ГАОУ ВО «Дагестанский государственный университет народного хозяйства»

Утверждена решением
Ученого совета ДГУНХ,
протокол № 13
от 06 июля 2020 г

Кафедра «Информационные технологии и информационная безопасность

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

Направление подготовки

10.03.01 Информационная безопасность,

профиль «Безопасность автоматизированных систем»

Уровень высшего образования - бакалавриат

Форма обучения – очная

Махачкала – 2020

УДК 004.056
ББК 32.973.202

Составитель – Меджидов ЗаурУруджалиевич, 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–ЗайналовДжабраилТажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза», эксперт-представитель работодателя.

Рабочая программа дисциплины «Проектирование защищенных автоматизированных систем» 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 1 декабря 2016 г., № 1515, 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 «Проектирование защищенных автоматизированных систем» размещена на официальном сайте www.dgunh.ru

Меджидов З.У. Рабочая программа дисциплины «Проектирование защищенных автоматизированных систем» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2020 г., -19 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 03 июля 2020 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» 30 июня 2020 г., протокол № 12

Содержание

Раздел 1. Перечень планируемых результатов обучения по дисциплине

Цель дисциплины – сформировать компетенции обучающегося в области использования информационных технологий, применяемых в автоматизированных системах, при организации защиты информации обрабатываемой в них.

Задачи дисциплины

- Рассмотреть технологии функционирования защищенной автоматизированной системы; методологии оценки защищенности автоматизированных систем
- Раскрыть принципы построения защищенных автоматизированных систем;
- Показать особенности методов и средств проектирования, создания и сопровождения защищенных автоматизированных систем.

1.1 Компетенции выпускников, формируемые в результате освоения дисциплины «Проектирование защищенных автоматизированных систем» как часть планируемых результатов освоения образовательной программы высшего образования

код компетенции	формулировка компетенции
ПК	**ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
ПК-15	способность организовать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ПСК	**ПРОФЕССИОНАЛЬНО-СПЕЦИАЛИЗИРОВАННЫЕ КОМПЕТЕНЦИИ**
ПСК-1	способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации

1.2. Планируемые результаты обучения по дисциплине

код и формулировка компетенции	компонентный состав компетенции		
	знать:	уметь:	владеть:
ПСК-1:способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	З1– аппаратные средства вычислительной техники; З2– операционные системы персональных ЭВМ; З3 – принципы построения информационных систем; З4– принципы и методы организационной защиты информации.	У1 –анализировать и оценивать угрозы информационной безопасности объекта.	В1 – методами и средствами выявления угроз безопасности автоматизированным системам; В2 – методами формирования требований по защите информации; методами анализа и формализации информационных процессов объекта и связей между ними.
ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	З1– аппаратные средства вычислительной техники; З2– операционные системы персональных ЭВМ; З3 – основы администрирования вычислительных сетей; З4– принципы организации информационных систем в соответствии с требованиями по защите информации; З5 – эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы.	У1 – формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; У2 – осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; У3 – применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.	В1 – методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; В2 – навыками выявления и уничтожения компьютерных вирусов; В3 – профессиональной терминологией; В4 – навыками безопасного использования технических средств в профессиональной деятельности.
ПК-5: способность принимать участие в организации и сопровождении аттестации	З1– основные нормативные правовые акты в области информационной безопасности и	У1 – пользоваться нормативными документами по защите информа-	В1 – методами организации и управления деятельностью служб защиты ин-

объекта информатизации по требованиям безопасности информации	защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; З2– принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; З3 – принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах.	ции; У2 –анализировать и оценивать степень риска проявления факторов опасности системы "человек - среда обитания", осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности.	формации на предприятии; В2 – методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.
ПК-13: способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	З1– технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; З2– принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; З3 – принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информацион-	У1 –анализировать и оценивать угрозы информационной безопасности объекта; У2 – осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; У3 – применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.	В1 – методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; В2 – методами и средствами выявления угроз безопасности автоматизированным системам; В3 – методами технической защиты информации; В4 – методами формирования требований по защите информации; В5 – методами расчета и инструментального контроля показателей технической защиты информации; В6 – методами анализа и формализации информационных

	ных системах; З4– принципы организации информационных систем в соответствии с требованиями по защите информации; З5 – эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы; З6– принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них.		процессов объекта и связей между ними.
ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	З1 – нормативные методические документы ФСБ России, ФСТЭК России в области защиты информации; З2 – принципы организации информационных систем в соответствии с требованиями по защите информации	У1 – определять критерии технологических процессов защиты информации ПАСЗИ для сопоставления с требованиями нормативных документов ФСБ, ФСТЭК; У2 – осуществлять меры противодействия нарушениям информационной безопасности.	В1 – навыками организации и обеспечения режима секретности; – навыками работы с нормативными и методическими документами ФСБ, ФСТЭК

