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

УТВЕРЖДАЮ
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Г.А. Матуров
подпись
«31» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ФТД.03 ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Направление подготовки 01.03.01 Математика

Направленность (профиль) Математическое моделирование
Преподавание математики и информатики

Форма обучения очная

Квалификация бакалавр

Краснодар 2024

Рабочая программа дисциплины Цифровая безопасность
составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки **01.03.01 Математика**

код и наименование направления подготовки

Программу составил(и):
А.В. Рожков, профессор, д.ф.-м.н., профессор

Рабочая программа дисциплины Цифровая безопасность
утверждена на заседании кафедры функционального анализа и алгебры
протокол № 12 «07» мая 2024 г.
Заведующий кафедрой функционального анализа и алгебры
Барсукова В.Ю.

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук
протокол № 3 «14» мая 2024 г.
Председатель УМК факультета Шмалько С.П.
фамилия, инициалы

подпись

Рецензенты:
Савин В.Н., к.тех.наук, доцент. и.о. заведующего кафедрой высшей математики КубГТУ

Лежнев А. В. к.ф.-м.н., зав. кафедрой математических и компьютерных методов КубГУ

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Цель освоения дисциплины – решение задач информатизации и защиты информации. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

1.2 Задачи дисциплины.

Задачи освоения дисциплины «Цифровая безопасность»: Изучение основных концепций, терминологии и принципов цифровой безопасности, приобретение практических навыков в области защиты сетевых инфраструктур и управления доступом, разработка и анализ политик безопасности и систем управления информационной безопасностью.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Цифровая безопасность» является факультативной дисциплиной. В соответствии с рабочим учебным планом дисциплина изучается на 3 курсе по очной форме. Вид промежуточной аттестации: зачет.

Курс «Цифровая безопасность» продолжает начатое на двух курсах математическое образование и студентов соответствующего направления подготовки. Слушатели должны владеть знаниями в рамках программы курсов «Алгебра», «Дискретная математика и математическая логика», «Технологии программирования и работы на ЭВМ»,.

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 следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ОПК-4. Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
ОПК-4.1 Обладает базовыми знаниями в области информатики, программирования и информационно-коммуникационных технологий, информационной безопасности ОПК-4.2 Использует имеющиеся знания в области информационно-коммуникационных технологий и с учетом основных требований информационной безопасности для решения задач математики ОПК-4.3 Применяет навыки решения профессиональных задач с использованием новейших информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать: о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности государства; о методологии создания систем защиты информации; Уметь: выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований; Владеть: анализом информационной инфраструктуры государства; формальной постановкой и решением задачи обеспечения информационной безопасности компьютерных систем.

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 2 зач. ед. (72 часа), их распределение по видам работ представлено в таблице.

Вид учебной работы		Всего часов	Семестры (часы)			
			5			
Контактная работа, в том числе:						
Аудиторные занятия (всего):		**34**	**34**			
Занятия лекционного типа		16	16	-	-	-
Лабораторные занятия		18	18	-	-	-
Занятия семинарского типа (семинары, практические занятия)				-	-	-
Иная контактная работа:						
Контроль самостоятельной работы (КСР)		4	4			
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:		**33.8**	**33.8**			
Курсовая работа		-	-	-	-	-
Проработка учебного (теоретического) материала		10	10	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		10	10	-	-	-
Реферат		6	6	-	-	-
Подготовка к текущему контролю		7,8	7,8	-	-	-
Контроль:						
Подготовка к экзамену		-	-			
Общая трудоемкость	**час.**	**72**	**72**	**-**	**-**	**-**
	в том числе контактная работа	**38,2**	**38,2**			
	зач. ед	**2**	**2**			

2.2 Содержание дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 5 семестре *(очная форма)*

