МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

УТВЕРЖДАЮ

Проректор по учебной работе

_____ Василенко В.Н.
(подпись) (Ф.И.О.)

«25» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации от утечки по техническим каналам

(наименование дисциплины (модуля))

Специальность

10.05.03 – Информационная безопасность автоматизированных систем
(код и наименование направления подготовки)

Специализация

Безопасность открытых информационных систем
(наименование направленности (профиля) подготовки)

Квалификация выпускника

Специалист по защите информации

(Бакалавр/Специалист/Магистр/Исследователь. Преподаватель-исследователь)

1. Цели и задачи дисциплины

Целями и задачами освоения дисциплины «Защита информации от утечки по техническим каналам» в соответствии с видами профессиональной деятельности контроль-аналитическая являются:

- Тестирование систем защиты информации автоматизированных систем.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины в соответствии с предусмотренными компетенциями обучающийся должен:

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ОПК-9	Способен решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ИД2$_{опк-9}$ – осуществляет эксплуатацию современных отечественных и зарубежных средств технической защиты, согласно текущему состоянию систем передачи информации

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД2$_{опк-9}$ – осуществляет эксплуатацию современных отечественных и зарубежных средств технической защиты, согласно текущему состоянию систем передачи информации	Знает: современные отечественные и зарубежные средства технической защиты по техническим каналам.
	Умеет: использовать современные отечественные и зарубежные средства технической защиты по техническим каналам
	Владеет: обеспечения защиты информации от утечки по техническим каналам с учетом современные отечественные и зарубежные средства технической защиты

3. Место дисциплины в структуре ОП ВО

Дисциплина «Защита информации от утечки по техническим каналам» относится к базовой части ОП ВО.

Приступая к изучению дисциплины, студент предварительно осваивает следующие дисциплины программы подготовки специалистов по специальности «Информационная безопасность автоматизированных систем»: «Методы и средства криптографической защиты информации», «Программно-аппаратные средства защиты информации». Дисциплина является предшествующей для следующих дисциплин: Знания, полученные в ходе изучения дисциплины, используются при подготовке к ГИА, производственной практики.

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет_____5_____ зачетных единиц.

Виды учебной работы	Всего академических часов	Распределение трудоемкости по семестрам, ак. ч
Общая трудоемкость дисциплины (модуля)	**180**	**180**
Контактная работа в т. ч. аудиторные занятия:	**93,7**	**93,7**
Лекции	30	30
в том числе в форме практической подготовки	-	-

Практические занятия	30	30
в том числе в форме практической подготовки	-	-
Лабораторные работы	30	30
в том числе в форме практической подготовки	-	-
Консультации текущие	3,7	3,7
Вид аттестации (экзамен)	**33,8**	**33,8**
Самостоятельная работа:	**52,5**	**52,5**
Проработка материалов по лекциям, учебникам, учебным пособиям к собеседованию, коллоквиуму	18	18
Домашнее задание	24	24
Подготовка доклада	10,5	10,5

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1 Содержание разделов дисциплины

№ п/п	Наименование разделов дисциплины	Содержание раздела
1	Характеристика государственной системы противодействия технической разведке	Введение. Характеристика государственной системы противодействия технической разведке. Нормативные документы по противодействию технической разведке. Демаскирующие признаки объектов наблюдения и сигналов. Средства и методы технической разведки. Способы и средства перехвата сигналов. Способы и средства наблюдения
2	Технические каналы утечки информации	Технические каналы утечки информации. Оптические и радиоэлектронные каналы утечки информации. Акустические и виброакустические каналы утечки информации. Средства обнаружения технических каналов утечки информации. Мероприятия по выявлению средств технической разведки.
3	Методы и средства защиты информации от утечки по техническим каналам.	Методы и средства защиты информации от утечки по техническим каналам. Скрытие речевой информации в каналах связи. Обнаружение и локализация закладных устройств. Концепция и методы инженерно-технической защиты информации. Виды контроля и расчёта эффективности защиты информации

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ЛР, час	ПЗ, час	СР, час
1	Характеристика государственной системы противодействия технической разведке	10	10	10	17,5
2	Технические каналы утечки информации	10	10	10	17,5
3	Методы и средства защиты информации от утечки по техническим каналам.	10	10	10	17,5

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, Час
1	Характеристика государственной системы противодействия технической разведке	Введение. Характеристика государственной системы противодействия технической разведке. Нормативные документы по противодействию технической разведке. Демаскирующие признаки объектов наблюдения и сигналов. Средства и методы технической разведки. Способы и средства перехвата сигналов. Способы и средства наблюдения	10
2	Технические каналы утечки информации	Технические каналы утечки информации. Оптические и радиоэлектронные каналы утечки информации. Акустические и виброакустические каналы утечки информации. Средства обнаружения технических каналов утечки информации. Мероприятия по выявлению средств технической разведки.	10
3	Методы и средства защиты информации от утечки по техническим каналам.	Методы и средства защиты информации от утечки по техническим каналам. Скрытие речевой информации в каналах связи. Обнаружение и локализация закладных устройств. Концепция и методы инженерно-технической защиты информации. Виды контроля и расчёта эффективности защиты информации	10

5.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, час
1	Характеристика государственной системы противодействия технической разведке	Практическая работа № 1. Многофункциональные поисковые приборы, ST-031 «Пиранья». Практическая работа №2. Универсальный анализатор проводных линий «УЛАН-2» Практическая работа № 3 Измерение ПЭМИ монитора и оценка величины зоны R2.	10
2	Технические каналы утечки информации	Практическая работа № 4. Акустоэлектрические преобразователи Практическая работа № 5. Многофункциональные поисковые приборы, ST-032 Практическая работа № 6. Обнаружение и локализация акустических закладных устройств, программный коррелятор «OSCOR».	10

3	Методы и средства защиты информации от утечки по техническим каналам.	Практическая работа № 7 . Детектор электромагнитного поля ST 07. Практическая работа № 7. Многофункциональные поисковые приборы, программный коррелятор «OSCOR» Практическая работа № 8. Принципы дозиметрической разведки. Дозиметрия ионизирующих излучений. Практическая работа № 9 Изучение устройства и работы лазерного микрофона	10

5.2.3 Лабораторный практикум

№ п/п	Наименование раздела дисциплины	Тематика лабораторных занятий	Трудоемкость, час
1	Технические каналы утечки информации	Лабораторная работа №1. Обнаружение и локализация источников радиоизлучений. Лабораторная работа №2. Цифровые диктофоны	14
2	Методы и средства защиты информации от утечки по техническим каналам.	Лабораторная работа №3. Генераторы радиошума и блокираторы источников радиосигналов Лабораторная работа №4. Обнаружение и локализация закладных устройств с помощью нелинейного локатора	16

