

**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  
10.03.01 Информационная безопасность,  
утвержденной первым проректором РУТ (МИИТ)  
Тимониным В.С.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Стандартизация и сертификация систем информационной безопасности**

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

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: 29.05.2026

## 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-4** - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

**ПК-8** - способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

**ПК-10** - способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

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

**Знать:**

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

- основные требования к оформлению рабочей технической документации с учетом действующих нормативных и методических документов;

- основные методы анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

**Уметь:**

применять на практике:

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

- перспективные схемы сертификации вычислительных систем и сетей на различных этапах жизненного цикла;

- основные методы анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

**Владеть:**

навыками:

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

- применения на практике методов и средств киберзащиты, перспективных схем сертификации вычислительных систем и сетей на различных этапах жизненного цикла;

- применения на практике основных методов анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

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	<p>Стандартизация и сертификация: цели, задачи, основные понятия и определения</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Техническое регулирование;</li> <li>- Требования технических регламентов;</li> <li>- Стандартизация и ее принципы: системность, повторяемость, вариантность, взаимозаменяемость;</li> <li>- Международный и национальный стандарты;</li> <li>- Унификация, агрегатирование, симплификация, типизация;</li> <li>- Нормативные документы по стандартизации;</li> <li>- Виды национальных стандартов;</li> <li>- Сертификация и ее основные этапы;</li> <li>- Добровольная и обязательная сертификация;</li> <li>- Дункции органа по сертификации. схемы декларирования соответствия;</li> <li>- Обязанности органа по сертификации;</li> <li>- Система сертификации систем качества и производств (регистр систем качества).</li> </ul>
2	<p>Организация стандартизации и сертификации продукции и услуг в РФ</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Организация и принципы стандартизации в РФ</li> <li>- Федеральное агентство по техническому регулированию и его функции;</li> <li>- Органы и службы стандартизации РФ;</li> <li>- Центры стандартизации и метрологии (ЦСМ) и их функции;</li> <li>- Виды и категории национальных стандартов РФ;</li> </ul>

№ п/п	Тематика лекционных занятий / краткое содержание
	<ul style="list-style-type: none"> <li>- Общероссийские классификаторы технико-экономической информации (ОКТЕИ);</li> <li>- Комплексная и опережающая стандартизации;</li> <li>- Межотраслевые системы стандартов;</li> <li>- Параметрическая стандартизация.</li> <li>- Основные принципы организации сертификации в РФ;</li> <li>- Сертификация в Законе «О техническом регулировании»;</li> <li>- Технические регламенты Таможенного союза и Евразийского экономического союза;</li> <li>- Виды сертификации продукции;</li> <li>- Формы сертификации продукции;</li> <li>- Отличия сертификата от декларации;</li> <li>- Продукция, подлежащая обязательной сертификации;</li> <li>- Органы, выдающие сертификаты;</li> <li>- Проверка подлинности сертификата;</li> <li>- Органы, проверяющие наличие сертификата;</li> <li>- Ответственность за подделку сертификата;</li> <li>- Сертификация производства в РФ.</li> </ul>
3	<p><b>Стандартизация и сертификация вычислительных систем и сетей</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- организации – разработчики стандартов вычислительных систем и сетей: ISO, ITU, IEEE, ECMA, SVEMA, EIA, ANSI;</li> <li>- стандартизация сетей;</li> <li>- стандартизация в телекоммуникациях;</li> <li>- стандартизация компьютерных систем;</li> <li>- понятие интерфейса, протокола и стека;</li> <li>- модель OSI: 7 уровней протоколов сети.</li> <li>- Методы коммутации в компьютерных сетях;</li> <li>- ГОСТы на автоматизированные системы: ГОСТ Р 59793–2021, ГОСТ 34.602–2020;</li> <li>- ГОСТы для высокопроизводительных вычислительных систем: ГОСТ Р 57700.36-2021, ГОСТ Р 57700.27— 2020.</li> </ul>
4	<p><b>Стандартизация и сертификация программного обеспечения</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Жизненный цикл ПО и его стандартизация;</li> <li>- Модели разработки ПО: каскадная, спиральная;</li> <li>- Стандартизация спецификаций программных модулей;</li> <li>- Стандартизация проектирования и кодирования ПО;</li> <li>- Оценка качества ПО в ГОСТах: ГОСТ 28195 и ИСО/МЭК 9126;</li> <li>- Системная и программная инженерия в ГОСТах: ГОСТ 25001-2017, ГОСТ 25051-2017, ГОСТ 25010-2015.</li> </ul>
5	<p><b>Стандартизация в области информационной безопасности</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Проблема стандартизации в области информационной безопасности в международных и национальных стандартах;</li> <li>- ГОСТы серии 27000;</li> <li>- Стандартизация терминологии в ISO/IEC 27000;</li> <li>- Стандартизация базовых требований в ISO/IEC 27001/27002;</li> <li>- Стандартизация порядка внедрения СМИБ в ISO/IEC 27003;</li> <li>- Стандартизация основных процессов в ISO/IEC 27004/27005/27007/27008;</li> <li>- Стандартизация корпоративного управления СМИБ в ISO/IEC 27014/27016.</li> </ul>
6	<p><b>Нормативные документы ФСТЭК в области информационной безопасности</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Федеральная служба по техническому и экспортному контролю (ФСТЭК), ее цели, задачи,</li> </ul>

