МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

подписано электронно-цифровой подписью

Программа дисциплины

Основы информационной безопасности Б3.В.7

Направление подготовки: 010300.62 - Фундаментальная информатика и информационные технологии
Профиль подготовки: Системный анализ и информационные технологии
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Ишмухаметов Ш.Т.

Рецензент(ы):

Латыпов Р.Х.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 916214

Казань
2014

Содержание

Программу дисциплины разработал(а)(и) профессор, д.н. (доцент) Ишмухаметов Ш.Т. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Shamil.Ishmukhametov@kpfu.ru

1. Цели освоения дисциплины

В курсе "Основы информационной безопасности" изучаются основы безопасной работы с информацией, виды угроз и типы нарушений, принципы построения безопасных информационных систем. Рассматриваются различные атаки и способы защиты от нападений, физические, организационно-технические, административные виды защиты, правовые законы и постановления в области информационной безопасности, методы аутентификации пользователей на основе паролей и сертификатов, криптографические методы защиты информации. Рассматриваются классы безопасности сертифицированных информационных систем.

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

Данная учебная дисциплина включена в раздел " Б3.В.7 Профессиональный" основной образовательной программы 010300.62 Фундаментальная информатика и информационные технологии и относится к вариативной части. Осваивается на 3 курсе, 6 семестр.

Данная дисциплина относится к профессиональным дисциплинам.

Читается на 3 курсе в 6 семестре для студентов обучающихся по направлению "Фундаментальная информатика и информационные технологии".

Изучение основывается на результатах изучения дисциплин "Программирование и алгоритмические языки", "Технологии баз данных".

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-10 (профессиональные компетенции)	знание кодекса профессиональной этики и следование ему в жизни
ПК-25 (профессиональные компетенции)	уверенное знание теоретических и методических основ, понимание функциональных возможностей, следующих предметных областей: Разработка информационных систем, Моделирование и анализ программного обеспечения, Технологии мультимедиа, Архитектура и организация компьютеров, Конфигурирование и использование операционных систем, Разработка и принципы сетевых технологий, Человеко-машинное взаимодействие, Приложения и использование баз данных, Социальные и этические вопросы ИТ, Анализ технических требований, Графика и визуализация, Интеллектуальные системы, Теория баз данных.

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-4 (профессиональные компетенции)	способность понимать и применять в исследовательской и прикладной деятельности современный математический аппарат, фундаментальные концепции и системные методологии, международные и профессиональные стандарты в области информационных технологий, способность использовать современные инструментальные и вычислительные средства (в соответствии с профилизацией)
ПК-5 (профессиональные компетенции)	способность в составе научно-исследовательского и производственного коллектива решать задачи профессиональной деятельности (в соответствии с профилем подготовки)
ПК-8 (профессиональные компетенции)	способность профессионально владеть базовыми математическими знаниями и информационными технологиями, эффективно применять их для решения научно-технических задач и прикладных задач, связанных с развитием и использованием информационных технологий

В результате освоения дисциплины студент:

1. должен знать:

- сущность и актуальность проблемы информационной безопасности; изучить концептуальные подходы к обеспечению информационной безопасности; угрозы информации, средства и методы обеспечения информационной безопасности

2. должен уметь:

- - ориентироваться в проблемах ИБ, методах и средствах защиты информации

3. должен владеть:

- теоретическими знаниями о принципах построения безопасных ИС;

- навыками представление о проблемах информационной безопасности, способах, методах и средств их решения

4. должен демонстрировать способность и готовность:

-применять полученные знания в своей профессиональной деятельности

4. Структура и содержание дисциплины/ модуля

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

Форма промежуточного контроля дисциплины зачет в 6 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. Задачи и проблемы информационной безопасности.	6		3	3	0	домашнее задание
2.	Тема 2. Методы контроля доступа к информации	6		2	2	0	домашнее задание
3.	Тема 3. Организационно-правовые средства защиты	6		3	3	0	домашнее задание
4.	Тема 4. Криптографические средства защиты информации. Метод RSA.	6		4	4	0	контрольная работа контрольная работа
5.	Тема 5. Сертификаты X.509. Аутентификация на основе сертификатов.	6		3	3	0	домашнее задание
6.	Тема 6. Системы шифрования на основе эллиптических кривых.	6		3	3	0	домашнее задание
.	Тема . Итоговая форма контроля	6		0	0	0	зачет
	Итого			18	18	0	

4.2 Содержание дисциплины

Тема 1. Задачи и проблемы информационной безопасности.

лекционное занятие (3 часа(ов)):

Сущность и задачи информационной безопасности. Введение в защиту информации. Угрозы безопасности информационным системам и их классификация. Меры противодействия угрозам безопасности ИС. Классификация средств и методов защиты.

практическое занятие (3 часа(ов)):

Практика построения безопасных информационных систем. Аудит системы безопасности. Классификация классов защиты. Разбор методов защиты и условий их применения.

Тема 2. Методы контроля доступа к информации

лекционное занятие (2 часа(ов)):

Методы идентификации и аутентификации пользователей, технических средств обработки, программ и баз данных. Классификация информационных систем по степени защищенности. Общие критерии стран Европейского сообщества, их основные положения. Парольная идентификация и аутентификация в сетевых операционных системах.

