

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт физики



подписано электронно-цифровой подписью

Программа дисциплины

Основы информационной безопасности М2.Б.1

Направление подготовки: 011800.68 - Радиофизика

Профиль подготовки: Информационные процессы и системы

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Автор(ы):

Карпов А.В.

Рецензент(ы):

Ишмуратов Р.А.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Шерстюков О. Н.

Протокол заседания кафедры No ____ от " ____ " _____ 201__ г

Учебно-методическая комиссия Института физики:

Протокол заседания УМК No ____ от " ____ " _____ 201__ г

Регистрационный No 6132314

Казань

2014

Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Программу дисциплины разработал(а)(и) профессор, д.н. (профессор) Карпов А.В. Кафедра радиофизики Отделение радиофизики и информационных систем , Arkadi.Karpov@kpfu.ru

1. Цели освоения дисциплины

Целью освоения дисциплины "Основы информационной безопасности" является обучение студентов принципам и методам защиты информации, комплексного проектирования, построения, обслуживания и анализа защищенных автоматизированных систем. Курс содержит основные положения криптографии, знакомит с наиболее распространенными типами шифров и методами их криптоанализа, понятиями целостности информации, криптографическими протоколами, электронной подписью.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " М2.Б.1 Профессиональный" основной образовательной программы 011800.68 Радиофизика и относится к базовой (общепрофессиональной) части. Осваивается на 1 курсе, 2 семестр.

Дисциплина входит в Профессиональный цикл. Магистрант приступает к изучению этой дисциплины после освоения основных образовательных программ бакалавриата и дисциплин общенаучного цикла магистратуры. Он должен владеть дисциплинами бакалаврского курса, уметь: понимать, излагать и критически анализировать базовую общефизическую информацию; использовать математический аппарат, использовать навыки экспериментальной работы и радиофизические методы на практике. Он должен использовать базовые теоретические знания для решения профессиональных задач, должен понимать принципы работы и методы эксплуатации современной радиоэлектронной и оптической аппаратуры и оборудования; владеть компьютером на уровне опытного пользователя, применять информационные технологии. В структуре магистратуры предшествующими дисциплинами является "Компьютерные технологии" и "Сети радиотелекоммуникаций".

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-21 (общекультурные компетенции)	способностью понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны
ПК-8 (профессиональные компетенции)	способностью понимать и использовать на практике теоретические основы организации и планирования физических исследований

В результате освоения дисциплины студент:

1. должен знать:

- место криптографии в задаче информационной безопасности и построения защищенных информационных систем ;
- основные понятия теории криптографии:
- криптографические протоколы электронной подписи;
- типичные слабости реализации криптографических систем;

-математические основы криптографии (неприводимые многочлены, теория чисел, псевдо-случайные последовательности,

2. должен уметь:

- правильно выбирать тип шифра в соответствии с поставленной задачей ;
- качественно реализовать алгоритм шифрования;
- реализовывать атаку на классические шифры (исторические и современные) , в частности - реализовать простейшие алгоритмы подбора паролей ;

3. должен владеть:

Математическими методами криптографии

4. должен демонстрировать способность и готовность:

Развить современные физические методы криптографии

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины зачет во 2 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Введение в информационную безопасность.	2	1-2	2	0	0	устный опрос
2.	Тема 2. Криптография с секретным ключом	2	3-8	4	6	0	устный опрос
3.	Тема 3. Криптография с открытым ключом. Электронная цифровая подпись	2	9-14	8	8	0	контрольная работа
4.	Тема 4. Криптографические системы, основанные на использовании уникальных свойств физических каналов связи	2	15-16	2	2	0	устный опрос

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
	Тема . Итоговая форма контроля	2		0	0	0	зачет
	Итого			16	16	0	

4.2 Содержание дисциплины

Тема 1. Введение в информационную безопасность.

