МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

МАТЕМАТИЧЕСКИЕ И ФИЗИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность
Код и наименование направления подготовки/специальности

«Организация и технология защиты информации
(по отрасли или в сфере профессиональной деятельности)»
Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

МАТЕМАТИЧЕСКИЕ И ФИЗИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ
Рабочая программа дисциплины

Составитель(и):
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

Ответственный редактор:
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин
……

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№8 от 23.03.2023

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины –изучение физических особенностей информативных сигналов акустической, электромагнитной, оптической и ядерной природы, являющихся основой для формирования технических каналов утечки информации, обучение студентов основным принципам и подходам к использованию математического аппарата для криптографической и комплексной защиты информации.

Задачи дисциплины:

- дать знанияпо физическим принципам и техническим основам формирования и функционирования акустических (речевых) каналов утечки информации, каналов утечки информации на основе побочных электромагнитных излучений и наводкам, оптических каналов утечки информации, каналов утечки информации на базе ядерных излучений;
- научить определять и учитывать качественные и количественные особенности составляющих криптографической и комплексной защиты информации;
- сформировать у студентов представления о механизмах смены параметров криптографической защиты;
- научить решать основополагающие теоретико-практические задачи защиты информации с применением необходимого математического аппарата и сформировать математический подход к их решению;
- ознакомить студентов с математическими основами криптографических методов защиты компьютерной информации;
- ознакомить студентов с основными математическими принципами алгоритмов создания электронной цифровой подписи;
- ознакомить студентов с основными принципами построения систем комплексной защиты информации.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-2 *Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач*	*ПК-2.1* *Знать архитектуру и принципы построения операционных систем, подсистем защиты информации, состав типовых конфигураций программно-аппаратных средств защиты информации, языки и системы программирования*	*Знать:* – *основные свойства и особенности распространения акустических и электромагнитных волн и потоков радиоактивных излучений;* – *основы акустики помещений, человеческой речи и слуха;* – *принципы электромагнитного экранирования и звукоизоляции помещений;* – *принципы работы и устройства источников и приемников электромагнитных, звуковых волн и потоков радиоактивных излучений*
	ПК-2.2 *Умеет*	*Уметь:* – *применять полученные знания при*

	противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации	*освоении последующих базовых дисциплин, спецкурсов и при решении практических задач организации защиты информации на объектах;* – *делать обоснованные выводы по результатам измерений;* – *самостоятельно работать с технической и справочной литературой*
	ПК-2.3 *Владеет контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах*	*Владеть:* – *методами проведения физических измерений, методами корректной оценки погрешностей измерений и расчётов*
ПК-11 *Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов*	*ПК-11.1* *Знает методики проведения теоретических исследований уровней защищённости информационной безопасности объектов и систем*	*Знать:* – *основные понятия, методы, принципы, подходы, алгоритмы и приёмы криптографии и комплексной защиты информации.*
	ПК-11.2 *Умеет составлять и оформлять аналитический отчёт по проведённым испытаниям, делать выводы по оценке защищённости на основании аналитического отчёта*	*Уметь:* – *применять основные методы, принципы, подходы, алгоритмы и приёмы криптографии и комплексной защиты информации с необходимыми формулами для решения профессиональных математических задач*
	ПК-11.3 *Владеет навыками использования профиля защиты и задания по безопасности, формулирования выводов по оценке защищённости*	*Владеть:* – *основными подходами к постановке и решению задач, навыками математического описания профессиональных прикладных задач*

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Математические и физические основы защиты информации» относится к части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Физика», «Электротехника», «Электроника и схемотехника», «Математический анализ», «Теория вероятностей и

математическая статистика», «Линейная алгебра и аналитическая геометрия», «Дискретная математика».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Сети и системы передачи информации», «Методы и средства криптографической защиты информации», «Программно-аппаратные средства защиты информации», «Методы и средства защиты информации от утечки по техническим каналам».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 5з.е., 180академическихчаса.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
4	Лекции	**22**
4	Практические занятия	**24**
Всего:		**46**
5	Лекции	**28**
5	Практические занятия	**32**
Всего:		**60**
Итого:		**106**

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 74 академических часа.

3. Содержание дисциплины

Тема 1. Физические основы информатики

Понятие информации: свойства, описание, меры, мера Хартли, формула Шеннона, принцип Ландауэра, выражение Шеннона-фон Неймана-Ландауэра;

Измерительная информация: процедура измерения, характеристики измерителя, оценка объема измерения, повышение точности;

Носитель информации и информационные процессы: вещественный и полевой носитель, процессы записи/считывания, характеристика систем;

Шумы и их влияние на информационные процессы: характеристика шумов, мультипликативный и аддитивный шум, шумы систем;

Физические основы технических каналов утечки информации: определения, характеристика, классификация, задачи ТСЗИ;

Тема 2. Акустический сигнал

Упругость среды и упругие волны: механические деформации, упругость объёма и формы, упругие волны и их типы (продольные и поперечные), спектр, акустическое поле

Характеристики акустического поля.

