КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

СТАНДАРТЫ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Форма промежуточной аттестации: зачет

2025

Рабочая программа по дисциплине «Стандарты в сфере информационной безопасности» по специальности 10.05.01 Компьютерная безопасность, специализации «Разработка защищенного программного обеспечения», составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.01 Компьютерная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от «26» ноября 2020 г. № 1459, профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. № 533н, профессионального стандарта 06.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. №525н.

Рабочая программа:

обсуждена и рекомендована к утверждению решением кафедры естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

одобрена Научно-методическим советом Казанского кооперативного института (филиала) от 2 апреля 2025 г., протокол № 3

СОДЕРЖАНИЕ

1. Цель и задачи освоения дисциплины 4
2. Место дисциплины в структуре образовательной программы 4
3. Перечень планируемых результатов обучения по дисциплине 4
4. Объем дисциплины и виды учебной работы 5
5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий 6
5.1. Содержание дисциплины 6
5.2. Разделы, темы дисциплины и виды занятий 7
6. Практические занятия 8
7. Лабораторные работы 9
8. Примерная тематика курсовых работ (проектов) 9
9. Самостоятельная работа студента 9
10. Оценивание результатов обучения и уровня сформированности компетенций 12
11. Учебно-методическое обеспечение дисциплины 12
12. Перечень программного обеспечения, профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины 14
13. Материально–техническое обеспечение дисциплины 14
Обновление рабочей программы дисциплины (модуля) 16

1. Цель и задачи освоения дисциплины

Целью преподавания и изучения дисциплины «Стандарты в сфере информационной безопасности» является подготовка студентов, обладающих глубокими теоретическими знаниями и практическими навыками в области стандартов информационной безопасности. Студенты должны быть способны эффективно анализировать и применять международные и национальные стандарты для обеспечения защиты информационных систем. Они должны уметь разрабатывать и внедрять политики безопасности, соответствующие современным требованиям, а также использовать стандартизированные методы и инструменты для обеспечения безопасности и надежности данных в различных организациях.

Задачи:

Студент должен знать основные стандарты и нормативные документы в области информационной безопасности; уметь применять стандарты для обеспечения защиты информационных систем; владеть методами и инструментами для разработки и внедрения политик безопасности, соответствующих международным и национальным требованиям комбинаторного анализа.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Стандарты в сфере информационной безопасности» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» основной образовательной программы – программы специалитета по специальности 10.05.01 Компьютерная безопасность специализация «Разработка защищенного программного обеспечения».

Код компетенции	Предшествующие дисциплины (модули), практики	Изучаемые в текущем семестре дисциплины (модули), практики	Последующие дисциплины (модули), практики
ОПК-5	Защита информации от утечки по техническим каналам	**Стандарты в сфере информационной безопасности**	

3. Перечень планируемых результатов обучения по дисциплине

Изучение дисциплины направлено на формирование у обучающихся компетенций.

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
ОПК-5 Способен применять	ОПК-5.1 Применяет в профессиональной	Знать: профессиональной деятельности знания нормативной правовой базы РФ в

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	деятельности знания нормативной правовой базы РФ в области информационной безопасности	области информационной безопасности Уметь: Проводить анализ знаний нормативной правовой базы РФ в области информационной безопасности Владеть: знаниями нормативной правовой базы РФ в области информационной безопасности
	ОПК-5.2 Демонстрирует умение решать стандартные профессиональные задачи с целью выполнения требований нормоконтролеров РФ	Знать. требования нормоконтролеров РФ Уметь: решать стандартные профессиональные задачи с целью выполнения требований нормоконтролеров РФ Владеть: Способностью применять на практике стандартные профессиональные задачи с целью выполнения требований нормоконтролеров РФ

4. Объем дисциплины и виды учебной работы

Объем дисциплины и виды учебной работы в академических часах с выделением объема контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся

очная форма обучения

Вид учебной деятельности		ак.часов	
		Всего	По семестрам
			А
1. Контактная работа обучающихся с преподавателем:		35	35
Аудиторные занятия, часов всего, в том числе:		34	34
• занятия лекционного типа		18	18
• занятия семинарского типа:		16	16
практические занятия		16	16
лабораторные занятия		-	-
в том числе занятия в форме практической подготовки		-	-
Консультации		0,5	0,5
Контактные часы на аттестацию в период экзаменационной сессии		0,5	0,5
2. Самостоятельная работа студентов всего, в том числе		73	73
- подготовка курсовой работы		-	-
- проработка учебного (теоретического) материала		25	25
- выполнение домашних заданий по практическим занятиям		25	25
- подготовка к зачету		23	23
Промежуточная аттестация: зачет			
ИТОГО:	часов	108	108
общая трудоемкость	зач. ед.	3	3

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Понятие безопасности информации.

Сущность и значение информационной безопасности. Основные принципы и подходы к обеспечению защиты информации. Роль информационной безопасности в современном мире.

Тема 2 Международные и российские стандарты по защите информации: их взаимосвязь и различия.

Международные и российские стандарты по защите информации: их взаимосвязь и различия.

Тема 3. Особенности процесса стандартизации и стандарты безопасности в сети Интернет

Процессы и методы стандартизации в контексте интернет-безопасности. Основные стандарты, регулирующие безопасность в сети. Проблемы и вызовы стандартизации в цифровой среде.

Тема 4. Раздел 4. Особенности государственных стандартов программных продуктов.

Государственные требования к программным продуктам в области безопасности. Особенности разработки и сертификации программного обеспечения. Влияние стандартов на качество и надежность программных решений.

Тема 5 Государственны е стандарты: общие положения

Основные положения и структура государственных стандартов в области информационной безопасности. Принципы разработки и внедрения стандартов. Роль стандартов в обеспечении национальной безопасности.

Тема 6 Государственные стандарты: общие положения

Руководящий документ Гостехкоммиссии: Межсетевые экраны.

Тема 7. Основы сертификации (на примере средств защиты информации).

Процессы и методы сертификации средств защиты информации. Основные этапы и требования сертификации. Роль сертификации в обеспечении доверия к системам безопасности.

Тема 8. Сертификация на соответствие требованиям по безопасности информации.

Критерии и процедуры сертификации для соответствия требованиям

безопасности информации. Методы оценки и подтверждения соответствия. Влияние сертификации на уровень защиты

Тема 9. Системы сертификации средств защиты информации: требования безопасности информации.

Структура и функционирование систем сертификации. Требования к средствам защиты информации в контексте сертификации. Взаимодействие систем сертификации с другими элементами информационной безопасности.

5.2. Разделы, темы дисциплины и виды занятий

очная форма обучения

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в часах)			Индикаторы достижения компетенций
		занятия лекционного типа	занятия семинарского типа / из них в форме практической подготовки (лабораторные работы)	самос-тоятельная работа	
1	Тема 1. Понятие безопасности информации.	2	2	8	ОПК-5.1, ОПК-5.2
2	Тема 2. Международные и российские стандарты по защите информации: их взаимосвязь и различия.	2	2	8	ОПК-5.1, ОПК-5.2
3	Тема 3. Особенности процесса стандартизации и стандарты безопасности в сети Интернет.	2	2	8	ОПК-5.1, ОПК-5.2
4	Тема 4. Особенности государственных стандартов программных продуктов	2	2	8	ОПК-5.1, ОПК-5.2
5	Тема 5. Государственные стандарты: общие положения.	2	2	8	ОПК-5.1, ОПК-5.2
6	Тема 6. Руководящий документ Гостехкоммиссии: Межсетевые экраны	2	2	8	ОПК-5.1, ОПК-5.2
7	Тема 7. Основы сертификации (на примере средств защиты информации).	2	2	8	ОПК-5.1, ОПК-5.2
8	Тема 8. Сертификация на соответствие требованиям по безопасности информации	2	2	8	ОПК-5.1, ОПК-5.2

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в часах)			Индикаторы достижения компетенций
		занятия лекционного типа	занятия семинарского типа / из них в форме практической подготовки (лабораторные работы)	самос-тоятельная работа	
9	Тема 9. Системы сертификации средств защиты информации: требования безопасности информации.	2		9	ОПК-5.1, ОПК-5.2
	Всего	**18**	**16**	**73**	

6. Практические занятия

№ п/п	Наименование раздела, темы дисциплины	Содержание практических работ	Объем (час.)
			Очная форма обучения
1.	Тема 1 Понятие безопасности информации	Определение безопасности информации. – Основные угрозы и уязвимости. – Модели безопасности (конфиденциальность, целостность, доступность).	2
2.	Тема2. Международные и российские стандарты по защите информации	Определение понятий "стандарт" и "нормативный документ". – Обзор международных стандартов (ISO/IEC 27001, ISO/IEC 27002).	2
3.	Тема3. Особенности процесса стандартизации	Определение понятия "стандартизация". – История и эволюция стандартизации. – Значение стандартизации для бизнеса и общества.	2
4.	Тема 4. Особенности государственных стандартов программных продуктов	Определение понятия "государственный стандарт". – История и развитие ГОСТ в области программного обеспечения. – Значение ГОСТ для разработки и внедрения программных продуктов.	2
5.	Тема 5. Государственные стандарты: общие положения	Определение государственных стандартов. – История возникновения и развития государственных стандартов. – Роль стандартов в обеспечении качества продукции и услуг.	2
6.	Тема 6.	Определение линейных однородных рекуррентных	2

№ п/п	Наименование раздела, темы дисциплины	Содержание практических работ	Объем (час.)
			Очная форма обучения
	Руководящий документ Гостехкоммиссии: Межсетевые экраны	соотношений	
7.	Тема 7. Основы сертификации (на примере средств защиты информации)	Определение сертификации. – Роль сертификации в обеспечении безопасности информации. – Основные стандарты и нормативные документы в области сертификации.	2
8.	Тема 8. Сертификация на соответствие требованиям по безопасности информации	Определение сертификации на соответствие. – Основные цели и задачи сертификации в области безопасности информации. – Важность сертификации для организаций и пользователей.	1
9	Тема 9. Системы сертификации средств защиты информации: требования безопасности информац	Определение системы сертификации. – Основные цели и задачи сертификации средств защиты информации. – Роль сертификации в обеспечении безопасности информационных систем.	1
	Всего		**16**

7. Лабораторные работы

Лабораторные работы не предусмотрены.

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Стандарты в сфере информационной безопасности» направлена на:

– освоение нормативных правовых актов и учебной литературы, необходимых для освоения дисциплины;

– самостоятельный поиск информации в Интернете и других источниках;

– выполнение домашних заданий по практическим занятиям;

– подготовку к зачету.

Краткие рекомендации по выполнению самостоятельной работы:

Успешное усвоение дисциплины предполагает большой, упорный, серьезный, систематический труд студентов. Важнейшая его составная часть – выполнение разных видов самостоятельной работы.

1. **Составление тематического конспекта** на основе изученной основной и дополнительной учебной литературы. В тематическом конспекте за основу берется содержание темы, вопросы для обсуждения.

Этапы работы.

1.1 Конспектирование делается только после того, как прочитан или усвоен материал для конспектирования.

1.2. Необходимо мысленно или письменно составить план конспекта. По этому плану и будет строиться конспект далее.

1.3. Составление самого конспекта. Можно сказать, что конспект – это расширенные тезисы, дополненные рассуждениями и доказательствами, содержащимися в материалах для конспекта, а также собственными мыслями и положениями составителя конспекта.

Писать конспект рекомендуется четко и разборчиво. В конспекте можно выделять места текста в зависимости от их значимости. Для этого применяются различного размера буквы, подчеркивания, замечания на полях.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Зачетно-экзаменационные материалыдля промежуточной аттестации (зачет)

1. Информационные ресурсы общества.
2. Модели для выявления и анализа возможностей, рисков и угроз.
3. Управление рисками в организации.
4. Модели для выявления и анализа возможностей, рисков и угроз.
5. Проблемы и перспективы использования внешних ИТ-услуг.
6. Нормативное регулирование построения и функционирование системы защиты информации. ISO/IES 27001-27005.
7. Аутсорсинг информационной безопасности — краткий обзор рынка
8. Нормативная совместимость. Нормативные акты корпоративного управления:
9. Федеральный закон «О персональных данных». Корпоративное управление.
10. Методы оценки эффективности в сфере защиты информации от утечек.
11. Законодательные акты, регулирующие экономические вопросы защиты информации.
12. Система защиты информации и непрерывность бизнеса предприятия.
13. Нормативное регулирование построения и функционирования

системы защиты информации.

14. Особенности применения международных и российских нормативных актов и стандартов.
15. Предмет и задачи курса. Становление и развитие
16. Стандартизация как научная дисциплины, её место в системе наук.
17. Методы исследования проблем стандартизации ,Общенаучные и специальные методы
18. Особенности стандартизации в сети Интернет.
19. Понятие безопасности информации в соответствии с существующими ГОСТами.
20. Основные функции Руководящих разъяснительных документов по защите информации, их особенности.
21. Общие положение международных стандартов информации.
22. Стандарт ISO\IEC 15408-1999 .
23. ГОСТ Р ИСО\ МЭК 15408-2002
24. Критерии безопасности по ГОСТу ИСО\ МЭК 15408-2002
25. Понятие носителя документированной информации
26. Общие и специфические свойства ГОСТа Р ИСО \МЭК 15408-2002
27. Понятия «способ документирования», «средство документирования», «система документирования».
28. Понятия «информационная ёмкость», «информативность», «информационная плотность ».
29. Понятие носителя документированной информации .
30. Тождественность и отличие ГОСТ ИСО\ МЭК 15408-2002 от Международного его аналога.
31. Протоколы защищенности передачи данных SSL(TSL), SET IP v.6.
32. Сущность и особенности IPSes.
33. Унифицированные системы документации.
34. Государственные стандарты на документацию.
35. Описание стандарта SET .
36. Протоколы стандартных способов шифрования.
37. Особенности российского рынка программных продуктов.
38. Регистрация документов и виды распорядительной документации.
39. Государственные стандарты общие положения.
40. РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации.

Образцы билетов

Билет №1

1. Особенности стандартизации в сети Интернет.
2. Понятие носителя документированной информации

Билет №2

1. Унифицированные системы документации.
2. Государственные стандарты общие положения.

10. Оценивание результатов обучения и уровня сформированности компетенций

Оценивание результатов обучения по дисциплине и уровня сформированности компетенций (части компетенции) осуществляется в рамках текущего контроля успеваемости и промежуточной аттестации в соответствии с оценочными материалами.

11. Учебно-методическое обеспечение дисциплины

Основная литература:

1. Мандрица, И. В. Управление проектами по информационной безопасности и экономика защиты информации. Часть 1 / И. В. Мандрица, В. И. Петренко, О. В. Мандрица. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-45723-6. — Текст : электронный // Лань : электронно-библиотечная система. — [Электронный ресурс] URL: https://e.lanbook.com/book/311825 .
2. Петренко В.И., Мандрица И.В. Защита персональных данных в информационных системах. Практикум. – М. Лань, 2022 - 108 с. [Электронный ресурс] – URL: https://lanbook.com/catalog/informatika/zashchita- personalnykh-dannykh-v-informatsionnykh-sistemakh-praktikum/
3. Кудашкин Я. В. Правовое обеспечение безопасности обработки персональных данных в сети интернет. Автореф. дис. на соискание уч. ст. к.ю.н. Специальность: 12.00.13 –Информационное право. Москва – 2019. [Электронный ресурс] – URL: https://istina.msu.ru/download/212806666/1hiKtk:UrCunoF4PcIPFMt1qAIZRF_dTmA/
4. Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы X Межрегиональной научно-практической конференции / под ред. О.М. Голембиовской, М.Ю. Рытова. – Брянск: БГТУ, 2018. – 187 с. [Электронный ресурс] – URL: https://www.tu-bryansk.ru/upload/medialibrary/8d4/Konf_IB_2018.pdf

Дополнительная литература

1. Лапина М. А. Защита персональных данных в информационных системах / М. А. Лапина, М. В. Песков. – Ставрополь: Изд-во СКФУ, 2014. – 199 с. [Электронный ресурс] – URL: https://www.ncfu.ru/export/uploads/imported-from-dle/op/doclinks2015/Metod_UPPDN_10.05.03_19.05.15.pdf