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Подсистема регистрации и учета Защита программ и данных от несанкционированного копирования	Подготовка доклада с визуальным представлением средствами PowerPoint	10
		Подготовка к коллоквиуму, тестированию	7,5
2	Защита от вредоносных воздействий компьютерных вирусов и программных закладок Аутентификация	Домашнее задание	10
		Подготовка к коллоквиуму, тестированию	7,5
3	Общие сведения о программных и программно-аппаратных методах и средствах обеспечения информационной безопасности Разграничение доступа	Домашнее задание. Подготовка к тестированию	17,5

6. Учебно-методическое и информационное обеспечение дисциплины

Для освоения дисциплины обучающийся может использовать:

6.1. Основная литература

1. Креопалов, В.В. Технические средства и методы защиты информации : учебно-практическое пособие / В.В. Креопалов. - М. : Евразийский открытый институт, 2011. - 278 с.

2. Проскурин В.Г. Защита программ и данных / В. Г. Проскурин. – М. : Академия, 2019 . – 208 с.

3. Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации: Книжный дом "Либроком", 2018.- 376 с.

6.2. Дополнительная литература

1. О. Зайцев. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors. Обнаружение и защита. СПб: «БХВ-Петербург». 2006. 304 с.

2. К. Касперский. Фундаментальные основы хакерства. М: «СОЛОН-Р». 2005. 448 с.

Дж. Козиол, Д. Личфилд, Д. Эйтел, К Энли, С. Эрен, Н. Мехта, Р. Хассель. Искусство взлома и защиты систем. СПб: «Питер». 2006. 416 с.

3. С. Норткатт, Новак Дж., Макхален Д., Обнаружение вторжений в сеть. – М.: Лори, 2001 г. – 384 с.: ил.

4. Мельников, В. П.. Информационная безопасность и защита информации: учеб. пособие для студ. вузов, обуч. по спец. 230201 "Информ. системы и технологии"/ В. П. Мельников, С. А. Клейменов, А. М. Петраков. - 3-е изд., стер.. - Москва: Академия, 2008. - 336 с.; 21 см. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328. - ISBN 978-5-7695-4884-0

5. Методы и средства инженерно-технической защиты информации : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. - 2-е изд., стер. - М. : Флинта, 2011. - 187 с. - (Организация и технология защиты информации)

6. Защита информации от утечки по техническим каналам: методические указания для самостоятельной работы студентов, обучающихся по специальности 10.05.03– «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрыпников**,** Е. В. Чернышова ; ВГУИТ, Кафедра информационной безопасности. - Воронеж : ВГУИТ, 2021. - 10 с.

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

1. Данылив, М. М. Методические указания для обучающихся по освоению дисциплин (модулей) в ФГБОУ ВО ВГУИТ [Электронный ресурс]: методические указания для обучающихся на всех уровнях высшего образования / М. М. Данылив, Р. Н. Плотникова; ВГУИТ, Учебно-методическое управление. - Воронеж: ВГУИТ, 2016. – 32 с. Режим доступа в электронной среде:
http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/100813.

6.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» - федеральный портал	http://www.edu.ru/index.php
Научная электронная библиотека	http://www.elibrary.ru/defaulttx.asp?
Федеральная университетская компьютерная сеть России	http://www.runnet.ru/
Информационная система «Единое окно доступа к образовательным ресурсам»	http://www.window.edu.ru/
Электронная библиотека ВГУИТ	http://biblos.vsuet.ru/megapro/web
Сайт Министерства науки и высшего образования РФ	http://minobrnauki.gow.ru
Портал открытого on-line образования	http://npoed.ru
Информационно-коммуникационные технологии в образовании. Система федеральных образовательных порталов	http://www.ict.edu.ru/
Электронная образовательная среда ФГБОУ ВО «ВГУИТ	http://education.vsuet.ru

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При изучении дисциплины используется программное обеспечение и информационные справочные системы: информационная среда для дистанционного обучения «Moodle», локальная сеть университета и глобальная сеть Internet.

При освоении дисциплины используется лицензионное и открытое программное обеспечение – ОС Windows; Microsoft Office.

7 Материально-техническое обеспечение дисциплины

Аудитории для проведения занятий лекционного типа, лабораторных и практических занятий	Ауд.332, 424, 420 Компьютеры - 12 шт., стенды – 5 шт. Компьютер РЕГАРД – 11 шт., стенды – 3 шт. Компьютеры Core i5-4460 – 10 шт., Core i5-4570 – 1 шт., проектор Acer projector X1383WH, экран, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ», средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-РЗ.1», система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ), профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной), портативный обнаружитель закладок Protect1203 (переносной), устройство активной защиты информации «ВЕТО-М», электронный замок Samsung SHS-2920, системный блок Supermicro Amibios 786 Q 2000, коммутатор TP-Link SG1024DE, маршрутизатор MikroTik RB2011iLS-IN,	ОС Astra Linux Альт Образование 8.2 [Лицензия № ААА.0217.00 с 21.12.2017 г. Лицензионный договор № РБТ-14/1623-01-ВУЗ от 18.12.2017 г.] бессрочно, Libre Office 6.1 [Лицензия № ААА.0217.00 с 21.12.2017 г. Включен в установочный пакет операционной системы Альт Образования 8.2] бессрочно , wxMaxima [Лицензия № ААА.0217.00 с 21.12.2017 г. Включен в установочный пакет операционной системы Альт Образование 8.2] бессрочно, Lazarus [(бесплатное ПО) https://ru.wikipedia.org/wiki/Lazarus] бессрочно, SMathStudio [(бесплатное ПО) https://ru.wikipedia.org/wiki/SMath_Studio] бессрочно, Avidemux [(бесплатное ПО) https://ru.wikipedia.org/wiki/Avidemux] бессрочно, Oracle VM Virtual Box [https://ru.wikipedia.org/wiki/VirtualBox] бессрочно, AnyLogic 8.3 [(бесплатное ПО) https://www.anylogic.ru/downloads/personal-learning-edition-download/] бессрочно. ОС Astra Linux Альт Образование 8.2 [Лицензия № ААА.0217.00 с 21.12.2017 г. Лицензионный договор № РБТ-14/1623-01-ВУЗ от 18.12.2017 г.] бессрочно, Libre Office 6.1 [Лицензия № ААА.0217.00 с 21.12.2017 г. Включен в установочный пакет операционной системы Альт Образование 8.2] бессрочно, wxMaxima [Лицензия № ААА.0217.00 с 21.12.2017 г.] бессрочно, Lazarus [(бесплатное ПО) https://ru.wikipedia.org/wiki/Lazarus] бессрочно, Oracle VM Virtual Box [(бесплатное ПО) https://ru.wikipedia.org/wiki/VirtualBox] бессрочно, FreePascal [(бесплатное ПО)https://ru.wikipedia.org/wiki/Free_Pascal] бессрочно. Microsoft Windows 7 [Microsoft Open License Microsoft Windows Professional 7 Russian Upgrade Academic OPEN 1 License No Level#47881748 от 24.12.2010г. http://eopen.microsoft.com] бессрочно, Microsoft Office 2007 Standart [Microsoft Open License Microsoft Office 2007 Russian Academic OPEN No Level #44822753 от 17.11.2008 http://eopen.microsoft.com] бессрочно, Adobe Reader XI [(бесплатное ПО) https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader/volume-distribution.html] бессрочно, Microsoft Visual Studio 2010 [Сублицензионный договор № 17623/VRN3От 07 июля 2010 г. на право использование программы для ЭВМ MSDN AA Developer Electronic Fulfillment, FreePascal[(бесплатноеПО)

