МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Стандартизация и сертификация систем информационной безопасности

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (в сфере связи, информационных и коммуникационных технологий)

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: 02.06.2026

1. Общие сведения о дисциплине (модуле).

Краткая аннотация дисциплины (модуля) (как правило, описываются основные цели и задачи дисциплины(модуля).

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ПК-3 - Способность проводить сертификационные испытания средств защиты информации;

ПК-8 - Способность разрабатывать технические задания, проектировать и исследовать подсистемы информационной безопасности автоматизированных систем с учетом требований стандартов и технико-экономических обоснований;

ПК-11 - Способность разрабатывать и формализовывать требования к безопасности информации, а также создавать и внедрять политики безопасности для компьютерных систем и сетей с учетом актуальных угроз и стандартов.

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

Знать:

- основные нормативные правовые акты, нормативные и методические документы, регламентирующие проведение сертификационных испытаний средств защиты информации;
- основные требования к разработке технических заданий, проектированию и исследованию подсистем информационной безопасности автоматизированных систем;
- основные методы разработки и формализации требований к безопасности информации, а также созданию и внедрению политики безопасности для компьютерных систем и сетей с учетом актуальных угроз и стандартов.

Уметь:

применять на практике:

- нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

- основные требования к разработке технических заданий, проектированию и исследованию подсистем информационной безопасности автоматизированных систем;

- основные методы разработки и формализации требований к безопасности информации, а также созданию и внедрению политики безопасности для компьютерных систем и сетей с учетом актуальных угроз и стандартов.

Владеть:

навыками:

- применения на практике нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации;

- применения на практике технических заданий, проектированию и исследованию подсистем информационной безопасности автоматизированных систем;

- применения на практике основных методов разработки и формализации требований к безопасности информации, а также созданию и внедрению политики безопасности для компьютерных систем и сетей с учетом актуальных угроз и стандартов.

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	Семестр №10
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	Стандартизация и сертификация: цели, задачи, основные понятия и определения Рассматриваемые вопросы: - Техническое регулирование; - Требования технических регламентов; - Стандартизация и ее принципы: системность, повторяемость, вариантность, взаимозаменяемость; - Международный и национальный стандарты; - Унификация, агрегатирование, симплификация, типизация; - Нормативные документы по стандартизации; - Виды национальных стандартов; - Сертификация и ее основные этапы; - Добровольная и обязательная сертификация; - Дункции органа по сертификации. схемы декларирования соответствия; - Обязанности органа по сертификации;
2	Организация стандартизации и сертификации продукции и услуг в РФ Рассматриваемые вопросы: - Организация и принципы стандартизации в РФ - Федеральное агентство по техническому регулированию и его функции; - Органы и службы стандартизации РФ; - Центры стандартизации и метрологии (ЦСМ) и их функции; - Виды и категории национальных стандартов РФ; - Общероссийские классификаторы технико-экономической информации (ОКТЭИ); - Комплексная и опережающая стандартизации; - Межотраслевые системы стандартов; - Параметрическая стандартизация.
3	Организация стандартизации и сертификации продукции и услуг в РФ (продолжение) Рассматриваемые вопросы: - Основные принципы организации сертификации в РФ; - Сертификация в Законе «О техническом регулировании»; - Технические регламенты Таможенного союза и Евразийского экономического союза;

