ГАОУ ВО «Дагестанский государственный университет народного хозяйства»

Утверждена решением
Ученого совета ДГУНХ,
протокол № 9
от 21 мая 2026 г

Кафедра «Информационные технологии и информационная безопасность»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки 09.03.03 Прикладная информатика,

профиль «Информационные системы в экономике»

Уровень высшего образования - бакалавриат

Формы обучения –

очная, очно-заочная, заочная

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A9E2DAF91A2F57E988B751E574CFCC
Владелец: Бучаев Ахмед Гамидович
Действителен: с 23.09.2025 до 17.12.2026

Махачкала – 2026

УДК 004.056.5
ББК 32.973.2

Составитель – Эмирбеков Эльдар Меликович, старший преподаватель кафедры «Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент - Гасанова Зарема Ахмедовна, кандидат педагогических наук, доцент кафедры «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Меджидов Зияудин Гаджиевич, кандидат физико-математических наук, старший научный сотрудник Отдела математики и информатики Дагестанского научного центра Российской Академии Наук

Представитель работодателя - Газимагомедов Ахмед Абдуллаевич, к.э.н., ведущий инженер-программист научно-организационного отдела Да-гестанского федерального исследовательского центра Российской академии наук.

Рабочая программа дисциплины «Информационная безопасность» разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 «Прикладная информатика», утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г., № 922, в соответствии с приказом Министерства образования и науки Российской Федерации от 06.04.2021г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»

Рабочая программа по дисциплине «Информационная безопасность» размещена на официальном сайте www.dgunh.ru

Эмирбеков Э.М. Рабочая программа по дисциплине «Информационная безопасность» для направления подготовки 09.03.03 Прикладная информатика, профиль «Информационные системы в экономике» – Махачкала: ДГУНХ, 2026. - 19 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 10 марта 2026 г.

Рекомендована к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 09.03.03 Прикладная информатика, профиль «Информационные системы в экономике», к.э.н., доцентом Раджабовым К.Я.

Одобрена на заседании кафедры «Информационные технологии и информационная безопасность» 24 февраля 2026 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 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	14
Раздел 6.	Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины	17
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	18
Раздел 9.	Образовательные технологии	19

Раздел 1. Перечень планируемых результатов обучения по дисциплине

Цель дисциплины – сформировать компетенции обучающегося в области информационной безопасности, заложить терминологический фундамент и ознакомить с общими методами и подходами обеспечения информационной безопасности.

Задачи дисциплины

- Рассмотреть основные методики и подходы обеспечения информационной безопасности в рамках современных автоматизированных систем.
- Раскрыть принципы построения защищенных информационных систем и поддержания подсистемы защиты информации в актуальном состоянии.
- Показать особенности реализации общих методик защиты информации на различных платформах.

1.1 Компетенции выпускников, формируемые в результате освоения дисциплины «Информационная безопасность» как часть планируемых результатов освоения образовательной программы

код компетенции	формулировка компетенции
ОПК	**ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ОПК -3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

1.2. Планируемые результаты обучения по дисциплине

Код и формулировка компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине (модулю)
ОПК -3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИОПК -3.2**. Учитывает основные требования информационной безопасности при решении задач профессиональной деятельности на основе информационной и библиографической культуры	**Знать**: основные информационно-коммуникационные технологии и основные требования информационной безопасности **Уметь:** решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности **Владеть:** культурой применения информационно-коммуникационных технологий с учетом основных требований

		информационной безопасности
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	**ИОПК – 4.1**. Обладает знаниями нормативной базы профессиональной деятельности, используемыми на различных стадиях жизненного цикла информационной системы	**Знать**: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. **Уметь**: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. **Владеть**: навыками составления технической документации на различных этапах жизненного цикла информационной системы

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

Код компетенции	Этапы формирования компетенций						
	Тема 1. Введение в информационную безопасность.	Тема 2. Задачи и методы информационной безопасности.	Тема 3. Угрозы информационной безопасности.	Тема 4. Потенциальные противники и атаки.	Тема 5. Основные положения теории информационной безопасности информационных систем.	Тема 6. Политика безопасности информационных систем.	Тема 7. Организационно-правовые методы информационной безопасности.
ОПК -3	+	+	+	+	+	+	+
ОПК-4	**+**	**+**	**+**	**+**	**+**	**+**	**+**

