ГАОУ ВО «Дагестанский государственный университет народного хозяйства»

Утверждена решением
Ученого совета ДГУНХ,
протокол № 9
от 24 марта 2025 г.

Кафедра «Информационные технологии и информационная безопасность»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

Направление подготовки

10.03.01 Информационная безопасность,

профиль «Безопасность автоматизированных систем»

Уровень высшего образования - бакалавриат

Формы обучения – очная, очно-заочная

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00C5A9FA0FAD6D6153888A98846B419FD3
Владелец: Бучаев Ахмед Гамидович
Действителен: с 11.07.2024 до 04.10.2025

Махачкала – 2025

УДК 681.518(075.8)
ББК 32.81.73

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

Внутренний рецензент – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент кафедры «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 дисциплины «Методы и средства криптографической защиты информации» разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г., № 1427, в соответствии с приказом Министерства науки и высшего образования Российской Федерации от 6.04.2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»

Рабочая программа по дисциплине «Методы и средства криптографической защиты информации» размещена на официальном сайте www.dgunh.ru

Гасанова З.А. Рабочая программа по дисциплине «Методы и средства криптографической защиты информации» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2025 г., 19 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 10 марта 2025 г.

Рекомендована к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

Одобрена на заседании кафедры «Информационные технологии и информационная безопасность» 24 февраля 2025 г., протокол № 7.

.

Содержание

Раздел 1. Перечень планируемых результатов обучения по дисциплине… 4

Раздел 2. Место дисциплины в структуре образовательной программы… 6

Раздел 3. Объем дисциплины 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 дисциплины, 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 дисциплины…….. 1
3

Раздел 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины…….. 1
6

Раздел 7. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных…… 17

Раздел 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине…… 1
7

Раздел 9. Образовательные технологии…….. 18

Лист актуализации рабочей программы дисциплины…… 19

Раздел 1. Перечень планируемых результатов обучения по дисциплине

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

Задачами преподавания дисциплины 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 дисциплины «Методы и средства криптографической защиты информации» как часть планируемых результатов освоения образовательной программы

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

1.2. Планируемые результаты обучения по дисциплине

Код и наименование компетенции	***Код и наименование индикатора достижения компетенции***	***Планируемые результаты обучения по дисциплине***
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной	ИОПК-9.1. Использует типовые криптографические средства защиты информации, в том числе средства электронной подписи	**Знать:** З1 – основные задачи и понятия криптографии; З2 – требования к шифрам и основные характеристики шифров; З3 – принципы построения криптографических алгоритмов. З4 – принципы построения ЭЦП З5 – криптографические стандарты и их использование в информационных системах. **Уметь:** У1 - использовать базовые знания теории чисел для реализации арифметических алгоритмов в криптографических системах У2 – использовать частотные характеристики открытых текстов для анализа простейших шиф-

деятельности		ров замены и перестановки; У3 – применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности У4 – применять средства ЭЦП **Владеть:** В1 – навыками математического моделирования в криптографии. В2 – криптографической терминологией В3 – навыками использования ПЭВМ в анализе простейших шифров; В4 – навыками программирования криптографических алгоритмов.

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

Код компетенции	Этапы формирования компетенций								
	Тема 1. Введение в криптографию. Основные понятия и определения.	Тема 2. Математические основы криптографии	Тема 3. Стойкость крипто алгоритмов	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
ОПК-9	+	+	+	+	+	+	+	+	+

Код компетенции	Этапы формирования компетенций (темы дисциплин)							
	Тема 10. Алгоритм ГОСТ 28147-89	Тема 11. Ассиметричные криптосистемы	Тема 12. Алгоритм RSA	Тема 13. Электронная цифровая подпись	Тема 14. Основные криптоаналитические методы	Тема 15. Дискретное логарифмирование	Тема 16. Факторизация целых чисел (Полларда)	Тема 17. Псевдослучайные последовательности. Линейные рекуррентные последовательности как псевдослучайные последовательности
ОПК-9	+	+	+	+	+	+	+	+

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.О.24 «Методы и средства криптографической защиты информации» относится к обязательной части Блока 1 «Дисциплины» учебного плана направления подготовки «Информационная безопасность», профиля «Безопасность автоматизированных систем».