лекционное занятие (2 часа(ов)):

Введение в информационную безопасность. Предмет защиты. Угрозы безопасности. Причины искажения информации. Виды атак. Каналы доступа. Методы противодействия. (Методы защиты информации). Политика безопасности.

Тема 2. Криптография с секретным ключом

лекционное занятие (4 часа(ов)):

История криптографии. Шифр сдвига. Шифр замены. Шифр Вернама. Вычислительно защищенная криптосистема. Абсолютно стойкая криптосистема. Теорема Шеннона об абсолютно стойкой криптосистеме. Теория вероятности и криптография. Симметричные шифры. Причины ненадежности криптосистем. Принцип Керкхоффа для криптосистемы. Поточные шифры. Генераторы псевдослучайных чисел. Важность подбора параметров Слабости реализаций Распределение симметричных ключей. Статичный ключ. Эфемерный ключ. Компрометация ключа. Реализация процедуры распределения ключей. Время жизни ключа. Разделение секрета. Энтропия. Неопределенность ключа. Расстояние единственности. Ложный ключ. Фиктивный ключ

практическое занятие (6 часа(ов)):

Разработка ПО шифра замены. Дешифрация шифротекста. Разработка ПО шифратора на основе генератора псевдослучайных чисел, основанного на свойствах ?M-последовательности.

Тема 3. Криптография с открытым ключом. Электронная цифровая подпись

лекционное занятие (8 часа(ов)):

Односторонние функции. Примеры односторонних функций. Факторизация. Целочисленное извлечение квадратных корней. Дискретное логарифмирование. Алгоритм RSA. Криптосистема Эль-Гамаль. Криптосистема Рабина.

практическое занятие (8 часа(ов)):

Программная реализация алгоритма RSA.

Тема 4. Криптографические системы, основанные на использовании уникальных свойств физических каналов связи

лекционное занятие (2 часа(ов)):

Криптографические системы, основанные на физических принципах защиты информации. Квантовая криптография, Криптографические системы основанные на свойствах многолучевого распространения радиоволн.

практическое занятие (2 часа(ов)):

Метеорная криптография.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
	Тема 1. Введение в					

информационную безопасность.

устному опросу

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. Криптография с секретным ключом	2	3-8	подготовка к устному опросу	10	устный опрос
3.	Тема 3. Криптография с открытым ключом. Электронная цифровая подпись	2	9-14	подготовка к контрольной работе	20	контрольная работа
4.	Тема 4. Криптографические системы, основанные на использовании уникальных свойств физических каналов связи	2	15-16	подготовка к устному опросу	6	устный опрос
	Итого				40	

5. Образовательные технологии, включая интерактивные формы обучения

Курс лекций читается на основе мультимедийных технологий, практические занятия проводятся в классе многопользовательского терминального доступа

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Введение в информационную безопасность.

устный опрос , примерные вопросы:

Введение в криптографию. Симметричные криптосистемы. Криптографические системы с открытым ключом. Криптографические системы, основанные на физических механизмах защиты информации

Тема 2. Криптография с секретным ключом

устный опрос , примерные вопросы:

Исторические шифры. Шифр сдвига. Шифр замены. Шифр Вернама. Вычислительно защищенная криптосистема. Абсолютно стойкая криптосистема. Теорема Шеннона об абсолютно стойкой криптосистеме. Энтропия. Неопределенность ключа. Расстояние единственности. Ложный ключ. Фиктивный ключ. Симметричные криптосистемы. Основные принципы современных симметричных алгоритмов. Поточные шифры. Блочные шифры. Причины ненадежности криптосистем. Принцип Керкхоффа для криптосистемы. Генераторы псевдослучайных чисел. Важность подбора параметров. Статичный ключ. Эфемерный ключ. Компрометация ключа. Реализация процедуры распределения ключей. Время жизни ключа. Схема порогового разделения. Пороговая схема Шамира. Протоколы распределения секретных ключей.