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Аппаратная часть компьютерных и информационных сетей. Протоколы интернета, выбор операционной системы. Устройство компьютера, основное программное обеспечение.	16	4		4	8
2.	Техническое обслуживание компьютера. Аппаратные неполадки. Работа с BIOS. Ошибки подключении внешних устройств, звук, монитор, принтер, сканер, фото, видео, ТВ, телефон-смартфон. Блоки питания, вентиляторы, источники питания. Дефрагментация диска и др.	16	4		4	8

3.	Программная защита компьютера. Восстановление потерянных данных. Обслуживание HDD и SSD. Антивирусы, наблюдение за периметром сети – вайерволы, защита от спама. Восстановление работоспособности сети. Анализ защищенности сети средствами пакета Kali Linux.	16	4		6	8
4.	Защита личной информации в интернете, смартфоне и компьютере. Проект Tor и VPN-анонимайзер. Шифрование файлов. Электронная подпись. Скачивание файлов. Облачные сервисы. Пять статьи УК РФ за компьютерные нарушения. Гл. 13 Административного кодекса РФ наказания за нарушения в области связи. Основные законы в области защиты информации.	5,8	4		4	9,8
	ИТОГО по разделам дисциплины	67,8	16		18	33,8
	Контроль самостоятельной работы (КСР)	4				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю					
	Общая трудоемкость по дисциплине	72				

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

№	Содержание лекционных занятий	Форма текущего контроля
1	3	4
1	Аппаратная часть компьютерных и информационных сетей. Протоколы интернета, выбор операционной системы. Сетевые фильтры, программы диагностики “компьютерного железа”, например, AIDA64, форматирование HDD при помощи Acronis Disk Director. Установка нескольких операционных систем на компьютере. См. [9,10,12]	Р
2	Различия операционных систем Windows 10 и 11. Особенности ОС Linux на примере Debian 12. Особенности Android устройств – смартфонов, телевизоров и других гаджетов. Почему нужно иметь несколько ОС на компьютере. Резервное копирование. Настройка браузеров и почтовых систем. Браузеры Google Chrome, Mozilla Firefox, Opera, Apple Safari, Яндекс.Браузер, Microsoft Internet Explorer, Microsoft Edge Browser. См.[4,5,8,10]	Р
3	Антивирусы, наблюдение за периметром сети – вайерволы, защита от спама. Восстановление работоспособности сети. Классификация атак по уровням иерархической модели OSI: Атаки на физическом уровне, Атаки на сетевом уровне и др. Атаки на беспроводные устройства Протокол WEP, Протокол WPA Проверка антивирусами Avira AntiVir PersonalEdition Classic и CureIt. [1,2,3]	Э
4	Анализ защищенности сети средствами пакета Kali Linux. Определение активных хостов, Протокол ICMP, Утилита ping [13]	Р
5	Защита личной информации в интернете, смартфоне и компьютере. Проект Tor и VPN-анонимайзер. Обеспечение безопасности в приложениях MS Word и Excel, Защита информации в БД на примере MS Access. Восстановление паролей к архивам с помощью	Р

	программы Advanced Archive Password Recovery. [2,5-11]	
6	Защита периметра локальной сети. Средства наблюдения и предупреждения компьютерных вторжений. Защита от несанкционированного доступа. Защита от внешних вторжений (программа Agnitum Outpost) Руководство по операционной системе Tail - максимальный уровень безопасности. [2-6,11]	Э
7	Шифрование файлов. Электронная подпись. Скачивание файлов. Облачные сервисы. Угрозы, возникающие при подключении к открытой сети Wi-Fi . Приватные режимы браузеров, Использование протокола HTTPS. Расширение HTTPS Everywhere. Удаление истории посещений и cookie-файлов. Признаки фишинговой атаки Защита от фишинговых атак. [2-6,11]	Р
8	Пять статьи УК РФ за компьютерные нарушения. Гл. 13 Административного кодекса РФ наказания за нарушения в области связи. Основные законы в области защиты информации: Об электронной подписи, Об информации, информатизации и защите информации, О связи, О госуслугах, О защите персональных данных и др. [2-6,11]	Р

2.3.2 Занятия семинарского типа.