Код компетенции	Этапы формирования компетенций					
	Тема 8. Основные понятия криптографии.	Тема 9. Криптографические протоколы.	Тема 10. Программно - технические методы защиты.	Тема 11. Защита данных и сервисов от воздействия вредоносных программ.	Тема 12. Стандарты обеспечения информационной безопасности	Тема 13. Основные технологии построения защищённых экономических информационных систем.
ОПК-3	+	+	+	+	+	+
ОПК-4					+	+

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.О.19 «Информационная безопасность» относится к обязательной части Блока 1 «Дисциплины» учебного плана направления подготовки «Прикладная информатика», профиля «Информационные системы в экономике».

Для изучения данной дисциплины необходимы знания, умения и навыки по дисциплинам "Вычислительные системы, сети и телекоммуникации"; "Дискретная математика"; "Введение в информационные технологии".

Освоение данной дисциплины необходимо обучающемуся для изучения дисциплин "Базы данных" и "Проектирование информационных систем".

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

Объем дисциплины в зачетных единицах составляет 5 зачетных единиц.

Очная форма обучения

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 75 часов, в том числе:

на занятия лекционного типа – 30 ч.

на занятия семинарского типа – 45 ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – 69 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 38 часов, в том числе:

на занятия лекционного типа – 15 ч.

на занятия семинарского типа – 23 ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – 106 ч.

Форма промежуточной аттестации: экзамен, 36 ч.

Заочная форма обучения

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 12 часов, в том числе:

на занятия лекционного типа – 6 ч.

на занятия семинарского типа – 6 ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – 164 ч.

Форма промежуточной аттестации: экзамен, 4 ч.

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

4.1. 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. Введение в информационную безопасность.	10	2	-	*1*	*2*	-	-	6	Проведение опроса Выполнение лабораторной (практической) работы
2.	Тема 2. Задачи и методы информационной безопасности.	10	2	-	*1*	*2*	-	-	6	Проведение опроса Выполнение лабораторной (практической) работы
3.	Тема 3. Угрозы информационной безопасности.	10	2	-	*1*	*2*	-	-	6	Проведение опроса Выполнение лабораторной (практической) работы
4.	Тема 4. Потенциальные противники и атаки.	10	2	-	*1*	*2*	-	-	6	Проведение опроса Выполнение лабораторной (практической) работы
5.	Тема 5. Основные положения теории информационной безопасности информационных систем.	10	2	-	*1*	*2*	-	-	6	Проведение опроса Выполнение лабораторной (практической) работы
6.	Тема 6. Политика безопасности информационных систем.	10	2	-	*1*	*2*	-	-	6	Проведение опроса

										Выполнение лабораторной (практической) работы Решение кейса
7.	Тема 7. Организационно-правовые методы информационной безопасности.	10	2	-	*1*	*2*	-	-	6	Проведение опроса Выполнение лабораторной (практической) работы
8.	Тема 8. Основные понятия криптографии.	10	2	-	*1*	*2*	-	-	6	Проведение опроса Выполнение лабораторной (практической) работы
9.	Тема 9. Криптографические протоколы.	10	2	-	*1*	*2*	-	-	6	Проведение опроса Выполнение лабораторной (практической) работы
10.	Тема 10. Программно-технические методы защиты.	14	4	-	*2*	*3*	-	-	6	Проведение опроса Выполнение лабораторной (практической) работы
11.	Тема 11. Защита данных и сервисов от воздействия вредоносных программ.	12	2	-	*1*	*3*	-	-	8	Проведение опроса Выполнение лабораторной (практической) работы
12.	Тема 12. Стандарты обеспечения информационной безопасности.	12	2	-	*1*	*3*	-	-	8	Проведение опроса Выполнение лабораторной (практической) работы
13.	Тема 13. Основные технологии построения защищённых экономических информационных систем.	16	4	-	*2*	*3*	-	-	8	Проведение опроса Выполнение лабораторной (практической) работы
ИТОГО		**144**	**30**	**-**	***15***	***30***	**-**	**-**	**69**	

Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	***36***	**Контроль**
ВСЕГО:	***180***	

