ГАОУ ВО «Дагестанский государственный университет народного хозяйства»

Утверждена решением
Ученого совета ДГУНХ,
протокол № 11
от 06 июня 2023 г

Кафедра «Информационные технологии и информационная безопасность»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Направление подготовки

10.03.01 Информационная безопасность,

профиль «Безопасность автоматизированных систем»

Уровень высшего образования - бакалавриат

Формы обучения – очная, очно-заочная

Махачкала – 2023

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 дисциплины «Стеганографические методы 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 «Стеганографические методы защиты информации» размещена на официальном сайте www.dgunh.ru

Гасанова З.А. Рабочая программа по дисциплине «Стеганографические методы защиты информации» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2023 г., 17 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 05 июня 2023 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» 31 мая 2023 г., протокол № 10.

Содержание

Раздел 1. Перечень планируемых результатов обучения по дисциплине

Цель дисциплины – сформировать компетенции обучающегося в области администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей, применения средств криптографической защиты информации для решения задач профессиональной деятельности.

Задачами преподавания дисциплины являются:

- Рассмотреть особенности применения стеганографии и предъявляемых к ней требования.
- Изучить атаки на стегосистемы и технологии противодействия им, оценки стойкости стеганографических систем и условия их достижения.
- Изучить алгоритмы встраивания информации в изображениях, видеопоследовательностях и аудиосигналах.

1.1. Компетенции выпускников, формируемые в результате освоения дисциплины «Стеганографические методы защиты информации» как часть планируемых результатов освоения образовательной программы

код компетенции	формулировка компетенции
ПК-1	Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей

1.2. Планируемые результаты обучения по дисциплине

Код и наименование компетенции	***Код и наименование индикатора достижения компетенции***	***Планируемые результаты обучения по дисциплине***
ПК-1. Способен выполнять комплекс задач администрирования подсистем информационной безопасности и	ИПК-1.4. Использует криптографическое методы защиты информации в автоматизированных системах	**Знать:** - основные методы и алгоритмы скрытного встраивания одних данных в другие; - методы обнаружения встроенных сообщений; - методы повышения пропускной способности стеганографических каналов передачи данных и обеспечения их стойкости; **Уметь:**

управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей		- применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности. **Владеть:** - основными методами прикладной стеганографии, в том числе методами встраивания, извлечения, анализа открытых каналов передачи информации.

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

Код компетенции	Этапы формирования компетенций						
	Тема 1. Области применения стеганографии и требования, предъявляемые к ней. Атаки на стегостистемы и технологии противодействия им	Тема 2. Пропускная способность каналов передачи скрываемой информации	Тема 3. Оценки стойкости стеганографических систем и условия их достижения	Тема 4. Технологии скрытия данных в неподвижных изображениях	Тема 5. Стегоалгоритмы встраивания информации в изображения	Тема 6. Технологии скрытия данных в аудиосигналах	Тема 7. Технологии скрытия данных в видеопоследовательностях
ПК-1	+	+	+	+	+	+	+

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.ДВ.03.01 «Стеганографические методы защиты информации» относится к дисциплина по выбору Блока 1 «Дисциплины» учебного плана направления подготовки 10.03.01 Информационная безопасность, профиля «Безопасность автоматизированных систем».

Для изучения данной дисциплины необходимы знания, умения и навыки по дисциплинам: «Дискретная математика», «Теория информация», «Методы и средства криптографической защиты информации».

Освоение данной дисциплины необходимо обучающемуся для изучения дисциплин «Мониторинг и аудит защищенности информации в автоматизированных системах», «Проектирование защищенных автоматизированных систем», «Проектирование защищенных автоматизированных систем», успешного прохождения производственной практики и выполнения выпускной квалификационной работы.

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 2 зачетные единицы.

Очная форма обучения

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 48 часов, в том числе:

на занятия лекционного типа – **16** ч.

на занятия семинарского типа – **32** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **24** ч.

Форма промежуточной аттестации: зачет.

Очно-заочная форма обучения

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 24 часа, в том числе:

на занятия лекционного типа – **8** ч.

на занятия семинарского типа – **16** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **48** ч.

Форма промежуточной аттестации: зачет.

Отдельные учебные занятия по дисциплине реализуются в форме практической подготовки.