Тема 3. Криптография с открытым ключом. Электронная цифровая подпись

контрольная работа , примерные вопросы:

Темы и примеры заданий на контрольных 1. Шифр замены Расшифровать зашифрованный текст, предложенный преподавателем, при отсутствии ключа шифрования. Взлом шифра осуществляется с помощью частотного криптоанализа. 2. Поточный шифр. На основе полинома обратной связи, заданного преподавателем, реализовать генератор M-последовательности. 3. Криптография с открытым ключом. Реализовать атаку на алгоритм RSA (вычисление закрытого ключа по известному открытому ключу) путём факторизации модуля n по методу p -эвристики Полларда. Входными параметрами программы должны являться: открытый ключ (n, e) . В качестве выходных данных предъявить числа p, q, d .

Тема 4. Криптографические системы, основанные на использовании уникальных свойств физических каналов связи

устный опрос , примерные вопросы:

Криптографические системы, основанные на физических механизмах защиты информации. Квантовая криптография. Многолучевая криптография. Метеорная криптография.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

Форма контроля - зачет

По материалам представленных тем предусмотрено выполнение одной контрольных

Темы и примерных заданий на контрольной

1. Шифр замены

Расшифровать зашифрованный текст, предложенный преподавателем, при отсутствии ключа шифрования. Взлом шифра осуществляется с помощью частотного криптоанализа.

2. Поточный шифр.

На основе полинома обратной связи, заданного преподавателем, реализовать генератор M-последовательности.

3. Криптография с открытым ключом.

Реализовать атаку на алгоритм RSA (вычисление закрытого ключа по известному открытому ключу) путём факторизации модуля n по методу p -эвристики Полларда. Входными параметрами программы должны являться: открытый ключ (n, e) . В качестве выходных данных предъявить числа p, q, d .

Вопросы к зачету

1. Основные понятия, термины, определения. Криптология, криптография, криптоанализ, аутентификация, идентификация. Основные причины использования криптосистем. Симметричная криптосистема.

2. Исторические шифры. Шифр сдвига. Шифр замены. Полиалфавитный шифр. Шифр Виженера. Шифр Вернама. Недостатки исторических шифров. (Информационная стойкость).

3. Информационная стойкость криптографических систем Вычислительно защищенная криптосистема. Основные проблемы вычислительно защищенной криптосистемы. Абсолютно стойкая (совершенная) криптосистема.

4. К какому классу криптосистем - вычислительно защищенной или абсолютно стойкой относятся следующие криптосистемы: Шифр сдвига. Шифр замены. Шифр Виженера. Шифр Вернама ?

5. Понятие "абсолютной стойкости" в терминах теории вероятности. Теорема Шеннона: критерий абсолютной стойкости шифра. Интерпретация на примере шифра Вернама.

6. Энтропия случайной величины. Свойства энтропии. совместная энтропия двух случайных величин. Условная энтропия двух случайных величин. Неопределенность ключа.

7. Энтропия естественного языка. Расстояние единственности шифра.

8. Криптосистема с секретным ключом. Принцип Керкхоффа. Поточные и блочные шифры.

9. Поточные шифры. Генератор ключевого потока. Свойства генератора ключевого потока. Генератор псевдослучайных чисел, основанный на использовании алгебраических свойств M-последовательностей