		https://ru.wikipedia.org/wiki/Free_Pascal] бессрочно, ФИКС 2.0.2 [Договор № ТРУБ 27/01/17 с ООО «ВСГРУПП» от 15.02.2017 г. Лицензия на право использования + установочный пакет], СТРАЖ NT 3.0 [Договор № ТРУБ 27/01/17 с ООО «ВСГРУПП» от 15.02.2017 г.], Панцирь [Договор № ТРУБ 27/01/17 с ООО «ВСГРУПП» от 15.02.2017 г.], Ревизор 1 XP [Договор № ТРУБ 27/01/17 с ООО «ВСГРУПП» от 15.02.2017 г. Лицензия на право использования + установочный пакет], Ревизор 3.0 [Договор № ТРУБ 27/01/17 с ООО «ВСГРУПП» от 15.02.2017 г. Лицензия на право использования + установочный пакет], СТРАЖ NT 4.0 [ДОГОВОР № 200016222100015 с ООО «Паскаль»], Secret Net[ДОГОВОР № 200016222100015 с ООО «Паскаль»], GIMP [(бесплатное ПО) https://ru.wikipedia.org/wiki/GIMP] бессрочно, Avidemux [(бесплатное ПО) https://ru.wikipedia.org/wiki/Avidemux] бессрочно, Virtual Dub [(бесплатное ПО) https://ru.wikipedia.org/wiki/VirtualDub] бессрочно, Oracle VM Virtual Box [(бесплатное ПО) https://ru.wikipedia.org/wiki/VirtualBox] бессрочно, Netbeans [(бесплатное ПО) https://netbeans.org/] бессрочно, СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК No2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК No2945 16.08.2013
Аудитории для самостоятельной работы, курсового и дипломного проектирования	Читальные залы библиотеки: Компьютеры со свободным доступом в сеть Интернет и Электронными библиотечными и информационно справочными системами; Ауд.424: Комплекты мебели для учебного процесса. Количество ПЭВМ – 12 (рабочая станция CPU Core 2Duo E6300 – 1.86 – 10 шт, Celeron D2.8 – 2 шт.), стенды – 3	

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

Оценочные материалы (ОМ) для дисциплины включают в себя:

- перечень компетенций с указанием индикаторов достижения компетенций, этапов их формирования в процессе освоения образовательной программы;
- описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности.

ОМ представляются отдельным комплектом и **входят в состав рабочей программы дисциплины.**

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

«Защита информации от утечки по техническим каналам»

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ОПК-9	Способен решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ИД2$_{опк-9}$ – осуществляет эксплуатацию современных отечественных и зарубежных средств технической защиты, согласно текущему состоянию систем передачи информации

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД2$_{опк-9}$ – осуществляет эксплуатацию современных отечественных и зарубежных средств технической защиты, согласно текущему состоянию систем передачи информации	Знает: современные отечественные и зарубежные средства технической защиты по техническим каналам.
	Умеет: использовать современные отечественные и зарубежные средства технической защиты по техническим каналам
	Владеет: обеспечения защиты информации от утечки по техническим каналам с учетом современные отечественные и зарубежные средства технической защиты

2 Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые модули/разделы/темы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные средства	Технология оценки (способ контроля)
1	Характеристика государственной системы противодействия технической разведке	ОПК-19	Экзамен	Проверка преподавателем
			Тесты (тестовые задания)	Компьютерное тестирование
			Кейс-задания к практическим работам	Проверка преподавателем
			Доклад	Проверка преподавателем
2	Технические каналы утечки информации	ОПК-9	Экзамен	Проверка преподавателем
			Тесты (тестовые задания)	Компьютерное тестирование
			Кейс-задания к практическим работам	Проверка преподавателем
			Вопросы к коллоквиуму	Проверка преподавателем
3	Методы и средства защиты информации от утечки по техническим каналам.	ОПК-9	Экзамен	Проверка преподавателем
			Тесты (тестовые задания)	Компьютерное тестирование
			Кейс-задания к практическим работам	Проверка преподавателем

