МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. В. Сенченко
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Техническая защита информации (лабораторный практикум)

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль) / специализация: **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **5**
Семестр: **9**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	9 семестр	Всего	Единицы
1	Лабораторные работы	36	36	часов
2	Всего аудиторных занятий	36	36	часов
3	Всего (без экзамена)	36	36	часов
4	Общая трудоемкость	36	36	часов
		1.0	1.0	З.Е.

Зачёт: 9 семестр

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 23.08.2017
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Томск

Согласована на портале № 49236

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от « 4 » 6 2020 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:
доцент каф. КИБЭВС _____ Е. М. Давыдова

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Д. В. Кручинин

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ А. А. Конев

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ К. С. Сарин

Согласована на портале № 49236

1. Цели и задачи дисциплины

1.1. Цели дисциплины

ическая подготовка студентов

- по вопросам защиты информации от утечки по техническим каналам (технической защиты информации) на объектах информатизации и в выделенных помещениях;
- по вопросам анализа защищенности автоматизированных систем;
- по вопросам проведения контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
- по вопросам участия в проведении экспериментально-исследовательских работ по сертификации средств защиты информации автоматизированных систем;
- по вопросам участия в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации;
- по вопросам проведения инструментального мониторинга защищенности информации в автоматизированной системе и выявления каналов утечки информации.

1.2. Задачи дисциплины

– Задачи дисциплины – дать основы: выявление на объекте информатизации или в
– выделенном помещении технических каналов утчки информации; оценка уровня
– шумов/информативных сигналов/помех; оценка соответствия объекта информатизации или
– выделенного помещения требованиям по безопасности от утечки информации по техническим
– каналам

2. Место дисциплины в структуре ОПОП

Дисциплина «Техническая защита информации (лабораторный практикум)» (ФТД.4) относится к блоку ФТД.4.

Предшествующими дисциплинами, формирующими начальные знания, являются: Теоретические основы компьютерной безопасности, Техническая защита информации.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Подготовка к сдаче и сдача государственного экзамена.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ по сертификации средств защиты информации автоматизированных систем;

– ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации;

В результате изучения дисциплины обучающийся должен:

– **знать** знать технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам.

– **уметь** уметь анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. пользоваться нормативными документами по защите информации.

– **владеть** владеть методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 1.0 зачетных единицы и представлена в табли-

Согласована на портале № 49236

це 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		9 семестр
Аудиторные занятия (всего)	36	36
Лабораторные работы	36	36
Оформление отчетов по лабораторным работам	35	35
Всего (без экзамена)	36	36
Общая трудоемкость, ч	36	36
Зачетные Единицы	1.0	1.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
9 семестр				
1 Технические средства добывания и инженерно-технической защиты информации	36	35	71	ПК-15, ПК-16
Итого за семестр	36	35	71	
Итого	36	35	71	

5.2. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.2.

Таблица 5.2 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин
	1
Предшествующие дисциплины	
1 Теоретические основы компьютерной безопасности	+
2 Техническая защита информации	+
Последующие дисциплины	
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+

Согласована на портале № 49236

2 Подготовка к сдаче и сдача государственного экзамена	+

5.3. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.3.

Таблица 5.3 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий	Формы контроля
	Лаб. раб.	
ПК-15	+	Опрос на занятиях, Зачёт, Тест
ПК-16	+	Опрос на занятиях, Зачёт, Тест

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
9 семестр			
1 Технические средства добывания и инженерно-технической защиты информации	Статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в охраняемом помещении.	4	ПК-15, ПК-16
	Нелинейная локация.	4	
	Обнаружение активных прослушивающих устройств с помощью индикатора электромагнитного поля.	6	
	Аппаратно-программный комплекс имитации сигналов закладочных устройств «АВРОРА-Т».	6	
	Охрана выделенных помещений. Пожарная сигнализация.	4	
	Охрана выделенных помещений. Охранная сигнализация.	4	
	Ограничение доступа в выделенное помещение. Система контроля и управления доступом	4	
	Охрана выделенных помещений. Система видеонаблюдения.	4	
	Итого	36	
Итого за семестр		36	

8. Практические занятия (семинары)

Не предусмотрено РУП.

Согласована на портале № 49236

9. Самостоятельная работа

Не предусмотрено РУП.

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
9 семестр				
Зачёт			40	40
Опрос на занятиях	10	10	10	30
Тест	10	10	10	30
Итого максимум за период	20	20	60	100
Нарастающим итогом	20	40	100	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

Согласована на портале № 49236

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Технические средства защиты информации [Электронный ресурс]: Учебное пособие / А. А. Титов - 2010. 194 с. — Режим доступа: https://edu.tusur.ru/publications/653 (дата обращения: 16.06.2020).
2. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс]: Сборник лабораторных работ / А. М. Голиков - 2015. 373 с. — Режим доступа: https://edu.tusur.ru/publications/5378 (дата обращения: 16.06.2020).
3. Технические средства охраны [Электронный ресурс]: Учебное пособие / А. Н. Дементьев, Г. В. Дементьева - 2012. 119 с. — Режим доступа: https://edu.tusur.ru/publications/2352 (дата обращения: 16.06.2020).

12.2. Дополнительная литература

1. Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г. № 5485-1. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]: — Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?
req=doc&n=220985&base=LAW&rnd=244973.2538529920&from=176315-6#07645778093816449
(дата обращения: 16.06.2020).
2. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. №149-ФЗ. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс]: — Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?
req=doc&n=296555&base=LAW&rnd=244973.246476619&from=200126-6#0018852774366745484
(дата обращения: 16.06.2020).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Защита информации [Электронный ресурс]: Методические указания к выполнению лабораторных работ / В. Г. Спицын - 2012. 77 с. — Режим доступа: https://edu.tusur.ru/publications/1826 (дата обращения: 16.06.2020).
2. Защита информации [Электронный ресурс]: Методические указания к выполнению самостоятельных работ / В. Г. Спицын - 2012. 78 с. — Режим доступа: https://edu.tusur.ru/publications/2261 (дата обращения: 16.06.2020).
3. Защита речевой информации от утечки по акустическим и виброакустическим каналам [Электронный ресурс]: Руководство к практическим занятиям и лабораторным работам / Р. С. Круглов, М. В. Южанин - 2007. 49 с. — Режим доступа: https://edu.tusur.ru/publications/994 (дата обращения: 16.06.2020).

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. https://lib.tusur.ru/ru/resursy/bazy-dannyh/elibrary-ru
2. http://www.consultant.ru/

Согласована на портале № 49236

3. https://e.lanbook.com/

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория технической защиты информации

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 512 ауд.

Описание имеющегося оборудования:

- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор;
- Нелинейный локатор NR 900 EM;
- Индикатор поля ST06 SEL SP-77 "Ловец";
- Многофунцкциональный поисковый прибор ST 034;
- Анализатор спектра цифровой GSP-7930;
- Ручной металлодетектор «АКА»;
- Блокиратор сотовых телефонов C-GUARD 300YK;
- Электронно-оптическое устройство "Алмаз";
- Электронно-оптическое устройство "Вега";
- Портативная установка НОРКА-МАКСИ-Д;
- Детектор радиополя D-008;
- RS turboMobile – L;
- Специализированное оборудование по защите информации от утечки по акустическому, акустоэлектрическому каналам, каналу побочных электромагнитных излучений и наводок: Система виброакустической защиты "Соната-АВ" мод. 1М, Пьезоизлучатель ПИ-45, Аудиоизлучатель АИ-65, Система защиты от утечки информации Гром ЗИ-4Б, Блок электропитания и управления «Соната-ИП4.3», Размыкатель телефонной линии «Соната-ВК4.1», Размыкатель слаботочной линии «Соната-ВК4.2», Размыкатель линии Ethernet «Соната-ВК4.3», Средство активной защиты информации от утечки за счет наводок информационного сигнала на цепи заземления и электропитания «Соната-РС3»;

Технические средства контроля эффективности защиты информации от утечки по акустическому каналу, каналу побочных электромагнитных излучений и наводок: Программно-аппаратный комплекс для проведения измерений «СПРУТ 7», Программно-аппаратный измерительный комплекс «Гриф АЭ-1001», ПАК Легенда;

- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Kaspersky endpoint security
– Microsoft Windows 10

Лаборатория защищенных автоматизированных систем

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 511 ауд.