№ п/п	Тематика лекционных занятий / краткое содержание
	- Виды сертификации продукции; - Формы сертификации продукции; - Отличия сертификата от декларации; - Продукция, подлежащая обязательной сертификации; - Органы, выдающие сертификаты; - Проверка подлинности сертификата; - Органы, проверяющие наличие сертификата; - Ответственность за подделку сертификата; - Сертификация производства в РФ.
4	Стандартизация и сертификация вычислительных систем и сетей Рассматриваемые вопросы: - организации – разработчики стандартов вычислительных систем и сетей: ISO, ITU, IEEE, ECMA, CBEMA, EIA, ANSI; - стандартизация сетей; - стандартизация в телекоммуникациях; - стандартизация компьютерных систем; - понятие интерфейса, протокола и стека; - модель OSI: 7 уровней протоколов сети. - Методы коммутации в компьютерных сетях;
5	Стандартизация и сертификация вычислительных систем и сетей (продолжение) Рассматриваемые вопросы: - ГОСТы на автоматизированные системы: ГОСТ Р 59793–2021, ГОСТ 34.602–2020; Стадии и этапы создания автоматизированных систем Содержание работ на каждом из этапов. Учет требований ИБ на этапе проектирования Перечень организаций, участвующих в разработке автоматизированной системы. Основные требования к техническому заданию на проектирование АС. - ГОСТы для высокопроизводительных вычислительных систем: ГОСТ Р 57700.36-2021, ГОСТР 57700.27— 2020. Оценка производительности высокопроизводительных ВС на алгоритмах, использующих сверточные сети. Методика оценки производительности.
6	Стандартизация и сертификация программного обеспечения Рассматриваемые вопросы: - Жизненный цикл ПО и его стандартизация; - Модели разработки ПО: каскадная, спиральная; - Стандартизация спецификаций программных модулей; - Стандартизация проектирования и кодирования ПО; - Оценка качества ПО в ГОСТах: ГОСТ 28195 и ИСО/МЭК 9126;
7	Системная и программная инженерия в ГОСТах: ГОСТ 25001-2017, ГОСТ 25051-2017, ГОСТ 25010-2015. Рассматриваемые вопросы: Требования и оценка качества систем и ПО. Учет требований к ИБ в оценке качества систем. Проектный план оценки качества Требования к оценке качества готового ПО. Оценка реализации требований к ПО в соответствии с ИБ. Модели качества и их использование при оценке систем и ПО.
8	Стандартизация в области информационной безопасности Рассматриваемые вопросы: - Проблема стандартизации в области информационной безопасности в международных и национальных стандартах; - ГОСТы серии 27000; - Стандартизация терминологии в ISO/IEC 27000;

№ п/п	Тематика лекционных занятий / краткое содержание
	-Стандартизация базовых требований в ISO/IEC 27001/27002; - Стандартизация порядка внедрения СМИБ в ISO/IEC 27003;
9	Стандартизация в области информационной безопасности (продолжение) Рассматриваемые вопросы: - Стандартизация основных процессов в ISO/IEC 27004/27005/27007/27008; Методы и средства обеспечения ИБ Общий обзор измерений, связанных с безопасностью Программа измерений и факторы успеха Результаты измерений и критерии принятия решений Менеджмент риска информационной безопасности Оценка риска ИБ
10	Стандартизация в области информационной безопасности (продолжение) Рассматриваемые вопросы: - Стандартизация корпоративного управления СМИБ в ISO/IEC 27014/27016. Руководство деятельностью по обеспечению ИБ Руководящие органы ИБ Лица, ответственные за оценку, управление и мониторинг СМИБ, Стандарты управления ИБ Обеспечение соответствия внутренним и внешним требованиям Требования к СМИБ
11	Нормативные документы ФСТЭК в области информационной безопасности Рассматриваемые вопросы: - Федеральная служба по техническому и экспортному контролю (ФСТЭК), ее цели, задачи, нормативные документы в области информационной безопасности вычислительных комплексов, систем и сетей; - Приказ ФСТЭК №117 от 11.04.2025; - Меры защиты информации в государственных информационных системах; - Методика оценки угроз безопасности; - Базовая модель угроз безопасности персональных данных при обработке в ИС, СТР-К.
12	Стандартизация и сертификация в области защиты информации Рассматриваемые вопросы: - Система ГОСТов в области защиты информации: ГОСТ Р 52069.0-2013; - Общие технические требования к защите от несанкционированного доступа к информации в ГОСТ Р 50739; - Основные требования и определения в ГОСТ Р 50922; - Порядок создания автоматизированных систем в защищенном исполнении в ГОСТ Р 51583; -Стандартизация номенклатуры качества защиты информации в ГОСТ Р 52447; - Стандартизация требований к средствам высоконадежной биометрической аутентификации в ГОСТ Р 52633.
13	Стандартизация в области системной и программной инженерии Рассматриваемые вопросы: - Международный стандарт ISO/IEC TR 19759-2015 (SWEBOK (Software Engineering Body of Knowledge); - Ядро знаний SWEBOK и международный стандарт ISO/IEC 12207:2008 Systems and software engineering — Software life cycle processes; - Процессы жизненного цикла программного обеспечения (ISO/IEC 12207:2008); - Основные процессы жизненного цикла ПО; - Вспомогательные процессы жизненного цикла ПО; - Организационные процессы жизненного цикла ПО; - Основные области знаний SWEBOK; Области управления SWEBOK; - Инженерия требований к ПО.

