МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»
Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ
Декан _____ Буднев Н.М.
«22» апреля 2020 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.В.07 Дополнительные главы технической защиты информации**

Направление подготовки 10.03.01 Информационная безопасность

Направленность (профиль) подготовки №7Техническая защита информации

Квалификация выпускника бакалавр

Форма обучения очная

Согласовано с УМК физического факультета

Протокол № 25 от «21» апреля 2020 г.
Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 8
От «20» марта 2020 г.
И.О.Зав. кафедрой _____ Колесник С.Н.

Иркутск 2020 г.

Содержание

1. Цели и задачи дисциплины (модуля)

Цели освоения учебной дисциплины «Дополнительные главы технической защиты информации»**:**

1. Изучение технических каналов утечки информации, методов и способов технической защиты информации.

2. Формирование профессиональных знаний о проведении организационно-технических и технических мероприятий по защите информации, организации контроля эффективности создаваемых систем защиты.

Задачи освоения учебной дисциплины**:**

- анализ и оценка угроз информационной безопасности объекта информатизации;
- изучение отечественных и зарубежных стандартов в области информационной безопасности;
- изучение нормативных документов по защите информации;
- применение на практике методов анализа технических каналов утечки информации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Дополнительные главы технической защиты информации» является вариативной дисциплиной профессионального цикла. Дисциплина является вводной в проблематику побочных электромагнитных излучений и наводок. Взаимосвязь данной дисциплины через компетенции отражена в рабочем учебном плане и матрице компетенций. Дисциплина опирается на знания, полученные в ходе изучения дисциплин «Физика», «Информатика», «Распространение радиоволн», «Радиотехнические цепи и сигналы», «Антенно-фидерные устройства», «Основы построения и функционирования технических средств защиты информации», которая должна быть освоена полностью и студенты должны владеть навыками работы на ПЭВМ в любой современной операционной системе.

Дисциплина является предшествующей для таких дисциплин профессионального цикла как «Аттестация объектов информатизации», «Технико-экономическое обоснование и управление проектами», а так же для учебной и производственной практики и итоговой государственной аттестации. Изучение данной дисциплины позволяет приобрести первичные навыки, необходимые для изучения технической защиты информации

3. Требования к результатам освоения дисциплины (модуля)

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций:

ОПК-3.1. Способен проводить специальные исследования на побочные электромагнитные излучения и наводки технических средств обработки информации

ОПК-3.3. Способен проводить контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок.

В результате изучения дисциплины студент должен:

Знать:

- физические основы и источники побочных электромагнитных излучений и наводок технических средств обработки информации;

- принципы настройки и эксплуатации средств контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок;

Уметь:

- проводить специальные исследования на побочные электромагнитные излучения и наводки технических средств обработки информации;

- проводить контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок;

Владеть:

- навыками проведения специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации.

- навыками проведения контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок.

4. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	**Всего часов / зачетных единиц**	**Семестры**			
		7			
Аудиторные занятия (всего)	66/1,83	66/1,83			
В том числе:	-	-	-	-	-
Лекции	26/0,72	26/0,72			
Практические занятия (ПЗ)	12/0,33	12/0,33			
Семинары (С)					
Лабораторные работы (ЛР)	26/0,72	26/0,72			
КСР	2/0,06	2/0,06			
Контроль					
Самостоятельная работа (всего)	42/1,17	42/1,17			
В том числе:	-	-	-	-	-

Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
Другие виды самостоятельной работы	42/1,17	42/1,17			
Вид промежуточной аттестации (*зачет, экзамен*)	зачет	зачет			
Контактная работа (всего)	66/1,83	66/1,83			
Общая трудоемкость часы	108	108			
зачетные единицы	3	3			

5. Содержание дисциплины (модуля)

5.1. Содержание разделов и тем дисциплины (модуля). Все разделы и темы нумеруются

РАЗДЕЛ 1. Технические каналы утечки информации, обрабатываемой на объектах вычислительной техники.

a. Побочные электромагнитные излучения.
b. Наводки в линии электропитания и заземления.
c. Утечка информации по волоконно-оптическим линиям связи.

РАЗДЕЛ 2. Технические каналы утечки речевой информации.

a. Акустический и виброакустический каналы утечки.
b. Акустоэлектрические преобразования.
c. Высокочастотное облучение и высокочастотное навязывание.
d. Паразитная генерация.