Не предусмотрены

2.3.3 Лабораторные занятия.

№	Наименование лабораторных работ	Форма текущего контроля
1	3	4
1	Устройство компьютера, основное программное обеспечение. Сетевые фильтры, программы диагностики “компьютерного железа”, например, AIDA64, форматирование HDD при помощи Acronis Disk Director. Установка нескольких операционных систем на компьютере. См. [9,10,12]	Р
2	Особенности ОС Linux на примере Debian 12. Особенности Android устройств – смартфонов, телевизоров и других гаджетов. Резервное копирование. Настройка браузеров и почтовых систем. Браузеры Google Chrome, Mozilla Firefox, Opera, Apple Safari, Яндекс.Браузер, Microsoft Internet Explorer, Microsoft Edge Browser. Установка двух операционных систем, работа в командной строке Linux. См.[4,5,8,10]	Р
3	Антивирусы, наблюдение за периметром сети – вайерволы, защита от спама. Восстановление работоспособности сети. Классификация атак по уровням иерархической модели OSI: Атаки на физическом уровне, Атаки на сетевом уровне и др. Атаки на беспроводные устройства Протокол WEP, Протокол WPA Проверка антивирусами Avira AntiVir PersonalEdition Classic и CureIt. [1,2,3]	Э
4	Анализ защищенности сети средствами пакета Kali Linux. Определение активных хостов, Протокол ICMP, Утилита ping — это сетевой инструмент для проверки доступности удаленного хоста в сети, Hping3 — это мощный инструмент командной строки, который можно описать как улучшенную версию классической утилиты ping со значительно большим количеством функций. Сканирование портов	Р

	Принцип работы сканеров уязвимостей [13]	
5	Защита личной информации в интернете, смартфоне и компьютере. Проект Tor и VPN-анонимайзер. Проект Tor и VPN-анонимайзер. Обеспечение безопасности в приложениях MS Word и Excel, Защита информации в БД на примере MS Access. Вирусы, черви, троянские программы. Восстановление поврежденных архивов с помощью программы Advanced RAR Repair. Восстановление ZIP-архивов с помощью программы DiskInternals ZIP Repair [6-11]	Р
6	Защита периметра локальной сети. Средства наблюдения и предупреждения компьютерных вторжений. Защита от несанкционированного доступа. Берпреступность Поддержка спамеров Организация сетевых атак Ботнеты Платные вызовы и SMS-сообщения. Кража электронных денег, Кража банковских данных ,Кибершантаж [2-6,11]	Э
7	Шифрование файлов. Электронная подпись. Анонимное скачивание файлов. Облачные сервисы. Открытые и закрытые ключи, сертификаты безопасности, отпечатки ключей. Практическое руководство по PGP-шифрованию. Приватный обмен информацией [2, 6-11]	Р
8	Пять статьи УК РФ за компьютерные нарушения. Гл. 13 Административного кодекса РФ наказания за нарушения в области связи. Основные законы в области защиты информации: Об электронной подписи, Об информации, информатизации и защите информации, О связи, О госуслугах, О защите персональных данных и др. [6,11]	Р
	Экстренная помощь при звонке мошенника, при зависании компьютера, при экстремальной ситуации при отключении электричества. Вызов экстренных служб. При атаке на компьютер вызов https://free.drweb.ru/ лечащей утилиты Dr.Web CureIt! И запрет на перезагрузку компьютера. Переход на windows 11 или на Linux. Периодическая очистка и дефрагментация носителей, например, O&O Defrag Professional и проверка утилитой Dr.Web CureIt!	

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т).

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Подготовка рефератов и научных сообщений	Рожков А.В. «Темы исследовательских работ и методические указания по их написанию», утвержденные кафедрой функционального анализа и алгебры, протокол № 12 от 7 мая 2024 г.
2	Самостоятельное освоение теории	Рожков А.В. «Перечень электронных источников информации для самостоятельных работ по циклу

		дисциплин Информационная безопасность магистерской программы АМЗИ и рекомендации по его использованию». Методические указания, утвержденные кафедрой функционального анализа и алгебры, протокол № 12 от 7 мая 2024

1. Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

2. Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

3. Методические указания по использованию интерактивных методов обучения. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

4. Методические указания по подготовке эссе, рефератов, курсовых работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

5. Методические указания по выполнению лабораторных работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

6. Методические указания по выполнению расчетно-графических заданий. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 8 от 16 мая 2024 г.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
– в печатной форме с 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,

3. Образовательные технологии.

Активные и интерактивные формы лекционных занятий, практических занятий, контрольных работ, тестовых заданий, типовых расчетов, докладов.

Семестр	Вид занятия	Используемые интерактивные образовательные технологии	Количество часов
3	Лекционные занятия	Тема Алгоритм проверки на простоту.	2
		Тема Алгоритм тестирования. Тест Эдуарда Люка	2
		Тема Тесты псевдопростоты.	4
		Тема Числа Кармайкла. Разложение чисел на простые числа.	2
	Лабораторные занятия	Дискуссия на тему: «. Метод локализации. Алгоритм пополнения.» с докладами-презентациями	2
		Круглый стол на тему: «Алгоритмы факторизации целых чисел.» с докладами-презентациями	2
		Мозговой штурм» («мозговая атака»): Базисы Грёбнера.	4

		Компьютерная симуляция: Решение системы полиномиальных уравнений	2
Итого:			18

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций со студентом при помощи электронной информационно-образовательной среды ВУЗа.

В рамках реализации компетентностного подхода предусматриваются следующие основные виды активных и интерактивных форм проведения учебных занятий, которые указываются в рабочих программах дисциплин, профессиональных модулей, практик в рамках которых они реализуются:

– применение электронных образовательных ресурсов;

– компьютерные симуляции;

– деловые и ролевые игры;

– индивидуальные и групповые проекты;

– групповые дискуссии и др.

1.4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Информационная безопасность».

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме и **промежуточной аттестации** в форме вопросов и заданий к зачету.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ОПК-4.1 Владеет языками программирования высокого уровня, навыками структурирования программ	Знать: о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности государства; о методологии создания систем защиты информации;	Контрольная работа №1- Значение информационной безопасности для субъектов информационных отношений.	1.Сущность и понятие информационной безопасности. 2.Значение информационной безопасности для субъектов информационных отношений. 3.Место информационной безопасности в системе национальной безопасности.
2	ОПК-4.2 Применяет современные методы разработки и реализации алгоритмов математических моделей на базе языков высокого уровня и пакетов прикладных программ моделирования	Уметь: выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;	Вопросы для устного (письменного) опроса по теме, разделу Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.	4.Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности. 5. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию. 6. Каналы и методы несанкционированного доступа к конфиденциальной

				информации.
3	ОПК-4.3 Применяет навыки решения профессиональных задач с использованием новейших информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать: основные педагогические методы и идеи Владеть: анализом информационной инфраструктуры государства; формальной постановкой и решением задачи обеспечения информационной безопасности компьютерных систем.	Тест по теме, разделу Круглый стол, Кейс Защита персональных данных Индивидуальная работа работа Система правовой ответственности за утечку информации и утрату носителей информации.	7 Методы правовой защиты информации. 8. Правовые основы защиты государственной, коммерческой, служебной, профессиональной и личной тайны. 9. Защита персональных данных. 10.Правовая основа допуска и доступа персонала к защищаемым сведениям. 11. Система правовой ответственности за утечку информации и утрату носителей информации. 12. Правовые основы деятельности подразделений защиты информации

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

Примерный перечень вопросов и заданий

1. Сущность и понятие информационной безопасности.
2. Значение информационной безопасности для субъектов информационных отношений.
3. Место информационной безопасности в системе национальной безопасности.
4. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.
5. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.
6. Каналы и методы несанкционированного доступа к конфиденциальной информации.
7. Методы правовой защиты информации.
8. Правовые основы защиты государственной, коммерческой, служебной, профессиональной и личной тайны.
9. Защита персональных данных.
10. Правовая основа допуска и доступа персонала к защищаемым сведениям.
11. Система правовой ответственности за утечку информации и утрату носителей информации.
12. Правовые основы деятельности подразделений защиты информации.
13. Отрасли права, обеспечивающие законность в области защиты информации.
14. Основные законодательные акты, правовые нормы и положения.
15. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации.
16. Основные правовые акты: закон об информатизации №149-ФЗ.

17. Основные правовые акты: закон о защите персональных данных №152-ФЗ.
18. Основные правовые акты: Доктрина информационной безопасности.
19. Интеллектуальная собственности и ее защита.
20. Принципы, силы, средства и условия организационной защиты информации.
21. Порядок засекречивания и рассекречивания сведений, документов и продукции.
22. Допуск и доступ к конфиденциальной информации и документам.
23. Организация внутри объектового и пропускного режимов на предприятиях.
24. История криптографии; классические шифры, шифры гаммирования.
25. Принципы построения криптографических алгоритмов.
26. Различие между программными и аппаратными реализациями шифров.
27. Особенности использования вычислительной техники в криптографии вопросы организации сетей засекреченной связи.
28. Криптографические хеш-функции.
29. Электронная подпись.
30. Криптографические протоколы.
31. Предмет и задачи программно-аппаратной защиты информации.
32. Идентификация субъекта, понятие протокола идентификации.
33. Основные подходы к защите данных от НСД.
34. Иерархический доступ к файлу.
35. Защита сетевого файлового ресурса, фиксация доступа к файлам.
36. Защиты программ от несанкционированного копирования.
37. Пароли и ключи, организация хранения ключей.
38. Защита программ от излучения.
39. Защита от отладки, защита от дизассемблирования.
40. Защита от разрушающих программных средств.
41. Антивирусы.
42. Межсетевые экраны.

Контрольная работа

Вариант 1

Применения и разработки шифровальных средств ……

Вариант 2

Применения электронной подписи.…….

Вариант 3

Модели, стратегии и системы обеспечения информационной безопасности.

Вариант 4

Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

Вариант 5

Компьютерная система как объект информационной безопасности.

Реферат

Тематика рефератов

1. Общая характеристика методов и средств защиты информации.
2. Криптографические методы обеспечения информационной безопасности.
3. Защита в операционных системах.
4. Защита от вирусов.
5. Защита от вторжений.
6. Анализ нарушений безопасности в информационных системах.

7. Указ Президента РФ. Об утверждении перечня сведений конфиденциального характера от 06.03.1997 № 188 (ред. от 13.07.2015 № 357).

8. Указ Президента РФ. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей

международного информационного обмена от 17.03.2008 № 351 (ред. от 22.05.2015 № 260).

9. Указ Президента РФ. О некоторых вопросах информационной безопасности Российской Федерации от 22.05.2015 № 260.

10. Указ Президента РФ. Об утверждении доктрины информационной безопасности Российской Федерации от 05.12.2016 № 486.

11. Обзор Сборника руководящих документов по защите информации от несанкционированного доступа. Гостехкомиссия России, 1998 г.

12. Понятие атаки.

13. Типы угроз.

14. Классификация атак по основным механизмам реализации угроз.

15. Сетевые сканеры.

16. Особенности сетевого сканеров фирмы CISCO.

17. Встроенные средства защиты ОС Windows 8.

18. Встроенные средства защиты серверной ОС CentOS 7

19. Встроенные средства защиты клиентской ОС Debian.

Тест

Варианты 1-10

1. Методы и средства ограничения доступа к компонентам ЭВМ.
2. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
3. Методы и средства хранения ключевой информации
4. Защита программ от изучения.
5. Защита от разрушающих программных воздействий.
6. Защита от изменения и контроль целостности.
7. Проблемы обеспечения безопасности при удалённом доступе.
8. Протоколы аутентификации PAP и CHAP.
9. Протоколы аутентификации удалённого доступа в программных средствах Microsoft.
10. Система аутентификации и авторизации Kerberos.

