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

«ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ»

Направление подготовки

10.03.01 Информационная безопасность,

профиль «Безопасность автоматизированных систем»

Уровень высшего образования - бакалавриат

Формы обучения – очная, очно-заочная

Махачкала – 2021

УДК 681.518(075.8)
ББК 32.81.73

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

Внутренний рецензент – Галяев Владимир Сергеевич, к.ф.-м.н., доцент, зав. кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры "Математические методы в экономике" Дагестанского государственного университета.

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

Рабочая программа дисциплины «Защита информации от утечки по техническим каналам» 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 «Защита информации от утечки по техническим каналам» размещена на официальном сайте www.dgunh.ru

Эмирбеков Э.М. Рабочая программа дисциплины «Защита информации от утечки по техническим каналам» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2021 г., 16 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

Целью дисциплины является формирование у обучающихся знаний по основам инженерно-технической защиты информации, а также навыков и умения в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.

Задачи дисциплины:

- ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
- ознакомление с техническими каналами утечки акустической (речевой) информации;
- изучение способов и средств защиты информации, обрабатываемой техническими средствами;
- изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
- изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам.

1.1. Компетенции выпускников, формируемые в результате освоения дисциплины «Защита информации от утечки по техническим каналам» как часть планируемых результатов освоения образовательной программы

код компетенции	формулировка компетенции
ОПК	**ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности
ОПК-4.3.	Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств 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***
ОПК-5. Способен применять нормативные правовые акты, нормативные	ОПК-5.2. Участвует в аттестационных испытаниях и аттестации объектов, помещений,	**Знать:** - основные нормативные и методические документы в области технической защиты информации. **Уметь:**

и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации	- определять ресурсы и объекты подлежащие защиты, а также требования к системе защиты. **Владеть**: - методами аттестации уровня защищенности объектов, помещений, технических средств и систем
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.2. Применяет методы и средства технической защиты информации для решения задач профессиональной деятельности	**Знать:** - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам. **Уметь:** - осуществлять меры противодействия утечки информации по техническим каналам. **Владеть:** - навыками моделирования технических каналов утечки информации
ОПК-4.3. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.2. Выполняет установку, настройку и обслуживание технических средств защиты информации автоматизированных систем	**Знать:** - методы и средства контроля эффективности технической защиты информации. **Уметь:** - обслуживать технические средства защиты информации. **Владеть:** - навыками установки и настройки средств технической защиты информации.

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

Код компетенции	Этапы формирования компетенций							
	Тема 1 Основные концептуальные положения инженерно-	Тема 2 Виды информации, защищаемой техническими	Тема 3 Демаскирующие признаки	Тема 4 Источники и носители информации, защищаемой техническими средствами,	Тема 5 Виды угроз безопасности информации, защищаемой	Тема 6 Принципы добывания и обработки информации техническими	Тема 7 Классификация и структура технических каналов утечки	Тема 8 Средства предотвращения утечки информации по

	техниче-ской за-щиты инфор-мации	сред-ствами	объек-тов за-щиты	принципы записи и съема ин-формации с носите-лей	техниче-скими сред-ствами	сред-ствами	инфор-мации	техниче-ским ка-налам
ОПК -5	+	+	+	+	+	+	+	+
ОПК-9	+	+	+	+	+	+	+	+
ОПК-4.3	+	+	+	+	+	+	+	+

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.О.26 «Защита информации от утечки по техническим каналам» относится к обязательной части Блока 1 «Дисциплины (модули)» Учебного плана по направлению подготовки «Информационная безопасность», профилю «Безопасность автоматизированных систем».

Для изучения данной дисциплины необходимы знания, умения и навыки по дисциплинам «Основы информационной безопасности», «Электротехника», «Электроника и схемотехника», «Аппаратные средства вычислительной техники», «Организационное и правовое обеспечение информационной безопасности».

Освоение данной дисциплины необходимо обучающемуся для изучения дисциплин «Проектирование защищенных автоматизированных систем», «Комплексное обеспечение защиты информации объекта информатизации», «Противодействие техническим разведкам», «Мониторинг и аудит защищенности информации в автоматизированных системах» 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 и форму(ы) 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 **64** часа, в том числе:

на занятия лекционного типа – **32** ч.

на занятия семинарского типа – 32 ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **44** ч.

Форма промежуточной аттестации: экзамен – 36ч.

Очно-заочная форма обучения

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет **34** часа, в том числе:

на занятия лекционного типа – **17** ч.

на занятия семинарского типа – 17 ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **74** ч.

