

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

*Утверждена решением  
Ученого совета ДГУНХ,  
протокол № 13  
от 29 мая 2021 г.*

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

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ  
«КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИ-  
ЗАЦИИ»**

**Направление подготовки**

**10.03.01 Информационная безопасность,**

**профиль «Безопасность автоматизированных систем»**

**Уровень высшего образования - бакалавриат**

**Формы обучения – очная, очно-заочная**

**Махачкала – 2021**

**УДК 004.056**

**ББК 32.973.202**

**Составитель** – Меджидов Заур Уруджалиевич, кандидат экономических наук, доцент кафедры «Информационные технологии и информационная безопасность» ДГУНХ.

**Внутренний рецензент** – Раджабов Карахан Якубович, кандидат экономических наук, доцент, декан факультета информационных технологий и управления ДГУНХ.

**Внешний рецензент** – Абдуллаев Ших-Саид Омаржанович, доктор технических наук, главный научный сотрудник Отдела математики и информатики Дагестанского научного центра Российской академии наук.

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

*Рабочая программа дисциплины «Комплексная защита объектов информатизации» 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 образования и науки Российской Федерации от 5.04.2017 г. № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»*

Рабочая программа дисциплины «Комплексная защита объектов информатизации» размещена на сайте [www.dgunh.ru](http://www.dgunh.ru)

Меджидов З.У. Рабочая программа дисциплины «Комплексная защита объектов информатизации» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2021 г. - 20 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 28 мая 2021 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 мая 2021 г., протокол № 10.

## 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 на форму промежуточной аттестации	7
Раздел 4.	Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий	8
Раздел 5.	Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	15
Раздел 6.	Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины	16
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
	Лист актуализации рабочей программы дисциплины	20

## Раздел 1. Перечень планируемых результатов обучения по дисциплине

**Цель** дисциплины - сформировать компетенции обучающегося в области комплексного подхода к решению задач информационной безопасности объекта информатизации.

**Задачи** дисциплины:

- Рассмотреть методологию комплексного анализа угроз информационной безопасности;
- Раскрыть общеметодологические принципы построения комплексных систем обеспечения информационной безопасности;
- Показать особенности методов и средств проектирования систем обеспечения информационной безопасности, методов оценки качества систем и моделей, аттестации средств.

**1.1 Компетенции выпускников, формируемые в результате освоения дисциплины «Комплексная защита объектов информатизации» как часть планируемых результатов освоения образовательной программы высшего образования**

код компетенции	Формулировка компетенции
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений
ОПК-4.4	Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем

## 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>
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нор-	ОПК-6.2. Подготавливает объект информатизации для прохождения аттестации на соответствие требованиям государственных и ведомственных нормативных документов	<b><u>Знать:</u></b> – виды аттестаций объектов информатизаций; – принципы выстраивания комплексной защиты информации в соответствии с нормативно-методическими документами ФСБ России, ФСТЭК России. <b><u>Уметь:</u></b> - определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты инфор-

<p>мативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p>		<p>мации ограниченного доступа;</p> <ul style="list-style-type: none"> <li>– применять отечественные и зарубежные стандарты в области информационной безопасности для оценки защищенности объектов информатизации;</li> <li>– пользоваться нормативными документами по защите информации;</li> </ul> <p><b><u>Владеть:</u></b></p> <ul style="list-style-type: none"> <li>- методами формирования требований по защите информации;</li> <li>– методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов</li> </ul>
<p>ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений</p>	<p>ОПК-12.2. Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений</p>	<p><b><u>Знать:</u></b></p> <ul style="list-style-type: none"> <li>- особенности основных показателей технико-экономического обоснования соответствующих проектных решений по защите информации;</li> <li>- модели оценки ценности информации;</li> </ul> <p><b><u>Уметь:</u></b></p> <ul style="list-style-type: none"> <li>- разрабатывать техническое задание на создание систем безопасности информации ограниченного доступа, проектировать такие системы с учетом требований нормативных документов;</li> <li>- определять перечень информации ограниченного доступа организации, подлежащей защите;</li> </ul> <p><b><u>Владеть:</u></b></p> <ul style="list-style-type: none"> <li>- методами анализа и обработки исходных данных для проектирования подсистем, средств обеспечения защиты информации;</li> </ul>
<p>ОПК-4.4 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем</p>	<p>ОПК-4.4.1. Контролирует уровень защищенности в автоматизированных системах</p>	<p><b><u>Знать:</u></b></p> <ul style="list-style-type: none"> <li>- виды аудита информационной безопасности;</li> <li>– принципы организации автоматизированных систем в соответствии с требованиями по защите информации</li> </ul> <p><b><u>Уметь:</u></b></p> <ul style="list-style-type: none"> <li>- выявлять уязвимости автоматизированных систем;</li> <li>- проводить мониторинг угроз безопасности автоматизированных систем;</li> </ul> <p><b><u>Владеть:</u></b></p> <ul style="list-style-type: none"> <li>- методами выявления угроз информационной безопасности автоматизированных систем;</li> <li>- методами диагностики систем защиты автоматизированных систем с использованием различных тестов на проникновение (ПенТестинг)</li> </ul>

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

код компетенции	Этапы формирования компетенций			
	Тема 1. Комплексное обеспечение информационной безопасности: сущность, компоненты и задачи. Тема 2. Состав защищаемой информации.	Тема 3. Автоматизированная информационная система как объект защиты. Тема 4. Управление инцидентами и рисками информационной безопасности.	Тема 5. Управление доступом в автоматизированных системах. Тема 6. Системы анализа защищенности.	Тема 7. Межсетевые экраны и виртуальные частные сети. Тема 8. Системы обнаружения и предотвращения вторжений.
ОПК-6	+	+		
ОПК-12		+	+	+
ОПК-4.4		+	+	+

код компетенции	Этапы формирования компетенций		
	Тема 9. Защита электронного документооборота. Тема 10. Особенности защиты информации в базах данных.	Тема 11. Концепция создания защищенных автоматизированных информационных систем. Тема 12. Разработка модели комплексной системы защиты информации.	Тема 13. Организация функционирования комплексных систем защиты информации.
ОПК-6.2		+	
ОПК-12.2		+	+
ОПК-4.4.1	+	+	+

### Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.О.30 «Комплексная защита объектов информатизации» относится к обязательной части 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 «Сети и системы передачи информации», «Аппаратные средства вычислительной техники», «Информатика», «Информационные технологии», «Теория информации», «Основы информационной безопасности», «Методы и средства криптографической защиты информации», «Методы и средства защиты информации от утечки по техническим каналам», «Организационное и правовое

обеспечение информационной безопасности», «Безопасность вычислительных сетей», «Проектирование защищенных автоматизированных систем».

Знания, умения и навыки, полученные студентами в рамках данной дисциплины, пригодятся им при написании выпускной квалификационной работы, а также при прохождении производственной и преддипломной практик.

### **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**

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 40 часов, в том числе:

на занятия лекционного типа – **20** ч.

на занятия семинарского типа – **20** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **104** 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.	Комплексное обеспечение информационной безопасности: сущность, компоненты и задачи	10	2	-	3	-	-	-	5	Тестирование Проведение опроса Подготовка презентации Решение кейс-задачи
2.	Состав защищаемой информации	10	2	-	3	-	-	-	5	Тестирование Проведение опроса Подготовка реферата Проведение деловой игры
3.	Автоматизированная информационная система как объект защиты	10	2	-	3	-	-	-	5	Тестирование Проведение опроса Выполнение письменной работы Выполнение проекта
4.	Управление инцидентами и рисками	10	2	-	3	-	-	-	5	Тестирование Проведение опроса Выполнение пись-



	информационной безопасности									менной работы Выполнение проекта
5.	Управление доступом в автоматизированных системах	10	2	-	3	-	-	-	5	Тестирование Проведение опроса Выполнение письменной работы Выполнение проекта
6.	Системы анализа защищенности	10	2	-	3	-	-	-	5	Тестирование Проведение опроса Подготовка реферата Проведение деловой игры
7.	Межсетевые экраны и виртуальные частные сети	10	2	-	3	-	-	-	5	Тестирование Проведение опроса Подготовка презентации Проведение деловой игры
8.	Системы обнаружения и предотвращения вторжений	10	2	-	3	-	-	-	5	Тестирование Проведение опроса Выполнение письменной работы Выполнение проекта
9.	Защита электронного документооборота	10	2	-	3	-	-	-	5	Тестирование Проведение опроса Подготовка презентации Решение кейс-задачи

10.	Особенности защиты информации в базах данных	10	2	-	3	-	-	-	5	Тестирование Проведение опроса Выполнение письменной работы Выполнение проекта Практическая работа
11.	Концепция создания защищенных автоматизированных информационных систем	14	2	-	6	-	-	-	6	Тестирование Проведение опроса Подготовка реферата Выполнение творческого задания (групповое/индивидуальное)
12.	Разработка модели комплексной системы защиты информации	16	4	-	6	-	-	-	6	Тестирование Проведение опроса Подготовка реферата Проведение деловой игры Поведение круглого стола
13.	Организация функционирования комплексных систем защиты информации	14	4	-	3	-	-	-	7	Тестирование Проведение опроса Подготовка презентации Проведение круглого стола
	<b>Итого</b>	<b>144</b>	<b>30</b>		<b>45</b>				<b>69</b>	
	<b>Экзамен</b>	<b>36</b>								Контроль