4.2. 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. Введение в информационную безопасность.	11	1	-	*1*	*1*	-	-	8	Проведение опроса Выполнение лабораторной (практической) работы
2.	Тема 2. Задачи и методы информационной безопасности.	11	1	-	*1*	*1*	-	-	8	Проведение опроса Выполнение лабораторной (практической) работы
3.	Тема 3. Угрозы информационной безопасности.	11	1	-	*1*	*1*	-	-	8	Проведение опроса Выполнение лабораторной (практической) работы
4.	Тема 4. Потенциальные противники и атаки.	11	1	-	*1*	*1*	-	-	8	Проведение опроса Выполнение лабораторной (практической) работы

5.	Тема 5. Основные положения теории информационной безопасности информационных систем.	11	1	-	*1*	*1*	-	-	8	Проведение опроса Выполнение лабораторной (практической) работы
6.	Тема 6. Политика безопасности информационных систем.	11	1	-	*1*	*1*	-	-	8	Проведение опроса Выполнение лабораторной (практической) работы Решение кейса
7.	Тема 7. Организационно-правовые методы информационной безопасности.	11	1	-	*1*	*1*	-	-	8	Проведение опроса Выполнение лабораторной (практической) работы
8.	Тема 8. Основные понятия криптографии.	11	1	-	*1*	*1*	-	-	8	Проведение опроса Выполнение лабораторной (практической) работы
9.	Тема 9. Криптографические протоколы.	11	1	-	-	*1*	-	-	10	Проведение опроса Выполнение лабораторной (практической) работы
10.	Тема 10. Программно-технические методы защиты.	11	1	-	-	*1*	-	-	10	Проведение опроса Выполнение лабораторной (практической) работы
11.	Тема 11. Защита данных и сервисов от воздействия вредоносных программ.	11	2	-	-	*4*	-	-	10	Проведение опроса Выполнение лабораторной (практической) работы
12.	Тема 12. Стандарты обеспечения информационной безопасности.	11	1	-	-	*1*	-	-	10	Проведение опроса Выполнение лабораторной (практической) работы

13.	Тема 13. Основные технологии построения защищённых экономических информационных систем.	12	2	-	-	-	-	-	10	Проведение опроса Выполнение лабораторной (практической) работы
ИТОГО		**144**	**15**	**-**	***8***	***15***	**-**	**-**	**106**	
Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)		***36***								**Контроль**
ВСЕГО:		***180***								

4.3. Заочная форма отделение

№ 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 информационную безопасность.	13	1	-	0	0	-	-	12	Проведение опроса Выполнение лабораторной (практической) работы
2.	Тема 2. Задачи и методы информационной безопасности.	13	1	-	0	0	-	-	12	Проведение опроса Выполнение лабораторной (практической) работы
3.	Тема 3. Угрозы информационной безопасности.	13	1	-	0	0	-	-	12	Проведение опроса Выполнение лабораторной (практической) работы
4.	Тема 4. Потенциальные противники и атаки.	12	-	-	0	0	-	-	12	Проведение опроса

										Выполнение лабораторной (практической) работы
5.	Тема 5. Основные положения теории информационной безопасности информационных систем.	12	0	-	-	0	-	-	12	Проведение опроса Выполнение лабораторной (практической) работы
6.	Тема 6. Политика безопасности информационных систем.	13	0	-	0	1	-	-	12	Проведение опроса Выполнение лабораторной (практической) работы
7.	Тема 7. Организационно-правовые методы информационной безопасности.	14	1	-	1	0	-	-	12	Проведение опроса Выполнение лабораторной (практической) работы
8.	Тема 8. Основные понятия криптографии.	13	1	-	-	0	-	-	12	Проведение опроса Выполнение лабораторной (практической) работы
9.	Тема 9. Криптографические протоколы.	13	-	-	0	1	-	-	12	Проведение опроса Выполнение лабораторной (практической) работы
10.	Тема 10. Программно-технические методы защиты.	13	0	-	0	1	-	-	12	Проведение опроса Выполнение лабораторной (практической) работы
11.	Тема 11. Защита данных и сервисов от воздействия вредоносных программ.	15	0	-	1	0	-	-	14	Проведение опроса Выполнение лабораторной (практической) работы
12.	Тема 12. Стандарты обеспечения информационной безопасности.	15	1	-	0	0	-	-	14	Проведение опроса

										Выполнение лабораторной (практической) работы
13.	Тема 13. Основные технологии построения защищённых экономических информационных систем.	17	0	-	0	1	-	-	16	Проведение опроса Выполнение лабораторной (практической) работы
12	**ИТОГО**	**176**	**6**		**2**	**4**			**164**	
Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)		**4**								**Контроль**
ВСЕГО:		**180**								