Возбуждение акустических волн, излучатели.

Детектирование акустического поля в воздухе и газовых средах, в жидкостях и твёрдых телах.

Волны в свободном пространстве. Акустические волны в ограниченном пространстве.

Акустические волны источники информации. Акустика помещений.

Акустические каналы утечки информации.

Тема 3. Электромагнитное излучение

Электромагнитное поле и его характеристики: силовые характеристики, уравнения Максвелла, волновой пакет, структура волны, поляризация, энергия и интенсивность, поглощение;

Физическая среда в распространении электромагнитной волны. Излучение и приём электромагнитных волн.

Свободное распространение электромагнитных волн. Распространение электромагнитных волн в атмосфере Земли. Электромагнитные волноводы.

Электромагнитные каналы утечки информации и методы борьбы.

Особенности оптического излучения. Источники и приёмники оптического излучения.

Оптические приборы. Приборы визуального наблюдения.

Системы технического зрения: конструкция цифровых систем регистрации изображения, ПЗС- и КМОП-матрица, тепловизор и прибор ночного видения;

Распространение света в атмосфере: излучение Солнца, атмосфера Земли, распространение света в атмосфере,

Оптическое излучение как источник информации: визуальные и оптические ТКУИ – классификация и характеристика;

Оптические волноводы: локализация и каналирование света в волноводе, конструкция световодов - оптоволокно, дырчатые волокна, основные параметры оптоволокон, применение волоконной техники;

Утечка информации через волоконно-оптические системы и сети;

Тема 4. Основы одноключевых криптосистем

Основные понятия и определения криптографии. Обобщённая модель симметричной криптосистемы. Принцип (правило) Кёркхоффа и его применение к одноключевым криптосистемам. Классификация методов шифрования информации. Криптозащита: при хранении информации, при передаче информации по каналу связи. Шифры простой замены; шифрующие таблицы Трисемуса. Шифры сложной замены; шифр Гронсфельда, система шифрования Вижинера, шифр “двойной квадрат” Уитстона. Шифрование перестановкой; использование маршрутов Гамильтона. Примеры.

Тема 5. Обратимость и теоретико-числовые основы криптографии

Обратимость как важное свойство, используемое в криптографии. Операция mod и её применение в задачах защиты информации. Алгоритм Евклида для отыскания наибольшего общего делителя. Вычисление обратных величин. Расширенный алгоритм Евклида и его применение. Конечные поля. Поле Галуа. Вычеты, кольца вычетов. Решение сравнений и систем сравнений. Функция Эйлера, теорема Эйлера. Понятие дискретного логарифма

Тема 6. Основы двухключевых криптосистем

Понятие о двухключевых асимметричных (несимметричных) криптосистемах. Обобщённая модель асимметричной криптосистемы в сравнении с симметричной криптосистемой. Понятия односторонней (однонаправленной) хеш-функции и электронной цифровой подписи и основные требования к ним. АлгоритмRSA и возможности его применения в двух режимах: шифрования (криптозащиты) и электронной цифровой подписи (ЭЦП)

Тема 7. Понятие о схемах разделения секрета и (древне)китайская теорема об остатках

(Древне)китайская теорема об остатках и возможности её использования в целях защиты информации. Задача о безопасном сохранении числового ключа между двумя компаньонами. Понятие совершенной схемы разделения секрета (совершенной СРС).

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебной работы	Образовательные технологии
1	2	3	4
1.	Физические основы информатики	Лекция 1.	Лекция с использованием компьютерной презентации в виде слайдов
		Практические занятия	Выполнение практической работы
2.	Акустический сигнал	Лекция 2.	Лекция с использованием компьютерной презентации в виде слайдов
		Практические занятия	Выполнение практической работы
3.	Электромагнитное излучение	Лекция3-4.	Лекция с использованием компьютерной презентации в виде слайдов
		Практические занятия	Выполнение практической работы
4.	Основы одноключевых криптосистем	Лекция 5.	Лекция с использованием компьютерной презентации в виде слайдов
		Практические занятия	Выполнение практической работы
5.	Обратимость и теоретико-числовые основы криптографии	Лекция 6.	Лекция с использованием компьютерной презентации в виде слайдов
		Практические занятия	Выполнение практической работы
6.	Основы двухключевых криптосистем	Лекция 7.	Лекция с использованием компьютерной презентации в виде слайдов
		Практические занятия	Выполнение практической работы в физическомпрактикуме
7.	Понятие о схемах разделения секрета и (древне)китайская теорема об остатках	Лекция 8.	Лекция с использованием компьютерной презентации в виде слайдов
		Практические занятия	Выполнение практической работы в физическомпрактикуме

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	Макс. количество баллов	
	За одну	Всего

	работу	
Текущий контроль:		
- выполнение практической работы 1	*6 баллов*	*6 баллов*
- выполнение практической работы 2…7	*9 баллов*	*54 балла*
Промежуточная аттестация – зачёт с оценкой (вопросы по билетам)	*40 баллов*	*40 баллов*
Итого за семестр		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (EuropeanCreditTransferSystem; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 –67	удовлетворительно		D
50 –55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично/ зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо/ зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
67-50/ D,E	удовлетво-рительно/ зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлет-ворительно/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Образцы тестовых заданий для реализации компетенций ПК-2 и ПК-11.

01. Упругие деформации являются
+обратимыми изменениями размеров/формы тела;
-необратимыми изменениями размеров/формы тела;
-пластичными изменениями размеров/формы тела;
-невосстанавливаемыми изменениями размеров/формы тела;

02. Проволока из алюминия с модулем упругости Юнга $7 \cdot 10^{10}$ Па длиной 10 м и поперечным сечением 10^{-6} м2 растягивается с силой 70 Н, тогда удлинение проволоки составит:
-0,7 см;
-1 см;
+10 см;
-70 см;

03. Шифр Виженера является
-шифром простой замены;
+шифром сложной замены;
-шифром перстановки;

Контрольные вопросы к зачету с оценкой для проверки сформированности компетенций ПК-2 и ПК-11.

1. Упругость среды и упругие волны.
2. Характеристики акустического поля.

3. Возбуждение акустических волн, излучатели
4. Детектирование акустического поля в воздухе и газовых средах
5. Детектирование акустического поля в жидкостях и твердых телах
6. Волны в свободном пространстве
7. Акустические волны в ограниченном пространстве
8. Акустические волны источники информации
9. Психофизические основы восприятия звуков человеком
10. Акустика помещений
11. Акустические каналы утечки информации
12. Методы защиты от утечки по акустическим каналам
13. Электромагнитное поле и его характеристики
14. Физическая среда в распространении электромагнитной волны
15. Излучение и прием электромагнитных волн
16. Свободное распространение электромагнитных волн
17. Распространение электромагнитных волн в атмосфере Земли
18. Электромагнитные волноводы
19. Электромагнитные каналы утечки информации и методы борьбы
20. Особенности оптического излучения
21. Источники и приемники оптического излучения
22. Приборы визуального наблюдения
23. Психофизические основы визуального восприятия человека (зрение
24. Распространение света в атмосфере
25. Оптические волноводы
26. Оптическое излучение как источник информации
27. Понятие ключа шифрования, принцип (правило) Кёркхоффа и его применение к одноключевым криптосистемам.
28. Алгоритм Евклида и его применение.
29. Обратимость как важное свойство, используемое в криптографии. Вычисление обратных величин. Расширенный алгоритм Евклида и его применение.
30. Основы одноключевых криптосистем.
31. Шифр Трисемуса и шифр Гронсфельда, примеры.
32. Шифр Гронсфельда и алгоритм RSA.
33. Шифр "двойной квадрат" Уитстона и шифр Гронсфельда, примеры.
34. Шифр Вижинера и шифр Гронсфельда.
35. Матричный (аналитический) метод шифрования-дешифрования.
36. Асимметричные криптосистемы.
37. Криптосистема (алгоритм) RSA.
38. Функция Эйлера и её применение в криптосистеме (алгоритме) RSA.
39. Задача факторизации и криптосистема (алгоритм) RSA.
40. (Древне)китайская теорема об остатках и возможности её использования в целях защиты информации.
41. Операция mod и её использование в криптографии.
42. Вычисление обратных величин.
43. Отличие между криптосистемой и схемой разделения секрета, примеры.
44. Односторонняя функция, заложенная в основу криптосистемы RSA.
45. Схема разделения секрета на основе (древне)китайской теоремы об остатках.
46. Возможности представления компьютерных программ графами: области отладки программы и их сравнительная характеристика.
47. Понятия кольца, вычета, поля Галуа.
48. Модель безопасности Белла-Лападула и возможные направления её совершенствования.
49. Модель “Китайской стены” (Брюэра и Нэша).
50. Шифрование маршрутами Гамильтона.

