

**ГАОУ ВО «Дагестанский государственный университет на-
родного хозяйства»**

*Утверждена решением
Ученого совета ДГУНХ,
протокол № 11
от 30 мая 2024 г*

**Кафедра «Информационные технологии и информационная
безопасность»**

**РАБОЧАЯ ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО
КУРСА**

«Криптографические средства защиты информации»

**Специальность 10.02.05 Обеспечение информацион-
ной безопасности автоматизированных систем**

Квалификация – техник по защите информации

Форма обучения – очная

Махачкала – 2024

УДК 681.518(075.8)

ББК 32.81.73

Составитель – Гасанова Зарема Ахмедовна, кандидат педагогических наук, заместитель заведующего кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, заведующий кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры прикладной математики Дагестанского государственного университета.

Представитель работодателя - Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза», эксперт-представитель работодателя.

Рабочая программа междисциплинарного курса «Криптографические средства защиты информации» разработана в соответствии с требованиями федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утверждённого приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 г., № 1553, в соответствии с приказом Минпросвещения России от 24.08.2022 г., № 762 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования».

Рабочая программа по междисциплинарному курсу «Криптографические средства защиты информации» размещена на официальном сайте www.dgunh.ru

Гасанова З.А. Рабочая программа по междисциплинарному курсу «Криптографические средства защиты информации» для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. – Махачкала: ДГУНХ, 2024 г., 15 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 28 мая 2024 г.

Рекомендована к утверждению руководителем образовательной программы СПО – программы подготовки специалистов среднего звена по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, к.пед.н., Гасановой З.А.

Одобрена на заседании кафедры «Информационные технологии и информационная безопасность» 23 мая 2024 г., протокол № 10.

Содержание

Раздел 1. Перечень планируемых результатов обучения по междисциплинарному курсу...	4
Раздел 2. Место междисциплинарного курса в структуре образовательной программы...	6
Раздел 3. Объем междисциплинарного курса в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), на самостоятельную работу обучающихся и форму(ы) промежуточной аттестации.....	6
Раздел 4. Содержание междисциплинарного курса, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий.....	7
Раздел 5. Перечень основной и дополнительной учебной литературы, необходимой для освоения междисциплинарного курса.....	10
Раздел 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения междисциплинарного курса.....	13
Раздел 7. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных.....	14
Раздел 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по междисциплинарному курсу.....	14
Раздел 9. Образовательные технологии.....	15

Раздел 1. Перечень планируемых результатов обучения по междисциплинарному курсу

Цель междисциплинарного курса – сформировать компетенции обучающегося в области математического аппарата криптозащиты и криптоанализа, современных криптографических протоколов, практического использования криптографических средств защиты информации.

Задачами преподавания междисциплинарного курса являются:

- Рассмотреть наиболее распространённые криптографические протоколы, а также основные методы криптоанализа.
- Раскрыть принципы математических и вычислительных моделей криптографических процессов, их оптимизация и выработка направлений совершенствования.
- Показать особенности различных криптографических протоколов и возможностей их применения.

1.1. Компетенции выпускников, формируемые в результате освоения междисциплинарного курса «Криптографические средства защиты информации» как часть планируемых результатов освоения образовательной программы

код компетенции	формулировка компетенции
ПК-2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК-2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК-2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.

1.2. Планируемые результаты обучения по междисциплинарному курсу

<i>Код и наименование компетенции</i>	<i>Планируемые результаты обучения по междисциплинарному курсу</i>
ПК-2.1. ПК-2.2. ПК-2.4.	<u>Знать:</u> 31 – основные задачи и понятия криптографии; 32 – требования к шифрам и основные характеристики шифров; 33 – принципы построения криптографических алгоритмов. 34 – принципы построения ЭЦП

	<p>35 – криптографические стандарты и их использование в информационных системах.</p> <p>Уметь:</p> <p>У1 - использовать базовые знания теории чисел для реализации арифметических алгоритмов в криптографических системах</p> <p>У2 – использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки;</p> <p>У3 – применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности</p> <p>У4 – применять средства ЭЦП</p> <p>Владеть:</p> <p>В1 – навыками математического моделирования в криптографии.</p> <p>В2 – криптографической терминологией</p> <p>В3 – навыками использования ПЭВМ в анализе простейших шифров;</p> <p>В4 – навыками программирования криптографических алгоритмов.</p>
--	--

1.3. Перечень компетенций с указанием этапов их формирования в процессе освоения междисциплинарного курса

Код компетенции	Этапы формирования компетенций								
	Тема 1. Введение в криптографию. Основные понятия и определения.	Тема 2. Математические основы криптографии	Тема 3. Стойкость криптоалгоритмов	Тема 4. Поточные шифры	Тема 5. Блочные шифры	Тема 6. Криптографические протоколы	Тема 7. Построение криптографических примитивов	Тема 8. Симметричные криптосистемы	Тема 9. Алгоритм DES
ПК-2.1	+	+	+	+	+	+	+	+	+
ПК-2.2	+	+	+	+	+	+	+	+	+
ПК-2.4	+	+	+	+	+	+	+	+	+

Код компетенции	Этапы формирования компетенций (темы дисциплин)							
	Тема 10. Алгоритм ГОСТ 28147-89	Тема 11. Ассиметричные	Тема 12. Алгоритм RSA	Тема 13. Электронная цифровая подпись	Тема 14. Основные криптоаналитические методы	Тема 15. Дискретное логарифм	Тема 16. Факторизация целых чисел	Тема 17. Псевдослучайные последовательности. Линейные рекуррентные последовательности

		крип- тоси- стемы		ь		иро- вание	(Пол- лард)	как псевдослучай- ные последователь- ности
ПК-2.1	+	+	+	+	+	+	+	+
ПК-2.2	+	+	+	+	+	+	+	+
ПК-2.4	+	+	+	+	+	+	+	+

Раздел 2. Место междисциплинарного курса в структуре образовательной программы

Междисциплинарный курс МДК.02.02 «Криптографические средства защиты информации» относится к профессиональному циклу учебного плана по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Для изучения данной междисциплинарного курса необходимы знания, умения и навыки по дисциплинам: «Математика», «Теория чисел», «Математический анализ», «Основы теории информации», «Основы алгоритмизации и программирования» и «Технологии и методы программирования».

Освоение данной междисциплинарного курса необходимо обучающемуся для изучения дисциплин «Техническая защита информации», «Программные и программно-аппаратные средства защиты информации», «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении», успешного прохождения производственной практики и выполнения выпускной квалификационной работы.

Раздел 3. Объем междисциплинарного курса в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), на самостоятельную работу обучающихся, на самостоятельную работу обучающихся и форму промежуточной аттестации

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 144 часа, в том числе:

на занятия лекционного типа – **64** ч.

на занятия семинарского типа – **80** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **0** ч.

Форма промежуточной аттестации: экзамен, 18 ч.

Раздел 4. Содержание междисциплинарного курса, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий.

Очная форма обучения

№ п/п	Тема междисциплинарного курса	Всего академических часов	В т.ч. занятия лекционного типа	В т.ч. занятия семинарского типа:					Самостоятельная работа	Форма текущего контроля успеваемости. Форма промежуточной аттестации
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия		
1.	Тема 1. Введение в криптографию. Основные понятия и определения.	4	2	-	1	1	-	-	-	<ul style="list-style-type: none"> - Устный опрос - Подготовка реферата; - Подготовка презентации; - Решение задач. - Лабораторная работа.
2.	Тема 2. Математические основы криптографии	5	2	-	1	2	-	-	-	<ul style="list-style-type: none"> - Устный опрос - Решение задач. - Лабораторная работа.
3.	Тема 3. Стойкость криптоалгоритмов	9	4	-	2	3	-	-	-	<ul style="list-style-type: none"> - Устный опрос - Подготовка реферата; - Подготовка презентации; - Лабораторная работа.
4.	Тема 4. Поточные шифры	9	4	-	2	3	-	-	-	<ul style="list-style-type: none"> - Устный опрос - Подготовка реферата; - Подготовка презентации; - Решение задач. - Лабораторная работа.
5.	Тема 5. Блочные шифры	9	4	-	2	3	-	-	-	<ul style="list-style-type: none"> - Устный опрос - Подготовка реферата; - Подготовка презентации; - Решение задач. - Лабораторная работа.
6.	Тема 6. Криптографические протоколы	9	4	-	2	3	-	-	-	<ul style="list-style-type: none"> - Устный опрос - Подготовка реферата;

										<ul style="list-style-type: none"> – Подготовка презентации; – Решение задач. – Лабораторная работа.
7.	Тема 7. Построение криптографических примитивов	9	4	-	2	3	-	-		<ul style="list-style-type: none"> – Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
8.	Тема 8. Симметричные криптосистемы	9	4	-	2	3	-	-		<ul style="list-style-type: none"> – Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
9.	Тема 9. Алгоритм DES	9	4	-	2	3	-	-		<ul style="list-style-type: none"> – Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
10.	Тема 10. Алгоритм ГОСТ 28147-89	9	4	-	2	3	-	-		<ul style="list-style-type: none"> – Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
11.	Тема 11. Ассиметричные криптосистемы	9	4	-	2	3	-	-		<ul style="list-style-type: none"> – Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
12.	Тема 12. Алгоритм RSA	9	4	-	2	3	-	-		<ul style="list-style-type: none"> – Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
13.	Тема 13. Электронная	9	4		2	3				<ul style="list-style-type: none"> – Устный опрос

	цифровая подпись									<ul style="list-style-type: none"> – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
14	Тема 14. Основные криптоаналитические методы	9	4		2	3				<ul style="list-style-type: none"> – Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
15	Тема 15. Дискретное логарифмирование	9	4		2	3				<ul style="list-style-type: none"> – Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
16.	Тема 16. Факторизация целых чисел (Поллард)	9	4		2	3				<ul style="list-style-type: none"> – Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
17.	Тема 17. Псевдослучайные последовательности. Линейные рекуррентные последовательности как псевдослучайные последовательности	9	4	-	2	3	-	-		<ul style="list-style-type: none"> – Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
	ИТОГО	144	64	-	32	48	-	-		
	ЭКЗАМЕН (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	18								Контроль

	ВСЕГО:	162	
--	---------------	------------	--

Раздел 5. Перечень основной и дополнительной учебной литературы, необходимой для освоения междисциплинарного курса

№ п/п	Автор	Название основной и дополнительной учебной литературы, необходимой для освоения междисциплинарного курса	Выходные данные	Количество экземпляров в библиотеке ДГУНХ/адрес доступа
I. Основная учебная литература				
1.	Лапоница О.Р.	Криптографические основы безопасности	Москва : Национальный Открытый Университет «ИНТУ-ИТ», 2016. - 244 с. ISBN 5-9556-00020-5	http://biblioclub.ru/index.php?page=book&id=429092
2.	Майстренко Н.В.	Основы теории информации и криптографии	Министерство образования и науки Российской Федерации, Тамбовский государственный технический университет. – Тамбов : ФГБОУ ВПО "ТГТУ", 2018. – 81 с.	http://biblioclub.ru/index.php?page=book&id=228963
3.	Фороузан Б.А.	Математика криптографии и теория шифрования	2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУ-ИТ», 2016. - 511 с. ISBN 978-5-9963-0242-0	http://biblioclub.ru/index.php?page=book&id=428998
II. Дополнительная литература				
А) Дополнительная учебная литература				
1.		Разработка моделей криптографической защиты информации : монография/ В.Г. Шубович, В.В. Капитанчук, Н.С. Знаенко, Ю.И.	Министерство образования и науки РФ, ФГБОУ ВПО «Ульяновский государ-	http://biblioclub.ru/index.php?page=book&id=278070

		Титаренко	ственный педагогический университет имени И.Н. Ульянова». - Ульяновск : УлГПУ, 2013. - 128 с. ISBN 978-5-86045-640-2	
2.	-	Теоретико-числовые методы в криптографии	Министерство образования и науки РФ, ФГАОУ ВО «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2017. - 107 с.	http://biblioclub.ru/index.php?page=book&id=483838
3.	Аграновский А.В.	Практическая криптография: алгоритмы и их программирование	А.В. Аграновский, Р.А. Хади. - Москва : СОЛОН-ПРЕСС, 2009. - 256 с. - (Аспекты защиты). - ISBN 5-98003-002-6	http://biblioclub.ru/index.php?page=book&id=117663
4.	Басалова Г.В	Основы криптографии : курс лекций	Г.В. Басалова ; Национальный Открытый Университет "ИНТУ-ИТ". - Москва : Интернет-Университет Информационных Технологий, 2011. - 253 с.	http://biblioclub.ru/index.php?page=book&id=233689
5.	Гулятьева Т.А.	Основы теории информации и криптографии : конспект лекций /	Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2010. - 88 с.	http://biblioclub.ru/index.php?page=book&id=228963

			ISBN 978-5-7782-1425-5	
6.	И.А. Калмыков, Д.О. Науменко	Криптографические методы защиты информации	Министерство образования и науки Российской Федерации и др. – Ставрополь : СКФУ, 2015. – 109 с.	http://biblioclub.ru/index.php?page=book&id=458059
7.	Ищукова, Е.А.	Криптографические протоколы и стандарты	Министерство образования и науки РФ, Южный федеральный университет, Инженерно-технологическая академия. – Таганрог : Издательство Южного федерального университета, 2016. – 80 с.	http://biblioclub.ru/index.php?page=book&id=493059
8.	Лидовский В.В.	Основы теории информации и криптографии	В.В. Лидовский ; Национальный Открытый Университет "ИНТУ-ИТ". - Москва : Интернет-Университет Информационных Технологий, 2007. - 125 с.	http://biblioclub.ru/index.php?page=book&id=234148
9.	Свон М.	Блокчейн: схема новой экономики	М. Свон. - Москва : Олимп-Бизнес, 2017. - 241 с. ISBN 978-5-9693-0360-7 ;	http://biblioclub.ru/index.php?page=book&id=494451
Б) Официальные издания: сборники законодательных актов, нормативно-правовых документов и кодексов РФ				
1.	Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями).			
2.	ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2008 г.			

	www.standartgost.ru
3.	ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. www.standartgost.ru
4.	ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств. 2002 г. www.standartgost.ru
5.	ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» www.standartgost.ru
6.	ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. www.standartgost.ru
7.	ГОСТ Р ИСО/МЭК 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» www.standartgost.ru
<i>В) Периодические издания</i>	
1.	Журнал для пользователей персональных компьютеров «Мир ПК»
2.	Научный журнал «Информатика и ее применение»
3.	Информатика и безопасность
4.	Журнал о компьютерах и цифровой технике «Computer Bild»
5.	Рецензируемый научный журнал «Информатика и система управления»
6.	Рецензируемый научный журнал «Проблемы информационной безопасности»
<i>Г) Справочно-библиографическая литература</i>	
1.	1. Краткий энциклопедический словарь по информационной безопасности : словарь / сост. В.Г. Дождиков, М.И. Салтан. – Москва : Энергия, 2010. – 240 с. http://biblioclub.ru/index.php?page=book&id=58393

Раздел 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения междисциплинарного курса

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к одной или нескольким электронно-библиотечным системам и к электронной информационно-образовательной среде университета (<http://e-dgunh.ru>). Электронно-библиотечная система и электронная информационно-образовательная среда обеспечивает возможность доступа, обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

Для самостоятельного изучения материала и ознакомления с регламентирующими документами и текущей практикой в области криптографической защиты информации, рекомендуется использовать следующие Интернет-ресурсы:

1. <http://www.fsb.ru/> – официальный сайт ФСБ
2. <http://fstec.ru/> – официальный сайт ФСТЭК
3. <http://www.consultant.ru/> – онлайн-версия информационно-правовой системы "КонсультантПлюс"
4. <http://Standartgost.ru> - Открытая база ГОСТов

Раздел 7. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных

7.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

- Windows 10
- Microsoft Office Professional
- Adobe Acrobat Reader DC
- VLC Media player
- 7-zip
- Microsoft Visual Studio
- Python
- Kali Linux

7.2. Перечень информационных справочных систем и профессиональных баз данных:

- информационно справочная система «Консультант+».

7.3. Перечень профессиональных баз данных:

- Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 (<http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sszi>).
- <http://Standartgost.ru> - Открытая база ГОСТов.

Раздел 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по междисциплинарному курсу

Для преподавания междисциплинарного курса «Криптографические средства защиты информации» используются следующие специальные помещения и учебные аудитории:

Учебная аудитория для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (367008, Республика Дагестан, г. Махачкала, пр-кт Али-Гаджи Акушинского, д 20, учебный корпус № 1, литер А, этаж 4, помещение № 5)

Перечень основного оборудования:

Комплект учебной мебели,

Доска меловая.

Набор технических средств: персональный компьютер с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека

ONLINE» (www.biblioclub.ru), ЭБС «ЭБС Юрайт» (www.urait.ru).

Перечень учебно-наглядных пособий:

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

Лаборатория программно-аппаратных средств защиты информации, учебная аудитория для проведения занятий всех видов, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (367008, Республика Дагестан,

г. Махачкала, пр-кт Али-Гаджи Акушинского, д 20, учебный корпус № 1, литер А, этаж 4, помещение № 9)

Перечень основного оборудования:

Комплект учебной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор.

Персональные компьютеры – 20 ед.

Типовой комплект учебного оборудования «Криптографические системы».

Перечень учебно-наглядных пособий:

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

Помещение для самостоятельной работы № 1-1 (367008, Республика Дагестан, г. Махачкала, пр-кт Али-Гаджи Акушинского, д 20, учебный корпус № 2, литер Б, этаж 4, помещение № 1)

Перечень основного оборудования:

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду.

Раздел 9. Образовательные технологии

Образовательные технологии, используемые при проведении учебных занятий по междисциплинарному курсу «Криптографические средства защиты информации», обеспечивают развитие у обучающихся необходимых знаний и навыков.

На занятиях лекционного типа применяются такие методы обучения как управляемая дискуссия, проблемная лекции, техники сторителлинга.

На практических занятиях, целью которых является приобретение учащимися определенных практических умений, научить их аналитически мыслить, уметь принимать верные решения в различных ситуациях эффективными будут такие методы как решение задач, выполнение лабораторных работ.