№ п/п	Тематика лекционных занятий / краткое содержание
14	Стандартизация и сертификация в условиях цифровой информации. Стандартизация и сертификация систем искусственного интеллекта Рассматриваемые вопросы: - Национальная Программа "Цифровая экономика Российской Федерации" и ее Федеральные проекты «Цифровое государственное управление», «Цифровые технологии», «Информационная безопасность», «Кадры для цифровой экономики», «Информационная инфраструктура», «Нормативное регулирование цифровой среды», «Искусственный интеллект», «Развитие кадрового потенциала ИТ-отрасли», «Обеспечение доступа в Интернет за счет развития спутниковой связи»;
15	Стандартизация и сертификация в условиях цифровой информации. Стандартизация и сертификация систем искусственного интеллекта (продолжение) Рассматриваемые вопросы: - Проблемы стандартизации и сертификации в Федеральных проектах. - Федеральный проект «Искусственный интеллект» и проблемы стандартизации и сертификации; - Стандартизация и унификация представления правовой информации для цифровой платформы «Государственная система правовой информации»; - ПНСТ «Умное производство; - Двойники цифровые производства» (части 1-4); - ПНСТ «Информационные технологии; Умный город; - Функциональная совместимость»; ПНСТ «Информационные технологии; Умный город; - Руководства по обмену и совместному использованию данных»; - ПНСТ «Информационные технологии; - Интернет вещей; - Протокол обмена для высокоемких сетей.
16	Сертификация информационных систем Рассматриваемые вопросы: - Информационные системы – это совокупность аппаратных, программных ресурсов, предназначенных для сбора, хранения, обработки, анализа, защиты информации и решения управленческих задач при ведении бизнеса; - К ним относятся компьютеры, серверы, сетевое оборудование, прочие технические средства, а также программные продукты – приложения, электронные учебные пособия, базы данных, специализированные программы; - Сертификация заключается в подтверждении соответствия выполняемой работы или предоставляемой услуги требованиям, установленным в следующих стандартах: ГОСТ Р 57392-2017 – управление услугами компаний в области ИТ; ГОСТ Р 57486-2017 – требования к услугам по информационному обеспечению населения; - ГОСТ Р ИСО/МЭК 38500-2017 – стратегия управления в сфере IT; -ISO/IEC (ГОСТ Р ИСО/МЭК) 27001 – требования к системам менеджмента информационной безопасности (СМИБ); - иных стандартах.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Основные принципы организации сертификации в РФ. Сертификация в Законе «О техническом регулировании» В результате выполнения практического задания студент получает навыки внедрения требований