51. Решение сравнений.
52. Решение систем сравнений.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Литература

Основная

1. Сагдеев, К. М. Физические основы защиты информации : учебное пособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. — 2-е изд., испр. и доп. — Санкт-Петербург : Интермедия, 2017. — 408 с. — ISBN 978-5-4383-0141-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161382. — Режим доступа: для авториз. пользователей.
2. Конспект лекций по курсу Математические основы защиты информации и информационной безопасности : учебное пособие / составители Б. Н. Воронков, Ю. А. Крыжановская. — Воронеж : ВГУ, 2017. — 77 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/154771. — Режим доступа: для авториз. пользователей.
3. Коржик, В. И. Основы криптографии : учебное пособие / В. И. Коржик, В. П. Просихин, В. А. Яковлев. — Санкт-Петербург :СПбГУТ им. М.А. Бонч-Бруевича, 2014. — 277 с. — ISBN 978-5-89160-097-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/181501. — Режим доступа: для авториз. пользователей.

Дополнительная

4. Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161337. — Режим доступа: для авториз. пользователей.
5. Рацеев, С. М. Математические методы защиты информации и их основы. Сборник задач / С. М. Рацеев. — Санкт-Петербург : Лань, 2023. — 140 с. — ISBN 978-5-507-45197-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/292913. — Режим доступа: для авториз. пользователей.

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Необходимо добавить то, что необходимо для изучения дисциплины

1. Журнал “Прикладная дискретная математика”:http://journals.tsu.ru/pdm/&journal_page=archive;
2. Журнал “Математические вопросы криптографии”: http://www.mathnet.ru/php/archive.phtml?jrnid=mvk&wshow=contents&option_lang=rus .
3. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс] / Проект Российского фонда фундаментальных исследований – Режим доступа:http://elibrary.ru, свободный. – Загл. с экрана.
4. «Лекторий Физтеха» [Электронный ресурс] / Проект Московского физико-технического института (Физтеха). – Режим доступа: http://lectoriy.mipt.ru/, свободный. – Загл. с экрана.
5. «Универсариум» — открытая система электронного образования. [Электронный ресурс] / ООО «КУРСАРИУМ» – Режим доступа: https://universarium.org/, свободный. – Загл. с экрана.
6. Национальная электронная библиотека (НЭБ) www.rusneb.ru
7. ELibrary.ru Научная электронная библиотека www.elibrary.ru

8. Электронная библиотека Grebennikon.ruwww.grebennikon.ru

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:
1. Windows
2. MicrosoftOffice
3. Foxit PDF reader
4. Kaspersky Endpoint Security

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

2) для проведения практическихзанятий– специализированная аудитория (учебная лаборатория), оборудованная техническими средствами для проведения
практических работ по ТЕМЕ_2_Акустическому сигналу

№	Оборудование
ПР_1.1.	Учебная экспериментальная установка
ПР_1.2.	Учебная экспериментальная установка
ПР_1.3.	Учебная экспериментальная установка

практическихработ по ТЕМЕ_3_Электромагнитному сигналу

№	Оборудование
ПР_2.1.	Учебная экспериментальная установка
ПР_2.2.	Учебная экспериментальная установка
ПР_2.3.	Учебная экспериментальная установка
ПР_3.1.	Учебная экспериментальная установка
ПР_3.2.	Учебная экспериментальная установка
ПР_3.3.	Учебная экспериментальная установка

Для остальных практических работ – компьютерный класс с ПО MS Office

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительныеметоды обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата:лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением;экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:устройством для сканирования и чтения с камерой SARA CE;дисплеем Брайля PAC Mate 20;принтером Брайля EmBrailleViewPlus;
- для глухих и слабослышащих:автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:передвижными, регулируемыми эргономическими партами СИ-1;компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы практических занятий

ТЕМА1 Физические основы информатики

ТЕМА2 Акустика

Практическая работа_1. Влияние различных факторов на разборчивость речи

Практическая работа_2. Виброакустический канал утечки речевой информации

Практическая работа_3.

ТЕМА3 Электромагнитное излучение

Практическая работа_1. Побочные электромагнитные излучения электрических кабельных систем

Практическая работа_2. Определение зоны разведдоступности по побочным электромагнитным излучениям настольного компьютера

Практическая работа_3.

Практическая работа_4. Паразитные акустические модуляции и наводки в элементах волоконно-оптических сетей: А. спектральный анализ.

Практическая работа_5. Паразитные акустические модуляции и наводки в элементах волоконно-оптических сетей: В. анализ артикуляционным методом.