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.	Полякова Т. А. [и др.]	Организационное и правовое обеспечение информационной безопасности: учебник для вузов / А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп.	Москва: Издательство Юрайт, 2024. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0.	https://urait.ru/bcode/555950
2.	Зенков А. В.	Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков.	Москва: Издательство Юрайт, 2024. — 107 с. 2 изд.— (Высшее образование). — ISBN 978-5-534-14590-8. — Образовательная платформа Юрайт	https://urait.ru/bcode/544290
3.	Суворова Г. М.	Информационная безопасность: учебное пособие для вузов / Г. М. Суворова.	Москва: Издательство Юрайт, 2024. — 277 с. 2 изд.— (Высшее образование). — ISBN 978-5-534-13960-0. — Образовательная платформа Юрайт	https://urait.ru/bcode/544029
4.	Щербак А.В.	Информационная безопасность: учебник для вузов / А. В. Щербак. — 2-е изд.	Москва: Издательство Юрайт, 2025. — 252 с. — (Высшее образование). — ISBN 978-5-9916-4299-6. —	https://urait.ru/bcode/569267

			Текст: электронный // Образовательная платформа Юрайт	
5.	Козырь Н.С.	Экономические аспекты информационной безопасности: учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян.	Москва: Издательство Юрайт, 2025. — 131 с. — (Высшее образование). — ISBN 978-5-534-17863-0. — Текст: электронный // Образовательная платформа Юрайт	https://urait.ru/bcode/568708
II. Дополнительная учебная литература				
А) Дополнительная учебная литература				
1.	Козырь Н.С.	Оценка рисков и аудит информационной безопасности: учебник для вузов / Н. С. Козырь, В. Н. Хализев.	Москва: Издательство Юрайт, 2025. — 186 с. — (Высшее образование). — ISBN 978-5-534-17864-7. — Текст: электронный // Образовательная платформа Юрайт	https://urait.ru/bcode/581501
2.	Петренко В.И.	Теоретические основы защиты информации: учебное пособие	Ставрополь: СКФУ, 2015. - 222 с.	https://biblioclub.ru/index.php?page=book_red&id=458204&sr=1
3.	Шилов, А.К.	Управление информационной безопасностью: учебное пособие /	Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2018. – 121 с.	https://biblioclub.ru/index.php?page=book_red&id=500065&sr=1
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 https://biblioclub.ru/index.php?page=book_red&id=58393&sr=1

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 менеджмента информационной безопасности, 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, профессиональных баз данных

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

1. Windows 10
2. Microsoft Office Professional
3. Adobe Acrobat Reader DC
4. VLC Media player
5. 7-zip
6. Microsoft Visual Studio
7. Справочно-правовая система «КонсультантПлюс»

7.2. Перечень информационных справочных систем:

– информационно справочная система «Консультант Плюс»;

7.3. Перечень профессиональных баз данных:

– Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00).
– Реестр операторов, осуществляющих обработку персональных данных (https://rkn.gov.ru/personal-data/register/);
– http://Standartgost.ru - Открытая база ГОСТов
– Научная электронная библиотека https://elibrary.ru/

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

Для преподавания дисциплины «Информационной безопасность» используются следующие специальные помещения – учебные аудитории:

Учебная аудитория для проведения учебных занятий № 4.11 (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 (моноблок) с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» (www.biblioclub.ru), «Образовательная платформа Юрайт» (www.urait.ru).

***Перечень учебно-наглядных пособий*:**

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

Компьютерный класс, учебная аудитория для проведения учебных занятий № 4.2 (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 с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» (www.biblioclub.ru), «Образовательная платформа Юрайт» (www.urait.ru) – 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, дом 5, учебный корпус № 2 литер «В»)

***Перечень основного оборудования*:**

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 19 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 «Информационная безопасность», обеспечивают развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств.

На занятиях лекционного типа применяются такие методы обучения как управляемая дискуссия, проблемная лекции. На практических занятиях, целью которых является приобретение учащимися определенных практических умений и навыков в области информационной безопасности, целесообразно научить их аналитически мыслить, уметь принимать верные решения в различных ситуациях, в ходе занятий (с целью повышения их результативности) применять деловые игры, метод дискуссий, методы проектов.