№ п/п	Тематика практических занятий/краткое содержание
	Закона «О техническом регулировании» в разрабатываемые или эксплуатируемые вычислительные системы и сети.
2	Стандартизация и сертификация вычислительных систем и сетей В результате выполнения практического задания студент получает навыки внедрения требований ГОСТов в разрабатываемые или эксплуатируемые вычислительные системы и сети.
3	Оценка качества ПО в ГОСТе 28195 В результате выполнения практического задания студент получает навыки оценки качества разработанного программного обеспечения в соответствии с требованиями ГОСТов.
4	Виды и формы сертификации продукции В результате выполнения практического задания студент получает навыки применения видов и форм сертификации продукции в соответствии с требованиями ГОСТов.
5	Стандартизация кибербезопасности вычислительного комплекса В результате выполнения практического задания студент получает навыки разработки методов и средств обеспечения кибербезопасности вычислительного комплекса в соответствии с требованиями ГОСТов.
6	Стадии и этапы создания автоматизированных систем. Содержание работ на каждом из этапов. Учет требований ИБ на этапе проектирования В результате выполнения практического задания студент получает навыки разработки разработки автоматизированных систем с учетом требований ИБ..
7	Оценка качества систем и ПО. Учет требований к ИБ в оценке качества систем. В результате выполнения практического задания студент получает навыки оценки качества систем с учетом требований ИБ..
8	Меры защиты информации в государственных информационных системах В результате выполнения практического задания студент получает навыки разработки мер защиты информации в государственных информационных системах в соответствии с требованиями ГОСТов и нормативных документов ФСТЭК.
9	Стандартизация в области системной и программной инженерии В результате выполнения практического задания студент получает навыки внедрения требований Международного стандарта ISO/IEC TR 19759-2015 (SWEBOK (Software Engineering Body of Knowledge) в разрабатываемые или эксплуатируемые вычислительные системы и сети
10	Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах В результате выполнения практического задания студент получает навыки внедрения требований Приказа ФСТЭК России №117.
11	Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) В результате выполнения практического задания студент получает навыки внедрения требований СТР-К, разработанных и утвержденных Гостехкомиссией при Президенте РФ.
12	Стандартизация при обеспечении информационной безопасности на основе облачных служб В результате выполнения практического задания студент получает навыки внедрения требований ГОСТ Р ИСО/МЭК 27017-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Правила применения мер безопасности на основе облачных служб».
13	Стандартизация при защите информационных данных (ПДн) в публичных облаках В результате выполнения практического задания студент получает навыки внедрения требований ГОСТ Р ИСО/МЭК 27018-2020 «Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по защите информационных данных (ПДн) в публичных облаках, используемых для их обработки».

№ п/п	Тематика практических занятий/краткое содержание
14	Категоризация КИИ в соответствии с распоряжением Правительства РФ №360-р от 26.02.2026 В результате выполнения практического задания студент получает навыки определения категории КИИ в соответствии с распоряжением Правительства РФ №360-р от 26.02.2026.
15	Классификация систем искусственного интеллекта в соответствии с ГОСТ Р 59277-2020 В результате выполнения практического задания студент получает навыки классификации СИИ в соответствии с ГОСТ Р 59277.
16	Искусственный интеллект в КИИ в соответствии с ПНСТ 1046-2026 «Искусственный интеллект в критической информационной инфраструктуре» В результате выполнения практического задания студент получает навыки обеспечения требований к ИИ в КИИ.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к практическим работам
3	Подготовка к тестированию
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Башлыкова А.А. Проектирование и стандартизация информационных, информационно-вычислительных и телекоммуникационных систем: Учебное пособие. МИРЭА-Российский технологический университет, 2021.- 69с.	https://e.lanbook.com/book/176534 (дата обращения: 27.05.2026) - - Текст электронный.
2	Гвоздева Т. В., Баллод Б. А. Проектирование информационных систем. Стандартизация. Издательство "Лань", 2022.-252с.- ISBN 978-5-8114-7963-4	https://e.lanbook.com/book/169810 (дата обращения: 27.05.2026) - Текст электронный.
3	Лагоша О. Н. Сертификация информационных систем. Издательство "Лань" (СПО), 2021- 112с.- ISBN 978-5-8114-7212-3	https://e.lanbook.com/book/156616 (дата обращения: 27.05.2026) - Текст электронный.

4	Семахин А. М. Методы верификации и оценки качества программного обеспечения: Учебное пособие. Курганский государственный университет, 2018- 150с.-ISBN 978-5-4217-0461-4	https://e.lanbook.com/book/177908 (дата обращения: 27.05.2026) - Текст электронный.
5	Миняев А. А., Юркин, Ковцур М. М., Ахрамееева К. А. Сертификация средств защиты информации: учебное пособие. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2020.- 88с.- ISBN 978-5-89160-213-7	https://e.lanbook.com/book/180100 (дата обращения: 27.05.2026) - Текст электронный.
6	Фот Ю. Д. Стандарты информационной безопасности: Учебное пособие. Оренбургский государственный университет, 2018.-226с.- ISBN 978-5-7410-2297-9	https://e.lanbook.com/book/159804 (дата обращения:27.05.2026) - 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).

Учебная аудитория для проведения учебных занятий (занятий лекционного типа, лабораторных работ):

- компьютер преподавателя, рабочие станции студентов, мультимедийное оборудование, доска.

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Экзамен в 10 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 ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова