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

«ПРОТИВОДЕЙСТВИЕ ТЕХНИЧЕСКИМ РАЗВЕДКАМ»

Направление подготовки

10.03.01 Информационная безопасность,

профиль «Безопасность автоматизированных систем»

Уровень высшего образования - бакалавриат

Формы обучения – очная, очно-заочная

Махачкала – 2023

УДК681.518(075.8)
ББК 32.81.73

Составитель – Гасанова Зарема Ахмедовна, кандидат педагогических наук, заместитель заведующего кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, зав. кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры прикладной математики Дагестанского государственного университета.

Рабочая программа дисциплины «Противодействие техническим разведкам» разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г., № 1427, в соответствии с приказом Министерства науки и высшего образования Российской Федерации от 6.04.2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»

Рабочая программа по дисциплине «Противодействие техническим разведкам» размещена на официальном сайте www.dgunh.ru

Гасанова З.А. Рабочая программа по дисциплине «Противодействие техническим разведкам» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2023 г., 20 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

Целью дисциплины «Противодействие техническим разведкам» является формирование у обучающихся компетенций в области организации технической защиты объекта информатизации с учетом используемых информационных технологий и особенностей средств защиты информации.

Задачи дисциплины:

- Рассмотреть основные возможные физические и технологические каналы утечки информации и методы ликвидации данных каналов.
- Раскрыть принципы построения комплексной системы противодействия техническим разведкам.

1.1. Компетенции выпускников, формируемые в результате освоения дисциплины «Противодействие техническим разведкам» как часть планируемых результатов освоения образовательной программы

код компетенции	формулировка компетенции
ПК-2.	Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации
ПК-3.	Способен учитывать и использовать особенности средств защиты информации при формировании системы защиты информации автоматизированных систем

1.2. Планируемые результаты обучения по дисциплине

Код и наименование компетенции	***Код и наименование индикатора достижения компетенции***	***Планируемые результаты обучения по дисциплине***
ПК-2. Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при	ИПК-2.1. Устанавливает и налаживает средства защиты информации в автоматизированных системах	**Знать:** – современные методы и средства технической разведки; – основные подходы к созданию средств технической защиты; **Уметь:** – выбирать и устанавливать технические средства защиты информации оценивать их эффективность средства защиты информации;

организации защиты обрабатываемой в них информации		– оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; **Владеть:** – методами технической защиты информации; – навыками внедрение и эксплуатации современных средств технической защиты информации методиками проверки защищенности объектов информатизации; –
ПК-3. Способен учитывать и использовать особенности средств защиты информации при формировании системы защиты информации автоматизированных систем	ИПК-3.2. Учитывает особенности средств защиты информации при проектировании системы защиты информации	**Знать:** – технические каналы утечки информации; **Уметь:** – определять источники угрозы информационной безопасности; – анализировать и оценивать угрозы информационной безопасности объекта; **Владеть:** – методами формирования документации; – методами расчета и инструментального контроля показателей технической защиты информации

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

Код компетенции	Этапы формирования компетенций					
	Тема 1. Цели, задачи и организация технической разведки	Тема 2. Демаскирующие признаки и источники информации для технических разведок	Тема 3. Защита от средств акустической разведки	Тема 4. Защита объектов от оптической и оптико-электронной разведки	Тема 5. Защита радиоэлектронных средств и информации от радио и радиотехнической разведки	Тема 6. Защита информации в линиях связи.
ПК-2			+	+	+	+
ПК-3	+	+				

Код компетенции	Этапы формирования компетенций					
	Тема 7. Защита информации в каналах сотовой связи	Тема 8. Защита технических средств передачи, обработки и хранения информации	Тема 9. Защита информации при использовании слаботочного оборудования	Тема 10. Защита информации в средствах	Тема 11. Методы и средства выявления закладных устройств	Тема 12. Технический контроль принятых мер защиты
ПК-2	+	+	+	+		
ПК-3					+	+

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.ДВ.04.01 «Противодействие техническим разведкам» относится к дисциплинам по выбору Блока 1 «Дисциплины (модули)» учебного плана по направлению подготовки 10.03.01 Информационная безопасность, профилю «Безопасность автоматизированных систем».

