ГАОУ ВО «Дагестанский государственный университет народного хозяйства»

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

Кафедра «Информационные технологии и информационная безопасность

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ»

Направление подготовки

10.04.01 Информационная безопасность,

профиль «Управление информационной безопасностью и технологии защиты информации»

Уровень высшего образования - магистратура

Форма обучения – очная

Махачкала – 2023

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

Рабочая программа дисциплины «Защищенные информационные системы» разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 26 ноября 2020 г., № 1455, в соответствии с приказом Министерства науки и высшего образования от 6.04.2021 г., № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам магистратуры, программам специалитета, программам магистратуры».

Рабочая программа дисциплины «Защищенные информационные системы» размещена на официальном сайте www.dgunh.ru

Меджидов З.У. Рабочая программа дисциплины «Защищенные информационные системы» для направления подготовки 10.04.01 Информационная безопасность, профиль «Управление информационной безопасностью и технологии защиты информации». – Махачкала: ДГУНХ, 2023 г., - 16 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 05 июня 2023 г.

Рекомендована к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

Одобрена на заседании кафедры «Информационные технологии и информационная безопасность» 31 мая 2023 г., протокол № 10.

Содержание

Раздел 1. Перечень планируемых результатов обучения по дисциплине

Цель дисциплины – сформировать компетенции обучающегося в области использования информационных технологий, применяемых в защищенных информационных системам, создания проектов на их создание.

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 «Защищенные информационные системы» как часть планируемых результатов освоения образовательной программы высшего образования

код компетенции	Формулировка компетенции
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание
ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности

1.2. Планируемые результаты обучения по дисциплине

Код и наименование компетенции	***Код и наименование индикатора достижения компетенции***	***Планируемые результаты обучения по дисциплине***
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ИОПК-1.2 Проектирует техническое задание на создание системы обеспечения информационной безопасности и защиты информации	**Знать:** – аппаратные средства вычислительной техники и операционные системы персональных ЭВМ; – принципы построения информационных систем; – принципы и методы организационной защиты информации **Уметь:** - проводить анализ уязвимостей внедряемой системы защиты информации **Владеть:** - навыками установки и настройки средств защиты информации в автоматизированных системах;

		- методами и средствами выявления угроз безопасности автоматизированным системам
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ИОПК-2.2 Проектирует систему обеспечения информационной безопасности, ее компоненты и подсистемы	**Знать:** - принципы построения информационных систем; - принципы и методы организационной защиты информации **Уметь:** - проводить диагностику системы защиты информации автоматизированных систем; - проводить аудит защищенности информации в автоматизированных системах **Владеть:** - навыками проведения мониторинга защищенности информации в автоматизированных системах

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.
ОПК-1	+	+	+
ОПК-2			

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.
ОПК-1			
ОПК-2	+	+	+

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.О.02 «Защищенные информационные системы» относится к обязательной части Блока 1 «Дисциплины (модули)» Учебного плана по направлению подготовки 10.04.01 Информационная безопасность, профилю «Управление информационной безопасностью и технологии защиты информации».

Для успешного освоения дисциплины, обучающиеся должны иметь знания, умения и навыки, полученные в рамках ранее пройденных дисциплин: «Технологии обеспечения информационной безопасности», «Нормативно-методическое обеспечение информационной безопасности».

Освоение данной дисциплины необходимо обучающемуся для успешного изучения следующих дисциплин: «Обеспечение информационной безопасности в государственных и муниципальных организациях», «Организация и технологии защиты персональных данных», «Управление информационной безопасностью».

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 **4** зачетные единицы.

Очная 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 – **68** ч.

Форма промежуточной аттестации: экзамен, 36 ч.

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. Форма промежуточной аттестации
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия		
1.	Современные тенденции в программной инженерии	6	1	-	1	-	-	-	4	Тестовые задания; Проведение опроса; Решение кейс-задачи; Подготовка презентации
2.	Нормативно-методическое обеспечение создания автоматизированных систем	6	1	-	1	-	-	-	4	Тестовые задания; Проведение опроса Выполнение проекта Подготовка реферата
3.	Организационные процессы создания автоматизированных систем	8	1	-	-	1	-	-	6	Тестовые задания; Проведение опроса; Проведение деловой игры Выполнение письменной работы Выполнение лабораторной работы

4.	Модели жизненного цикла автоматизированных систем	8	1	-	-	1	-	-	6	Тестовые задания; Проведение опроса; Подготовка презентации Выполнение лабораторной работы
5.	Общие принципы проектирования автоматизированных систем	10	2	-	1	1	-	-	6	Тестовые задания; Проведение опроса; Решение кейс-задачи; Выполнение письменной работы Выполнение лабораторной работы
6.	Особенности проектирования комплексной системы информационной безопасности	10	2	-	1	1	-	-	6	Тестовые задания; Проведение опроса; Решение кейс-задачи; Подготовка реферата Выполнение лабораторной работы
7.	Проектирование системы защиты от НСД	10	2	-	1	1	-	-	6	Тестовые задания; Проведение опроса Выполнение практической работы (проекта) Подготовка реферата Выполнение лабораторной работы
8.	Реализация системы	10	2	-	1	1	-	-	6	Тестовые задания; Проведение опроса;

	управления доступом									Решение кейс-задачи; Подготовка презентации Выполнение лабораторной работы
9.	Реализация моделей защиты информации	10	2	-	1	1	-	-	6	Тестовые задания; Проведение опроса Выполнение письменной работы Подготовка реферата Выполнение лабораторной работы
10.	Методы оценки качества комплексных систем информационной безопасности	10	2	-	1	1	-	-	6	Тестовые задания; Проведение опроса; Решение кейс-задачи; Подготовка презентации Выполнение лабораторной работы
11.	Аттестация автоматизированной системы по требованиям безопасности	10	2	-	1	1	-	-	6	Тестовые задания; Проведение опроса; Выполнение письменной работы Выполнение практической работы (проекта) Подготовка реферата Выполнение лабораторной работы
12.	Особенности эксплуатации комплекс-	10	2	-	1	1	-	-	6	Тестовые задания; Проведение опроса; Подготовка презентации Выполнение лаборатор-

	ной системы информационной безопасности									ной работы
	Итого	**0**	**0**	**-**	**10**	**0**	**-**	**-**	**0**	Контроль
	Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	**36**								
	ВСЕГО	**144**								

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-университетинформ.те	http://biblioclub.ru/

			хнологий, 2010. - 176с.	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/ tekhnicheskayazashchitainformat-sii/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 «Защищенные информационные системы» используются следующие специальные помещения **и учебные аудитории**:

Учебная аудитория для проведения учебных занятий 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 технологий обеспечения информационной безопасности и защищенных информационных систем, 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.

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 «Защищенные информационные системы» 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

«Защищенные информационные системы»

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 _____