Описание имеющегося оборудования:

- Компьютеры: AMD A6-3670/ Asus F1A75-M Pro / DDR3 4 Gb/ ST3250410AS 250 Gb / мышь/ клавиатура/ монитор (5 шт.);
- ИБП Ippon;
- Стенд "Средства контроля и управления доступом" в составе: Сетевой контроллер СКУД Gate-4000 UPS, контроллер управления доступом UnitECO LOCK 2S-LO-SMB, турникет PERCo-KT03/600-1;

Согласована на портале № 49236

- Стенд "Пожаро-охранные сигнализации" в составе: Охранное устройство Мираж-GSM-А4-03, ИК извещатель, «стандарт» РАПИД, извещатель радиоволновый Астра-552, комбинированный извещатель Астра-8;

- Климатическая станция Vantage PRO2;

- Приемопередатчики видеосигнала по витой паре на TTP111VLH; видеосервер Domination D7-8-H264;

- Видеорегистратор Videorox DVR VR 3294;

- Стандартная цветная видеокамера под объектив MSC-512S;

- Купольная видеокамера SCW-422;

- Пульт управления камерами SPEED DOME SCJ-200;

- Видео камера сетевая SPEED DOME Beward BD75-5;

- Уличная видеокамера SPEED;

- Комплект специализированной учебной мебели;

- Рабочее место преподавателя.

Программное обеспечение:

– Kaspersky endpoint security

– Microsoft Windows 7 Pro

– Аппаратно-программные средства управления доступом к данным, шифрования: DallasLock

– Аппаратно-программные средства управления доступом к данным, шифрования: КриптоПро CSP

– Аппаратно-программные средства управления доступом к данным, шифрования: ПО ViPNet Administrator 4.x, ПО ViPNet Coordinator for Windows 4.x, ПО ViPNet Coordinator for Linux 4.x, ПО ViPNet Client for Windows 4.x, ПО ViPNet Crypto Service 4.x

– Сервер архивации Windows Server 2012

– Средство мониторинга состояния автоматизированных систем: Система мониторинга Zabbix

– Средство мониторинга состояния автоматизированных систем: MaxPatrol Education

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

Согласована на портале № 49236

14.1.1. Тестовые задания

1. Устройство, используемое для проведения измерений ТС на побочные электромагнитные излучения (ПЭМИ)?
1) Анализатор спектра
2) Шумомер
3) Низкочастотный анализатор
4) Все варианты
2. Устройства, подлежащие исследованию на побочные электромагнитные излучения и наводки (ПЭМИН)?
1) Накопители на жестких дисках
2) Принтер
3) Клавиатура
4) Все варианты
3. Что изучается при определении значений сигналов АЭП речевого диапазона частот в отходящей от ВТСС линии, выходящей за пределы КЗ?
1) Телефония
2) Система сигнализации
3) Цепи электропитания
4) Все перечисленное
4. Какой канал утечки информации использует эффект высокочастотного облучения для перехвата информации обрабатываемой в технических средствах?
1) Акустоэлектрический
2) Параметрический
3) Электрический
47350
19
4) Электромагнитный
Какой канал утечки информации использует эффект высокочастотного облучения для перехвата информации обрабатываемой в технических средствах?
1) Акустоэлектрический
2) Параметрический
3) Электрический
4) Электромагнитный
5. Как называется устройство про помощи которого выполняется измерение ограждающих конструкций при проведении виброакустических измерений разборчивости речи?
1) Акселерометр
2) Микрофон
3) Акустический излучатель
4) Лучевая трубка
6. Каким каналом утечки речевой информации является дверь в выделенное помещение?
1) Параметрический
2) Видовой
3) Акустический
4) Оптико-электронный
7. При превышении какого значения разборчивости речи можно говорить о достижении уровня непреднамеренного прослушивания?
1) 10%
2) 20%
3) 30%
4) 40%
8. Какая из среднегеометрических частот не входит в стандартные октавные полосы?
1) 250 Гц
2) 1 кГц
3) 500 Гц

Согласована на портале № 49236

4) 750 Гц

9. При передачи информации по каналам связи, какой канал утечки информации возникает в результате возникновения вокруг высокочастотного кабеля электромагнитного поля?

1) Электромагнитный канал

2) Индукционный канал

3) Паразитные связи

4) Электрический канал

10. Каким методом может осуществляться контроль эффективности мер защиты информации?