			ДЗ	Проверка преподавателем

3 Оценочные средства для промежуточной аттестации

3.1 Вопросы к собеседованию на экзамене

3.1.1. ОПК-9 - Способен решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

№ задания	Формулировка вопроса
1.	Роль информации в обеспечении безопасности всех сфер жизнедеятельности общества. Критерии информационной безопасности.
2.	Обобщенная схема системы передачи информации, принципы формирования угроз информационной безопасности.
3.	Основные направления защиты информации от утечки по техническим каналам.
4.	Классификация угроз информационной безопасности ТКС.
5.	Виды представления информации в ТКС и возможные каналы ее утечки.
6.	Классификация видов и средств технической разведки.
7.	Основное понятие разведки, разведывательного процесса.
8.	Возможности видов технической разведки.
9.	Классификация методов и средств защиты информации от утечки по техническим каналам.
10.	Классификация методов и средств защиты речевой информации.
11.	Классификация методов и средств защиты телефонных линий.
12.	Классификация демаскирующих признаков электронных устройств перехвата информации.
13.	Классификация методов и средств поиска электронных устройств перехвата информации.
14.	Государственное лицензирование деятельности в области защиты информации.
15.	Сертификация средств защиты информации.
16.	Аттестование объектов информатизации.
17.	Классификация методов и средств защиты информации, обрабатываемой ТСПИ, от утечки по техническим каналам.
18.	Состав и классификация ОИ.
19.	Угрозы ОИ.
20.	Комплексное исследование ОИ на выявление угроз.
21.	Специальная проверка.
22.	Специальное исследование.
23.	Специальное обследование зон
24.	Специальная зона 2.
25.	Специальная зона 1.
26.	Объекты технической защиты информации.
27.	Средства защиты выделенных помещений.
28.	Средства защиты сети секретной телефонной связи.
29.	Средства защиты систем звукоусиления и звукового сопровождения кинофильмов.
30.	Средства защиты информации, обрабатываемой СВТ от утечки за счет ПЭМИН.
31.	Средства защиты информации, обрабатываемой СВТ от НСД.
32.	Средства защиты СИРД.
33.	Требования и рекомендации к системе электропитания и заземления.
34.	Контроль эффективности внедренных мер защиты.
35.	Обеспечение безопасности ПДн при их обработке.
36.	Аттестация ОИ.
37.	Состав процесса технической защиты информации.
38.	Порядок проведения мероприятий по ТЗИ.

3.2 Контрольные вопросы к текущим опросам на лабораторных работах

3.2.1. ОПК-9 - Способен решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

№ задания	Формулировка вопроса
1	Какова последовательность действий для того, чтобы настроить интерфейсы на маршрутизаторе DioNIS?
2	Чем режим администратора маршрутизатора DioNIS FW 16000 KB2 отличается от режима оператора?
3	По нажатию на какую функциональную клавишу открывается карточка интерфейса в криптомаршрутизаторе DioNIS FW 16000 KB2?
4	Можно ли изменить имя IP-фильтра после его создания?
5	Для чего нужна метрика в таблице маршрутов?
6	Какая стратегия межсетевого экранирования лежит в основе IP-фильтров маршрутизатора DioNIS FW 16000 KB2?
7	В каком порядке маршрутизатор DioNIS FW 16000 KB2 проверяет правила IP-фильтрации?
8	Каково минимальное количество криптографических маршрутизаторов DioNIS FW 16000 KB2, требуемое для организации 10 статических туннелей?
9	Что обозначает параметр «номер серии ключей» в карточке статического туннеля DioNIS FW 16000 KB2?
10	Что собой представляет идентификатор туннеля DioNIS FW 16000 KB2?
11	Какая информация хранится на отчуждаемом ключевом носителе DioNIS?
12	Этапы первоначальной настройки маршрутизатора DioNIS.
13	Таблица маршрутов в маршрутизаторе DioNIS. Описание параметров. Примеры записи правил прямой и косвенной адресации.
14	Перечислить и кратко описать механизмы защиты в маршрутизаторе DioNIS.
15	Механизм IP-фильтрации в маршрутизаторе DioNIS. Назначение, специфика реализации, основные параметры.
16	Подсистема криптографии в маршрутизаторе DioNIS. Основные параметры, элементы управления.
17	Механизм создания VPN в маршрутизаторе DioNIS. Назначение, специфика реализации, основные параметры.
18	Фильтр в маршрутизаторе DioNIS. Виды, назначение, параметры фильтрации.
19	Статический туннель в маршрутизаторе DioNIS. Назначение, параметры карточки туннеля.
20	Как настроить интерфейс маршрутизатора на работу с буфером обмена в 100 блоков?
21	Какова последовательность действий для того, чтобы настроить интерфейсы на маршрутизаторе DioNIS?
22	Чем режим администратора маршрутизатора DioNIS FW 16000 KB2 отличается от режима оператора?
23	По нажатию на какую функциональную клавишу открывается карточка интерфейса в криптомаршрутизаторе DioNIS FW 16000 KB2?
24	Можно ли изменить имя IP-фильтра после его создания?
25	Для чего нужна метрика в таблице маршрутов?
26	Какая стратегия межсетевого экранирования лежит в основе IP-фильтров маршрутизатора DioNIS FW 16000 KB2?
27	В каком порядке маршрутизатор DioNIS FW 16000 KB2 проверяет правила IP-фильтрации?
28	Каково минимальное количество криптографических маршрутизаторов DioNIS FW 16000 KB2, требуемое для организации 10 статических туннелей?
29	Что обозначает параметр «номер серии ключей» в карточке статического туннеля DioNIS FW 16000 KB2?
30	Что собой представляет идентификатор туннеля DioNIS FW 16000 KB2?
31	Какая информация хранится на отчуждаемом ключевом носителе DioNIS?
32	Этапы первоначальной настройки маршрутизатора DioNIS.
33	Таблица маршрутов в маршрутизаторе DioNIS. Описание параметров. Примеры записи правил прямой и косвенной адресации.
34	Перечислить и кратко описать механизмы защиты в маршрутизаторе DioNIS.

35	Механизм IP-фильтрации в маршрутизаторе DioNIS. Назначение, специфика реализации, основные параметры.
36	Подсистема криптографии в маршрутизаторе DioNIS. Основные параметры, элементы управления.
37	Механизм создания VPN в маршрутизаторе DioNIS. Назначение, специфика реализации, основные параметры.
38	Фильтр в маршрутизаторе DioNIS. Виды, назначение, параметры фильтрации.
39	Статический туннель в маршрутизаторе DioNIS. Назначение, параметры карточки туннеля.
40	Как настроить интерфейс маршрутизатора на работу с буфером обмена в 100 блоков?