Для освоения курса «Противодействие техническим разведкам» обучающийся должен изучить дисциплины: «Теория информации», «Аппаратные средства вычислительной техники», «Электротехника», «Электроника и схемотехника», «Системы и сети передачи информации», «Безопасность вычислительных сетей», и «Защита информации от утечки по техническим каналам».

Освоение данной дисциплины необходимо обучающемуся для успешного прохождения производственной практики и выполнения выпускной квалификационной работы.

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

Объем дисциплины в зачетных единицах составляет 4 зачетные единицы.

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 – **33** 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 50 часов, в том числе:

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

на занятия семинарского типа – **30** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **58** ч.

Форма промежуточной аттестации: экзамен, 36 ч.

Отдельные учебные занятия по дисциплине реализуются в форме практической подготовки.

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

Очная форма обучения

№ п/п	Тема дисциплины	Всего академических часов	В т.ч. занятия лекционного типа	В т.ч. занятия семинарского типа:					Самостоятельная работа	Форма текущего контроля успеваемости. Форма промежуточной аттестации
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные анологичные занятия		
1.	Тема 1. Цели, задачи и организация технической разведки.	6	2		2	0			2	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа
2.	Тема 2. Демаскирующие признаки и источники информации для технических разведок	6	2		2	0			2	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа
3.	Тема 3. Защита от средств акустической разведки	12	4		4	2			2	Устный опрос Тестирование Подготовка реферата Подготовка презентации

										Практическая работа Лабораторная работа
4.	Тема 4. Защита объектов от оптической и оптикоэлектронной разведки	9	2		2	2			3	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа
5.	Тема 5. Защита радиоэлектронных средств и информации от радио и радиотехнической разведки	8	2		2	1			3	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа
6.	Тема 6. Защита информации в линиях связи	8	2		2	1			3	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа
7.	Тема 7. Защита информации в каналах сотовой связи	9	2		2	2			3	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа

										Лабораторная работа
8.	Тема 8. Защита технических средств передачи, обработки и хранения информации*	13	4*		4*	2*			3	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа
9.	Тема 9. Защита информации при использовании слаботочного оборудования	8	2		2	1			3	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа
10.	Тема 10. Защита информации в средствах ЭВМ*	13	4*		4*	2*			3	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа
11.	Тема 11. Методы и средства выявления закладных устройств*	9	2*		2*	2*			3	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа

12.	Тема 12. Технический контроль принятых мер защиты*	7	2*		2*	0			3	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа
	ИТОГО:	**108**	**30**		**30**	**15**			**33**	
	Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	**36**								**Контроль**
	ВСЕГО:	**144**								

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 анологичные занятия		
1.	Тема 1. Цели, задачи и организация технической разведки.	5	1		-	-			4	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа
2.	Тема 2. Демаскирующие признаки и источники информации для технических разведок	5	1		-	-			4	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа

3.	Тема 3. Защита от средств акустической разведки	8	1		2	1			4	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа
4.	Тема 4. Защита объектов от оптической и оптикоэлектронной разведки	8	1		2	1			4	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа
5.	Тема 5. Защита радиоэлектронных средств и информации от радио и радиотехнической разведки	9	2		2	1			4	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа
6.	Тема 6. Защита информации в линиях связи.	9	2		2	1			4	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа

7.	Тема 7. Защита информации в каналах сотовой связи	9	2		2	1			4	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа
8.	Тема 8. Защита технических средств передачи, обработки и хранения информации*	11	2*		2*	1*			6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа
9.	Тема 9. Защита информации при использовании слаботочного оборудования	11	2		2	1			6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа
10.	Тема 10. Защита информации в средствах ЭВМ*	11	2*		2*	1*			6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа

11.	Тема 11. Методы и средства выявления закладных устройств*	11	2*		2*	1*			6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа
12.	Тема 12. Технический контроль принятых мер защиты*	11	2*		2*	1*			6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Практическая работа Лабораторная работа
	ИТОГО:	**108**	**20**		**20**	**10**			**58**	
	Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	**36**								**Контроль**
	ВСЕГО:	**144**								