1) Инструментальным методом

2) Инструментально-расчетным методом

3) Расчетным методом

4) Все варианты

11. Мероприятия технического контроля состоят в осуществлении инструментальных проверок эффективности защиты информации от утечки по техническим каналам, возникающим

за счет:

1) Побочных электромагнитных излучений (ПЭМИ) при работе основных технических средств и систем (ОТСС) объекта информатизации

2) Наводок информационного сигнала на соединительных линиях ВТСС, расположенных в зоне действия ПЭМИ ОТСС

3) Неравномерности потребления тока в сети электропитания ОТСС

4) Все варианты

12. Какой канал утечки информации возникает за счет преобразований акустических сигналов в электрические различными радиоэлектронными устройствами, обладающими «микрофонным эффектом», а также путем «высокочастотного навязывания»

1) Акустоэлектрический канал

47350

20

2) Оптико-электронный канал

3) Гидроакустический канал

4) Вибрационный канал

13. Что включают в себя демаскирующие признаки автономных некамуфлированных акустических закладок?

1) Наличие автономных источников питания

2) Наличие полупроводниковых элементов, выявляемых при облучении обследуемого устройства нелинейным радиолокатором

3) Наличие в устройстве проводников или других деталей, определяемых при просвечивании его рентгеновскими лучами

4) Все перечисленное

14. Какие объекты информатизации подлежат обязательной аттестации?

1) Для обработки информации, составляющей государственную тайну

2) Для ведения секретных переговоров

3) Для управления экологически опасными объектами

4) Все перечисленное

15. На каком расстоянии от пола должен располагаться излучатель тестового акустического сигнала при проведении акустических измерений разборчивости речи через ограждающие конструкции?

1) 0.5м

2) 1м

3) 1.5м

4) 1.7м

16. На каком расстоянии от ограждающей конструкции должен располагаться микрофон при проведении акустических измерений разборчивости речи через ограждающие конструк-

Согласована на портале № 49236

ции?

1) 0.5м
2) 1м
3) 1.5м
4) 0.7м

17. Каким каналом утечки речевой информации являются системы отопления в помещении?
1) Акустический
2) Видовой
3) Виброакустический
4) Все варианты

18. Каким из каналов утечки речевой информации является окно?
1) Акустическим
2) Виброакустическим
3) Оптическим
4) Все варианты

19. Какой из каналов утечки речевой информации возникает при облучении лазерным лучом вибрирующих поверхностей?
1) Акустический канал
2) Акустоэлектрический канал
3) Оптико-электронный
4) Виброакустический канал

20. При превышении какого значения разборчивости речи можно говорить о достижении уровня сокрытия факта переговоров?
1) 10%
2) 20%
3) 30%
4) 40%

14.1.2. Зачёт

Дайте определение информации, документированной информации. Каково отличие
47350
21
государственной тайны, конфиденциальной информации и открытой информации.
2. Классификация технической разведки. Эффективность добывания информации технической разведкой.
3. Государственная система защиты информации. Эффективность защиты информации.
4. Основные объекты защиты информации.
5. Дайте определение демаскирующих признаков. Для чего они используются. Приведите примеры.
6. Дайте определение терминам Контролируемая зона, Опасная зона, Опасная зона 1, Опасная зона 2.
7. Состав технического канала утечки информации.
8. Классификация технических каналов утечки информации.
9. Перечислите технические каналы утечки информации, обрабатываемой ОТСС. Приведите примеры.
10. Перечислите технические каналы утечки информации при передаче по каналам связи. Приведите примеры.
11. Перечислите каналы утечки речевой информации. Приведите примеры.
12. Перечислите каналы утечки видовой информации. Приведите примеры.
13. Каково влияние паразитных емкостных, индуктивных и резистивных связей в каналах связи.
14. Перечислите методы противодействия утечке информации по техническим каналам.
15. Способы скрытого видеонаблюдения. Характеристики оборудования для скрытого видеонаблюдения.
16. Способы скрытого прослушивания переговоров в помещении. Демаскирующие

Согласована на портале № 49236

признаки радиозакладок. Демаскирующие признаки проводных закладок.
17. Способы прослушивания переговоров по телефонным линиям. Демаскирующие признаки акустических закладок типа «телефонное ухо».
18. Направленные микрофоны. Принцип действия.
19. Охранные системы. Назначение. Структура. Приведите примеры охранных систем объектов и помещений.
20. Датчики охранных систем. Принципы действия датчиков.
21. Охранное видеонаблюдение. Назначение. Структура. Основные характеристики.
22. Средства радиотехнической разведки. Состав. Характеристики.
23. Охрана объектов. Особенности охраны объектов различного класса. Задачи средств охраны объектов.
24. Периметровые средства охраны. Датчики периметровых систем охраны.
25. Охрана выделенных (защищаемых) помещений. Технические средства охраны помещений.
26. Экранирование электромагнитных волн.
27. Экранирование акустических сигналов.
28. Фильтрация опасных сигналов. Приведите примеры.
29. Маскировка опасных сигналов зашумлением. Приведите примеры.
30. Металлодетекторы. Сферы применения. Принцип действия.
31. Локаторы нелинейностей. Сферы применения. Принцип действия.
32. Аттестация объектов информатизации по требованиям безопасности. Назначение.