практическое занятие (2 часа(ов)):

Изучение методов аутентификации пользователей в сети. Ацтентификация на основе процедуры "Вызов-ответ". Хеш-функции и их использование в криптографии.

Тема 3. Организационно-правовые средства защиты

лекционное занятие (3 часа(ов)):

Законодательный уровень защиты информации. Основные положения законодательства РФ в области информационной безопасности. Особенности федерального законы Российской Федерации от 28 июня 2014 г. N 184-ФЗ "Об электронной подписи".

практическое занятие (3 часа(ов)):

Изучение свойств и схем построения электронной подписи на основе разных криптографических методов. Схема Эль-Гамаля.

Тема 4. Криптографические средства защиты информации. Метод RSA.

лекционное занятие (4 часа(ов)):

Классические защиты шифрования информации на основе одного ключа. Криптографические примитивы. Подстановки и перестановки. Математические основы современной криптологии. Открытое распределение ключей.

практическое занятие (4 часа(ов)):

Построение защит на основе подстановок и перестановок. Схема Фейстеля - ее анализ криптостойкости. Алгоритм RSA.

Тема 5. Сертификаты X.509. Аутентификация на основе сертификатов.

лекционное занятие (3 часа(ов)):

Сертификаты электронной цифровой подписи, их состав и назначение. Состав сертификата. Виды сертификатов и порядок их получения.

практическое занятие (3 часа(ов)):

Свойства электронной подписи и ее юридические основы. Построение различных выдов подписи на основе двуключевых схем.

Тема 6. Системы шифрования на основе эллиптических кривых.

лекционное занятие (3 часа(ов)):

Конечные поля. Эллиптические кривые в конечных полях. Групповые свойства множеств точек эллиптических кривых. Задач вычисления кратного точки ЭК.

практическое занятие (3 часа(ов)):

Построение систем шифрования на основе эллиптических кривых. Вычисление кратного точки ЭК в афинных и проективных координтатах.

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
1.	Тема 1. Задачи и проблемы информационной безопасности.	6		подготовка домашнего задания	6	домашнее задание
2.	Тема 2. Методы контроля доступа к информации	6		подготовка домашнего задания	4	домашнее задание
3.	Тема 3. Организационно-правовые средства защиты	6		подготовка домашнего задания	6	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
4.	Тема 4. Криптографические средства защиты информации. Метод RSA.	6		подготовка домашнего задания	4	домашнее задание
				подготовка к контрольной работе	0	контрольная работа
				подготовка к контрольной работе	4	контрольная работа
5.	Тема 5. Сертификаты X.509. Аутентификация на основе сертификатов.	6		подготовка домашнего задания	6	домашнее задание
6.	Тема 6. Системы шифрования на основе эллиптических кривых.	6		подготовка домашнего задания	6	домашнее задание
	Итого				36	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекционных и практических занятий, а также самостоятельной работы студентов.

Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель - формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи зачета минимум и дополнительная литература.

Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов дисциплины "Основы информационной безопасности" на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать частные утверждения.

Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы.

Кроме того, самостоятельная работа включает подготовку к зачету. При подготовке к сдаче зачета весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к зачету, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда всегда будет резерв времени.

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

Тема 1. Задачи и проблемы информационной безопасности.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Обсуждение. Решение задач.

Тема 2. Методы контроля доступа к информации

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Обсуждение. Решение задач.

Тема 3. Организационно-правовые средства защиты

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Обсуждение. Решение задач.

Тема 4. Криптографические средства защиты информации. Метод RSA.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Обсуждение. Решение задач.

контрольная работа , примерные вопросы:

Выполнение контрольной работы по шифрованию на основе RSA.

контрольная работа , примерные вопросы:

Выполнение контрольной работы по шифрованию на основе RSA.

Тема 5. Сертификаты X.509. Аутентификация на основе сертификатов.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Обсуждение. Решение задач.

Тема 6. Системы шифрования на основе эллиптических кривых.

домашнее задание , примерные вопросы:

Решение задач по построению систем шифрования на эллиптических кривых. Вычисления в афинных и проективных координатах.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

По данной дисциплине предусмотрено проведение зачета. Примерные вопросы для зачета - Приложение1.

Вариант контрольной работы - Приложение 2.

ВОПРОСЫ К ЗАЧЕТУ

1. Введение в защиту информации.
2. Роль информации в жизнедеятельности современного общества.
3. Влияние информации на современное общество и повышение в связи с этим интерес к ней.
4. Определение информационной безопасности.
5. Современная постановка задачи защиты информации.
6. Основные составляющие информационной безопасности: конфиденциальность, целостность и доступность информации.
7. Угрозы безопасности информационным системам и их классификация. Угрозы конфиденциальности, целостности и доступности информации.
8. Меры противодействия угрозам безопасности ИС.
9. Классификация средств и методов защиты: административные, техни-ческие, организационно-правовые, физические методы защиты, их подразделение на предупреждающие, выявляющие (обнаруживающие), корректирующие средства.
10. Методы идентификации и аутентификации пользователей, технических средств обработки, программ и баз данных.
11. Метод паролей.
12. Биометрическая аутентификация.
13. Способы разграничения доступа, методы и средства их реализации.
14. Краткая характеристика современных средств разграничения доступа. Дискреционный и мандатный методы доступа.
15. Классификация информационных систем по степени защищенности.

