных сетях и цифровом маркетинге Рассматриваемые вопросы: - социальные сети и их «жители»; - проблемы сбора, хранения и обработки больших данных и их решение; - цифровой маркетинг в социальных сетях и проблемы манипуляции мнением человека; - виртуальный мир и управление его трансформацией; - компьютерные вирусы и методы защиты от них; - способы распространения компьютерных вирусов; - классификация компьютерных вирусов; - макровирусы; - защита от компьютерных вирусов: профилактика, диагностика, лечение. Антивирусные программы.
8	Тема 8 Технологические и системные проблемы кибербезопасности Рассматриваемые вопросы: - цифровые технологии и проблемы уязвимости; - проблемы компьютерной и информационной безопасности в цифровой экономике; - комплексное решение проблемы кибербезопасности: защита Интернета, компьютеров, данных,

№ п/п	Тематика лекционных занятий / краткое содержание
	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 работы на практическом занятии студенты ознакомятся с нормативно-правовой базой обеспечения кибербезопасночти технологических решений.
2	Кибербезопасность в корпоративных информационных системах В результате работы на практическом занятии студенты ознакомятся с административными (организационными) методами обеспечения кибербезопасности технологических решений.
3	Кибербезопасность в системах искусственного интеллекта (СИИ) и машинного обучения В результате работы на практическом занятии студенты ознакомятся с программно-техническими методами обеспечения кибербезопасности технологических решений.
4	Кибербезопасность в нейронных логических сетях. В результате работы на практическом занятии студенты ознакомятся с криптографическими методами обеспечения кибербезопасности.
5	Кибербезопасность в системах виртуальной и дополненной реальности В результате работы на практическом занятии студенты ознакомятся со стеганографическими методами обеспечения кибербезопасности.
6	Технологические и системные проблемы кибербезопасности В результате работы на практическом занятии студенты получат представление о разработке комплексных методик обеспечения кибербезопасности технологических решений.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение лекционного материала. Изучение литературы по дисциплине (модулю). Выполнение курсового проекта.
2	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	Логические нейронные сети Барский А.Б. 2013. М.: ИНТУИТ; БИНОМ.	https://techlibrary.ru/b/2i1a1r1s1l1j1k_2h.2i._2v1f1k1r1p1o1o2c1f_1s1f1t1j._2y1a1s1q1p1i1o1a1c1a1o1j1f,_1u1q1r1a1c1m1f1o1j1f,_1q1r1j1o2g1t1j1f_1r1f1z1f1o1j1k._2004.pdf

	Лаборатория знаний, 2013	
2	Нейросетевые технологии искусственного интеллекта. (Учебный курс). Интернет-Университет информационных технологий. Барский А.Б.	https://intuit.ru/studies/courses/3521/763/info
3	Криптографические методы защиты информации. (Учебный курс). Интернет-Университет информационных технологий. Жданов О.,Ушаков Ю.	https://intuit.ru/studies/professional_skill_improvements/20679/courses/1234/info
4	Межсетевые	https://intuit.ru/studies/curriculums/20635/courses/1286/info

	экраны. Учебный курс). Интернет - Университет информационных технологий. Лопонина О.	
5	Техническая защита информации. (Учебный курс). Интернет - Университет информационных технологий Скрипник Д.	https://intuit.ru/studies/courses/3649/891/info
6	Машинное обучение. (Учебный курс). Интернет - Университет информационных технологий Воронцо	https://intuit.ru/studies/courses/13844/1241/info

	в К.	
7	Безопасность в интернете. (Учебный курс). Интернет-Университет информационных технологий Заика А.	https://intuit.ru/studies/educational_groups/1549/courses/704/info
8	Информационная безопасность. Национальные стандарты Российской Федерации. (Учебное пособие) Родичев Ю.А. 2019.С.-Пб.:Питер,Библ. МИИТА, 2019	https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf
9	Организационное и правовое обеспечение информационной	ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ)

	безопасности Под ред. Т.А. Полякова, А.А. Стрельцов Книга Издательство Юрайт, 2019	

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

- http://citforum.ru/ - Форум специалистов по информационным технологиям
- http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ.
- http://elibrary.ru/ - научно-электронная библиотека.

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

- Операционная система Windows;
- Microsoft Office;
- ZOOM;
- MS Teams;
- Поисковые системы;

При организации обучения по дисциплине (модулю) с применением электронного обучения и дистанционных образовательных технологий необходим доступ каждого студента к информационным ресурсам – библиотечному фонду Университета, сетевым ресурсам и информационно-телекоммуникационной сети «Интернет».

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 14 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. Клычева