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

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: 19.01.2023

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Стандартизация и сертификация систем информационной безопасности» является формирование компетенций по основным разделам стандартизации и сертификации систем информационной безопасности вычислительных комплексов, систем и сетей.

Основными задачами дисциплины являются:

• Изучение основ и базовых понятий стандартизации и сертификации систем информационной безопасности вычислительных комплексов, систем и сетей.

• Изучение требований российских и международных стандартов к разработке, внедрению и эксплуатации средств информационной безопасности вычислительных комплексов, систем и сетей.

• Изучение структуры органов стандартизации и сертификации в области обеспечения информационной безопасности вычислительных комплексов, систем и сетей.

• Изучение требований российских и международных стандартов к обеспечению информационной безопасности 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.

Дисциплина предназначена для получения знаний, необходимых для решения следующих профессиональных задач (в соответствии с видами деятельности):

Производственно-технологическая деятельность

• Разработка требований к стандартизации и сертификации технологических решений для обеспечения информационной безопасности вычислительных комплексов, систем и сетей;

• Разработка требований к стандартизации и сертификации технологических решений в области многофакторной аутентификации для обеспечения информационной безопасности вычислительных комплексов, систем и сетей;

• Разработка требований к стандартизации и сертификации технологических решений в области обеспечения информационной безопасности при внедрении, настройке и самообучении систем искусственного интеллекта, нейронных сетей, систем распознавания, вычислительных комплексов, систем и сетей.

Организационно-управленческая деятельность

• Организация и управление стандартизацией и сертификацией

технологических решений для обеспечения информационной безопасности вычислительных комплексов, систем и сетей;

• Организация и управление стандартизацией и сертификацией технологических решений в области многофакторной аутентификации для обеспечения информационной безопасности вычислительных комплексов, систем и сетей;

• Организация и управление стандартизацией и сертификацией технологических решений в области обеспечения информационной безопасности при внедрении, настройке и самообучении систем искусственного интеллекта, нейронных сетей, систем распознавания, вычислительных комплексов, систем и сетей.

Проектная деятельность

• Проектирование программных и аппаратных средств (систем, устройств, деталей, программ, баз данных и т.п.) в соответствии с требованиями российских и международных стандартов в области информационной безопасности;

• Разработка и оформление проектной и рабочей технической документации в соответствии с требованиями российских и международных стандартов в области информационной безопасности;

• Контроль соответствия разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам в области информационной безопасности.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-3 - Способен использовать необходимые математические методы для решения задач профессиональной деятельности;

ОПК-9 - Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности .

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

Знать:

-основные методы и принципы стандартизации и сертификации вычислительных комплексов, систем и сетей, регламентирующие деятельность по защите информации.

Уметь:

-применять на практике российские и международные стандарты, регламентирующие требования к информационной безопасности вычислительных комплексов, систем и сетей на различных этапах их жизненного цикла.

Владеть:

-навыками проведения анализа разрабатываемых или действующих вычислительных комплексов, систем и сетей на соответствие требованиям стандартов в области информационной безопасности.

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	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; - Функции органа по сертификации; - Схемы декларирования соответствия; - Обязанности органа по сертификации.; - Система сертификации систем качества и производств (регистр систем качества).
2	Организация и принципы стандартизации в РФ. Рассматриваемые вопросы: - 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.
3	Организация сертификации продукции и услуг в РФ. -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.
4	Стандартизация и сертификация вычислительных систем и сетей. Рассматриваемые вопросы: -Организации – разработчики стандартов вычислительных систем и сетей: ISO, ITU, IEEE, ECMA,

№ п/п	Тематика лекционных занятий / краткое содержание
	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.
5	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; - Системная и программная инженерия в ГОСТах: ГОСТ 25001-2017, ГОСТ 25051-2017, ГОСТ 25010-2015.
6	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; - Стандартизация кибербезопасности в ISO/IEC 27103.
7	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.
8	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.
9	Стандартизация в области системной и программной инженерии. Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	-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.
10	Стандартизация и сертификация в условиях цифровой информации. 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»; - Проблемы стандартизации и сертификации в Федеральных проектах.
11	Стандартизация и сертификация систем искусственного интеллекта. Рассматриваемые вопросы: -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 цифрового 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 с большим радиусом действия и низким энергопотреблением».
12	Стандартизация при проектировании автоматизированных систем. Рассматриваемые вопросы: -Этапы создания продукции и их особенности; - Предпроектная стадия, проектирование и внедрение: особенности выполнения и обеспечения информационной безопасности; - ГОСТ 34.602-2020; -Комплекс стандартов на автоматизированные системы; - ГОСТ 34.601-90; - Автоматизированные системы; - Стадии создания; - ГОСТ Р 54869-2011; - Требования к управлению проектом; - ГОСТ р 51275-2006; - Объект информатизации; - Факторы, воздействующие на информацию.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	1. 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. 2. Стандартизация спецификаций программных модулей. В результате выполнения практического задания студент получает навыки оформления разработанных программ или программных модулей в соответствии с требованиями ГОСТов. 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 средств обеспечения кибербезопасности вычислительного комплекса в соответствии с требованиями ГОСТов. 5. 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. 6. 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.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к практическим занятиям
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: 18.01.2023) - 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: 18.01.2023) - 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: 18.01.2023) - 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: 18.01.2023) - 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: 18.01.2023) - 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: 18.01.2023) - 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

В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий может понадобиться наличие следующего программного обеспечения (или их аналогов): ОС Windows, Microsoft Office, Интернет-браузер, Microsoft Teams и т.д.

В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта и т.п.

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

1. Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций

-Проектор для вывода изображения на экран для студентов;

- акустическая система;

место для преподавателя оснащенное компьютером ;

-Аудитория подключена к интернету МИИТ.

2. Учебная аудитория для проведения практических работ

-персональные компьютеры.

В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации.

Допускается замена оборудования его виртуальными аналогами.

9. Форма промежуточной аттестации:

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 ВССиИБ Б.В. Желенков

Председатель учебно-методической комиссии Н.А.Клычева