Зачетно-экзаменационные материалы для промежуточной аттестации (зачет)

1. Правовые основы деятельности подразделений защиты информации.
2. Отрасли права, обеспечивающие законность в области защиты информации.
3. Основные законодательные акты, правовые нормы и положения.
4. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации.
5. Основные правовые акты: закон об информатизации №149-ФЗ.
6. Основные правовые акты: закон о защите персональных данных №152-ФЗ.
7. Основные правовые акты: Доктрина информационной безопасности.
8. Интеллектуальная собственности и ее защита.
9. Принципы, силы, средства и условия организационной защиты информации.
10. Порядок засекречивания и рассекречивания сведений, документов и продукции.
11. Допуск и доступ к конфиденциальной информации и документам.
12. Организация внутри объектового и пропускного режимов на предприятиях.
13. История криптографии; классические шифры, шифры гаммирования.
14. Принципы построения криптографических алгоритмов.
15. Различие между программными и аппаратными реализациями шифров.
16. Особенности использования вычислительной техники в криптографии вопросы организации сетей засекреченной связи.
17. Криптографические хеш-функции.

18. Электронная подпись.
19. Криптографические протоколы.
20. Предмет и задачи программно-аппаратной защиты информации.
21. Идентификация субъекта, понятие протокола идентификации.
22. Основные подходы к защите данных от НСД.
23. Иерархический доступ к файлу.
24. Защита сетевого файлового ресурса, фиксация доступа к файлам.
25. Защиты программ от несанкционированного копирования.
26. Пароли и ключи, организация хранения ключей.
27. Защита программ от излучения.
28. Защита от отладки, защита от дизассемблирования.
29. Защита от разрушающих программных средств.
30. Антивирусы.
31. Межсетевые экраны.

Критерии оценивания результатов обучения

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, знает формы допускает незначительные ошибки; студент умеет правильно объяснять материал, иллюстрируя его примерами

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести примеры, довольно ограниченный объем знаний программного материала.

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 экзамене;

– 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.

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

5.1 Основная литература:

а) основная литература:

1. Кудинов Ю.И., Пащенко Ф.Ф. Основы современной информатики, 6-е изд. [Электронный ресурс]. - СПб.: Лань, 2024. – URL: https://reader.lanbook.com/book/392393
2. Кудинов Ю.И., Пащенко Ф.Ф., Келина А.Ю. Практикум по основам современной информатики. [Электронный ресурс]. - СПб.: Лань, 2022. - URL: https://reader.lanbook.com/book/210749
3. Акмаров П.Б. Компьютерные сети. Лабораторный практикум: Учебное пособие для вузов [Электронный ресурс]. – СПб.: Лань, 2024. – URL: https://reader.lanbook.com/book/362873
4. Окороков В.А. Безопасность операционных систем: Учебное пособие для вузов [Электронный ресурс]. – СПб.: Лань, 2024. – URL: https://reader.lanbook.com/book/367472

5.2 Дополнительная литература:

5. Лозовецкий В.В., Комаров Е.Г., Лебедев В.В. Защита автоматизированных систем обработки информации и телекоммуникационных сетей: Учебное пособие для вузов, 2-е изд. [Электронный ресурс]. – СПб.: Лань, 2024. - URL: https://e.lanbook.com/reader/book/ 397355
6. Никифоров С.Н. Методы защиты информации. Защищенные сети, 2-е изд. [Электронный ресурс]. - СПб.: Лань, 2021. - URL: https://e.lanbook.com/reader/book/171868/
7. Никифоров С.Н. Методы защиты информации. Защита от внешних вторжений, 5-е изд. [Электронный ресурс]. - СПб.: Лань, 2023. - https://reader.lanbook.com/book/288974
8. Никифоров С.Н. Методы защиты информации. Пароли, скрытие, шифрование, 5-е изд. [Электронный ресурс]. - СПб.: Лань, 2023. - https://reader.lanbook.com/book/338018