№ п/п	Тематика лекционных занятий / краткое содержание
	<p>нормативные документы в области информационной безопасности вычислительных комплексов, систем и сетей;</p> <ul style="list-style-type: none"> <li>- Приказ ФСТЭК №17 от 11.02.2013;</li> <li>- Меры защиты информации в государственных информационных системах;</li> <li>- Методика оценки угроз безопасности;</li> <li>- Базовая модель угроз безопасности персональных данных при обработке в ИС, СТР-К.</li> </ul>
7	<p><b>Стандартизация и сертификация в области защиты информации</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Система ГОСТов в области защиты информации: ГОСТ Р 52069.0-2013;</li> <li>- Общие технические требования к защите от несанкционированного доступа к информации в ГОСТ Р 50739;</li> <li>- Основные требования и определения в ГОСТ Р 50922;</li> <li>- Порядок создания автоматизированных систем в защищенном исполнении в ГОСТ Р 51583;</li> <li>- Стандартизация номенклатуры качества защиты информации в ГОСТ Р 52447;</li> <li>- Стандартизация требований к средствам высоконадежной биометрической аутентификации в ГОСТ Р 52633.</li> </ul>
8	<p><b>Стандартизация в области системной и программной инженерии</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Международный стандарт ISO/IEC TR 19759-2015 (SWEBOK (Software Engineering Body of Knowledge));</li> <li>- Ядро знаний SWEBOK и международный стандарт ISO/IEC 12207:2008 Systems and software engineering — Software life cycle processes;</li> <li>- Процессы жизненного цикла программного обеспечения (ISO/IEC 12207:2008);</li> <li>- Основные процессы жизненного цикла ПО;</li> <li>- Вспомогательные процессы жизненного цикла ПО;</li> <li>- Организационные процессы жизненного цикла ПО;</li> <li>- Основные области знаний SWEBOK; Области управления SWEBOK;</li> <li>- Инженерия требований к ПО.</li> </ul>
9	<p><b>Стандартизация и сертификация в условиях цифровой информации.</b></p> <p><b>Стандартизация и сертификация систем искусственного интеллекта</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- 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»;</li> <li>- Проблемы стандартизации и сертификации в Федеральных проектах.</li> <li>- Федеральный проект «Искусственный интеллект» и проблемы стандартизации и сертификации;</li> <li>- Стандартизация и унификация представления правовой информации для цифровой платформы «Государственная система правовой информации»;</li> <li>- ПНСТ «Умное производство»;</li> <li>- Двойники цифровые производства» (части 1-4);</li> <li>- ПНСТ «Информационные технологии; Умный город»;</li> <li>- Функциональная совместимость»; ПНСТ «Информационные технологии; Умный город»;</li> <li>- Руководства по обмену и совместному использованию данных»;</li> <li>- ПНСТ «Информационные технологии»;</li> <li>- Интернет вещей»;</li> <li>- Протокол обмена для высокоскоростных сетей.</li> </ul>
10	<p><b>Сертификация информационных систем</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Информационные системы – это совокупность аппаратных, программных ресурсов,</li> </ul>

