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
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

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-1.4 - Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями;

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 ;

ПК-13 - способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

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

Знать:

- основные методы и принципы стандартизации и сертификации интеллектуальных систем, нейронных сетей, вычислительных систем и сетей на различных этапах их жизненного цикла;

- 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;

- основные методы и принципы организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами ФСБ и ФСТЭК.

Уметь:

применять на практике:

- российские и международные стандарты в области интеллектуальных систем, нейронных сетей, вычислительных систем и сетей;

- 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;

- нормативные правовые акты и нормативные методические документы ФСБ и ФСТЭК.

Владеть:

навыками:

- применения на практике российских и международных стандартов в области интеллектуальных систем, нейронных сетей, вычислительных систем и сетей;

- 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;

- применения на практике нормативных правовых актов и нормативных методических документов ФСБ и ФСТЭК.

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 №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 104 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;

№ п/п	Тематика лекционных занятий / краткое содержание
	- 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; - Система сертификации систем качества и производств (регистр систем качества).
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 клас¬сификаторы технико-экономической информации (ОКТЭИ); - Комплексная и опережающая стандартизации; - Межотраслевые системы стандартов; - 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.
3	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; - ГОСТы на автоматизированные системы: ГОСТ Р 59793–2021, ГОСТ 34.602–2020; - ГОСТы для высокопроизводительных вычислительных систем: ГОСТ Р 57700.36-2021, ГОСТР 57700.27— 2020.
4	Стандартизация и сертификация программного обеспечения Рассматриваемые вопросы: - Жизненный цикл ПО и его стандартизация; - Модели разработки ПО: каскадная, спиральная; - Стандартизация спецификаций программных модулей;

№ п/п	Тематика лекционных занятий / краткое содержание
	- 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.
5	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; -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.
6	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 №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.
7	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.
8	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.
9	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»,

№ п/п	Тематика лекционных занятий / краткое содержание
	«Нормативное регулирование цифровой среды», «Искусственный интеллект», «Развитие кадрового потенциала ИТ-отрасли», «Обеспечение доступа в Интернет за счет развития спутниковой связи»; - 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.
10	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 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	Стандартизация кибербезопасности вычислительного комплекса В результате выполнения практического задания студент получает навыки разработки методов и

№ п/п	Тематика практических занятий/краткое содержание
	средств обеспечения кибербезопасности вычислительного комплекса в соответствии с требованиями ГОСТов.
5	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.
6	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
7	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 №17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
8	Специальные требования и рекомндации 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.	https://e.lanbook.com/book/176534 (дата обращения: 14.04.2025) - - 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: 14.04.2025) - Текст электронный.
3	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:14.04.2025) - 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: 14.04.2025) - 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: 14.04.2025) - 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 "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:

Зачет 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, сети и
информационная безопасность» С.В. Малинский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова