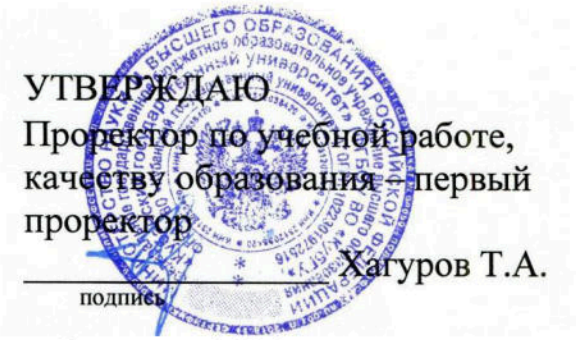
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет компьютерных технологий и прикладной математики



УТВЕРЖДАЮ
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Хагуров Т.А.
подпись
«2» июня 2026г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.01 «ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление
подготовки/специальность 10.04.01 Информационная безопасность

Направленность (профиль) / специализация Информационная безопасность интеллектуальных автоматизированных систем

Форма обучения _____очная_____

Квалификация _____магистр_____

Краснодар
2026

Рабочая программа дисциплины «ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.04.01 «Информационная безопасность»

Программу составили:

Шиян Валерий Игоревич, ст. преподаватель _____
Ф.И.О., должность, ученая степень, ученое звание подпись

Приходько Татьяна Александровна, доцент, к. т. н. _____
Ф.И.О., должность, ученая степень, ученое звание подпись

Рабочая программа дисциплины «ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» обсуждена на заседании кафедры Вычислительных технологий
протокол № 11 «14 » мая 2026 г.
И.о. заведующего кафедрой (разработчика) Приходько Т.А. _____
фамилия, инициалы подпись

Рабочая программа дисциплины «ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» утверждена на заседании кафедры Вычислительных технологий
протокол № 11 «14 » мая 2026 г.
И.о. заведующего кафедрой (разработчика) Приходько Т.А. _____
фамилия, инициалы подпись

Утверждена на заседании учебно-методической комиссии факультета Компьютерных Технологий и Прикладной Математики
протокол №3 от «15» мая 2026 г.
Председатель УМК факультета

Н. Ю. Добровольская _____
подпись

Рецензенты:

Гаркуша О.В., доцент кафедры информационных технологий ФБГОУ ВО «Кубанский государственный университет», кандидат физико-математических наук.

Схаляхо Ч.А., доцент КВВУ им. С.М. Штеменко, к.ф.-м.н., доцент

1. Цели и задачи освоения дисциплины

1.1 Цель освоения дисциплины

Целью преподавания и изучения дисциплины «Теоретические основы информационной безопасности» является подготовка студентов, обладающих глубокими теоретическими знаниями и практическими навыками в области информационной безопасности. Студенты должны быть способны эффективно анализировать и проектировать защищенные информационные системы, а также применять современные технологии и инструменты для обеспечения безопасности и надежности данных в различных организациях.

1.2 Задачи дисциплины

Студент должен знать основные понятия, методы и технологии информационной безопасности; уметь применять методы обеспечения информационной безопасности; владеть технологиями реализации систем защиты информации.

1.3 Место дисциплины (модуля) в образовательной программе

Дисциплина «Теоретические основы информационной безопасности» относится к Части, формируемой участниками образовательных отношений блока Б1 Дисциплины (модули).

Знания, получаемые при изучении теоретических основ информационной безопасности, используются при изучении таких дисциплин профессионального цикла учебного плана магистратуры как “ Стандарты в сфере информационной безопасности”, “Спецсеминар”, “Безопасные методы извлечения информации из сетевых источников”, “Вероятностные модели защищенных компьютерных сетей”, “Прикладные логики интеллектуальных автоматизированных систем”, “Спецификация и верификация программ методом Model Checking”, “Подготовка к сдаче и сдача государственного экзамена”, “Подготовка к процедуре защиты и защита выпускной квалификационной работы ”, а также при работе над выпускной работой.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся универсальных/ общепрофессиональных/ профессиональных компетенций (УК/ОПК/ПК):

Код и наименование индикатора*	**Результаты обучения по дисциплине** ***(знает, умеет, владеет (навыки и/или опыт деятельности))***
ПК-3 Способен разрабатывать проекты инструкций и методических документов по обеспечению информационной безопасности в организации	
ПК-3.1 Знает структуру внутренних методических документов и инструкций по информационной безопасности в организации	Знает структуру внутренних методических документов и инструкций по информационной безопасности в организации, включая разработку и внедрение политик безопасности, процедуры управления рисками, а также методики оценки и контроля соблюдения требований информационной безопасности.
ПК-3.2 Умеет разрабатывать проекты инструкций по информационной безопасности для организации	Умеет разрабатывать проекты инструкций по информационной безопасности для организации, применяя теоретические и практические знания для создания и внедрения эффективных процедур и методик, обеспечивающих защиту информации и соответствие требованиям безопасности.

Код и наименование индикатора*	Результаты обучения по дисциплине *(знает, умеет, владеет (навыки и/или опыт деятельности))*
ПК-3.3 Умеет разрабатывать методические документы по обеспечению информационной безопасности в организации	Владеет навыками разработки методических документов по обеспечению информационной безопасности в организации, включая создание политик и процедур, а также использование современных технологий и инструментов для мониторинга безопасности, анализа инцидентов и реагирования на угрозы.

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.
Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 4 зач. ед. (144 часа), их распределение по видам работ представлено в таблице (для студентов ОФО).

Вид учебной работы	Всего часов	Семестры (часы)	
		1	
Контактная работа в том числе:	**92,2**	**92,2**	
Аудиторные занятия (всего):	72	72	
В том числе:			
Занятия лекционного типа	36	36	
Занятия семинарского типа (семинары, практ. занятия)			
Лабораторные занятия	36	36	
Иная контактная работа	20,2	20,2	
Контроль самостоятельной работы (КСР)	20	20	
Промежуточная аттестация (ИКР)	0,2	0,2	
Самостоятельная работа, в том числе	**51,8**	**51,8**	
В том числе:			
Курсовая работа			
Проработка учебного (теоретического) материала	25	25	
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)	20	20	
Реферат			
Подготовка к текущему контролю	6,8	6,8	
Контроль:	**зачёт**	**зачёт**	
Общая трудоёмкость	**в час**	**144**	
	в т.ч. контактная работа	**92,2**	

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоёмкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 1 семестре *(очная форма)*

№ раздела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Раздел 1. Защита информации как объективная закономерность эволюции постиндустриального общества.	16,5	5		5	6,5
2.	Раздел 2. Информационная безопасность личности, общества и государства: социально-правовые аспекты.	16,5	5		5	6,5
3.	Раздел 3. Угрозы информационной безопасности в компьютерных системах.	16,5	5		5	6,5
4.	Раздел 4. Общая характеристика средств и методов защиты информации	16,5	5		5	6,5
5.	Раздел 5. Организационно-правовое обеспечение защиты информации.	16,5	5		5	6,5
6.	Раздел 6. Защита компьютерных систем от несанкционированного вмешательства.	16,5	5		5	6,5
7.	Раздел 7. Криптографические методы защиты информации.	16,5	5		5	6,5
8.	Раздел 8. Комплексная защита информации в компьютерных системах.	8,3	1		1	6,3
	ИТОГО по разделам дисциплины	123,8	36		36	51,8
	Контроль самостоятельной работы (КСР)	20				
	Промежуточная аттестация (ИКР)	0,2				
	Общая трудоёмкость по дисциплине	144				

2.3 Содержание разделов дисциплины

2.3.1 Занятия лекционного типа

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Раздел 1. Защита информации как объективная закономерность эволюции постиндустриального общества.	Предмет, содержание и задачи курса, его место среди других дисциплин учебного плана. Формы отчетности, основная и дополнительная литература. Информация и ее роль в современном обществе. Эволюция информационных процессов и информационных отношений. Сущность и цели информатизации. Глобализация информационных отношений. Информационные технологии. Информационные ресурсы услуги. Объективная необходимость и общественная потребность в защите информации. Сущность защиты информации. Правовое регулирование вопросов защиты информации.	ЛР
2	Раздел 2. Информационная безопасность личности, общества и государства: социально-правовые аспекты.	Право на информацию в системе гражданских прав личности. Возможные ограничения. Массовая информация и информация ограниченного доступа. Неприкосновенность частной жизни, персональные данные. Виды тайн. Коммерческая тайна. Государственная тайна. Документированная информация как объект права собственности. Информационная безопасность как составляющая национальной безопасности РФ. Информационные войны, информационное оружие. Доктрина информационной безопасности РФ.	ЛР
3	Раздел 3. Угрозы информационной безопасности в компьютерных системах.	Компьютерная система (КС) как объект защиты информации. Понятие угрозы информационной безопасности в КС. Классификация и общий анализ угроз информационной безопасности в КС. Случайные угрозы информационной безопасности. Преднамеренные угрозы информационной безопасности. Сбои и отказы. Общие сведения о кодах для обнаружения и исправления случайных ошибок. Система охраны объектов КС. Основные виды технических каналов утечки информации. Техника промышленного шпионажа. Общие сведения о компьютерных вирусах. Классификация компьютерных вирусов. Механизмы заражения компьютерными вирусами.	ЛР

4	Раздел 4. Общая характеристика средств и методов защиты информации	Эволюция концепции информационной безопасности в компьютерных системах. Реализация угроз информационной безопасности путём несанкционированного доступа. Модель поведения потенциального нарушителя Обобщённые модели систем защиты информации. Основные принципы обеспечения информационной безопасности в КС. Понятие комплексной системы защиты информации (КСЗИ).	ЛР
5	Раздел 5. Организационно-правовое обеспечение защиты информации.	Общая характеристика организационного обеспечения защиты информации. Основные задачи службы безопасности предприятия. Организационные мероприятия, обеспечивающие защиту информации. Необходимость правового регулирования в области защиты информации. Законодательство РФ в этой области. Стандартизация в области обеспечения информационной безопасности; международные и отечественные нормативные и руководящие документы.	ЛР
6	Раздел 6. Защита компьютерных систем от несанкционированного вмешательства.	Модели управления доступом к информации в КС. Идентификация и аутентификация пользователей и разграничение их доступа к компьютерным ресурсам. Защита программных средств от несанкционированного копирования и исследования. Защита от несанкционированного изменения структуры КС в процессе эксплуатации. Контроль целостности программ и данных в процессе эксплуатации. Регистрация и контроль действий пользователей.	ЛР
7	Раздел 7. Криптографические методы защиты информации.	Основные понятия и этапы развития криптографии. Классификация криптографических средств. Основные методы шифрования. Шифрование методами замены и перестановки. Аналитические и аддитивные методы шифрования. Системы шифрования с открытым ключом.	ЛР
8	Раздел 8. Комплексная защита информации в компьютерных системах.	Концепция создания КСЗИ в КС. Технология разработки КСЗИ. Функционирование комплексных систем защиты информации. Аудит в защищенных КС. Организационная структура КСЗИ.	ЛР

2.3.2 Занятия семинарского типа

Учебным планом не предусмотрены.

2.3.3 Лабораторные занятия

№ работы	№ раздела дисциплины	Наименование лабораторных работ

1	1	Лабораторная работа №1.1. Роль информации в современном мире.
2	1	Лабораторная работа №1.2. Основные понятия в информационной безопасности.
2	2	Лабораторная работа №2.1. Виды информации.
2	2	Лабораторная работа №2.2. Доктрина информационной безопасности РФ.
3	3	Лабораторная работа №3.1. Классификация и общий анализ угроз информационной безопасности в КС.
3	3	Лабораторная работа №3.2. Система охраны объектов КС.
4	4	Лабораторная работа №4.1. Средства защиты информации в КС.
4	4	Лабораторная работа №4.2. Методы защиты информации в КС..
5	5	Лабораторная работа №5.1. Основные задачи службы безопасности предприятия.
5	5	Лабораторная работа №5.2. Стандартизация в области обеспечения информационной безопасности..
6	6	Лабораторная работа №6.1. Модели управления доступом к информации в КС.
6	6	Лабораторная работа №6.2. Регистрация и контроль действий пользователей.
7	7	Лабораторная работа №7.1. Классификация криптографических средств.
7	7	Лабораторная работа №7.2. Аналитические и аддитивные методы шифрования.
8	8	Лабораторная работа №8.1. Технология разработки КСЗИ.

2.3.4 Примерная тематика курсовых работ (проектов)

Учебным планом не предусмотрены.

2.3.5 Самостоятельное изучение разделов дисциплины

Раздел 4. Общая характеристика средств и методов защиты информации
Раздел 5. Организационно-правовое обеспечение защиты информации.

3. Образовательные технологии

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
1	Л	Компьютерные презентации и обсуждение	18
	ЛР	Разбор конкретных ситуаций (задач) с использованием штатного ПО, выполнение тестов на знание терминологии и сведений из области теоретические основы информационной безопасности	36
Итого:			54

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

4.1 Фонд оценочных средств для проведения текущего контроля

Фонд оценочных средств дисциплины состоит из средств текущего контроля выполнения заданий, лабораторных работ, средств итоговой аттестации (зачет в 1 семестре).

Оценка успеваемости осуществляется по результатам:

- выполнения лабораторных работ;
- ответов на теоретические вопросы при сдаче лабораторных работ;
- ответа на зачете (для выявления знания и понимания теоретического материала дисциплины).

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на зачете;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1.	Раздел 1. Защита информации как объективная закономерность эволюции постиндустриального общества.	ПК-3	ЛР	Вопросы 1-6
2.	Раздел 2.	ПК-3	ЛР	Вопросы 7-12

	Информационная безопасность личности, общества и государства: социально-правовые аспекты.			
3.	Раздел 3. Угрозы информационной безопасности в компьютерных системах.	ПК-3	ЛР	Вопрос 13-18
4.	Раздел 4. Общая характеристика средств и методов защиты информации	ПК-3	ЛР	Вопросы 19-24
5.	Раздел 5. Организационно-правовое обеспечение защиты информации.	ПК-3	ЛР	Вопросы 25-30
6.	Раздел 6. Защита компьютерных систем от несанкционированного вмешательства.	ПК-3	ЛР	Вопросы 31-36
7.	Раздел 7. Криптографические методы защиты информации.	ПК-3	ЛР	Вопросы 37-42
8.	Раздел 8. Комплексная защита информации в компьютерных системах.	ПК-3	ЛР	Вопросы 43-47

Показатели, критерии и шкала оценки сформированных компетенций

№ п/п	Код и наименование индикатора	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежу-точная аттестация
Соответствие освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **удовлетворительно /зачтено**)				
<u>на пороговом уровне</u>:				
1	ПК-3.1 Знает структуру внутренних методических документов и инструкций по информационной безопасности в организации	Знает основные элементы структуры внутренних методических документов и инструкций по информационной безопасности в организации, понимает принципы разработки и внедрения политик безопасности, умеет	опрос по теме, лабораторная работа	Вопросы 1-15, выносимые на зачет

		ориентироваться в процедурах управления рисками и методиках оценки и контроля соблюдения требований информационной безопасности.		
2	ПК-3.2 Умеет разрабатывать проекты инструкций по информационной безопасности для организации	Умеет разрабатывать простые проекты инструкций по информационной безопасности для организации, применяя базовые теоретические и практические знания для создания и внедрения процедур и методик, обеспечивающих защиту информации и соответствие требованиям безопасности.	опрос по теме, лабораторная работа	Вопросы 16-31, выносимые на зачет
3	ПК-3.3 Умеет разрабатывать методические документы по обеспечению информационной безопасности в организации	Владеет базовыми навыками разработки методических документов по обеспечению информационной безопасности в организации, включая участие в создании политик и процедур, а также использование типовых технологий и инструментов для мониторинга безопасности, анализа инцидентов и реагирования на угрозы.	опрос по теме, лабораторная работа	Вопросы 32-47, выносимые на зачет
Соответствие освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **хорошо /зачтено**)				
<u>на базовом уровне:</u>				
4	ПК-3.1 Знает структуру внутренних методических документов и инструкций по информационной безопасности в организации	Знаком со структурой внутренних методических документов и инструкций по информационной безопасности в организации, имеет представление о разработке и внедрении политик безопасности, процедурах управления рисками, а также	опрос по теме, лабораторная работа	Вопросы 1-15, выносимые на зачет

		методиках оценки и контроля соблюдения требований информационной безопасности.		
5	ПК-3.2 Умеет разрабатывать проекты инструкций по информационной безопасности для организации	Может принимать участие в разработке инструкций по информационной безопасности для организации, используя базовые теоретические и практические знания для создания и внедрения простых процедур и методик, обеспечивающих защиту информации и соответствие требованиям безопасности.	опрос по теме, лабораторная работа	Вопросы 16-31, выносимые на зачет
6	ПК-3.3 Умеет разрабатывать методические документы по обеспечению информационной безопасности в организации	Обладает начальными навыками разработки методических документов по обеспечению информационной безопасности в организации, включая участие в создании политик и процедур, а также использовании базовых инструментов для мониторинга безопасности и анализа инцидентов.	опрос по теме, лабораторная работа	Вопросы 32-47, выносимые на зачет
Соответствие освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **отлично /зачтено**)				
<u>на продвинутом уровне:</u>				
7	ПК-3.1 Знает структуру внутренних методических документов и инструкций по информационной безопасности в организации	Знает структуру внутренних методических документов и инструкций по информационной безопасности в организации, включая разработку и внедрение политик безопасности, процедуры управления рисками, а также методики оценки и контроля соблюдения требований информационной	опрос по теме, лабораторная работа	Вопросы 1-15, выносимые на зачет

		безопасности.		
8	ПК-3.2 Умеет разрабатывать проекты инструкций по информационной безопасности для организации	Умеет разрабатывать проекты инструкций по информационной безопасности для организации, применяя теоретические и практические знания для создания и внедрения эффективных процедур и методик, обеспечивающих защиту информации и соответствие требованиям безопасности.	опрос по теме, лабораторная работа	Вопросы 16-31, выносимые на зачет
9	ПК-3.3 Умеет разрабатывать методические документы по обеспечению информационной безопасности в организации	Владеет навыками разработки методических документов по обеспечению информационной безопасности в организации, включая создание политик и процедур, а также использование современных технологий и инструментов для мониторинга безопасности, анализа инцидентов и реагирования на угрозы.	опрос по теме, лабораторная работа	Вопросы 32-47, выносимые на зачет

Фонд оценочных средств дисциплины состоит из средств текущего контроля выполнения заданий, лабораторных работ, средств для итоговой аттестации (зачет в 1 семестре).

Оценка успеваемости осуществляется по результатам:
- выполнения лабораторных работ;
- ответа на зачёте

Текущий контроль включает контрольную работу по итогам первой половины курса.

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 материалы для промежуточной аттестации (экзамен/зачет)

1. Информация как средство отражения окружающего мира и как средство его познания. Количественные оценки и показатели качества информации.
2. Эволюция информационных процессов в обществе. Информатизация и компьютеризация. Информационные ресурсы, продукты и услуги. Объективная необходимость и общественная потребность защиты информации.
3. Информационная безопасность личности, общества и государства. Массовая и конфиденциальная информация. Виды тайн.
4. Информационная безопасность как составляющая национальной безопасности. Задачи государства в этой области. Информационное оружие, информационные войны и терроризм. Государственные органы РФ, реализующие функции обеспечения информационной безопасности.
5. Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в КС. Классификация угроз.
6. Общая характеристика случайных угроз информационной безопасности в КС.
7. Общая характеристика преднамеренных угроз информационной безопасности в КС.
8. Эволюция концепции информационной безопасности в КС. Основные принципы обеспечения информационной безопасности в КС. Политика безопасности.
9. Реализация угроз информационной безопасности в КС путем несанкционированного доступа (НСД). Классификация каналов НСД. Собирательный образ потенциального нарушителя.
10. Обобщенные модели системы защиты информации в КС. Одноуровневые, многоуровневые и многозвенные модели. Общая характеристика средств и методов защиты информации в КС.
11. Общая характеристика организационных мероприятий, обеспечивающих информационную безопасность КС. Основные задачи службы безопасности.
12. Необходимость правового регулирования в области защиты информации. Информация как объект права собственности. Правоотношения собственника, и правообладателя информационных ресурсов.
13. Отечественное законодательство в области информации и защиты информации.
14. Ответственность за правонарушения при работе с компьютерными системами.
15. Эксплуатационная надежность КС как источник возникновения случайных угроз информационной безопасности. Пути ее повышения. Резервирование технических средств. Программно-аппаратный контроль и тестирование.
16. Оптимизация взаимодействия пользователя с КС как средство предотвращения ошибочных операций случайного характера.
17. Помехоустойчивое кодирование. Избыточные коды для обнаружения и исправления случайных ошибок в работе КС.
18. Дублирование информации как средство парирования угроз безопасности в КС. Многоуровневое дублирование. Технология RAID.
19. Минимизация ущерба, наносимого КС авариями и стихийными бедствиями.
20. Система охраны объектов КС.
21. Общая характеристика технических каналов утечки информации в КС.
22. Методы и средства защиты информации в КС от утечки по каналам побочных электромагнитных излучений и наводок.
23. Средства противодействия подслушивания и дистанционному наблюдению.
24. Базовые принципы, лежащие в основе моделей политики безопасности в КС. Матричная (дискреционная) модель и мандатная (полномочная) модель управления доступом к ресурсам КС.
25. Идентификация и аутентификация субъектов доступа к ресурсам КС. Парольные методы и оценка их эффективности. Биометрические методы.
26. Средства и методы разграничения доступа к ресурсам КС.
27. Защита программных средств КС от несанкционированного копирования и исследования.
28. Защита от несанкционированного изменения структуры КС в процессе эксплуатации.
29. Общие понятия, история развития и классификация криптографических средств.

30. Общая характеристика различных методов шифрования. Криптостойкость. Шифрование с симметричным и несимметричным ключами.
31. Шифрование методом замены. Простая, полиалфавитная и многозначная замена.
32. Аналитические методы шифрования.
33. Шифрование методом гаммирования.
34. Отечественные и зарубежные стандарты шифрования.
35. Общая характеристика и классификация компьютерных вирусов.
36. Механизм заражения файловыми и загрузочными вирусами. Особенности макровирусов.
37. Средства, используемые для обнаружения компьютерных вирусов.
38. Профилактика заражения компьютерными вирусами.
39. Антивирусные средства для лечения и удаления компьютерных вирусов. Программыполифаги. Эвристические анализаторы.
40. Чем вызвана необходимость разработки стандартов по защите информации? Охарактеризуйте отечественные нормативы и зарубежные стандарты в этой области.
41. Содержательный смысл понятия комплексной системы защиты информации (КСЗИ) в компьютерных системах. Основные принципы и положения, реализующие системный подход к построению КСЗИ.
42. Функции и задачи защиты, механизмы защиты, уровень защищенности, управление защитой и другие базовые понятия, используемые при формировании КСЗИ.
43. Общетеоретическая постановка задачи оптимизации КСЗИ на основе выбранного критерия эффективности защиты.
44. Основные технологические этапы разработки КСЗИ.
45. Средства моделирования, применяемые для оптимизации КСЗИ.
46. Организационно-технические мероприятия, проводимые в процессе эксплуатации КСЗИ.
47. Задачи, решаемые подсистемой аудита в составе защищенных КС.

Образцы билетов

Билет №1

1. Механизм заражения файловыми и загрузочными вирусами. Особенности макровирусов.
2. Содержательный смысл понятия комплексной системы защиты информации (КСЗИ) в компьютерных системах. Основные принципы и положения, реализующие системный подход к построению КСЗИ.

Билет №2

1. Основные технологические этапы разработки КСЗИ.
2. Задачи, решаемые подсистемой аудита в составе защищенных КС.

4.2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

4.2.1 Методические рекомендации к сдаче зачета

Оценка успеваемости осуществляется по результатам:

- выполнения лабораторных работ;
- ответов на теоретические вопросы при сдаче лабораторных работ;
- ответа на зачете (для выявления знания и понимания теоретического материала дисциплины).

4.2.2 Критерии оценивания результатов обучения

Оценка «зачтено»: точные формулировки алгоритмов, теорем и правильные

доказательства; точные определения математических объектов и ясные и правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «не зачтено»: отсутствует ответ хотя бы на один из вопросов или имеются существенные неточности в формулировках алгоритмов, теорем, приведены неправильные доказательства; неверные определения математических объектов и неправильные определения объектов, характеризующихся неформализованными понятиями.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

- при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на зачете;
- при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;
- при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
– в печатной форме увеличенным шрифтом,
– в форме электронного документа.
Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

5.1 Основная литература

1. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем[Электронный ресурс]: учебное пособие / Е.В. Глинская, Н.В. Чичварин. -

Москва: ИНФРА-М, 2021. -118 с. + Доп. материалы. - (Высшее образование: Бакалавриат).- Режим доступа: https://znanium.com/read?id=362430.

2. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс]: учебное пособие / В.Ф. Шаньгин. - Москва: ФОРУМ: ИНФРА-М, 2022. - 592 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Режим доступа: https://znanium.com/read?id=389857.
3. Нестеров, С. А. Основы информационной безопасности : учебник / С. А. Нестеров. - 3-е изд., стер. - Санкт-Петербург : Лань, 2024. - 324 с. - URL: https://e.lanbook.com/book/370967 - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-49077-6. - Текст : электронный..
4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. - Москва : Юрайт, 2023. - 325 с. - URL: https://urait.ru/bcode/511239. - Режим доступа: для авториз. пользователей. - ISBN 978-5-534-03600-8. - Текст : электронный..

5.2 Дополнительная литература

5. М. Ховард, Д. Лебланк Защищенный код. М.: ИД Русская редакция, 2004.− 704 с.
6. Проскурин В. Г. Защита программ и данных. М.: ИДАкадемия, 2012.− 208 с.
7. T. Howlett Open source security tools. Practical applications for security. Prantice Hall, 2004.− 600 p.
8. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие.− М.: ИД Форум – Инфра, 2013.− 416 с.
9. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. М.: Горячая линия – Телеком, 2000.− 452 с.
10. Хорев П. Б. Методы и средства защиты информации в компьютерных системах. М.: Академия, 2008.− 256 с.
11. Девянин П. Н. Модели безопасности компьютерных систем. Учебное пособие.−М.: Академия, 2005.− 144 с
12. Расторгуев, С. П. Основы информационной безопасности : учебное пособие для студентов вузов / С. П. Расторгуев. - 2-е изд., стер. - М. : Академия, 2009. - 187 с. : ил. - (Высшее профессиональное образование. Информационная безопасность). - Библиогр.: с. 180-181. - ISBN 9785769564864 : 240.90. - Текст : непосредственный.
13. Галатенко, В. А. Основы информационной безопасности : учебное пособие для студентов вузов / В. А. Галатенко ; под ред. В. Б. Бетелина. - Изд. 4-е. - М. : Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний, 2008. - 205 с. - (Основы информационных технологий). - Библиогр.: с. 200-202. - ISBN 9785947748215 : 224.00. - Текст : непосредственный..

5.2 Периодические издания

1. Базы данных компании «ИВИС» https://eivis.ru/
2. Полнотекстовая коллекция журналов на платформе РЦНИ (электронные версии научных журналов РАН) https://journals.rcsi.science/

5.3 Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронная библиотека Научной библиотеки КубГУ http://megapro.kubsu.ru/MegaPro/Web

Электронный каталог

Поступления литературы в библиотеки филиалов

Поступления диссертаций и авторефератов

Статьи из периодики и научных сборников с 2016 г.
Статьи из периодики и научных сборников до 2016 г.
Газеты и журналы
Электронная библиотека трудов ученых КубГУ

Электронно-библиотечные системы (ЭБС)

1. ЭБС «Университетская библиотека онлайн» http://www.biblioclub.ru/
2. ЭБС «Лань» https://e.lanbook.com
3. Образовательная платформа «Юрайт» https://urait.ru/
4. ЭБС «ZNANIUM» https://znanium.ru/
5. ЭБС «BOOK.ru» https://www.book.ru