№ п/п	Тематика лекционных занятий / краткое содержание
	<p>предназначенных для сбора, хранения, обработки, анализа, защиты информации и решения управленческих задач при ведении бизнеса;</p> <p>- К ним относятся компьютеры, серверы, сетевое оборудование, прочие технические средства, а также программные продукты – приложения, электронные учебные пособия, базы данных, специализированные программы;</p> <p>- 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 ИТ; -ISO/IEC (ГОСТ Р ИСО/МЭК) 27001 – требования к системам менеджмента информационной безопасности (СМИБ); - иных стандартах.</p>

#### 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>
3	<p>Оценка качества ПО в ГОСТе 28195</p> <p>В результате выполнения практического задания студент получает навыки оценки качества разработанного программного обеспечения в соответствии с требованиями ГОСТов.</p>
4	<p>Стандартизация кибербезопасности вычислительного комплекса</p> <p>В результате выполнения практического задания студент получает навыки разработки методов и средств обеспечения кибербезопасности вычислительного комплекса в соответствии с требованиями ГОСТов.</p>
5	<p>Меры защиты информации в государственных информационных системах</p> <p>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.</p>
6	<p>Стандартизация в области системной и программной инженерии</p> <p>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</p>
7	<p>Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах</p> <p>В результате выполнения практического задания студент получает навыки внедрения требований Приказа ФСТЭК России №17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».</p>

№ п/п	Тематика практических занятий/краткое содержание
8	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.
9	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».
10	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».

#### 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.	<a href="https://e.lanbook.com/book/176534">https://e.lanbook.com/book/176534</a> (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	<a href="https://e.lanbook.com/book/169810">https://e.lanbook.com/book/169810</a> (дата обращения: 27.05.2026) - Текст электронный.
3	Фот Ю. Д. Стандарты информационной безопасности: Учебное пособие. Оренбургский	<a href="https://e.lanbook.com/book/159804">https://e.lanbook.com/book/159804</a> (дата обращения:27.05.2026) - Текст электронный.

	государственный университет, 2018.-226с.- ISBN 978-5-7410-2297-9	
4	Семахин А. М. Методы верификации и оценки качества программного обеспечения: Учебное пособие. Курганский государственный университет, 2018- 150с.-ISBN 978-5-4217-0461-4	<a href="https://e.lanbook.com/book/177908">https://e.lanbook.com/book/177908</a> (дата обращения: 27.05.2026) - 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	<a href="https://e.lanbook.com/book/180100">https://e.lanbook.com/book/180100</a> (дата обращения: 27.05.2026) - Текст электронный.
6	Лагоша О. Н. Сертификация информационных систем. Издательство "Лань" (СПО), 2021- 112с.- ISBN 978-5-8114-7212-3	<a href="https://e.lanbook.com/book/156616">https://e.lanbook.com/book/156616</a> (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.mii.ru/>
- Образовательная платформа «Юрайт» <https://urait.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  
Интернет-браузер (Yandex и др.)

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Учебная аудитория для проведения учебных занятий (занятий лекционного типа, практических занятий, лабораторных работ, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации):

- компьютер преподавателя, проектор, экран проекционный, рабочие станции студентов, маркерная 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