Практическая работа_6.

Методические указания к практическим работам 1…3 приведены в отдельном документе.

Тема 4. Основы одноключевых криптосистем

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, методы, модели, критерии и показатели для решения задач дисциплины, оформив в виде таблиц для каждого случая.

2. Научиться оценивать границы применимости основных подходов, приёмов, алгоритмов, методов, моделей, критериев и показателей для решения задач дисциплины – её разделов “Математический аппарат, используемый в криптографии” и “Математический аппарат для задач комплексной защиты информации”.

Тема 5 Обратимость и теоретико-числовые основы криптографии

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, методы, модели, критерии и показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Оценить границы применимости основных подходов, приёмов, алгоритмов, методов, моделей, критериев и показателей для решения задач по теме занятия.

3. Обсудить и проанализировать основные подходы к решению задач по теме занятия.

4. Попрактиковаться в грамотной постановке задач, учитывающих особенности комплексной защиты объектов информатизации, соотносящихся с изучаемой дисциплиной, с учётом основных требований выпускающей кафедры “Комплексная защита информации”.

Тема 6. Основы двухключевых криптосистем

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, методы, модели, критерии и показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Оценить границы применимости основных подходов, приёмов, алгоритмов, методов, моделей, критериев и показателей для решения задач по теме занятия.

3. Обсудить и проанализировать основные подходы к решению задач по теме занятия.

4. Попрактиковаться в грамотной постановке задач, учитывающих особенности комплексной защиты объектов информатизации, соотносящихся с изучаемой дисциплиной, с учётом основных требований выпускающей кафедры “Комплексная защита информации”.

Тема 7. Понятие о схемах разделения секрета и (древне)китайская теорема об остатках

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, способы, критерии и показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Оценить границы применимости основных подходов, приёмов, алгоритмов, методов, моделей, критериев и показателей для решения задач по теме занятия.

3. Обсудить и проанализировать основные подходы к решению задач по теме занятия.

4. Попрактиковаться в грамотной постановке задач, учитывающих особенности комплексной защиты объектов информатизации, соотносящихся с изучаемой дисциплиной

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Математические и физические основы защиты информации» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины –изучение физических особенностей информативных сигналов акустической, электромагнитной, оптической и ядерной природы, являющихся основой для формирования технических каналов утечки информации, обучение студентов основным принципам и подходам к использованию математического аппарата для криптографической и комплексной защиты информации.

Задачи дисциплины:

- дать знанияпо физическим принципам и техническим основам формирования и функционирования акустических (речевых) каналов утечки информации, каналов утечки информации на основе побочных электромагнитных излучений и наводкам, оптических каналов утечки информации, каналов утечки информации на базе ядерных излучений;
- научить определять и учитывать качественные и количественные особенности составляющих криптографической и комплексной защиты информации;
- сформировать у студентов представления о механизмах смены параметров криптографической защиты;
- научить решать основополагающие теоретико-практические задачи защиты информации с применением необходимого математического аппарата и сформировать математический подход к их решению;
- ознакомить студентов с математическими основами криптографических методов защиты компьютерной информации;
- ознакомить студентов с основными математическими принципами алгоритмов создания электронной цифровой подписи;
- ознакомить студентов с основными принципами построения систем комплексной защиты информации.

Дисциплина направлена на формирование следующих компетенций:

- ПК-2 – Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
- ПК-11 – Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов

В результате освоения дисциплиныобучающийся должен:

- Знать: основные свойства и особенности распространения акустических и электромагнитных волн и потоков радиоактивных излучений; основы акустики помещений, человеческой речи и слуха; принципы электромагнитного экранирования и звукоизоляции помещений; принципы работы и устройства источников и приёмников электромагнитных, звуковых волн и потоков радиоактивных излучений; основные понятия, методы, принципы, подходы, алгоритмы и приёмы криптографии и комплексной защиты информации
- Уметь: применять полученные знания при освоении последующих базовых дисциплин, спецкурсов и при решении практических задач организации защиты информации на объектах; делать обоснованные выводы по результатам измерений;

самостоятельно работать с технической и справочной литературой; применять основные методы, принципы, подходы, алгоритмы и приёмы криптографии и комплексной защиты информации с необходимыми формулами для решения профессиональных математических задач

- Владеть: методами проведения физических измерений, методами корректной оценки погрешностей измерений и расчётов; основными подходами к постановке и решению задач, навыками математического описания профессиональных прикладных задач.

По дисциплине предусмотрена промежуточная аттестация в формезачета с оценкой.
Общая трудоёмкость дисциплины составляет 5 зачётных единиц.