16. "Оранжевая книга" США как критерий классификации систем информационной безопасности.

17. "Общие критерии" стран Европейского сообщества, их основные по-ложения.

18. Парольная идентификация и аутентификация в сетевых операционных системах: многоразовые и одноразовые пароли, смарт-карты, аутентификация на основе сертификатов.

19. Законодательный уровень защиты информации.

20. Основные положения Конституции РФ о защите информации, правах граждан на получение и распространение информации, законы и законодательные акты Российской Федерации в области защиты информации.

21. Основные положения закона "Об информации, информатизации и за-щите информации" от 20 февраля 1995 года, определение понятий информации, документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов.

22. Закон "О лицензировании отдельных видов деятельности" от 8 августа 2001 г. определение понятий лицензии, лицензируемого вида деятельности, лицензирования, лицензирующие органов, лицензиата. Положение статьи 17 Закона о видах деятельности, на осуществление которых требуются лицензии.

23. Основные положения закона РФ "Об электронной цифровой подписи" (от 13 декабря 2001 года) об электронном документе и электронной цифровой подписи, сертификате ЭЦП, владельце ЭЦП, закрытом и открытом ключе ЭЦП.

24. Криптографические средства защиты информации.

25. Основные понятия и задачи криптологии (криптографии).

26. Краткий исторический экскурс развития.

27. Примеры шифров замены и перестановки. Методы их дешифрования.

28. Криптосистемы с секретным ключом (симметричные).

29. Криптографические примитивы: перестановки, подставки, гаммирование.

30. Блочные и потоковые криптосистемы.

31. Проблема распределения ключей.

32. Математические основы современной криптологии.

33. Криптосистемы с открытым ключом (ассиметричные).

34. Система RSA.

35. Хэш-функции. Их свойства.

36. Использование хэш-функций для защиты паролей, целостности и конфиденциальности информации.

37. Открытое распределение ключей.

38. Использование RSA для защиты конфиденциальности сообщений, целостности данных и определения авторства сообщения.

39. Математические основы построения эллиптических кривых.

40. Прямые и обратные операции в конечных полях.

41. Система шифрования Эль-Гамаля.

42. Реализации системы Эль - Гамаля на ЭК.

43. Алгоритм электронной подписи на эллиптических кривых.

Приложение 2. Контрольная работа. Шифрование на основе RSA.

1. Проверить число n=89 на простоту, используя одну итерацию теста Миллера-Рабина с базой a=2.

2. Используя заданные значения p, q и e, вычислить остальные параметры RSA и расшифровать число m. Для вычисления d использовать расширенный алгоритм Евклида: p=17, q=41, e=291, m=16.

3. Нехороший мальчик Плохиш назначил встречу у башенных часов вражескому агенту Крису для передачи военных секретов, закодировав время встречи с помощью RSA. Но бдительный мальчик Вова перехватил записку. Помоги Вове узнать время встречи (оно находится в интервале от 10 до 24 часов): n=943, e=673, m=793

7.1. Основная литература:

1. Расторгуев, С. П. Основы информационной безопасности: учебное пособие / С.П. Расторгуев.?Москва: Академия, 2007.?186 с.

2. Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие, 2012. - URL: http://kpfu.ru/docs/F366166681/mzi.pdf

3. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. URL: http://www.znanium.com/bookread.php?book=420047

4. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. URL: http://www.znanium.com/bookread.php?book=405000

5. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с. URL: http://znanium.com/bookread.php?book=335362

7.2. Дополнительная литература:

Информационная безопасность, Ярочкин, Владимир Иванович, 2005г.

ЭМС и информационная безопасность в системах телекоммуникаций, Кечиев, Леонид Николаевич;Степанов, Павел Владимирович, 2005г.

Информационная безопасность, Малюк, Анатолий Александрович, 2004г.

7.3. Интернет-ресурсы:

Википедия - http://ru.wikipedia.org

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

Курс лекций - http://old.kpfu.ru/f9/bin_files/metod_tzis!113.doc

материалы к занятиям - http://kpfu.ru/docs/F366166681/mzi.pdf

Форум по ИТ - http://www.citforum.ru/

8. Материально-техническое обеспечение дисциплины(модуля)

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

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.

Лекции по дисциплине проводятся в аудитории, оснащенной доской и мелом(маркером), практические занятия по дисциплине проходят в компьютерном классе.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010300.62 "Фундаментальная информатика и информационные технологии" и профилю подготовки Системный анализ и информационные технологии .

Автор(ы):
Ишмухаметов Ш.Т. _____
"__" _____ 201 __ г.

Рецензент(ы):
Латыпов Р.Х. _____
"__" _____ 201 __ г.