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

код компетенции	Этапы формирования компетенций		
	Тема 1. Современные тенденции в программной инженерии. Тема 2. Нормативно-методическое обеспечение создания автоматизированных систем.	Тема 3. Организационные процессы создания автоматизированных систем. Тема 4. Модели жизненного цикла автоматизированных систем.	Тема 5. Общие принципы проектирования автоматизированных систем. Тема 6. Особенности проектирования комплексной системы информационной безопасности.
ПСК-1	+	+	+

ПК-4			
ПК-5		+	+
ПК-13			+
ПК-15			

код компетенции	Этапы формирования компетенций		
	Тема 7. Проектирование системы защиты от НСД. Тема 8. Реализация системы управления доступом.	Тема 9. Реализация моделей защиты информации. Тема 10. Методы оценки качества комплексных систем информационной безопасности.	Тема 11. Аттестация автоматизированной системы по требованиям безопасности. Тема 12. Особенности эксплуатации комплексной системы информационной безопасности.
ПСК-1			
ПК-4	+	+	
ПК-5	+		
ПК-13		+	+
ПК-15		+	+

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.ОД.6 «Проектирование защищенных автоматизированных систем» относится к вариативной части Блока 1 «Дисциплины (модули)» Учебного плана по направлению подготовки «Информационная безопасность», профилю «Безопасность автоматизированных систем».

Для успешного освоения дисциплины, обучающиеся должны иметь знания, умения и навыки, полученные в рамках ранее пройденных дисциплин: «Сети и системы передачи информации», «Аппаратные средства вычислительной техники», «Информатика», «Информационные технологии», «Теория информации», «Основы информационной безопасности», «Криптографические методы защиты информации», «Техническая защита информации», «Организационное и правовое обеспечение защиты информации», «Программно-аппаратные средства защиты информации», «Безопасность вычислительных сетей».

Освоение данной дисциплины необходимо обучающемуся для успешного изучения следующих дисциплин: «Комплексное обеспечение защиты информации объекта информатизации», «Защита от внутренних ИТ-угроз».

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

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

Объем дисциплины в зачетных единицах составляет **3** зачетные единицы.

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

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

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

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

Форма промежуточной аттестации: зачет.

*Реализуется в форме практической подготовки

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

№ 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.	Современные тенденции в программной инженерии	8	2	-	1	1	-	-	4	Тестовые задания; Проведение опроса; Решение кейс-задачи; Подготовка презентации Выполнение лабораторной работы
2.	Нормативно-методическое обеспечение создания автоматизированных систем	8	2	-	1	1	-	-	4	Тестовые задания; Проведение опроса Выполнение проекта Подготовка реферата Выполнение лабораторной работы
3.	Организационные процессы создания автоматизированных систем	8	2	-	1	1	-	-	4	Тестовые задания; Проведение опроса; Проведение деловой игры Выполнение письменной работы Выполнение лабораторной работы
4.	Модели жизненно-	8	2	-	1	1	-	-	4	Тестовые задания; Проведение опроса;

	го цикла автоматизированных систем									Перечень дискуссионных тем для проведения круглого стола; Подготовка презентации Выполнение лабораторной работы
5.	Общие принципы проектирования автоматизированных систем	8	2	-	1	1	-	-	4	Тестовые задания; Проведение опроса; Решение кейс-задачи; Выполнение письменной работы Выполнение лабораторной работы
6.	Особенности проектирования комплексной системы информационной безопасности*	12	4*	-	2*	2*	-	-	4	Тестовые задания; Проведение опроса; Решение кейс-задачи; Подготовка реферата Выполнение лабораторной работы
7.	Проектирование системы защиты от НСД	12	4	-	2	2	-	-	4	Тестовые задания; Проведение опроса Выполнение практической работы (проекта) Подготовка реферата Выполнение лабораторной работы
8.	Реализация системы управления досту-	12	4*	-	2*	2*	-	-	4	Тестовые задания; Проведение опроса; Решение кейс-задачи; Подготовка презентации

	пом*									Выполнение лабораторной работы
9.	Реализация моделей защиты информации*	10	4*	-	2*	2*	-	-	2	Тестовые задания; Проведение опроса Выполнение письменной работы Подготовка реферата Выполнение лабораторной работы
10.	Методы оценки качества комплексных систем информационной безопасности	6	2	-	-	2	-	-	2	Тестовые задания; Проведение опроса; Решение кейс-задачи; Подготовка презентации Выполнение лабораторной работы
11.	Аттестация автоматизированной системы по требованиям безопасности*	6	2*	-	1*	1*	-	-	2	Тестовые задания; Проведение опроса; Выполнение письменной работы Выполнение практической работы (проекта) Подготовка реферата Выполнение лабораторной работы
12.	Особенности эксплуатации комплексной системы ин-	8	4	-	1	1	-	-	2	Тестовые задания; Проведение опроса; Перечень дискуссионных тем для проведения круглого стола; Подготовка презентации