Профессиональные базы данных российские

1. Национальная электронная библиотека https://rusneb.ru/
2. Базы данных компании «ИВИС» https://eivis.ru/
3. Научная электронная библиотека eLIBRARY.RU http://www.elibrary.ru/
4. МИАН. Полнотекстовая коллекция математических журналов http://www.mathnet.ru
5. Журнал «Квантовая электроника» https://quantum-electron.lebedev.ru/arhiv/
6. Журнал «Успехи физических наук» https://ufn.ru/
7. Полнотекстовая коллекция журналов на платформе РЦНИ https://journals.rcsi.science/
8. Президентская библиотека им. Б. Н. Ельцина https://www.prlib.ru/
9. Электронная библиотечная система социогуманитарного знания «SOCHUM» https://sochum.ru/

Информационные справочные системы

1. КонсультантПлюс — справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Профессиональные базы данных зарубежные

1. Журналы издательства Wiley https://onlinelibrary.wiley.com/
2. Полнотекстовая коллекция книг eBook Collections издательства SAGE Publications https://sk.sagepub.com/books/discipline
3. Полнотекстовая коллекция книг EBSCO eBook https://books.kubsu.ru/
4. Ресурсы Springer Nature https://link.springer.com/; https://www.nature.com/
5. Chemical Abstracts Service (CAS) SciFinder Discovery Platform https://scifinder-n.cas.org
6. Questel. База данных Orbit Premium edition https://www.orbit.com
7. Полнотекстовые коллекции книг American Institute of Physics Publishing (AIPP Ebook) https://pubs.aip.org/books
8. Полнотекстовая архивная коллекция журналов American Institute of Physics Publishing (AIPP Digital Archive) https://pubs.aip.org/
9. China National Knowledge Infrastructure. БД CNKI Academic Reference https://ar.oversea.cnki.net/

Базы данных открытого доступа

1. КиберЛенинка http://cyberleninka.ru/
2. Американская патентная база данных https://www.uspto.gov/patents/search/patent-public-search
3. Лекториум ТВ — видеолекции ведущих лекторов России http://www.lektorium.tv/
4. Приоритетные научные направления РУДН. Специальные коллекции https://priority-lib.rudn.ru/

Базы данных КубГУ

1. Открытая среда модульного динамического обучения КубГУ https://openedu.kubsu.ru/
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://infoneeds.kubsu.ru/
3. Электронный архив документов КубГУ http://docspace.kubsu.ru/

6. Методические указания для обучающихся по освоению дисциплины

По курсу предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал, лабораторных работ, контрольной работы, зачета и экзамена.

Важнейшим этапом курса является самостоятельная работа по дисциплине с использованием указанных литературных источников и методических указаний автора курса.

Виды и формы СР, сроки выполнения, формы контроля приведены выше в данном документе.

Для лучшего освоения дисциплины при защите ЛР студент должен ответить на несколько вопросов из лекционной части курса.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

7. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

7.1 Перечень информационных технологий

– Проверка домашних заданий и консультирование посредством электронной почты.
– Использование электронных презентаций при проведении лекций и практических занятий.

7.2 Перечень необходимого программного обеспечения

1. OS Windows, MS Office
2. Microsoft Visual Studio Community.
3. СУБД PostgreeSQL
4. СУБД MS SQL Server Developer Edition.
5. Lucidchart – онлайн-платформа.
6. Star UML.
7. Антивирус.

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа (ауд. 129, 131, А305.)	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	PowerPoint.
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (ауд. 147,148)	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	Аудитория, (кабинет) – компьютерный класс
Учебные аудитории для проведения лабораторных работ. Лаборатория 102,105,106	Мебель: учебная мебель Технические средства обучения: компьютер	Лаборатория, укомплектованная специализированными техническими средствами обучения – компьютерный класс, с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную

		среду университета

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	OS Windows, MS Office Microsoft Visual Studio Community. СУБД MS SQL Server Developer Edition. СУБД PostgreeSQL Lucidchart – онлайн-платформа. Star UML. Антивирус.
Помещение для самостоятельной работы обучающихся (ауд. 105, 148,150)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	OS Windows, MS Office Microsoft Visual Studio Community. СУБД PostgreeSQL СУБД MS SQL Server Developer Edition. Lucidchart – онлайн-платформа. Star UML. Антивирус.