

**ГАОУ ВО «Дагестанский государственный университет народного хозяйства»**

*Утверждена решением  
Ученого совета ДГУНХ,  
протокол № 12  
от 30 мая 2024 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 – 2024**

**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 «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](http://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, 2024 г., 17 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 28 мая 2024 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» 23 мая 2024 г., протокол № 10.

## Содержание

Раздел 1. Перечень планируемых результатов обучения по дисциплине...	4
Раздел 2. Место дисциплины в структуре образовательной программы...	5
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 1
Раздел 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.....	1 4
Раздел 7. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных.....	15
Раздел 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.....	1 5
Раздел 9. Образовательные технологии.....	16
Лист актуализации рабочей программы дисциплины.....	17

## 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 стegosистемы и технологии противодействия им, оценки стойкости стеганографических систем и условия их достижения.
- Изучить алгоритмы встраивания информации в изображениях, видео-последовательностях 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

<i>Код и наименование компетенции</i>	<i>Код и наименование индикатора достижения компетенции</i>	<i>Планируемые результаты обучения по дисциплине</i>
ПК-1. Способен выполнять комплекс задач администрирования подсистем информацио	ИПК-1.4. Использует криптографические методы защиты информации в автоматизированных системах	<b><u>Знать:</u></b> - 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; <b><u>Уметь:</u></b> - применять средства криптографической и

нной безопасност и и управления информацио нной безопасност ью операционн ых систем, систем управления базами данных и компьютерн ых сетей		технической защиты информации для решения задач профессиональной деятель- ности. <b>Владеть:</b> - 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 стегосистемы 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 информации», «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 применения стеганографии и требования, предъявляемые к ней. Атаки на стегостисемы и технологии противодействия им	7	2	-	2	-	-	-	3	<ul style="list-style-type: none"> <li>- Устный опрос</li> <li>- Тестирование;</li> <li>- Подготовка реферата;</li> <li>- Подготовка презентации;</li> <li>- Выполнение практического задания.</li> </ul>
2.	Тема 2. Пропускная способность каналов передачи скрываемой информации	9	2	-	4	-	-	-	3	<ul style="list-style-type: none"> <li>- Устный опрос</li> <li>- Тестирование;</li> <li>- Подготовка реферата;</li> <li>- Подготовка презентации;</li> <li>- Выполнение практического задания.</li> </ul>
3.	Тема 3. Оценки стойкости стеганографических систем и условия их достижения	9	2	-	4	-	-	-	3	<ul style="list-style-type: none"> <li>- Устный опрос</li> <li>- Тестирование;</li> <li>- Подготовка реферата;</li> <li>- Подготовка презентации;</li> <li>- Выполнение практического задания.</li> </ul>
4.	Тема 4. Технологии скрытия данных в неподвижных изображениях*	9	2	-	4	-	-	-	3	<ul style="list-style-type: none"> <li>- Устный опрос</li> <li>- Тестирование;</li> <li>- Подготовка реферата;</li> <li>- Подготовка презентации;</li> </ul>

										– 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					–
	<b>ИТОГО</b>	<b>72</b>	<b>0</b>	<b>-</b>	<b>2</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>24</b>	

### 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 применения	9	1	-	2	-	-	-	6	– Устный опрос – Тестирование;

	стеганографии и требования, предъявляемые к ней. Атаки на стегостисемы и технологии противодействия им									<ul style="list-style-type: none"> <li>– Подготовка реферата;</li> <li>– Подготовка презентации;</li> <li>– Выполнение практического задания.</li> </ul>
2.	Тема 2. Пропускная способность каналов передачи скрываемой информации	9	1	-	2	-	-	-	6	<ul style="list-style-type: none"> <li>– Устный опрос</li> <li>– Тестирование;</li> <li>– Подготовка реферата;</li> <li>– Подготовка презентации;</li> <li>– Выполнение практического задания.</li> </ul>
3.	Тема 3. Оценки стойкости стеганографических систем и условия их достижения	9	1	-	2	-	-	-	6	<ul style="list-style-type: none"> <li>– Устный опрос</li> <li>– Тестирование;</li> <li>– Подготовка реферата;</li> <li>– Подготовка презентации;</li> <li>– Выполнение практического задания.</li> </ul>
4.	Тема 4. Технологии скрытия данных в неподвижных изображениях*	9	1	-	2	-	-	-	6	<ul style="list-style-type: none"> <li>– Устный опрос</li> <li>– Тестирование;</li> <li>– Подготовка реферата;</li> <li>– Подготовка презентации;</li> <li>– Выполнение практического задания.</li> </ul>
5.	Тема 5. Стегоалгоритмы встраивания информации в изображения*	14	2*	-	2*	-	-	-	10	<ul style="list-style-type: none"> <li>– Устный опрос</li> <li>– Тестирование;</li> <li>– Подготовка реферата;</li> <li>– Подготовка презентации;</li> <li>– Выполнение практического задания.</li> </ul>
6.	Тема 6. Технологии скрытия данных в аудиосигналах *	10	1*	-	2*	-	-	-	7	<ul style="list-style-type: none"> <li>– Устный опрос</li> <li>– Тестирование;</li> <li>– Подготовка реферата;</li> <li>– Подготовка презентации;</li> <li>– Выполнение практического</li> </ul>