Форма промежуточной аттестации: экзамен – 36ч

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.
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия		
1.	Основные концептуальные положения инженерно-технической защиты информации	12	4	-	2	2	-	-	4	Проведение опроса Выполнение лабораторной работы
2.	Виды информации, защищаемой техническими средствами	12	4	-	2	2	-	-	4	Проведение опроса Выполнение лабораторной работы
3.	Демаскирующие признаки объектов защиты	14	4	-	2	2	-	-	6	Проведение опроса Тестирование
4.	Источники и носители информации, защищаемой техническими средствами, принципы записи и съема информации с носителей	12	4	-	2	2	-	-	4	Проведение опроса Тестирование Выполнение лабораторной работы

5.	Виды угроз безопасности информации, защищаемой техническими средствами	12	4	-	2	2	-	-	4	Проведение опроса Решение кейса
6.	Принципы добывания и обработки информации техническими средствами	14	4	-	2	2	-	-	6	Проведение опроса Выполнение практического задания/ лабораторной работы
7.	Классификация и структура технических каналов утечки информации	14	4	-	2	2	-	-	6	Проведение опроса Решение кейса Выполнение лабораторной работы
8.	Средства предотвращения утечки информации по техническим каналам	18	4	-	2	2	-	-	10	Проведение опроса Тестирование Выполнение лабораторной работы
9.	**Итого**	**108**	**32**	**-**	**16**	**16**	**-**	**-**	**44**	
10.	Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	**36**								**контроль**
11.	**ВСЕГО:**	**144**								

Очно-заочная форма обучения

	Тема дисциплины			В т.ч. занятия семинарского типа:		

№ п/п		Всего академических часов	В т.ч. занятия лекционного типа	семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия	Самостоятельная работа	Форма текущего контроля успеваемости.
1	Основные концептуальные положения инженерно-технической защиты информации	12	2	-	1	1	-	-	4	Проведение опроса Выполнение лабораторной работы
2.	Виды информации, защищаемой техническими средствами	12	2	-	1	1	-	-	4	Проведение опроса Выполнение лабораторной работы
3.	Демаскирующие признаки объектов защиты	14	2	-	1	1	-	-	6	Проведение опроса Тестирование
4.	Источники и носители информации, защищаемой техническими средствами, принципы записи и съема информации с носителей	12	2	-	1	1	-	-	4	Проведение опроса Тестирование Выполнение лабораторной работы
5.	Виды угроз безопасности информации, защищаемой техническими средствами	12	2	-	1	1	-	-	4	Проведение опроса Решение кейса

6.	Принципы добывания и обработки информации техническими средствами	14	2	-	1	1	-	-	6	Проведение опроса Выполнение практического задания/ лабораторной работы
7.	Классификация и структура технических каналов утечки информации	14	2	-	1	1	-	-	6	Проведение опроса Решение кейса Выполнение лабораторной работы
8.	Средства предотвращения утечки информации по техническим каналам	18	3	-	1	2	-	-	10	Проведение опроса Тестирование Выполнение лабораторной работы
9.	**Итого**	**108**	**17**	**-**	**8**	**9**	**-**	**-**	**44**	
10.	Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	**36**								**контроль**
11.	**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.	Защита информации от утечки по техническим каналам : учебное пособие	Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 256 с	https://biblioclub.ru/index.php?page=book&id=480636
2.	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
II Дополнительная учебная литература				
а) Дополнительная учебная литература				
1.	Креопалов, В.В.	Технические средства и методы защиты информации : учебно-практическое пособие /	Москва : Евразийский открытый институт, 2011. – 278 с.	https://biblioclub.ru/index.php?page=book&id=90753
2.	Титов, А.А.	Инженерно-техническая защита информации : учебное пособие	Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. – 195 с.	https://biblioclub.ru/index.php?page=book_red&id=208567&sr=1
Б) Официальные издания: сборники законодательных актов, нормативно-правовых документов и кодексов РФ				
1.	Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями).			
2.	ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2008 г. www.standartgost.ru			
3.	ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. www.standartgost.ru			
4.	ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств. 2002 г. www.standartgost.ru			

5.	ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» www.standartgost.ru
6.	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 «Computer Bild»
3.	Рецензируемый научный журнал «Проблемы информационной безопасности»
Г) Справочно-библиографическая литература	
4.	Краткий энциклопедический словарь по информационной безопасности https://biblioclub.ru/index.php?page=book_red&id=58393&sr=1

Раздел 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к одной или нескольким электронно-библиотечным системам и к электронной информационно-образовательной среде университета (http://e-dgunh.ru). Электронно-библиотечная система и электронная информационно-образовательная среда обеспечивает возможность доступа, обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

Для самостоятельного изучения материала и ознакомления с регламентирующими документами и текущей практикой в области менеджмента информационной безопасности, рекомендуется использовать следующие Интернет-ресурсы:

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

Раздел 7. Перечень лицензионного программного обеспечения, информационных справочных систем 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. Программное обеспечением для ST031M
7. Специальное программное обеспечение «Сигурд»

8. «Сигурд-Тест» (тестовая программа для проведения специальных исследований)

9. Microsoft Visio Professional 2019

7.2.Перечень информационных справочных систем:

– Справочно-правовая система «КонсультантПлюс».

7.3. Перечень профессиональных баз данных:

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

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

Для преподавания дисциплины «Защита информации от утечки по техническим каналам» 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.

Компьютерный стол.

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.biblio-online.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 – 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 «Техническая защита информации» используются следующие образовательные технологии:

- Информационная лекция
- Лекция-визуализация
- Практическое занятие в форме практикума
- Практическое занятие на основе кейс-метода
- Информационный проект
- Использование медиаресурсов, энциклопедий, электронных библиотек и Интернет;
- Консультирование студентов с использованием электронной почты.

Лист актуализации рабочей программы дисциплины

«Защита информации от утечки по техническим каналам»

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 _____