14.1.3. Темы опросов на занятиях

Характеристика инженерно-технической защиты информации. Технические средства и методы защиты информации. Основные проблемы и параметры инженерно-технической защиты информации. Представление методов и средств защиты информации как системы. Показатели эффективности инженерно-технической защиты информации.

47350

22

Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации.

Основные направления инженерно-технической защиты информации. Принципы защиты информации техническими средствами.

Информация как предмет защиты. Особенности информации как предмета защиты.

Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения и сигналов. Понятие о текущей и эталонной признаковой структуре.

Источники опасных сигналов. Понятие об опасном сигнале. Опасные сигналы и их источники. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Состав и характеристика основных и вспомогательных технических средств и систем.

Побочные электромагнитные излучения и наводки. Виды побочных опасных электромагнитных излучений. Случайные антенны. Виды опасных сигналов на объектах информатизации.

Характеристика технической разведки. Основные задачи и органы технической разведки.

Принципы технической разведки. Основные этапы и процедуры добывания информации технической разведкой. Классификация технической разведки по видам носителя информации и средств разведки. Возможности видов технической разведки. Основные направления развития технической разведки.

Технические каналы утечки информации. Понятие и особенности утечки информации.

Согласована на портале № 49236

Структура, классификация и основные характеристики технических каналов утечки информации.

Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их возможности.

Методы инженерной защиты и технической охраны объектов. Классификация методов инженерной защиты и технической охраны объектов. Инженерные конструкции. Автономные и централизованные системы охраны объектов. Модели злоумышленников. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара.

Методы скрытия информации и ее носителей. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение. Энергетическое скрытие радио и электрических сигналов. Виды и условия зашумления сигналов.

Физические основы побочных электромагнитных излучений и наводок.

Акустоэлектрические преобразования. Источники побочных излучений, их физическая природа.

Характер электромагнитных излучений в ближней и дальней зонах. Виды паразитных связей и наводок. Паразитная генерация радиоэлектронных средств. Физические явления, вызывающие утечку информации по цепям электропитания, заземления и токопроводящим конструкциям здания.

Распространение сигналов в технических каналах утечки информации. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в световодах.

Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Основные показатели среды распространения сигналов различных технических каналов утечки информации.

Физические процессы подавление опасных сигналов. Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование электрических, магнитных, и электромагнитных полей. Требования к экранам. Компенсация полей. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами.

Средства технической разведки. Визуально-оптические приборы. Фотоаппараты.

Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания. Автономные средства разведки.

Средства инженерной защиты и технической охраны. Методы и средства инженерной защиты и технической охраны объектов. Скрытие объектов наблюдения. Основные инженерные

конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны.

Согласована на портале № 49236

Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны.

Средства предотвращения утечки информации по техническим каналам. Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Скрытие речевой информации в каналах связи. Энергетическое скрытие акустических информативных сигналов.

Средства звукоизоляции из звукопоглощения. Обнаружение и локализация закладных устройств, подавление их сигналов. Подавление опасных сигналов акустоэлектрических преобразователей, экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземления и электропитания. Подавление опасных сигналов. Генераторы линейного и пространственного зашумления.

Государственная система защиты информации. Характеристика государственной системы противодействия технической разведке. Нормативные документы по противодействию технической разведке. Основные организационные и технические меры по защите информации.

Аттестация объектов, лицензирование деятельности по защите информации и сертификация ее средств.

Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности защиты информации. Основные положения методологии инженерно-технической защиты информации. Требования по защите информации от утечки по техническим каналам.

Методы расчета и инструментального контроля показателей защиты информации. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

Моделирование инженерно-технической защиты информации. Концепция и методы инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации.

Принципы оценки эффективности инженерно-технической защиты информации. Принципы оценки эффективности охраны объектов защиты. Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в защищаемых помещениях. Принципы оценки размеров опасных зон I и II.

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями	Тесты, письменные самостоятельные	Преимущественно письменная

Согласована на портале № 49236

слуха	работы, вопросы к зачету, контрольные работы	проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

14.3. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 49236