10. Статистические тесты генераторов ключевого потока.
11. Блочные шифры. Алгоритм DES. Перестановки. Раунды. Алгоритм Фейстеля при шифровании и дешифровании.
12. Сравнение блочных и поточных шифров. Методы организации процедуры исправления ошибок.
13. Статичный ключ. Эфемерный ключ. Распределение ключей. Основные пути решения проблемы распределения ключей. (физические методы, Протоколы с секретным ключом, Протоколы с открытым ключом, современные физические методы).
14. Разделение секрета. Схема порогового разделения секрета. (T, W) - пороговая схема Шамира.
15. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Барроуза.
16. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Нидхейма-Шредера
17. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Отвэй-Риса.
18. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Цербер
19. Арифметика остатков. Сравнение по модулю. Решение уравнения $ax = b \pmod{N}$.
20. Функция Эйлера. Мультипликативные обратные по модулю N. Теорема Лагранжа. Малая теорема Ферма. Применение в криптографии.
21. Алгоритм Евклида. Китайская теорема об остатках. Расширенный алгоритм Евклида. Применение в криптографии.
22. Криптосистема с открытым ключом. Криптографическая односторонняя функция. Важнейшие криптографические односторонние функции.
23. Оценка сложности задач. Сложность алгоритма: Полиномиальная, экспоненциальная, субэкспоненциальная Оракул. Сравнительный анализ сложности криптографических алгоритмов (без доказательства).
24. Алгоритм RSA. Шифрование в RSA. Дешифрование в RSA. Доказательство алгоритма.
25. Алгоритм RSA. Задача криптоаналитика. Криптостойкость RSA
26. Криптосистема Эль-Гамаль. Параметры домена. Шифрование. Дешифрование.
27. Криптосистема Рабина. Алгоритм. Шифрование. Дешифрование.
28. Простые числа. Важность проблемы тестирования простых чисел. Пробное деление. Вероятностный подход при определении простого числа. Тест Ферма. Тест Миллера ? Рабина.
29. Распределение ключей Диффи ? Хеллмана. Алгоритм. Стойкость. Атака человек посередине. Необходимость использования цифровой подписи.
30. Алгоритмом цифровой подписи RSA
31. Криптографическая Хэш-функция. Свойства криптографической хэш-функции. Свойство односторонности Защищенность от повторений, защищенностью от вторых прообразов.
32. Алгоритмом цифровой подписи DSA
33. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94
34. Квантовая криптография
35. Передача секретных ключей по радиоканалу

7.1. Основная литература:

1. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.:
<http://znanium.com/bookread.php?book=474838>

2. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с.
<http://znanium.com/bookread.php?book=432654>
3. Баранова Е. К. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с.
<http://znanium.com/bookread.php?book=476047>
4. Партыка Т. Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с.
<http://znanium.com/bookread.php?book=420047>
5. Молдовян Н. А. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. - СПб.: БХВ-Петербург, 2010. - 293 с. - (Учебное пособие)
<http://znanium.com/bookread.php?book=351283>

7.2. Дополнительная литература:

1. Чмора А. Л.. Современная прикладная криптография: Учеб. пособие : Гелиос АРВ, 2001.256с.: 1
2. Лопатин В. Н. Информационная безопасность России: СПб.: Фонд "Университет", 2000. 426с.. 3
3. Бабаш, А. В. Криптография М.: СОЛОН-Р, 2002. 509с. 1
4. Левин М. Криптография: Руководство пользователя М.: Познавательная книга плюс, 2001.319с. 1
5. Столлингс В. Основы защиты сетей. Приложения и стандарты ?М.: Издат. Дом "Вильямс", 2002.429с 1
6. Столлингс, Вильям. Криптография и защита сетей. Принципы и практика ?М.: Издат. Дом "Вильямс", 2001.669с.: 1

7.3. Интернет-ресурсы:

- Глоссарий по криптографии - <https://hpc.name/text/get/82/p1.html>
литература по криптографии - <http://www.proklondike.com/books/crypto.html>
Сайт лаборатории радиосистемы (кафедра радиофизики) - <http://radiosys.ksu.ru>
Сайт по криптографии - <http://kek.ksu.ru/Student/Crypto/Main.htm>
электронные книги по криптографии - <http://www.knigka.info/kriptograf>

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Основы информационной безопасности" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB, audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудование имеет соответствующее лицензионное программное обеспечение.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Класс многопользовательского терминального доступа, сервер.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 011800.68 "Радиофизика" и магистерской программе Информационные процессы и системы .

Автор(ы):

Карпов А.В. _____

"__" _____ 201__ г.

Рецензент(ы):

Ишмуратов Р.А. _____

"__" _____ 201__ г.