*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.	Защита информации от утечки по техническим каналам	Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 256 с.	http://biblioclub.ru/index.php?page=book&id=480636
2.	Н.А. Свинарев, О.В. Ланкин, А.П. Данилкин	Инструментальный контроль и защита информации	Воронеж : Воронежский государственный университет инженерных технологий, 2013. - 192 с. ISBN 978-5-00032-018-1	http://biblioclub.ru/index.php?page=book&id=255905
II Дополнительная учебная литература				
а) Дополнительная учебная литература				
1.	Иванов А.В.	Защита речевой информации от утечки по акустоэлектрическим каналам	Новосибирск : НГТУ, 2012. - 43 с. : ил.,табл., схем. - ISBN 978-5-7782-1888-8	http://biblioclub.ru/index.php?page=book&id=228846
2.	Креопалов, В.В.	Технические средства и методы защиты информации	Москва : Евразийский открытый институт, 2011. – 278 с.	http://biblioclub.ru/index.php?page=book&id=90753
3.	Скрипник Д.А.	Общие вопросы технической защиты информации	Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с.	http://biblioclub.ru/index.php?page=book&id=429070
4.	Титов А.А.	Технические средства защиты информации	Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. - 194 с.	http://biblioclub.ru/index.php?page=book&id=208661
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.	Р 50.1.056-2005. Техническая защита информации. Основные термины и определения www.standartgost.ru
В) Периодические издания	
1.	Информатика и безопасность
2.	Журнал о компьютерах и цифровой технике «ComputerBild»
3.	Рецензируемый научный журнал «Проблемы информационной безопасности»
Г) Справочно-библиографическая литература	
4.	1. Краткий энциклопедический словарь по информационной безопасности : словарь / сост. В.Г. Дождиков, М.И. Салтан. – Москва : Энергия, 2010. – 240 с. http://biblioclub.ru/index.php?page=book&id=58393

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 технической защиты информации, рекомендуется использовать следующие Интернет-ресурсы:

1. http://fstec.ru/ – официальный сайт ФСТЭК
2. http://www.consultant.ru/ – онлайн-версия информационно-правовой системы "КонсультантПлюс"
3. http://Standartgost.ru - Открытая база ГОСТов

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

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

- Windows 10
- Microsoft Office Professional
- Adobe Acrobat Reader DC
- VLC Media player
- 7-zip
- Программное обеспечением для ST031M
- Специальное программное обеспечение «Сигурд»
- «Сигурд-Тест» (тестовая программа для проведения специальных исследований)
- Microsoft Visio Professional 2019

7.2. Перечень информационных справочных систем:

- информационно справочная система «КонсультантПлюс».

7.3. Перечень профессиональных баз данных:

- Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 (http://fstec.ru/ tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sszi).
  http://Standartgost.ru - Открытая база ГОСТов

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

Для преподавания дисциплины «Организация защиты сведений, составляющих государственную тайну» используются следующие специальные помещения:

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), 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 технической защиты информации, 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.

Основное оборудование: SEL SP-21 «Баррикада» генератор пространственного зашумления, устройство акустических помех "Соната АВ", акустический приемник AOR 8200 Mk3, многофункциональный поисковый прибор ST 031M «ПИРАНЬЯ», Нелинейный локатор «Люкс», индикатор поля Bug Hunter Professional BH-02, детектор скрытых камер Spider LD-B1, автоматизированная система оценки защищенности технических средств от утечки информации по каналу ПЭМИН «Сигурд-М19».

Перечень учебно-наглядных пособий:

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

Помещение для самостоятельной работы № 4.5 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)

Перечень основного оборудования:

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 24 ед.

Помещение для самостоятельной работы № 1-1 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 1)

Перечень основного оборудования:

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 60 ед.

Раздел 9. Образовательные технологии

Образовательные технологии, используемые при проведении учебных занятий по дисциплине «Противодействием техническим разведкам», обеспечивают формирование необходимых знаний и развитие у обучающихся навыков.

На занятиях лекционного типа применяются такие методы обучения как Управляемая дискуссия, Проблемная лекции, техники сторителлинга.

На практических занятиях, целью которых является приобретение учащимися определенных практических умений, научить их аналитически мыслить, уметь принимать верные решения в различных ситуациях эффективными будут такие методы как кейс-метод, лабораторный практикум, решение практических задач.

Лист актуализации рабочей программы дисциплины
«Противодействием техническим разведкам»

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 _____