3.3. Домашнее задание

3.3.1. ОПК-9 - Способен решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

<table>
<tr><th>№ задания</th><th>Формулировка задания</th></tr>
<tr><td>1</td><td>Помещение третьей категории находится в пятиэтажном здании на втором этаже. Граница контролируемой зоны проходит по внешней поверхности здания. В результате инструментального контроля получены следующие данные:
<table>
<tr><th>Среднегеометрическая частота октавной полосы, Гц</th><th>Уровень тестового сигнала, $\mathbf{L_{Ti}}$, дБ</th><th>Уровень естественного акустического (виброакустического) шума, $\mathbf{L_{ші}}$, дБ</th><th>Уровень суммарного акустического (виброакустического) сигнала и шума, $\mathbf{L_{(с+ш)i}}$, дБ</th></tr>
<tr><td colspan="4">Данные по виброакустическому сигналу для контрольной точки на внешнем остеклении окна</td></tr>
<tr><td>250</td><td>88</td><td>38</td><td>46</td></tr>
<tr><td>500</td><td>92</td><td>33</td><td>50</td></tr>
<tr><td>1000</td><td>95</td><td>26</td><td>52</td></tr>
<tr><td>2000</td><td>96</td><td>22</td><td>49</td></tr>
<tr><td>4000</td><td>90</td><td>20</td><td>44</td></tr>
</table>
Требуется:
1. Кратко охарактеризовать возможные каналы утечки речевой информации через указанную ограждающую конструкцию.
2. По имеющимся данным, с помощью поправочных коэффициентов и графиков, приведенных в НМД АРР, рассчитать значение показателя противодействия.
3. Сравнить полученные значения с нормативными и сделать вывод о возможности утечки речевой информации.</td></tr>
<tr><td>2</td><td>Помещение третьей категории находится в пятиэтажном здании на втором этаже. В результате инструментального контроля получены следующие данные:
<table>
<tr><th>Среднегеометрическая частота октавной полосы, Гц</th><th>Уровень тестового сигнала, L_{Ti}, дБ</th><th>Уровень естественного акустического (виброакустического) шума, $L_{ші}$, дБ</th><th>Уровень суммарного акустического (виброакустического) сигнала и шума, $L_{(с+ш)i}$, дБ</th></tr>
<tr><td colspan="4">Данные по акустическому сигналу для контрольной точки на расстоянии 0,5 м от внешней поверхности двери</td></tr>
<tr><td>250</td><td>88</td><td>30</td><td>52</td></tr>
<tr><td>500</td><td>92</td><td>26</td><td>54</td></tr>
<tr><td>1000</td><td>95</td><td>24</td><td>52</td></tr>
<tr><td>2000</td><td>96</td><td>22</td><td>47</td></tr>
<tr><td>4000</td><td>90</td><td>20</td><td>45</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td>Требуется:

1. Кратко охарактеризовать возможные каналы утечки речевой информации через указанную ограждающую конструкцию.

2. По имеющимся данным, с помощью поправочных коэффициентов и графиков, приведенных в НМД АРР, рассчитать значение показателя противодействия.

3. Сравнить полученные значения с нормативными и сделать вывод о возможности утечки речевой информации.</td></tr>
<tr><td>3</td><td>Помещение третьей категории находится в пятиэтажном здании на втором этаже. Граница контролируемой зоны проходит по внешней поверхности здания. Помещение не оборудовано системой звукоусиления. Местоположение источника речи не зафиксировано в пределах помещения. Входная дверь в помещение одностворчатая, двойная с тамбуром. Входная дверь находится в пределах контролируемой зоны.
В качестве тестового сигнала для измерений использовался шумовой сигнал. В результате инструментального контроля получены следующие данные:
<table>
<tr><th>Среднегеометрическая частота октавной полосы, Гц</th><th>Уровень тестового сигнала, L_{Ti}, дБ</th><th>Уровень естественного акустического (виброакустического) шума, $L_{ши}$, дБ</th><th>Уровень суммарного акустического (виброакустического) сигнала и шума, $L_{(с+ш)i}$, дБ</th></tr>
<tr><td colspan="4">Данные по акустическому сигналу для контрольной точки на расстоянии 0,5 м от внешней поверхности двери</td></tr>
<tr><td>250</td><td>88</td><td>34</td><td>53</td></tr>
<tr><td>500</td><td>92</td><td>32</td><td>55</td></tr>
<tr><td>1000</td><td>95</td><td>28</td><td>51</td></tr>
<tr><td>2000</td><td>96</td><td>25</td><td>48</td></tr>
<tr><td>4000</td><td>90</td><td>22</td><td>45</td></tr>
</table>
Требуется:

1. Кратко охарактеризовать возможные каналы утечки речевой информации через указанную ограждающую конструкцию.

2. По имеющимся данным, с помощью поправочных коэффициентов и графиков, приведенных в НМД АРР, рассчитать значение показателя противодействия.

3. Сравнить полученные значения с нормативными и сделать вывод о возможности утечки речевой информации.</td></tr>
<tr><td>4</td><td>Помещение третьей категории находится в пятиэтажном здании на втором этаже. В качестве тестового сигнала для измерений использовался шумовой сигнал. В результате инструментального контроля получены следующие данные:
<table>
<tr><th>Среднегеометрическая частота октавной полосы, Гц</th><th>Уровень тестового сигнала, L_{Ti}, дБ</th><th>Уровень естественного акустического (виброакустического) шума, $L_{ши}$, дБ</th><th>Уровень суммар акустического (виброак ческого) сигнала и ш $L_{(с+ш)i}$, дБ</th></tr>
<tr><td colspan="4">Данные по акустическому сигналу для контрольной точки на расстоянии 0,5 м от вне поверхности стены</td></tr>
<tr><td>250</td><td>88</td><td>29</td><td>49</td></tr>
<tr><td>500</td><td>92</td><td>36</td><td>48</td></tr>
<tr><td>1000</td><td>95</td><td>31</td><td>45</td></tr>
<tr><td>2000</td><td>96</td><td>29</td><td>41</td></tr>
<tr><td>4000</td><td>90</td><td>26</td><td>34</td></tr>
</table></td></tr>
</table>

	Требуется: 1. Кратко охарактеризовать возможные каналы утечки речевой информации через указанную ограждающую конструкцию. 2. По имеющимся данным, с помощью поправочных коэффициентов и графиков, приведенных в НМД АРР, рассчитать значение показателя противодействия. 3. Сравнить полученные значения с нормативными и сделать вывод о возможности утечки речевой информации.

3.4. Темы докладов

3.4.1. ОПК-9 - Способен решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

№ задания	Формулировка задания
1.	Мероприятия технической эксплуатации.
2.	Характеристика объекта эксплуатации.
3.	Техническое обеспечение связи.
4.	Основные эксплуатационные характеристики систем специальной связи.
5.	Ввод в эксплуатацию аппаратуры связи.
6.	Планирование и учёт технической эксплуатации.
7.	Мониторинг и диагностика каналов связи.
8.	Порядок приемки и ввода в эксплуатацию.
9.	Паспортизация систем связи.
10.	Измерительная техника для эксплуатационных измерений.
11.	Эксплуатационные измерения.
12.	Параметры ошибок и методы их измерений по G.821.
13.	Параметры ошибок и методы их измерений по G.826.
14.	Особенности методологии по рекомендации M.2100.
15.	Мероприятия технической эксплуатации.
16.	Характеристика объекта эксплуатации.
17.	Техническое обеспечение связи.

3.5. Вопросы к коллоквиуму

3.5.1. ОПК-9 - Способен решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

№ задания	Формулировка задания
1	Обобщенная схема системы передачи информации, принципы формирования угроз информационной безопасности.
2	Основные направления защиты информации от утечки по техническим каналам.
3	Классификация угроз информационной безопасности ТКС.
4	Виды представления информации в ТКС и возможные каналы ее утечки.
5	Классификация видов и средств технической разведки.
6	Основное понятие разведки, разведывательного процесса.
7	Возможности видов технической разведки.
8	Классификация методов и средств защиты информации от утечки по техническим каналам.
9	Классификация методов и средств защиты речевой информации.
10	Классификация методов и средств защиты телефонных линий.
11	Классификация демаскирующих признаков электронных устройств перехвата информации.
12	Классификация методов и средств поиска электронных устройств перехвата информации.
13	Государственное лицензирование деятельности в области защиты информации.
14	Сертификация средств защиты информации.
15	Аттестование объектов информатизации.

3.6. Кейс-задания к практическим работам

3.6.1. ОПК-9 - Способен решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

№ задания	Формулировка задания
1.	Осуществить поиск неисправности в сети передачи информации.
2.	Рассчитать параметры канала передачи.
3.	Произвести конфигурацию системы оперативной телефонной связи «Регион-120ХТ».
4.	Произвести конфигурацию системы оперативно-диспетчерской связи «Набат».
5.	Осуществить монтаж патчкорда и подключение оборудования в локальной вычислительной сети без применения коммутатора.
6.	Осуществить монтаж патчкорда и подключение оборудования в локальной вычислительной сети с применением коммутатора.
7.	Зарисовать схему из 3 ЛВС (на выходе которых стоят КМ DioNIS), соединенных по топологии "кольцо". Составить таблицы маршрутов для любых трех внешних интерфейсов.
8.	Зарисовать схему из 4 ЛВС (на выходе которых стоят КМ DioNIS), соединенных по топологии "кольцо". Составить таблицы маршрутов для любых трех внешних интерфейсов.
9.	Зарисовать схему из 5 ЛВС (на выходе которых стоят КМ DioNIS), соединенных по топологии "кольцо". Составить таблицы маршрутов для любых трех внешних интерфейсов.
10.	Зарисовать схему из 3 ЛВС (на выходе которых стоят КМ DioNIS), соединенных в линию. Составить таблицы маршрутов для любых трех внешних интерфейсов.
11.	Зарисовать схему из 4 ЛВС (на выходе которых стоят КМ DioNIS), соединенных «Т-образно». Составить таблицы маршрутов для любых трех внешних интерфейсов.
12.	Зарисовать схему из 5 ЛВС (на выходе которых стоят КМ DioNIS), соединенных «Р-образно». Составить таблицы маршрутов для любых трех внешних интерфейсов.
13.	Зарисовать схему из 5 ЛВС (A,B,C,D,E, на выходе которых стоят КМ DioNIS). Прописать правила фильтрации на фильтрах int_in (указав задействованные для фильтрации интерфейсы на схеме), чтобы отфильтровывался следующий трафик: 1. A - D; 2. B - C (TCP); 3. E - A (UDP, 8080).
14.	Зарисовать схему из 5 ЛВС (A,B,C,D,E, на выходе которых стоят КМ DioNIS). Прописать правила фильтрации на фильтрах int_in (указав задействованные для фильтрации интерфейсы на схеме), чтобы отфильтровывался следующий трафик: 1. C - A (ICMP, 0-100); 2. D - E (1024-3000); 3. B - A.
15.	Зарисовать схему из 5 ЛВС (A,B,C,D,E, на выходе которых стоят КМ DioNIS). Прописать правила фильтрации на фильтрах int_in (указав задействованные для фильтрации интерфейсы на схеме), чтобы отфильтровывался следующий трафик: 1. D - B (TCP, UDP); 2. D - A (ICMP, 30-1024); 3. E - C (TCP, 8080).
16.	Зарисовать схему из 5 ЛВС (A,B,C,D,E, на выходе которых стоят КМ DioNIS). Прописать правила фильтрации на фильтрах ext_in (указав задействованные для фильтрации интерфейсы на схеме), чтобы отфильтровывался следующий трафик: 1. A - D; 2. B - C (TCP); 3. E - A (UDP, 8080).
17.	Зарисовать схему из 5 ЛВС (A,B,C,D,E, на выходе которых стоят КМ DioNIS). Прописать правила фильтрации на фильтрах ext_out (указав задействованные для фильтрации интерфейсы на схеме), чтобы отфильтровывался следующий трафик: 1. B - C; 2. D - E (ICMP, UDP); 3. A - D (TCP, 10-120).
18.	Зарисовать схему из 5 ЛВС (A,B,C,D,E, на выходе которых стоят КМ DioNIS). Прописать правила фильтрации на фильтрах ext_out (указав задействованные для фильтрации интерфейсы на схеме), чтобы отфильтровывался следующий трафик: 1. E - A (1024-8080); 2. A - C (ICMP); 3. A - B (80).
19.	Зарисовать схему из 5 ЛВС (A,B,C,D,E, на выходе которых стоят КМ DioNIS). Прописать правила фильтрации на фильтрах ext_out (указав задействованные для фильтрации интерфейсы на схеме), чтобы отфильтровывался следующий трафик: 1. B - C (ICMP, 10); 2. B - E (UDP, 800-

	1024); 3. D - A (TNL, 680).
20.	Зарисовать схему из 5 ЛВС (A,B,C,D,E, на выходе которых стоят КМ DioNIS), соединенных по топологии "звезда" (центр звезды - сеть А), где присутствуют альтернативные маршруты между: В и D, С и Е. Составить таблицы маршрутов.
21.	Зарисовать схему из 5 ЛВС (A,B,C,D,E, на выходе которых стоят КМ DioNIS), соединенных по топологии "звезда" (центр звезды - сеть А), где присутствуют альтернативные маршруты между: С и D, И и Е. Составить таблицы маршрутов.
22.	Зарисовать схему из 5 ЛВС (A,B,C,D,E, на выходе которых стоят КМ DioNIS), соединенных по топологии "кольцо" (друг за другом по кругу), где присутствуют альтернативный маршрут между А и С. Составить таблицы маршрутов.
23.	Зарисовать схему из 5 ЛВС (A,B,C,D,E, на выходе которых стоят КМ DioNIS), соединенных по топологии "кольцо" (друг за другом по кругу), где присутствуют альтернативный маршрут между Е и В. Составить таблицы маршрутов.
24.	Зарисовать пример схемы из 5 ЛВС (A,B,C,D,E, на выходе которых стоят КМ DioNIS). Прописать карточки туннелей для туннелей A-C и D-B.
25.	Зарисовать пример схемы из 5 ЛВС (A,B,C,D,E, на выходе которых стоят КМ DioNIS). Прописать карточки туннелей для туннелей B-E и C-B.
26.	Зарисовать пример схемы из 5 ЛВС (A,B,C,D,E, на выходе которых стоят КМ DioNIS). Прописать карточки туннелей для туннелей A-B и C-B.

3.7. Тестирование

3.7.1. ОПК-9 - Способен решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

№ задания	Формулировка задания
1.	Защита информации от утечки это деятельность по предотвращению: **- получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;** - воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации; - воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений; - неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; - несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации
2.	Способы получения информации по оптическим каналам: **- наблюдение** **- фотографирование объектов** **- съемка документов** - маскировка
3.	**С**редой распространения и перехвата виброакустических каналов не являются: - строительные конструкции, - элементы арматуры, - оконные стекла, **- светодиод офисного светильника**
4.	Технические каналы съема информации делятся на: **- электрические. Закладные устройства подключаются напрямую к проводам телефонной связи, коаксиальным и низкочастотным кабелям связи;** **- электромагнитные. По ним передается электромагнитное излучение, модулированное информационным сигналом, так прослушиваются мобильные телефоны, рации;** **- индукционные. При ведении переговоров по спутниковой связи возникает индукционное высокочастотное излучение, которое может быть перехвачено и преобразовано**

	в информацию - производственные. Производимые зарубежной и отечественной промышленностью закладные устройства, которые могут быть внедрены в компьютер и другое оборудование
5.	К техническим каналам утечки данных не относится: - источника сигнала — человека или телефона для акустических каналов, компьютера или кабеля связи для каналов ПЭМИН; - среды распространения — воздуха, безвоздушного пространства, кабелей электропитания, строительных конструкторов; - закладного устройства разведки, перехватывающего информацию и часто передающего ее вовне по радиоканалу **- приемник сигнала – устройства принимающего запросы от перехватчика и передающего на устройство администратора**
6.	Средствами защиты информации по каналам ПЭМИН не являются: - генераторы шума - сетевые помехоподавляющие фильтры - генераторы линейного зашумления - средства пассивной защиты **- средства защиты слаботочных линий**
7.	Средствами защиты акустической речевой информации не являются: **- системы виброакустической защиты** **- средства защиты слаботочных линий** **- электромагнитные подавители сотовых телефонов**
8.	Техническая защита информации: **- защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств** - воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений - совокупность программных и аппаратных средств
9.	Принцип защиты, который предполагает возможность оперативно изменять меры защиты, особенно в случае, если принимаемые меры станут известны злоумышленнику - целеустремленность **- гибкость** -скрытность - рациональность
10.	Совокупность специальных органов, технических средств и мероприятий по их использованию для защиты конфиденциальной информации - организационная защита информации **- инженерно-техническая защита информации** - правовая защита информации - территориальная защита информации
11.	Активный перехват информации это перехват, который: - заключается в установке подслушивающего устройства в аппаратуру средств обработки информации; - основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций; - неправомерно использует технологические отходы информационного процесса; - осуществляется путем использования оптической техники; **- осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера**
12.	. К внутренним нарушителям информационной безопасности относится: - клиенты; - пользователи системы; - посетители; - любые лица, находящиеся внутри контролируемой территории; - представители организаций, взаимодействующих по вопросам обеспечения жизнедея-

	тельности организации. - персонал, обслуживающий технические средства. - сотрудники отделов разработки и сопровождения ПО; **- технический персонал, обслуживающий здание**
13.	Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется: - активный перехват; - пассивный перехват; **- аудиоперехват;** - видеоперехват; - просмотр мусора
14.	Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется: - активный перехват; **- пассивный перехват;** - аудиоперехват; - видеоперехват; - просмотр мусора
15.	Перехват, который осуществляется путем использования оптической техники называется: - активный перехват; - пассивный перехват; - аудиоперехват; **- видеоперехват;** - просмотр мусора
16.	Активный перехват информации это перехват, который: - заключается в установке подслушивающего устройства в аппаратуру средств обработки информации; - основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций; - неправомерно использует технологические отходы информационного процесса; - осуществляется путем использования оптической техники; **- осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.**
17.	Естественные угрозы безопасности информации вызваны: - деятельностью человека; - ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения; **- воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;** - корыстными устремлениями злоумышленников; - ошибками при действиях персонала
18.	Искусственные угрозы безопасности информации вызваны: **- деятельностью человека;** - ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения; - воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека; - корыстными устремлениями злоумышленников; - ошибками при действиях персонала
19.	Защита информации это: - процесс сбора, накопления, обработки, хранения, распределения и поиска информации; - преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа; - получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств; - совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

	- деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё
20.	Установка генератора шума для создания эффекта маскировки речевого сигнала в защищаемом помещении относится к: - организационным мерам обеспечения безопасности **- техническим мерам обеспечения безопасности** - морально-этическим мерам обеспечения безопасности - физическим мерам обеспечения безопасности
21.	Установка аппаратного межсетевого экрана относится к: - организационным мерам обеспечения безопасности **- техническим мерам обеспечения безопасности** - морально-этическим мерам обеспечения безопасности - физическим мерам обеспечения безопасности
22.	Регламентация доступа в защищаемое помещение относится к: **- организационным мерам обеспечения безопасности** - техническим мерам обеспечения безопасности - морально-этическим мерам обеспечения безопасности - физическим мерам обеспечения безопасности
23.	Какое свойство информации нарушено, если в результате действий злоумышленников легитимный пользователь не может получить доступ к социальной сети? - конфиденциальность **- доступность** - целостность - неотказуемость
24.	Если в результате DDOS-атаки новостной сайт на какое-то время вышел из строя и был недоступен для пользователей, какое свойство информации было нарушено? - конфиденциальность **- доступность** - целостность - неотказуемость
25.	Как называется состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право? - конфиденциальность - доступность **- целостность** - неотказуемость
26.	Если злоумышленник получил доступ к чужому письму, прочитал его и отправил легитимному получателю без изменений, какое свойство информации он нарушил? **- конфиденциальность** - доступность - целостность - неотказуемость
27.	Как называется состояние информации, при котором доступ к ней могут осуществить только субъекты, имеющие на него право? **- конфиденциальность** - доступность - целостность - неотказуемость
28.	Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации? - атака **- угроза** - источник угрозы - цель злоумышленника
29.	Что является выходами системы защиты информации? - внешние и внутренние угрозы