2. Комплексные системы защиты информации предприятия: учебное пособие / В.Т. Еременко, М.Ю. Рытов, О.М. Голембиовская, П.Н. Рязанцев. – Орел: ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», 2016. –116 с. [Электронный ресурс] – URL: https://studfile.net/preview/16707511/page:12/#16707511
3. Такидзе Д.Т. Защита персональных данных в России. // Вестник магистратуры. 2021 №5-4
(116) с. 108-111. [Электронный ресурс] – URL: https://cyberleninka.ru/article/n/zaschita- personalnyh-dannyh-v-rossii
4. Виссия, Х. Э. Принятие решений в информационном обществе : учебное пособие / Х. Э. Виссия, В. В. Краснопрошин, А. Н. Вальвачев. — Санкт-Петербург : Лань, 2022. — 228 с.
— ISBN 978-5-8114-3747-4. — Текст : электронный // Лань : электронно-библиотечная система. [Электронный ресурс] — URL: https://e.lanbook.com/book/206723 .
5. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации – 2-е изд., испр. и доп. – СПб:Университет ИТМО, 2018. – 100 с. [Электронный ресурс] – URL: https://books.ifmo.ru/file/pdf/2372.pdf
6. Исаев А.С., Хлюпина Е.А. «Правовые основы организации защиты персональных данных» – СПб: НИУ ИТМО, 2014. – 106 с. [Электронный ресурс] – URL: https://books.ifmo.ru/file/pdf/1570.pdf
7. Кондрашов А.Э., Варламова Л.Н. Национальные стандарты РФ по различным аспектам защиты информации и информационной безопасности. [Электронный ресурс] – URL: https://www.top-personal.ru/officeworkissue.html?510

Электронные библиотечные системы (ЭБС) и электронные образовательные ресурсы

1. Электронно-библиотечная система ZNANIUM https:// www.znanium.com
2. Универсальная справочно-информационная полнотекстовая база данных периодических изданий «East View» (ИВИС) https://dlib.eastview.com/
3. Электронно-библиотечная система «BOOK.ru» www.book.ru
4. Электронно-библиотечная система «IPRbooks» http://www.iprbookshop.ru/
5. ЭБС «Национальный цифровой ресурс «Руконт» https://lib.rucont.ru/search
6. Образовательная платформа ЮРАЙТ http://www.urait.ru

Электронный каталог Университета – Автоматизированная информационная библиотечная система (АИБС «МегаПро»)

12. Перечень программного обеспечения, профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины

Лицензионное программное обеспечение, в том числе отечественного производства:

– DsktpEdu ALNG LicSARk OLV F1 1Y Acdmc Ent (MS Windows) (подписка на ПО).

Свободно распространяемое программное обеспечение, в том числе отечественного производства:

– 7-Zip (свободный файловый архиватор с высокой степенью сжатия данных) (отечественное ПО).

– FastStone Image Viewer (программа для просмотра изображений в Microsoft Windows (лицензия бесплатного программного обеспечения)).

– Foxit Reader (Бесплатное прикладное программное обеспечение для просмотра электронных документов в стандарте PDF (лицензия бесплатного программного обеспечения)).

– Indigo (система программ для создания и проведения компьютерного тестирования знаний).

– Google Crome, ЯндексБраузер (браузер).

– Adobe Acrobat Reader DC (• ПО для просмотра, печати и комментирования документов в формате PDF)

– Visual Studio Code (интегрированная среда разработки программного обеспечения)

Профессиональные базы данных не используются.

Информационные справочные системы:

– СПС КонсультантПлюс. Компьютерная справочная правовая система, широко используется учеными, студентами и преподавателями (подписка на ПО)

Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронно-библиотечной

13. Материально–техническое обеспечение дисциплины

Образовательный процесс обеспечен учебными аудиториями для проведения учебных занятий, а именно для проведения занятий лекционного типа, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещениями для самостоятельной работы студентов.

Учебная аудитория для проведения занятий лекционного типа

Рабочее место преподавателя (стол, стул), рабочие места обучающихся, доска для написания мелом, кафедра.

Технические средства обучения: персональный компьютер-1, мультимедийное оборудование (проектор, проекционный экран) - 1

Учебная аудитория для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Рабочее место преподавателя (стол, стул), рабочие места обучающихся, доска для написания мелом, кафедра.

Технические средства обучения: персональный компьютер-1, мультимедийное оборудование (проектор, проекционный экран) – 1.

Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду института.

Рабочие места обучающихся.

Технические средства обучения: персональный компьютер - 13.

Учебные аудитории соответствуют действующим противопожарным правилам и нормам, укомплектованы учебной мебелью

Обновление рабочей программы дисциплины (модуля)

Наименование раздела рабочей программы, в который внесены изменения

(измененное содержание раздела)

обсуждено и рекомендовано к утверждению решением кафедры наименование кафедры
от ___ _____ 20_ г., протокол № ___

одобрено Научно-методическим советом _____ от ___ _____ 20__ г., протокол №____