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.
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия		
1.	Тема 1. Области применениястеганографии и требования, предъявляемые к ней. Атаки на стегостистемы и технологии противодействия им	7	2	-	2	-	-	-	3	– Устный опрос – Тестирование; – Подготовка реферата; – Подготовка презентации; – Выполнение практического задания.
2.	Тема 2. Пропускная способность каналов передачи скрываемой информации	9	2	-	4	-	-	-	3	– Устный опрос – Тестирование; – Подготовка реферата; – Подготовка презентации; – Выполнение практического задания.
3.	Тема 3. Оценки стойкостистеганографических систем и условия их достижения	9	2	-	4	-	-	-	3	– Устный опрос – Тестирование; – Подготовка реферата; – Подготовка презентации; – Выполнение практического задания.
4.	Тема 4. Технологии скрытия данных в неподвижных изображениях*	9	2	-	4	-	-	-	3	– Устный опрос – Тестирование; – Подготовка реферата; – Подготовка презентации;

										– Выполнение практического задания.
5.	Тема 5. Стегоалгоритмы встраивания информации в изображения*	14	4*	-	6*	-	-	-	4	– Устный опрос – Тестирование; – Подготовка реферата; – Подготовка презентации; – Выполнение практического задания.
6.	Тема 6. Технологии скрытия данных в аудиосигналах *	12	2*	-	6*	-	-	-	4	– Устный опрос – Тестирование; – Подготовка реферата; – Подготовка презентации; – Выполнение практического задания.
7.	Тема 7. Технологии скрытия данных в видеопоследовательностях*	10	2*	-	4*	-	-	-	4	– Устный опрос – Тестирование; – Подготовка реферата; – Подготовка презентации; – Выполнение практического задания.
	Зачет	2	0		2					–
	ИТОГО	**72**	**16**	**-**	**32**	**-**	**-**	**-**	**24**	

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.
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия		
1.	Тема 1. Области применениястеганографии	9	1	-	2	-	-	-	6	– Устный опрос – Тестирование;

	и требования, предъявляемые к ней. Атаки на стегостистемы и технологии противодействия им									– Подготовка реферата; – Подготовка презентации; – Выполнение практического задания.
2.	Тема 2. Пропускная способность каналов передачи скрываемой информации	9	1	-	2	-	-	-	6	– Устный опрос – Тестирование; – Подготовка реферата; – Подготовка презентации; – Выполнение практического задания.
3.	Тема 3. Оценки стойкостистеганографических систем и условия их достижения	9	1	-	2	-	-	-	6	– Устный опрос – Тестирование; – Подготовка реферата; – Подготовка презентации; – Выполнение практического задания.
4.	Тема 4. Технологии скрытия данных в неподвижных изображениях*	9	1	-	2	-	-	-	6	– Устный опрос – Тестирование; – Подготовка реферата; – Подготовка презентации; – Выполнение практического задания.
5.	Тема 5. Стегоалгоритмы встраивания информации в изображения*	14	2*	-	2*	-	-	-	10	– Устный опрос – Тестирование; – Подготовка реферата; – Подготовка презентации; – Выполнение практического задания.
6.	Тема 6. Технологии скрытия данных в аудиосигналах *	10	1*	-	2*	-	-	-	7	– Устный опрос – Тестирование; – Подготовка реферата; – Подготовка презентации; – Выполнение практического задания.

7.	Тема 7. Технологии скрытия данных в видеопоследовательностях*	10	1*	-	2*	-	-	-	7	– Устный опрос – Тестирование; – Подготовка реферата; – Подготовка презентации; – Выполнение практического задания.
	Зачет	2	0		2					–
	ИТОГО	**72**	**8**	**-**	**16**	**-**	**-**	**-**	**48**	

*Реализуется в форме практической подготовки

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.	Зенков, А. В.	Информационная безопасность и защита информации :	Учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с.	https://urait.ru/bcode/497002
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. Ульянова». - Ульяновск : УлГПУ, 2013. - 128 с. ISBN 978-5-86045-640-2	http://biblioclub.ru/index.php?page=book&id=278070

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, 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 "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.	Научный журнал «Информатика и ее применение»
2.	Информатика и безопасность
3.	Рецензируемый научный журнал «Информатика и система управления»
4.	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
- Steganography OpenPuff

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 «Стеганографические методы 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.

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 «Стеганографические методы защиты информации», обеспечивают развитие у обучающихся необходимых знаний и навыков.

При изучении дисциплины предусматривается использование интерактивных методов и технологий формирования компетенций у студентов:

- применение разноуровневого обучения, обеспечивающего дифференцированный подход к подготовке студентов при освоении материала дисциплины до соответствующего уровня формируемой компетенции;
- проведение лекционных и практических занятий с применением мультимедийных технологий;
- проведение практических занятий в малых группах с обсуждением результатов в форме групповых дискуссий.

В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по собственной траектории в рамках индивидуального рабочего плана, изучение данной дисциплины базируется на следующих возможностях: обеспечение внеаудиторной работы со студентами, в том числе в электронной образовательной среде с использованием соответствующего программного оборудования, дистанционных форм обучения, возможностей интернет-ресурсов, индивидуальных консультаций и т.д.

Лист актуализации рабочей программы дисциплины

«Стеганографические методы 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 _____