	- злоумышленники и владельцы информации - сведения **- средства и методы защиты**
30.	Что является входами системы защиты информации? **- внешние и внутренние угрозы** - злоумышленники и владельцы информации - сведения - средства и методы защиты
31.	Защита информации как слабоформализуемая задача обладает следующими свойствами: - маленькое количество факторов, влияющих на построение эффективной защиты **- большое количество факторов, влияющих на построение эффективной защиты** - точные входные данные **- неточные входные данные** - наличие математических методов получения оптимальных результатов **- отсутствие математических методов получения оптимальных результатов**
32.	Основные рекомендации при разработке системы защиты не включают: **- не размещать объекты защиты в пространстве так, чтобы избежать отражения света в сторону гипотетического нахождения злоумышленника, фотоаппарата или видеокамеры;** - снижать отражающие свойства объекта защиты; - существенно понизить освещенность документа, оборудования или другого объекта; - снизить уровень отраженного света, используя ширмы, затемнение окон, матовые перегородки, иные преграды; - использовать средства маскировки объекта, смены его различительных характеристик
33.	Зрительная информация чаще всего перехватывается в результате - уязвимости видеокамер - неточных входных данных **- небрежности ее владельца** - сложности устройств
34.	Общие меры, реализуемые в ситуации, когда полное переоборудование помещения невозможно не включают: **- невозможность проверки помещения приборами, определяющими работу микрофонов, — сканерами, рентгеновскими установками, комплексными средствами выявления ЗУ, способными обнаружить радиоизлучение мощностью выше 30 кГц;** - смена стекол в окнах на защищенные, рифленые, расположенные в раме под углом; - ведение переговоров только в защищенных помещениях, отказ от разговоров в автотранспорте или на оживленных улицах.
35.	Подготовки помещений к аттестации ФСТЭК РФ подразумевает: **- невозможность появление новых каналов утечки информации с использованием рекомендаций ведомства** - блокировки и дополнительной изоляции точек входа в помещение вентиляционных каналов - использования средств акустического зашумления помещений - внедрения звукопоглощающих покрытий стен, пола, двойных потолков
36.	Бесконтрольный выход секретной или конфиденциальной информации за пределы организации или круга лиц, которым она была доверена - уязвимость **- утечка** - защита - разблокировка
37.	Совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал - **ТКУИ** - ПЭМИН - ФСТЭК - ИБ
38.	Каналы для телекоммуникационной информации:

	- **Параметрические** - Воздушные (прямые акустические) - Вибрационные (виброакустические) - Электроакустические
39.	Любая система связи (система передачи информации) не включает: - Источника информации - Передатчика - Канала передачи информации - **Брандмауэр** - Получателя сведений
40.	Технические средства, непосредственно обрабатывающие конфиденциальную информацию - Приемной аппаратуры на стороне злоумышленника - **Технические средства приема, обработки, хранения и передачи информации** - Канал утечки информации - Вспомогательные технические средства и системы

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания в ходе изучения дисциплины знаний, умений и навыков, характеризующих этапы формирования компетенций, регламентируются положениями:

- П ВГУИТ 2.4.03 Положение о курсовых, экзаменах и зачетах;
- П ВГУИТ 4.1.01 Положение о рейтинговой оценке текущей успеваемости

Итоговая оценка по дисциплине определяется на основании определения средневзвешенному значения баллов по каждому заданию.

5 Описание показателей и критериев оценивания уровня сформированности компетенций

Результаты обучения по этапам формирования компетенций	Методика оценки (объект, продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
ОПК-9 - Способен решать задачи профессиональной деятельности с учётом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации					
ЗНАТЬ современные отечественные и зарубежные средства технической защиты по техническим каналам.	собеседование на экзамене	Уровень знаний при ответе на вопросы	ответил на все вопросы, допустил не более 1 ошибки в ответе	Отлично	Освоена (повышенный)
			ответил на все вопросы, допустил более 1, но менее 3 ошибок	Хорошо	Освоена (повышенный)
			ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена (базовый)
			ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена (недостаточный)
	Тест	Результат тестирования	85% и более правильных ответов	Отлично	Освоена (повышенный)
			75-84% правильных ответов	Хорошо	Освоена (повышенный)
			65-74% правильных ответов	Удовлетворительно	Освоена (базовый)
			Менее 64% правильных ответов	Не удовлетворительно	Не освоена (недостаточный)
УМЕТЬ использовать современные отечественные и зарубежные средства технической защиты по техническим каналам	Кейс-задания для практических работ	Уровень умения	студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе	Отлично	Освоена (повышенный)
			студент выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок	Хорошо	Освоена (повышенный)

			студент выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена (базовый)
			студент ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена (недостаточный)
ВЛАДЕТЬ обеспечения защиты информации от утечки по техническим каналам с учетом современные отечественные и зарубежные средства технической защиты	Доклад	Уровень владения	выставляется студенту при наличии доклада, преобразовании информации в единую форму, т.е. презентации по выбранной теме	Зачтено	Освоена (базовый, повышенный)
			выставляется студенту при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме	Не зачтено	Не освоена (недостаточный)
	Домашняя работа	Уровень навыков	студент выбрал верную методику решения задач, ответил на все вопросы, допустил не более 1 ошибки в ответе	Отлично	Освоена (повышенный)
			студент выбрал верную методику решения задач, проведен верный расчет ответил на все вопросы, имеются незначительные замечания по тексту и оформлению работы, допустил не более 3 ошибок в ответе	Хорошо	Освоена (повышенный)
			студент выбрал верную методику решения задач, проведен верный расчет, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту и оформлению работы, допустил	Удовлетворительно	Освоена (базовый)

			не более 5 ошибок в ответе		
			студент выбрал верную методику решения задач, проведен верный расчет, выполнил правильно графическую часть, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту и оформлению работы, допустил более 5 ошибок в ответе	Не удовлетворительно	Не освоена (недостаточный)
	Коллоквиум	Уровень владения	ответил на все вопросы, допустил не более 1 ошибки в ответе	Отлично	Освоена (повышенный)
			ответил на все вопросы, допустил более 1, но менее 3 ошибок	Хорошо	Освоена (повышенный)
			ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена (базовый)
			ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена (недостаточный)