Для изучения данной дисциплины необходимы знания, умения и навыки по дисциплинам: «Алгебра», «Теория чисел», «Дискретная математика», «Теория информация», «Языки программирования» и «Технологии и методы программирования».

Освоение данной дисциплины необходимо обучающемуся для изучения дисциплин «Защита информации от утечки по техническим каналам», «Программно-аппаратные средства защиты информации», «Комплексное обеспечение защиты информации объекта информатизации», «Проектирование защищенных автоматизированных систем», успешного прохождения производственной практики и выполнения выпускной квалификационной работы.

Раздел 3. Объем дисциплины 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

Объем дисциплины в зачетных единицах составляет 4 зачетные единицы.

Очная форма обучения

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 68 часов, в том числе:

на занятия лекционного типа – **34** ч.

на занятия семинарского типа – **34** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **40** ч.

Форма промежуточной аттестации: экзамен, 36 ч.

Очно-заочная форма обучения

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 34 часа, в том числе:

на занятия лекционного типа – **17** ч.

на занятия семинарского типа – **25** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **66** ч.

Форма промежуточной аттестации: экзамен, 36 ч.

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

Очная форма обучения

№ п/п	Тема дисциплины	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.	6	2	-	1	1	-	-	2	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
2.	Тема 2. Математические основы криптографии	6	2	-	1	1	-	-	2	– Устный опрос – Решение задач. – Лабораторная работа.
3.	Тема 3. Стойкость криптоалгоритмов	8	2	-	1	1	-	-	4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Лабораторная работа.
4.	Тема 4. Поточные шифры	6	2	-	1	1	-	-	2	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
5.	Тема 5. Блочные шифры	6	2	-	1	1	-	-	2	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
6.	Тема 6. Криптографические протоколы	6	2	-	1	1	-	-	2	– Устный опрос – Подготовка реферата; – Подготовка презентации;

										– Решение задач. – Лабораторная работа.
7.	Тема 7. Построение криптографических примитивов	6	2	-	1	1	-	-	2	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
8.	Тема 8. Симметрич-ные криптосистемы	6	2	-	1	1	-	-	2	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
9.	Тема 9. Алгоритм DES	6	2	-	1	1	-	-	2	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
10.	Тема 10. Алгоритм ГОСТ 28147-89	6	2	-	1	1	-	-	2	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
11.	Тема 11. Ассиметрич-ные криптосистемы	6	2	-	1	1	-	-	2	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
12.	Тема 12. Алгоритм RSA	6	2	-	1	1	-	-	2	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
13.	Тема 13. Электронная цифровая подпись	6	2		1	1			2	– Устный опрос – Подготовка реферата;

										– Подготовка презентации; – Решение задач. – Лабораторная работа.
14	Тема 14. Основные криптоаналитические методы	8	2		1	1			4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
15	Тема 15. Дискретное логарифмирование	8	2		1	1			4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
16.	Тема 16. Факторизация целых чисел (Поллард)	6	2		1	1			2	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
17.	Тема 17. Псевдослучайные последовательности. Линейные рекуррентные последовательности как псевдослучайные последовательности	6	2	-	1	1	-	-	2	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
	ИТОГО	**108**	**30**	**-**	**17**	**17**	**-**	**-**	**40**	
	ЭКЗАМЕН (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	**36**								**Контроль**
	ВСЕГО:	**144**								

Очно-заочная форма обучения

№ п/п	Тема дисциплины	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.	5	1	-	1	1	-	-	2	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
2.	Тема 2. Математические основы криптографии	7	1	-	1	1	-	-	4	– Устный опрос – Решение задач. – Лабораторная работа.
3.	Тема 3. Стойкость криптоалгоритмов	7	1	-	1	1	-	-	4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Лабораторная работа.
4.	Тема 4. Поточные шифры	7	1	-	1	1	-	-	4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
5.	Тема 5. Блочные шифры	7	1	-	1	1	-	-	4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
6.	Тема 6. Криптографические протоколы	7	1	-	1	1	-	-	4	– Устный опрос – Подготовка реферата; – Подготовка презентации;

