

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 направлению подготовки
02.03.02 Фундаментальная информатика и
информационные технологии,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Стандартизация и сертификация вычислительных систем и сетей

Направление подготовки: 02.03.02 Фундаментальная информатика и
информационные технологии

Направленность (профиль): Квантовые вычислительные системы и сети

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: 06.06.2026

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины (модуля) является:

- формирование компетенций по основным разделам стандартизации и сертификации вычислительных систем и сетей.

Основными задачами дисциплины являются:

- изучение основ и базовых понятий стандартизации и сертификации вычислительных комплексов, систем и сетей;

- изучение требований российских и международных стандартов к разработке, внедрению и эксплуатации вычислительных комплексов, систем и сетей;

- изучение структуры органов стандартизации и сертификации в области вычислительных комплексов, систем и сетей;

- изучение требований российских и международных стандартов вычислительных комплексов, систем и сетей на различных этапах их жизненного цикла;

- изучение схем и методов сертификации средств обеспечения информационной безопасности вычислительных комплексов, систем и сетей.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-5 - Способен участвовать в разработке технической документации программных продуктов и комплексов с использованием стандартов, норм и правил, а также в управлении проектами создания информационных систем на стадиях жизненного цикла;

ПК-9 - Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

ПК-10 - Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

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

Знать:

- основные стандарты, нормы и правила, регулирующие разработку технической документации программных продуктов и комплексов;

- действующие нормативные и методические документы для оформления рабочей технической документации;

- основные методы подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзоров по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

Уметь:

применять на практике:

- основные стандарты, нормы и правила, регулирующие разработку технической документации программных продуктов и комплексов;

- действующие нормативные и методические документы для оформления рабочей технической документации;

- основные методы подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзоров по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

Владеть:

- навыками применения на практике российских и международных стандартов, норм и правил, регулирующих разработку технической документации программных продуктов и комплексов;

- навыками применения действующих нормативных и методических документов для оформления рабочей технической документации;

- навыками подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзоров по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 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):	40	40
В том числе:		
Занятия лекционного типа	20	20
Занятия семинарского типа	20	20

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 68 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;
2	Стандартизация и сертификация: цели, задачи, основные понятия и определения(продолжение) Рассматриваемые вопросы: - Виды национальных стандартов; - Сертификация и ее основные этапы; - Добровольная и обязательная сертификация; - Дункции органа по сертификации. схемы декларирования соответствия; - Обязанности органа по сертификации; - Система сертификации систем качества и производств (регистр систем качества).
3	Организация стандартизации и сертификации продукции и услуг в РФ Рассматриваемые вопросы: - Организация и принципы стандартизации в РФ

№ п/п	Тематика лекционных занятий / краткое содержание
	<ul style="list-style-type: none"> - 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 (ОКТЕИ); - Комплексная и опережающая стандартизации; - Межотраслевые системы стандартов.
4	<p>Организация стандартизации и сертификации продукции и услуг в РФ(продолжение)</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Параметрическая стандартизация. - Основные принципы организации сертификации в РФ; - Сертификация в Законе «О техническом регулировании»; - Технические регламенты Таможенного союза и Евразийского экономического союза; - 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.
5	<p>Стандартизация и сертификация вычислительных систем и сетей</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - организации – разработчики стандартов вычислительных систем и сетей: ISO, ITU, IEEE, ECMA, SVEMA, 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; - ГОСТы на автоматизированные системы: ГОСТ Р 59793–2021, ГОСТ 34.602–2020; - ГОСТы для высокопроизводительных вычислительных систем: ГОСТ Р 57700.36-2021, ГОСТ Р 57700.27— 2020.
6	<p>Стандартизация и сертификация программного обеспечения</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - 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; - Системная и программная инженерия в ГОСТах: ГОСТ 25001-2017, ГОСТ 25051-2017, ГОСТ 25010-2015.
7	<p>Стандартизация в области информационной безопасности</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - 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
	<ul style="list-style-type: none"> -Стандартизация базовых требований в ISO/IEC 27001/27002; - Стандартизация порядка внедрения СМИБ в ISO/IEC 27003; - Стандартизация основных процессов в ISO/IEC 27004/27005/27007/27008; - Стандартизация корпоративного управления СМИБ в ISO/IEC 27014/27016.
8	<p>Нормативные документы ФСТЭК в области информационной безопасности</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Федеральная служба по техническому и экспортному контролю (ФСТЭК), ее цели, задачи, нормативные документы в области информационной безопасности вычислительных комплексов, систем и сетей; - Приказ ФСТЭК №17 от 11.02.2013; - Меры защиты информации в государственных информационных системах; - Методика оценки угроз безопасности; - Базовая модель угроз безопасности персональных данных при обработке в ИС, СТР-К.
9	<p>Стандартизация и сертификация в области защиты информации</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - 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.
10	<p>Стандартизация в области системной и программной инженерии</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - 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.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	<p>Основные принципы организации сертификации в РФ. Сертификация в Законе «О техническом регулировании»</p> <p>В результате выполнения практического задания студент получает навыки внедрения требований Закона «О техническом регулировании» в разрабатываемые или эксплуатируемые вычислительные системы и сети.</p>
2	<p>Стандартизация и сертификация вычислительных систем и сетей</p> <p>В результате выполнения практического задания студент получает навыки внедрения требований ГОСТов в разрабатываемые или эксплуатируемые вычислительные системы и сети.</p>

№ п/п	Тематика практических занятий/краткое содержание
3	Стандартизация спецификаций программных модулей В результате выполнения практического задания студент получает навыки оформления разработанных программ или программных модулей в соответствии с требованиями ГОСТов.
4	Оценка качества ПО в ГОСТе 28195 В результате выполнения практического задания студент получает навыки оценки качества разработанного программного обеспечения 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	Стандартизация при разработке модели угроз безопасности персональных данных в информационных системах В результате выполнения практического задания студент получает навыки разработки модели угроз безопасности персональных данных в информационных системах в соответствии с требованиями ГОСТов и нормативных документов ФСТЭК.
7	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.
8	Стандартизация требований к средствам высоконадежной биометрической аутентификации в ГОСТ Р 52633 В результате выполнения практического задания студент получает навыки разработки средств высоконадежной биометрической аутентификации в соответствии с требованиями ГОСТов.
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	Стандартизация и сертификация систем искусственного интеллекта В результате выполнения практического задания студент получает навыки внедрения требований российских стандартов (ПНСТ) в области искусственного интеллекта в разрабатываемые или эксплуатируемые вычислительные системы и сети.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к практическим работам
3	Подготовка к промежуточной аттестации.
4	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: 04.06.2026) - - 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: 04.06.2026) - 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: 04.06.2026) - 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: 04.06.2026) - Текст электронный.
5	Миняев А. А., Юркин, Ковцур М. М., Ахрамеева 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: 04.06.2026) - 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: 04.06.2026) - Текст электронный.
7	Селифанов В. В., Звягинцева П. А. Нормативные акты и стандарты по информационной безопасности. Оценка соответствия средств защиты информации: учебное пособие. Сибирский государственный университет геосистем и технологий, 2024.-46с.-ISBN 978-5-907711-70-9	https://e.lanbook.com/book/484949 (дата обращения: 04.06.2026) - 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.mii.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).

Интернет-браузер (Yandex и др.)

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, практических занятий):

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

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Экзамен 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 и
квантовые коммуникации»

С.В. Малинский

Согласовано:

Заведующий кафедрой ВССиИБ

Б.В. Желенков

Председатель учебно-методической
комиссии

Н.А. Андриянова