РАЗДЕЛ 3. Побочные электромагнитные излучения и наводки ОТСС.

a. Источники ПЭМИН ОТСС.
b. Затухание электрической и магнитной составляющей электромагнитного поля.
c. Спектры информативных сигналов ОТСС.

РАЗДЕЛ 4. Методы оценки защищенности информации от утечки за счет ПЭМИН

a. Оценка радиусов зоны 2 и зоны 1.
b. Оценка затухания информативного сигнала в проводящих линиях.

РАЗДЕЛ 5. Акустический и виброакустический каналы утечки информации.

a. Основные характеристики речи и слуха.
b. Понятие о разборчивости речи.
c. Звуковое поле в помещении.
d. Формантная теория разборчивости речи.

РАЗДЕЛ 6. Оценка защищенности информации от утечки по акустическому и виброакустическому каналам

a. Расчет коэффициента звукоизоляции.
b. Расчет словесной разборчивости речи.

РАЗДЕЛ 7. Акустоэлектрические преобразования в ВТСС.

a. Природа акустоэлектрических преобразований в ВТСС.
b. ВТСС, наиболее подверженные акустоэлектрическим преобразованиям.

РАЗДЕЛ 8. Оценка защищенности информации от утечки за счет акустоэлектрических преобразований.

a. Оценка уровней сигналов акустоэлектрического преобразования.
b. Оценка разборчивости речи сигналов АЭП.

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

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№№ разделов (тем) данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин
1	Аттестация объектов информатизации	1-8
2	Технико-экономическое обоснование и управление проектами	1-8
3	Практика по получению первичных профессиональных умений и навыков	1-8
4	Эксплуатационная практика	1-8
5	Проектно-технологическая практика	1-8

5.3. Разделы и темы дисциплин (модулей) и виды занятий

№ п/п	Наименование раздела	Наименование темы	Виды занятий в часах					
			Лекц.	Практ. зан.	Семин	Лаб. зан.	СРС	Всего
1.	***Раздел 1***	Технические каналы утечки информации, обрабатываемой на объектах вычислительной техники	4	2		4	6	16
2.	***Раздел 2***	Технические каналы утечки речевой информации	4	2		4	6	16
3.	***Раздел 3***	Побочные электромагнитные излучения и наводки основных технических средств и систем	3	2		3	5	13
4.	***Раздел 4***	Методы оценки защищенности информации от утечки за счет ПЭМИН	3	1		3	5	12
5.	***Раздел 5***	Акустический	3	2		3	5	13

		и виброакустический каналы утечки информации						
6.	***Раздел 6***	Оценка защищенности информации от утечки по акустическому и виброакустическому каналам	3	1		3	5	12
7.	***Раздел 7***	Акустоэлектрические преобразования во вспомогательных технических средствах и системах	3	1		3	5	12
8.	***Раздел 8***	Оценка защищенности информации от утечки за счет акустоэлектрических преобразований	3	1		3	5	12

6. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)	Оценочные средства	Формируемые компетенции
1	**2**	**3**	**4**	**5**	**6**
1.	***Раздел 1***	Технические каналы утечки информации, обрабатываемой на объектах вычислительной техники	2	Собеседование, тест	ОПК-3.1., ОПК-3.3.
2.	***Раздел 2***	Технические каналы утечки речевой информации	2	Собеседование, тест	ОПК-3.1., ОПК-3.3.
3.	***Раздел 3***	Побочные электромагнитные излучения и наводки основных технических средств и систем	2	Собеседование, тест	ОПК-3.1., ОПК-3.3.
4.	***Раздел 4***	Методы оценки защищенности информации от утечки за счет ПЭМИН	1	Собеседование, тест	ОПК-3.1., ОПК-3.3.
5.	***Раздел 5***	Акустический и виброакустический каналы утечки информации	2	Собеседование, тест	ОПК-3.1., ОПК-3.3.