	(групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	
	<b>ВСЕГО</b>	<b>180</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. Форма промежуточной аттестации
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия		
	Комплексное обеспечение информационной безопасности: сущность, компоненты и задачи	10	1	-	1	-	-	-	8	Тестирование Проведение опроса Подготовка презентации Решение кейс-задачи
2.	Состав защищаемой	10	1	-	1	-	-	-	8	Тестирование Проведение опроса

	информации									Подготовка реферата Проведение деловой игры
3.	Автоматизированная информационная система как объект защиты	10	1	-	1	-	-	-	8	Тестирование Проведение опроса Выполнение письменной работы Выполнение проекта
4.	Управление инцидентами и рисками информационной безопасности	10	1	-	1	-	-	-	8	Тестирование Проведение опроса Выполнение письменной работы Выполнение проекта
5.	Управление доступом в автоматизированных системах	10	1	-	1	-	-	-	8	Тестирование Проведение опроса Выполнение письменной работы Выполнение проекта
6.	Системы анализа защищенности	10	1	-	1	-	-	-	8	Тестирование Проведение опроса Подготовка реферата Проведение деловой игры
7.	Межсетевые экраны и виртуальные частные сети	12	2	-	2	-	-	-	8	Тестирование Проведение опроса Подготовка презентации Проведение деловой игры

8.	Системы обнаружения и предотвращения вторжений	12	2	-	2	-	-	-	8	Тестирование Проведение опроса Выполнение письменной работы Выполнение проекта
9.	Защита электронного документооборота	12	2	-	2	-	-	-	8	Тестирование Проведение опроса Подготовка презентации Решение кейс-задачи
10.	Особенности защиты информации в базах данных	12	2	-	2	-	-	-	8	Тестирование Проведение опроса Выполнение письменной работы Выполнение проекта Практическая работа
11.	Концепция создания защищенных автоматизированных информационных систем	12	2	-	2	-	-	-	8	Тестирование Проведение опроса Подготовка реферата Выполнение творческого задания (групповое/индивидуальное)
12.	Разработка модели комплексной системы защиты ин-	12	2	-	2	-	-	-	8	Тестирование Проведение опроса Подготовка реферата Проведение дело-

	формации									вой игры Поведение круглого стола
13.	Организация функциони- рования комплекс- ных систем защиты ин- формации	12	2	-	2	-	-	-	8	Тестирование Проведение опроса Подготовка презент- тации Проведение круг- лого стола
	<b>Итого</b>	<b>144</b>	<b>20</b>		<b>20</b>				<b>104</b>	
	<b>Экзамен (групповая консульта- ция в тече- ние семест- ра, группо- вая кон- сультация перед про- межуточной аттестаци- ей, экзамен)</b>	<b>36</b>								Контроль
	<b>ВСЕГО</b>	<b>180</b>								

**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 по стандарту	Количество экземпляров в библиотеке ДГУНХ/адрес доступа
<b>І. Основная учебная литература</b>				
1.	Аверченков, В.И.	Служба защиты информации: организация и управление	Москва : ФЛИНТА, 2016. – 186 с.	<a href="https://biblioclub.ru/index.php?page=book&amp;id=93356">https://biblioclub.ru/index.php?page=book&amp;id=93356</a>
2.	Лапина М.А., Марков Д.М., Гиш Т.А., Песков М.В., Меденец В.В.	Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум	Ставрополь: СКФУ, 2016. - 242 с.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=458012">http://biblioclub.ru/index.php?page=book&amp;id=458012</a>
3.	Пелешенко В. С., Говорова С. В., Лапина М. А.	Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие	Ставрополь: СКФУ, 2017. - 86 с.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=467139">http://biblioclub.ru/index.php?page=book&amp;id=467139</a>
<b>Дополнительная учебная литература</b>				
<b>а) Дополнительная учебная литература</b>				
1.	А.В. Душкин, О.В. Ланкин, С.В. Потехецкий и др.	Методологические основы построения защищенных автоматизированных систем: учебное пособие	Воронеж: Воронежская государственная лесотехническая академия, 2013. –258с.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=255851">http://biblioclub.ru/index.php?page=book&amp;id=255851</a>
2.	Анисин А.А.	Менеджмент в сфере информационной безопасности	М.:Интернет-Университет Информационных Технологий,2009. -176с.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=232981">http://biblioclub.ru/index.php?page=book&amp;id=232981</a>
<b>Б) Официальные издания: сборники законодательных актов, нормативно-правовых документов и кодексов РФ</b>				
1.	Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями)»			
2.	ГОСТ 34.320-96.Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы. 2001 г. <a href="http://www.standartgost.ru">www.standartgost.ru</a>			