5.3 Периодические издания:

Не предусмотрены

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

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods

https://experiments.springernature.com/sources/springer-protocols

13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Нормативно-правовые документы

1. Федеральный закон. Об электронной подписи от 06.04.2011 № 63-ФЗ (ред. от 04.08.2023).
2. Федеральный закон. О связи от 07.07.2003 № 126-ФЗ (ред. от 06.04.2024).
3. Федеральный закон. Об информации, информационных технологиях и о защите информации от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023).
4. Федеральный закон. О персональных данных от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023).
5. Федеральный закон. Об организации предоставления государственных и муниципальных услуг от 27.07.2010 № 210-ФЗ (ред. от 25.12.2023) Охватывает и Интернет вещей (IoT).
6. Федеральный закон. Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации от 31.07.2020 № 258-ФЗ (ред. от 02.07.2021). Это то, что образно называют Интернет вещей (IoT)
7. Федеральный закон. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ (ред. от 12.06.2024)
8. Федеральный закон. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 12.06.2024)

2.

Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/
2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка (http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование" http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
10. Справочно-информационный портал "Русский язык" http://gramota.ru/;
11. Служба тематических толковых словарей http://www.glossary.ru/;
12. Словари и энциклопедии http://dic.academic.ru/;
13. Образовательный портал "Учеба" http://www.ucheba.com/;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

6. Методические указания для обучающихся по освоению дисциплины (модуля).

Согласно учебному плану дисциплины «Информационная безопасность» итоговой формой контроля является зачет. Для сдачи зачета студент должен научиться на лабораторных занятиях решать практические задания по темам разделов 1-3, выполнять домашние задания. Типы практических заданий на зачет соответствуют заданиям. Также на зачете студентам предлагаются и теоретические задания, состоящие в письменном ответе на один из вопросов. Количество практических и теоретических заданий зависит от активности и результативности работы студента в течение семестра.

Важнейшим этапом курса является самостоятельная работа по дисциплине (модулю).

Для подготовки к ответам на теоретические вопросы в ходе контрольных работ и на зачете студентам достаточно использовать материал лекций. Весь этот теоретический материал содержится в учебных пособиях из списка основной литературы. Для изучения теоретического материала, необходимого для подготовки реферативного доклада, кроме основных источников литературы возможно использование дополнительных источников и Интернет-ресурса. В случае затруднений, возникающих у студентов в процессе самостоятельного изучения теории, преподаватель разъясняет сложные моменты на консультациях.

7. 7. Материально-техническое обеспечение по дисциплине (модулю)

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

При заполнении таблицы учитывать все виды занятий, предусмотренные учебным планом по данной дисциплине: лекции, занятия семинарского типа (практические занятия, лабораторные работы), а также курсовое проектирование, консультации, текущий контроль и промежуточную аттестацию.

При использовании лаборатории указать ее наименование «Лаборатория…».

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование:	
Учебные аудитории для проведения лабораторных работ.	Мебель: учебная мебель Технические средства обучения:	

Лаборатория…	экран, проектор, компьютер Оборудование:	
Учебные аудитории для курсового проектирования (выполнения курсовых работ)	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование:	

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)	
Помещение для самостоятельной работы обучающихся (ауд._____)	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)	

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) Программы, демонстрации видео материалов (проигрыватель «Windows Media Player»). Программы для демонстрации и создания презентаций («Microsoft Power Point»).
2.	Семинарские занятия	Не предусмотрены

3.	Лабораторные занятия	Лаборатория, укомплектованная специализированной мебелью и техническими средствами обучения – компьютерами с предустановленными GAP и Sage
4.	Курсовое проектирование	Не предусмотрено
5.	Групповые (индивидуальные) консультации	Аудитория для групповых занятий
6.	Текущий контроль, промежуточная аттестация	Аудитория для групповых занятий
7.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.