6.	***Раздел 6***	Оценка защищенности информации от утечки по акустическому и виброакустическому каналам	1	Собеседование, тест	ОПК-3.1., ОПК-3.3.
7.	***Раздел 7***	Акустоэлектрические преобразования во вспомогательных технических средствах и системах	1	Собеседование, тест	ОПК-3.1., ОПК-3.3.
8.	***Раздел 8***	Оценка защищенности информации от утечки за счет акустоэлектрических преобразований	1	Собеседование, тест	ОПК-3.1., ОПК-3.3.
9	***Разделы 1, 3, 4***	Лабораторная работа №1. Побочные электромагнитные излучения средств вычислительной техники. Меры и средства защиты информации от утечки по каналу ПЭМИ	9	Защита лабораторной работы	ОПК-3.1., ОПК-3.3.
10	***Разделы 2, 5, 6***	Лабораторная работа №2. Экспериментально-расчетная оценка коэффициентов звуко- и виброизоляции	9	Защита лабораторной работы	ОПК-3.1., ОПК-3.3.
11	***Разделы 7, 8***	Лабораторная работа №3. Оценка защищенности технических средств от утечки информации по каналам акустоэлектрических преобразований	8	Защита лабораторной работы	ОПК-3.1., ОПК-3.3.

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-3	Технические каналы утечки информации, обрабатываемой на объектах вычислительной техники	Самостоятельное изучение теоретического материала	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	Основная литература	6
4-6	Технические каналы утечки речевой информации	Самостоятельное изучение теоретического материала	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта	Учебный сайт	6

			лекций, литературы, Интернет - ресурсов		
7-9	Побочные электромагнитные излучения и наводки основных технических средств и систем	Самостоятельное изучение теоретического материала	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	Учебный сайт	5
10,11	Методы оценки защищенности информации от утечки за счет ПЭМИН	Самостоятельное изучение теоретического материала	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	Учебный сайт	5
12-15	Акустический и виброакустический каналы утечки информации	Самостоятельное изучение теоретического материала	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	Учебный сайт	5
16,17	Оценка защищенности информации от утечки по акустическому и виброакустическому каналам	Самостоятельное изучение теоретического материала	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	Учебный сайт	5

18	Акустоэлектрические преобразования во вспомогательных технических средствах и системах	Самостоятельное изучение теоретического материала	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов		5

6.2. Методические указания по организации самостоятельной работы студентов

Текущая самостоятельная работа по дисциплине «Дополнительные главы технической защиты информации», направленная на углубление и закрепление знаний студента, на развитие практических умений, включает в себя следующие виды работ:

- работа с лекционным материалом;
- подготовка к практическим занятиям;
- выполнение индивидуальных проектов;
- подготовка к лабораторным работам;
- подготовка к зачету.

Творческая проблемно-ориентированная самостоятельная работа по дисциплине «Дополнительные главы технической защиты информации», направленная на развитие интеллектуальных умений, общекультурных и профессиональных компетенций, развитие творческого мышления у студентов, включает в себя следующие виды работ по основным проблемам курса:

- поиск, анализ, структурирование информации;
- выполнение графических работ, обработка и анализ данных;
- участие в конференциях, олимпиадах и конкурсах.

Оценка результатов самостоятельной работы организуется как единство двух форм: самоконтроль и контроль со стороны преподавателя.

Самоконтроль зависит от определенных качеств личности, ответственности за результаты своего обучения, заинтересованности в положительной оценке своего труда, материальных и моральных стимулов, от того насколько обучаемый мотивирован в достижении наилучших результатов. Задача преподавателя состоит в том, чтобы создать условия для выполнения самостоятельной работы (учебно-методическое обеспечение), правильно использовать различные стимулы для реализации этой работы (рейтинговая

система), повышать её значимость, и грамотно осуществлять контроль самостоятельной деятельности студента (фонд оценочных средств).

7. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля):

1. Стукалов С.Б. Защита информации от утечки по техническим каналам радиоэлектронных систем: учебное пособие. / С.Б. Стукалов. — Воронеж: ООО «МИР», 2019. — 64 с. ISBN 978-5-6042751-5-3.
http://storage.mstuca.ru:8080/xmlui/handle/123456789/8421

2. Ефанов В.И., Тихомиров А.А. Защита информации от утечки по техническим каналам радиоэлектронных средств и систем. Учебное пособие. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2012. – 228 с. - ISBN 5- 86889-188-0.
https://edu.tusur.ru/publications/748/download

3. Малков, Н.А. Защита информации от утечки по техническим каналам радиоэлектронных средств :
учеб. пособие / Н.А. Малков, А.П. Пудовкин. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2007. – 88 с. – ISBN 978-5-8265-0659-2. https://www.tstu.ru/book/elib/pdf/2007/malkov_.pdf

4. Пудовкин, А.П. Защита информации от утечки по техническим каналам и помехозащищённость РЭС :
учебное пособие / А.П. Пудовкин, Ю.Н. Панасюк, Т.И. Чернышова. – Тамбов : Изд-во ФГБОУ ВПО «ТГТУ», 2013. – 92 с. – ISBN 978-5-8265-1194-7.
https://www.tstu.ru/book/elib2/pdf/2013/pudovkin3.pdf

б) базы данных, информационно-справочные и поисковые системы

1. Поисковые системы Google, Yandex.
2. Электронные ресурсы доступные по логину и паролю, предоставляемые Научной библиотекой ИГУ.