										задания.
7.	Тема 7. Технологии скрытия данных в видеопоследовательностях*	10	1*	-	2*	-	-	-	7	<ul style="list-style-type: none"> <li>- Устный опрос</li> <li>- Тестирование;</li> <li>- Подготовка реферата;</li> <li>- Подготовка презентации;</li> <li>- Выполнение практического задания.</li> </ul>
	Зачет	2	0		2					-
	<b>ИТОГО</b>	<b>72</b>	<b>0</b>	<b>-</b>	<b>2</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>48</b>	

\*Реализуется в форме практической подготовки

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

<b>№ п/п</b>	<b>Автор</b>	<b>Название основной и дополнительной учебной литературы, необходимой для освоения дисциплины</b>	<b>Выходные данные</b>	<b>Количество экземпляров в библиотеке ДГУНХ/адрес доступа</b>
<b>I. Основная учебная литература</b>				
1.	Лапониная О.Р.	Криптографические основы безопасности	Москва : Национальный Открытый Университет «ИНТУ-ИТ», 2016. - 244 с. ISBN 5-9556-00020-5	<a href="http://biblioclub.ru/index.php?page=book&amp;id=429092">http://biblioclub.ru/index.php?page=book&amp;id=429092</a>
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.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=228963">http://biblioclub.ru/index.php?page=book&amp;id=228963</a>
3.	Зенков, А. В.	Информационная безопасность и защита информации :	Учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с.	<a href="https://urait.ru/bcode/497002">https://urait.ru/bcode/497002</a>
<b>II. Дополнительная литература</b>				
<b>А) Дополнительная учебная литература</b>				
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. -	<a href="http://biblioclub.ru/index.php?page=book&amp;id=278070">http://biblioclub.ru/index.php?page=book&amp;id=278070</a>

			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.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=483838">http://biblioclub.ru/index.php?page=book&amp;id=483838</a>
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	<a href="http://biblioclub.ru/index.php?page=book&amp;id=117663">http://biblioclub.ru/index.php?page=book&amp;id=117663</a>
4.	Басалова Г.В	Основы криптографии : курс лекций	Г.В. Басалова ; Национальный Открытый Университет "ИНТУ-ИТ". - Москва : Интернет-Университет Информационных Технологий, 2011. - 253 с.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=233689">http://biblioclub.ru/index.php?page=book&amp;id=233689</a>
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. ISBN 978-5-7782-1425-5	<a href="http://biblioclub.ru/index.php?page=book&amp;id=228963">http://biblioclub.ru/index.php?page=book&amp;id=228963</a>
6.	И.А. Калмыков, Д.О. Науменко	Криптографические методы защиты информации	Министерство образования и науки Российской Федерации и др. –	<a href="http://biblioclub.ru/index.php?page=book&amp;id=458059">http://biblioclub.ru/index.php?page=book&amp;id=458059</a>

			Ставрополь : СКФУ, 2015. – 109 с.	
7.	Ищуква, 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.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=493059">http://biblioclub.ru/index.php?page=book&amp;id=493059</a>
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.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=234148">http://biblioclub.ru/index.php?page=book&amp;id=234148</a>
9.	Свон М.	Блокчейн: схема новой экономики	М. Свон. - Москва : Олимп-Бизнес, 2017. - 241 с. ISBN 978-5-9693-0360-7 ;	<a href="http://biblioclub.ru/index.php?page=book&amp;id=494451">http://biblioclub.ru/index.php?page=book&amp;id=494451</a>

**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. <a href="http://www.standartgost.ru">www.standartgost.ru</a>
3.	ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. <a href="http://www.standartgost.ru">www.standartgost.ru</a>
4.	ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств. 2002 г.

	<a href="http://www.standartgost.ru">www.standartgost.ru</a>
5.	ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» <a href="http://www.standartgost.ru">www.standartgost.ru</a>
6.	ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. <a href="http://www.standartgost.ru">www.standartgost.ru</a>
7.	ГОСТ Р ИСО/МЭК 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» <a href="http://www.standartgost.ru">www.standartgost.ru</a>
<b><i>В) Периодические издания</i></b>	
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»
<b><i>Г) Справочно-библиографическая литература</i></b>	
1.	1. Краткий энциклопедический словарь по информационной безопасности : словарь / сост. В.Г. Дождиков, М.И. Салтан. – Москва : Энергия, 2010. – 240 с. <a href="http://biblioclub.ru/index.php?page=book&amp;id=58393">http://biblioclub.ru/index.php?page=book&amp;id=58393</a>

## **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](http://www.biblioclub.ru)), ЭБС «ЭБС Юрайт» ([www.urait.ru](http://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 программ-

ного 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 \_\_\_\_\_