	формацион-ной без-опасности									Выполнение лаборатор-ной работы
	Зачет	2	-	-	2	-	-	-	-	Контроль
	ИТОГО:	**108**	**34**	**-**	**17**	**17**	**-**	**-**	**40**	

*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
Основная учебная литература				
1.	Голиков А. М.	Основы проектирования защищенных телекоммуникационных систем: учебное пособие	Томск: ТУСУР, 2016. – 396 с.	http://biblioclub.ru/index.php?page=book&id=480796
2.	Долозов Н. Л., Гультяева Т. А.	Программные средства защиты информации: конспект лекций	Новосибирск: НГТУ, 2015. - 63 с.	http://biblioclub.ru/index.php?page=book&id=438307
3.	Кияев В., Граничин О.	Безопасность информационных систем	М.:Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с.	http://biblioclub.ru/index.php?page=book&id=429032
4.	Ю.Ю. Громов, О.Г. Иванова, К.В. Стародубов, А.А. Кадыков	Программно-аппаратные средства защиты информационных систем: учебное пособие	Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2017. – 194 с.	http://biblioclub.ru/index.php?page=book&id=499013
II. Дополнительная учебная литература				
А) Дополнительная учебная литература				
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.	http://biblioclub.ru/index.php?page=book&id=255851
2.	Анисимов А.А.	Менеджмент в сфере информационной безопасности	М.:Интернет-университет-тин-форм.технологий, 2010. - 176с.	http://biblioclub.ru/index.php?page=book&id=232981
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.	http://biblioclub.ru/index.php?page=book&id=467139

4.	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с.	http://biblioclub.ru/index.php?page=book&id=438331
5.	Сергеева Ю.С.	Защита информации. Конспект лекций: учебное пособие.	М.: А-Приор, 2011. - 128 с.	http://biblioclub.ru/index.php?page=book&id=72670

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 34.320-96.Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы. 2001 г.www.standartgost.ru
3.	ГОСТ Р ИСО/МЭК ТО 12182-2002. Информационная технология. Классификация программных средств. 2002 г.www.standartgost.ru
4.	ГОСТ Р ИСО/МЭК 15288-2005. Информационная технология. Системная инженерия. Процессы жизненного цикла систем. 2006 г.www.standartgost.ru
5.	ГОСТ Р ИСО/МЭК 12119-2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование. 2005 г.www.standartgost.ru
6.	ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. 2009 г.www.standartgost.ru
7	ГОСТ 28195-89. Оценка качества программных средств. Общие положения. 2001 г.www.standartgost.ru
8	ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.www.standartgost.ru
В) Периодические издания	
1.	Рецензируемый научный журнал «Проблемы информационной безопасности»
2.	Научный журнал «Прикладная дискретная математика»
3.	Научный журнал «Информатика и ее применение»
4.	Журнал о компьютерах и цифровой технике «ComputerBild»
5.	Рецензируемый научный журнал «Информатика и система управления»
6.	Рецензируемый научный журнал «Проблемы информационной безопасности»
7.	Рецензируемый научный журнал «Прикладная информатика»
Г) Справочно-библиографическая литература	
1.	Краткий энциклопедический словарь по информационной безопасности https://biblioclub.ru/index.php?page=book_red&id=58393&sr=1
2	Энциклопедия информатики ИНФОПЕДИЯ - http://s-infopedia.com/

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 обучающимся рекомендуется ознакомление с ресурсами правовых систем (онлайн-версии), а также сайты официальных регуляторов в области информационной безопасности:

- http://www.consultant.ru/ Информационно-правовая система "КонсультантПлюс";
- http://rkn.gov.ru/ Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;
- http://fstec.ru/ Федеральная служба по техническому и экспортному контролю;
- http://Standartgost.ru - Открытая база ГОСТов

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

7.1. Необходимый комплект лицензионного программного обеспечения:

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-K
9. «ФИКС»
10. «Terrier-2.0»
11. «Ревизор-1 XP»
12. «Ревизор-2 XP»
13. AstraLinux
14. DLP-система "Контур информационной безопасности Searchinform"

15. РЕД ОС
16. Kaspersky Endpoint Security 11

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/ tekhnicheskayazashchitainformatsii/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 «Проектирование защищенных автоматизированных систем» используются следующие специальные помещения **и учебные аудитории**:

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации № 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).

Лаборатория защищенных автоматизированных систем, учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации № 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.

Персональные компьютеры – 20 ед.

Типовой комплект учебного оборудования «Криптографические системы».

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 «Проектирование защищенных автоматизированных систем» используются следующие образовательные технологии:

–деловые игры для выработки навыков принятия командных решений;;

–практические занятия 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

«Проектирование защищенных автоматизированных систем»

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «22» сентября 2020 № 2

Зав. кафедрой Татаев В.С.

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «22» мая 2021 № 10

Зав. кафедрой Татаев В.С.

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «____»_____20___ №___

Зав. кафедрой_____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «____»_____20___ №___

Зав. кафедрой_____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «____»_____20___ №___

Зав. кафедрой_____