9. Материально-техническое обеспечение дисциплины (модуля)

Лаборатория 313 и лекционная аудитория 225, оснащенные мультимедийными средствами.

Учебно-лабораторное оборудование:

Чтение лекций сопровождается демонстрацией информации (мультимедийный проектор, офисное оборудование для оперативного размножения иллюстративного и раздаточного лекционного материалов).

В ходе лабораторных работ задействовано следующее оборудование:

1. Селективный микровольтметр SMV-8.
2. Измерительная антенна электрическая АИ 5-0.
3. Персональный компьютер, используемый в качестве источника ПЭМИ.
4. Измеритель шума и вибраций СКМ-21 с микрофоном и акселерометром.
5. Генератор тестового шума.
6. Акустическая колонка.

7. Селективный микровольтметр В6-9.
8. Генератор низкочастотных сигналов Г3/112.
9. Усилитель.
10. Акустический излучатель.

Программное обеспечение:

1. Microsoft PowerPoint
2. Microsoft Windows.
3. Сборник тестовых программ для выполнения лабораторных работ.

10. Образовательные технологии

Для достижения планируемых результатов обучения, в дисциплине «Дополнительные главы технической защиты информации» используются различные образовательные технологии:

Информационно-развивающие технологии, направленные на формирование системы знаний, запоминание и свободное оперирование ими.

Используется лекционно-семинарский метод, самостоятельное изучение литературы, применение новых информационных технологий для самостоятельного пополнения знаний, включая использование технических и электронных средств информации.

Деятельностные практико-ориентированные технологии, направленные на формирование системы профессиональных практических умений при проведении экспериментальных исследований, обеспечивающих возможность качественно выполнять профессиональную деятельность.

Используется анализ, сравнение методов проведения химических исследований, выбор метода, в зависимости от объекта исследования в конкретной производственной ситуации и его практическая реализация.

Развивающие проблемно-ориентированные технологии, направленные на формирование и развитие проблемного мышления, мыслительной активности, способности видеть и формулировать проблемы, выбирать способы и средства для их решения. Используются виды проблемного обучения: освещение основных проблем общей и неорганической химии на лекциях, учебные дискуссии, коллективная деятельность в группах при выполнении лабораторных работ, решение задач повышенной сложности. При этом используются первые три уровня (из четырех) сложности и самостоятельности: проблемное изложение учебного материала преподавателем; создание преподавателем проблемных

ситуаций, а обучаемые вместе с ним включаются в их разрешение; преподаватель создает проблемную ситуацию, а разрешают её обучаемые в ходе самостоятельной деятельности.

Личностно-ориентированные технологии обучения, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе. Личностно-ориентированные технологии обучения реализуются в результате индивидуального общения преподавателя и студента при защите лабораторных работ, при выполнении домашних индивидуальных заданий, решении задач повышенной сложности, на еженедельных консультациях.

11. Оценочные средства (ОС):

11.1. Оценочные средства для входного контроля

Не предусмотрено

11.2. Оценочные средства текущего контроля

Вопросы к практическим занятиям (8 тем). Представляют собой перечень вопросов, проверяющих знание теоретического лекционного материала и тем, вынесенных на самостоятельную проработку:

1. Технические каналы утечки информации, обрабатываемой на объектах вычислительной техники.
2. Технические каналы утечки речевой информации.
3. Побочные электромагнитные излучения и наводки основных технических средств и систем.
4. Методы оценки защищенности информации от утечки за счет ПЭМИН.
5. Акустический и виброакустический каналы утечки информации.
6. Оценка защищенности информации от утечки по акустическому и виброакустическому каналам.
7. Акустоэлектрические преобразования во вспомогательных технических средствах и системах.
8. Оценка защищенности информации от утечки за счет акустоэлектрических преобразований**.**

11.3. Оценочные средства для текущего контроля в форме тестирования

Представляют собой тестовые работы, проверяющих знание теоретического лекционного материала и тем, вынесенных на самостоятельную проработку:

Демонстрационный вариант теста №1

1) К средствам вычислительной техники относятся:
Программное беспечение
Техническое обеспечение
Канал связи

2) К техническим средствам обработки информации относятся:
ПК, проектор, принтер

ПК, программное обеспечение, канал связи
Локальная сеть, Интернет, радиоканалы
Система сигнализации, система электроосвещения, электроприборы

3) К вспомогательным техническим средствам НЕ относятся
Системы сигнализации
Электроприборы
Системы электроосвещения
Вычислительная техника

4)Объект средств вычислительной техники состоит из
Технических средств
Вспомогательных технических средств
Технических и вспомогательных средств
Технических, вспомогательных средств, системы электропитания, заземления

5)Физическая среда несанкционированного распространения информации от источника к нарушителю называется
Каналом утечки информации
Утечкой информации
Взломом информации
Каналом связи

6)К элементам технического канала утечки информации НЕ относятся
Источник информации
Программное обеспечение
Техническое средство разведки
Среда распространения информации

7)Акустический канал утечки информации состоит из следующих элементов
Источник видовой информации – Среда распространения сигнала – Оптический приемник информации
Источник цифровой информации – Среда распространения сигнала – Приемник цифровой информации
Источник звуковой информации – среда распространения сигнала – приемник звуковой информации
Источник сигнала – Среда распространения сигнала – Приемник сигнала

8)К среде распространения акустической информации относятся
Разговор, колонки, наушники
Микрофон, диктофон
Локальная сеть, интернет, радиоканал
Воздух, жидкости, твердые тела

9)Оптический канал утечки информации состоит из следующих элементов
Источник сигнала – Среда распространения сигнала – Приемник сигнала
Источник звуковой информации – среда распространения сигнала – приемник звуковой информации
Источник видовой информации – Среда распространения сигнала – Оптический приемник информации
Источник цифровой информации – Среда распространения сигнала – Приемник цифровой информации

10)Приемником оптической информации может выступать
Микрофон, диктофон, стетоскоп
Фотоаппарат, тепловизор, приборы ночного видения
Монитор, проектор, телевизор
Колонки, наушники

11)Возможна ли утечка информации из оптического волокна
Только при подключении к оптическому волокну
Нет
Только при установке фотодетектора непосредственно на самом кабеле
Только при подключении фотодетектора на изгибе кабеля

12)Зависимость от времени суток влияет на … канал утечки информации
Акустический
Оптический
Радиоэлектронный
На все перечисленные

13)Радиоэлектронный канал утечки информации состоит из следующих элементов
Источник сигнала – Среда распространения сигнала – Приемник сигнала
Источник звуковой информации – среда распространения сигнала – приемник звуковой информации
Источник видовой информации – Среда распространения сигнала – Оптический приемник информации
Источник цифровой информации – Среда распространения сигнала – Приемник цифровой информации

14)Источником радиоэлектронного канала утечки информации являются
Разговор, колонки
Объекты отражающие и излучающие внешний свет
Передающие устройства, объекты отражающие излучение
Воздух, космос, направляющие линии (например, кабели электропитания)

15)Найдите соответствие
1.экранирование
2.рассеивание
3.зашумление
Варианты ответов
Ослабление носителя информации (сигнала) различными способами
Создание дополнительного воздействия на носитель информации (сигнал), создающем маскирующие информацию помехи
Создание непреодолимого для носителя информации (сигнала) барьера между источником и средой распространения

16)К правовым методам, обеспечивающим информационную безопасность, относятся:
Разработка аппаратных средств обеспечения правовых данных
Разработка и установка во всех компьютерных правовых сетях журналов учета действий

Разработка и конкретизация правовых нормативных актов обеспечения безопасности

17) Основными источниками угроз информационной безопасности являются все указанное в списке:
Хищение жестких дисков, подключение к сети, инсайдерство
Перехват данных, хищение данных, изменение архитектуры системы
Хищение данных, подкуп системных администраторов, нарушение регламента работы

18) Виды информационной безопасности:
Персональная, корпоративная, государственная
Клиентская, серверная, сетевая
Локальная, глобальная, смешанная

19) Цели информационной безопасности – своевременное обнаружение, предупреждение:
несанкционированного доступа, воздействия в сети
инсайдерства в организации
чрезвычайных ситуаций

20) Основные объекты информационной безопасности:
Компьютерные сети, базы данных
Информационные системы, психологическое состояние пользователей
Бизнес-ориентированные, коммерческие системы