										– Решение задач. – Лабораторная работа.
7.	Тема 7. Построение криптографических примитивов	7	1	-	1	1	-	-	4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
8.	Тема 8. Симметрич-ные криптосистемы	7	1	-	1	1	-	-	4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
9.	Тема 9. Алгоритм DES	6	1	-	-	1	-	-	4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
10.	Тема 10. Алгоритм ГОСТ 28147-89	6	1	-	-	1	-	-	4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
11.	Тема 11. Ассиметрич-ные криптосистемы	6	1	-	-	1	-	-	4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
12.	Тема 12. Алгоритм RSA	6	1	-	-	1	-	-	4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
13.	Тема 13. Электронная цифровая подпись	6	1		-	1			4	– Устный опрос – Подготовка реферата;

										– Подготовка презентации; – Решение задач. – Лабораторная работа.
14	Тема 14. Основные криптоаналитические методы	6	1		-	1			4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
15	Тема 15. Дискретное логарифмирование	6	1		-	1			4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
16.	Тема 16. Факторизация целых чисел (Поллард)	6	1		-	1			4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
17.	Тема 17. Псевдослучайные последовательности. Линейные рекуррентные последовательности как псевдослучайные последовательности	6	1	-	-	1	-	-	4	– Устный опрос – Подготовка реферата; – Подготовка презентации; – Решение задач. – Лабораторная работа.
	ИТОГО	**108**	**17**	**-**	**8**	**17**	**-**	**-**	**66**	
	ЭКЗАМЕН (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	**36**								**Контроль**
	ВСЕГО:	**144**								

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

№ п/п	Автор	Название основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Выходные данные	Количество экземпляров в библиотеке ДГУНХ/адрес доступа
I. Основная учебная литература				
1.	Лапонина О.Р.	Криптографические основы безопасности	Москва : Национальный Открытый Университет «ИНТУИТ», 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 «ИНТУИТ», 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. Титаренко	Министерство образования и науки РФ, ФГБОУ ВПО «Ульяновский государственный педагогический университет имени И.Н. Ульяно-	http://biblioclub.ru/index.php?page=book&id=278070

			ва». - 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.	Агранов-ский А.В.	Практическая криптография: алгоритмы и их программирование	А.В. Агранов-ский, 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 "ИНТУИТ". - Москва : Интернет-Университет Информационных Технологий, 2011. - 253 с.	http://biblioclub.ru/index.php?page=book&id=233689
5.	Гультяева Т.А.	Основы теории информации и криптографии : конспект лекций /	Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2010. - 88 с. ISBN 978-5-7782-1425-5	http://biblioclub.ru/index.php?page=book&id=228963
6.	И.А. Калмыков,	Криптографические методы защиты информа-	Министерство образования и на-	http://biblioclub.ru/

	Д.О. Науменко	ции	уки Российской Федерации и др. – Ставрополь : СКФУ, 2015. – 109 с.	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 "ИНТУИТ". - 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
В) Периодические издания	
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»
Г) Справочно-библиографическая литература	
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 дисциплины

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 дисциплине

Для преподавания дисциплины «Методы и средства криптографической защиты информации» используются следующие специальные помещения и учебные аудитории:

Учебная аудитория для проведения учебных занятий № 4.9 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)

Перечень основного оборудования:

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, персональный компьютер с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» (www.biblioclub.ru), ЭБС «ЭБС Юрайт» (www.urait.ru), интерактивная доска, акустическая система.

Перечень учебно-наглядных пособий:

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации,

видеоролики).

Компьютерный класс, учебная аудитория для проведения учебных занятий № 4.13 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)

Перечень основного оборудования:

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, акустическая система.

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 № 4.5 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)

Перечень основного оборудования:

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 24 ед.

Помещение для самостоятельной работы № 1-1 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 1)

Перечень основного оборудования:

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 60 ед.

Раздел 9. Образовательные технологии

Образовательные технологии, используемые при проведении учебных занятий по дисциплине «Методы и средства криптографической 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.

Лист актуализации рабочей программы дисциплины

«Методы и средства криптографической защиты информации»

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____