3.	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>
4.	ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. <a href="http://www.standartgost.ru">www.standartgost.ru</a>
5.	ГОСТ Р ИСО/МЭК 12119-2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование. 2005 г. <a href="http://www.standartgost.ru">www.standartgost.ru</a>
6.	ГОСТ Р ИСО/МЭК ТО 16326-2002. Программная инженерия. Руководство по применению ГОСТ Р ИСО/МЭК 12207 при управлении проектом. 2002 г. <a href="http://www.standartgost.ru">www.standartgost.ru</a>
7.	ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2008 г. <a href="http://www.standartgost.ru">www.standartgost.ru</a>
<b><i>В) Периодические издания</i></b>	
1.	Информатика и безопасность
2.	Информационная безопасность. Рецензируемый научный журнал «Проблемы информационной безопасности»
<b><i>Г) Справочно-библиографическая литература</i></b>	
1.	Краткий энциклопедический словарь по информационной безопасности <a href="https://biblioclub.ru/index.php?page=book_red&amp;id=58393&amp;sr=1">https://biblioclub.ru/index.php?page=book_red&amp;id=58393&amp;sr=1</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.

Так как в рамках занятия регулярно поднимаются вопросы соответствия используемых для организации защиты информации технологий соответствующим государственным стандартам, а также другим правовым актам современного российского законодательства, то студентам рекомендуется ознакомление с ресурсами правовых систем (онлайн-версии), а также сайты официальных регуляторов в области информационной безопасности:

- <http://www.consultant.ru/> Информационно-правовая система "Консультант-Плюс";
- <http://www.garant.ru/> Информационно-правовая система "Гарант";
- <http://rkn.gov.ru/> Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;
- <http://fsb.ru/> Федеральная служба безопасности;
- <http://fstec.ru/> Федеральная служба по техническому и экспортному контролю.



Для самостоятельного изучения материала и ознакомления с новинками в области информационной безопасности рекомендуется использовать следующие Интернет-ресурсы:

1. <http://www.ixbt.com>
2. <http://www.intuit.ru>
3. <http://www.itsec.ru>
4. <http://www.iso27000.ru>
5. <http://www.infosec.ru/>
6. <http://www.infosecurity.ru/>
7. <http://www.securrity.ru/>
8. <http://xakep.ru/>
9. <http://www.ferra.ru/>
10. <http://www.3dnews.ru/>

## **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:**

1. Windows 10
2. Microsoft Office Professional
3. Adobe Acrobat Reader DC
4. VLC Media player
5. 7-zip
6. ПАК Соболь
7. МДЗ-Эшелон
8. Dallas Lock 8.0-К
9. «ФИКС»
10. «Terrier-2.0»
11. «Ревизор-1 XP»
12. «Ревизор-2 XP»
13. Microsoft Visio Professional 2019
14. Программное обеспечение ViPNet
15. Kaspersky Endpoint Security

### **7.2. Перечень информационных справочных систем:**

- Справочно-правовая система «КонсультантПлюс».

### **7.3. Перечень профессиональных баз данных:**

- Государственный реестр сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 (<http://fstec.ru/tehnicheskayazashchitainformatsii/dokumenty-po-sertifikatsii/153-sistemasertifikatsii/591-gosudarstvennyj-reestr-sszi>).
- Государственный реестр сертифицированных средств защиты информации (<http://clsz.fsb.ru/certification.htm>);
- Научная электронная библиотека «Elibrary» (<https://elibrary.ru>);
- Реестр операторов, осуществляющих обработку персональных данных (<https://rkn.gov.ru/personal-data/register/>).

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

Для преподавания дисциплины «Комплексное обеспечение защиты информации объекта информатизации» используются следующие специальные помещения—**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.

Программно-аппаратные комплексы ViPNet

### ***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 – 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**

При освоении дисциплины «Комплексное обеспечение защиты информации объекта информатизации» используются следующие образовательные технологии:

- деловые игры для выработки навыков принятия командных решений;
- лабораторные работы для экспериментальной работы с аналоговыми моделями реальных объектов, а также закрепления теоретического материала при решении практических задач;
- практическое занятие на основе кейс-метода для анализа конкретных ситуаций и задач, поиска верного подхода к их решению;
- внеаудиторная работа в форме обязательных консультаций и индивидуальных занятий со студентами (помощь в понимании тех или иных моделей и концепций, подготовка рефератов, а также тезисов для студенческих конференций и т.д.).

**Лист актуализации рабочей программы дисциплины  
«Комплексное обеспечение защиты информации объекта информатизации»**

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 \_\_\_\_\_