

**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 бакалавриата  
по направлению подготовки  
23.03.01 Технология транспортных процессов,  
утвержденной первым проректором РУТ (МИИТ)  
Тимониным В.С.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Информационная и кибербезопасность**

Направление подготовки: 23.03.01 Технология транспортных процессов

Направленность (профиль): Цифровой транспорт и логистика

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: 13.04.2023

## 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-19** - Способен использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности с учетом требований информационной безопасности.

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

**Знать:**

- основные принципы алгоритмизации;
- методы программирования на языке C++.

**Уметь:**

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

**Владеть:**

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

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

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 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. №7
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
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 80 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>Тема 1 Цифровизация и цифровая трансформация экономики</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>Тема 2 Кибербезопасность в цифровых технологиях и цифровой трансформации</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 кибербезопасности;</li> <li>- вирусы и программы-вымогатели;</li> <li>- основные правила компьютерной «гигиены»: пароли и их обновление, отношение к непонятным ссылкам, работа в социальных сетях.</li> </ul>
3	<p>Тема 3 Кибербезопасность в корпоративных информационных системах</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> <li>- электронная подпись;</li> <li>- классы безопасности электронных систем.</li> </ul>
4	<p>Тема 4 Кибербезопасность в системах искусственного интеллекта (СИИ) и машинного обучения</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- цифровой мир и его многообразие;</li> </ul>

№ п/п	Тематика лекционных занятий / краткое содержание
	<ul style="list-style-type: none"> <li>- разработка интеллектуальных систем;</li> <li>- основные подсистемы интеллектуальных систем;</li> <li>- признаковое пространство и его метрики;</li> <li>- решающие правила и методы их построения;</li> <li>- основные проблемы в обеспечении кибербезопасности СИИ;</li> <li>- методы и средства защиты информации;</li> <li>- классификация методов: управление, препятствие, маскировка, регламентация, принуждение, понуждение;</li> <li>- классификация средств: физические, аппаратные, программные, организационные, законодательные, морально-этические.</li> </ul>
5	<p><b>Тема 5 Кибербезопасность в нейронных логических сетях</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- цифровизация и нейронные логические сети;</li> <li>- проблема моделирования работы мозга и принятия решений;</li> <li>- персептрон и его применение в цифровых технологиях;</li> <li>- обучение персептронов;</li> <li>- применение нейронных логических сетей в экономике и управлении;</li> <li>- кибербезопасность в нейронных логических сетях;</li> <li>- идентификация, аутентификация и авторизация;</li> <li>- методы аутентификации: пароли, электронные карточки, биометрические параметры, координаты;</li> <li>- идентификаторы доступа: механические, магнитные, оптические, электронные контактные, электронные радиочастотные, акустические, биометрические, комбинированные.</li> </ul>
6	<p><b>Тема 6 Кибербезопасность в системах виртуальной и дополненной реальности</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- многообразие мира и методов его цифровизации и трансформации;</li> <li>- виртуальный мир и его особенности;</li> <li>- виртуальная реальность и задачи математического и имитационного моделирования;</li> <li>- имитационное моделирование транспортных процессов и систем;</li> <li>- дополненная реальность и ее перспективы в задачах цифровизации;</li> <li>- виртуальная реальность в обучении, управлении и экономике;</li> <li>- кибербезопасность в системах виртуальной и дополненной реальности;</li> <li>- криптография и стеганография;</li> <li>- симметричное и асимметричное шифрование;</li> <li>- асимметричное шифрование открытым и закрытым ключами;</li> <li>- криптографическое ПО, алгоритмы и стандарты.</li> </ul>
7	<p><b>Тема 7 Кибербезопасность в социальных сетях и цифровом маркетинге</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- социальные сети и их «жители»;</li> <li>- проблемы сбора, хранения и обработки больших данных и их решение;</li> <li>- цифровой маркетинг в социальных сетях и проблемы манипуляции мнением человека;</li> <li>- виртуальный мир и управление его трансформацией;</li> <li>- компьютерные вирусы и методы защиты от них;</li> <li>- способы распространения компьютерных вирусов;</li> <li>- классификация компьютерных вирусов;</li> <li>- макровирусы;</li> <li>- защита от компьютерных вирусов: профилактика, диагностика, лечение. Антивирусные программы.</li> </ul>
8	<p><b>Тема 8 Технологические и системные проблемы кибербезопасности</b></p> <p>Рассматриваемые вопросы:</p> <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 кибербезопасности: защита Интернета, компьютеров, данных,</li> </ul>

№ 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 кибербезопасности 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 получают 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
2	Подготовка практическим занятиям
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

#### 4.4. Примерный перечень тем курсовых работ

Курсовая работа 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 организационных, экономических и программно-аппаратных мер, обеспечивающих кибербезопасность конкретного технологического решения. Предлагаемые к разработке меры предусматривают такие решения как:

- 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> (дата обращения: 31.03.2023).- Текст электронный.
2	Сэрра Э. Кибербезопасность: правила игры. Как руководители и сотрудники влияют на культуру безопасности в компании. Издательство "Альпина Паблицер", 2022 - 192с. – ISBN 978-5-907534-38-4	<a href="https://e.lanbook.com/book/213989">https://e.lanbook.com/book/213989</a> (дата обращения: 31.03.2023).- 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	<a href="https://e.lanbook.com/book/183115">https://e.lanbook.com/book/183115</a> (дата обращения: 31.03.2023).- 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> (дата обращения: 31.03.2023).- 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> (дата обращения: 31.03.2023).- 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> (дата обращения: 31.03.2023).- 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> (дата обращения: 31.03.2023).- 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> (дата обращения: 31.03.2023).- Текст электронный.

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:

Курсовая работа в 7 семестре.

Экзамен в 7 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