21) Основными рисками информационной безопасности являются:
Искажение, уменьшение объема, перекодировка информации
Техническое вмешательство, выведение из строя оборудования сети
Потеря, искажение, утечка информации

22) К основным принципам обеспечения информационной безопасности относится:
Экономической эффективности системы безопасности
Многоплатформенной реализации системы
Усиления защищенности всех звеньев системы

23) Основными субъектами информационной безопасности являются:
руководители, менеджеры, администраторы компаний
органы права, государства, бизнеса
сетевые базы данных, фаерволлы

24) К основным функциям системы безопасности можно отнести все перечисленное:
Установление регламента, аудит системы, выявление рисков
Установка новых офисных приложений, смена хостинг-компании
Внедрение аутентификации, проверки контактных данных пользователей

25) Принципом информационной безопасности является принцип недопущения:
Неоправданных ограничений при работе в сети (системе)
Рисков безопасности сети, системы
Презумпции секретности

26) Принципом политики информационной безопасности является принцип:
Невозможности миновать защитные средства сети (системы)
Усиления основного звена сети, системы
Полного блокирования доступа при риск-ситуациях

27) Принципом политики информационной безопасности является принцип:

Усиления защищенности самого незащищенного звена сети (системы)
Перехода в безопасное состояние работы сети, системы
Полного доступа пользователей ко всем ресурсам сети, системы

28) Принципом политики информационной безопасности является принцип:
Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
Одноуровневой защиты сети, системы
Совместимых, однотипных программно-технических средств сети, системы

29) К основным типам средств воздействия на компьютерную сеть относится:
Компьютерный сбой
Логические закладки («мины»)
Аварийное отключение питания

30) Когда получен спам по e-mail с приложенным файлом, следует:
Прочитать приложение, если оно не содержит ничего ценного – удалить
Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
Удалить письмо с приложением, не раскрывая (не читая) его

11.4. Оценочные средства для промежуточной аттестации

(в форме зачета).

Проверяется степень усвоения теоретических и практических знаний, приобретенных умений на репродуктивном и продуктивном уровне.

Примерный перечень вопросов и заданий к зачету

1. Электромагнитное поле и уравнения Максвелла.
2. Поле элементарного электрического и магнитного излучателя.
3. Поле в ближней и дальней волновой зоне. Диаграмма направленности.
4. Границы ближней и дальней волновой зоны. Промежуточная зона.
5. Широкополосный и узкополосный приемники сигнала.
6. Спектральные характеристики сигналов.
7. Спектр сигнала. Спектр одиночного импульса.
8. Спектр последовательности импульсов. Зависимость спектра от параметров сигнала.
9. Режимы работы технических средств, спектры тестовых сигналов: VGA, DVI, LVDS.
10. Режимы работы технических средств, спектры тестовых сигналов: клавиатуры PS/2 и USB.
11. Режимы работы технических средств, спектры тестовых сигналов: USB, USB 2.0 LS, FS, HS.
12. Режимы работы технических средств, спектры тестовых сигналов: SATA I, II, III.
13. Наводки информативных сигналов на линии ВТСС, цепи питания и заземления, каналы утечки.
14. Оценка защищенности информации от утечки за счет ПЭМИ.
15. Меры защиты информации от утечки за счет ПЭМИ.
16. Оценка эффективности защиты информации от утечки за счет ПЭМИ.
17. Утечка информации за счет паразитных связей внутри ОТСС.
18. Меры защиты цепей питания и заземления.
19. Строение уха и восприятие звука, порог слышимости и болевой порог.

20. Звуковое поле в помещении, диффузное поле и акустическое отношение, основные параметры звукового поля в помещении.
21. Акустические параметры ограждающих конструкций помещения, коэффициенты отражения, поглощения, проводимости.
22. Расчет звукоизоляции помещения и перегородки.
23. Речеобразование, параметры речи.
24. Разборчивость речи. Виды разборчивости речи.
25. Формантная разборчивость речи.
26. Расчет разборчивости речи.
27. Утечка информации за счет акустоэлектрических преобразований.
28. Защита слаботочных линий связи.

Разработчики:

доцент (занимаемая должность) Марков В.П. (Ф.И.О.)

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ПООП по направлению и профилю подготовки **10.03.01 Информационная безопасность**.

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «20» 03 2020 г. Протокол № 8

И.о.зав. кафедрой  Колесник С.Н.