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

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Минзарипов Р.Г.

подписано электронно-цифровой подписью

Программа дисциплины

Основы информационной безопасности Б3.В.8

Направление подготовки: 010400.62 - Прикладная математика и информатика
Профиль подготовки: Численные методы
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Ишмухаметов Ш.Т.

Рецензент(ы):

Рубцова Р.Г.

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 968114

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.8 Профессиональный" основной образовательной программы 010400.62 Прикладная математика и информатика и относится к вариативной части. Осваивается на 3 курсе, 6 семестр.

"Основы информационной безопасности" входит в состав профессиональных дисциплин. Читается на 3 курсе, в 6 семестре.

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)	способность применять в профессиональной деятельности современные языки программирования и языки баз данных, операционные системы, электронные библиотеки и пакеты программ, сетевые технологии.
ПК-4 (профессиональные компетенции)	способность в составе научно-исследовательского и производственного коллектива решать задачи профессиональной деятельност
ПК-5 (профессиональные компетенции)	способность критически переосмысливать накопленный опыт, изменять при необходимости вид и характер своей профессиональной дея-тельности;
ПК-8 (профессиональные компетенции)	способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций;

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.

4. должен демонстрировать способность и готовность:

-

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. Сущность, задачи и проблемы информационной безопасности	6		0	6	0	
2.	Тема 2. Методы контроля доступа к информации	6		0	8	0	
3.	Тема 3. Организационно-правовые средства защиты	6		0	8	0	
4.	Тема 4. Криптографические средства защиты информации	6		0	6	0	контрольная работа
5.	Тема 5. Эллиптические кривые.	6		0	8	0	
.	Тема . Итоговая форма контроля	6		0	0	0	зачет
	Итого			0	36	0	

4.2 Содержание дисциплины

Тема 1. Сущность, задачи и проблемы информационной безопасности

практическое занятие (6 часа(ов)):

Сущность, задачи и проблемы информационной безопасности 1.1. Введение в защиту информации. Роль информации в жизнедеятельности современного общества. Влияние информации на современное общество и повышение в связи с этим интерес к ней. Определение информационной безопасности. 1.2. Современная постановка задачи защиты информации. Основные составляющие информационной безопасности: конфиденциальность, целостность и доступность информации.

Тема 2. Методы контроля доступа к информации

практическое занятие (8 часа(ов)):

Методы контроля доступа к информации 2.1. Методы идентификации и аутентификации пользователей, технических средств обработки, программ и баз данных. Метод паролей. Биометрическая аутентификация. Способы разграничения доступа, методы и средства их реализации. Краткая характеристика современных средств разграничения доступа. Дискреционный и мандатный методы доступа.

Тема 3. Организационно-правовые средства защиты

практическое занятие (8 часа(ов)):

Организационно-правовые средства защиты 3.1. Законодательный уровень защиты информации. Основные положения Конституции РФ о защите информации, правах граждан на получение и распространение информации, законы и законодательные акты Российской Федерации в области защиты информации.

Тема 4. Криптографические средства защиты информации

практическое занятие (6 часа(ов)):

Криптографические средства защиты информации 4.1. Криптографические средства защиты информации. Основные понятия и задачи криптологии (криптографии). Краткий исторический экскурс развития. Примеры шифров замены и перестановки. Методы их дешифрования. 4.2. Криптосистемы с секретным ключом (симметричные). Криптографические примитивы: перестановки, подставки, гаммирование. Блочные и потоковые криптосистемы. Проблема распределения ключей.

Тема 5. Эллиптические кривые.

практическое занятие (8 часа(ов)):

Эллиптические кривые. 5.1. Математические основы построения ЭК. Прямые и обратные операции в конечных полях. 5.2. Система шифрования Эль-Гамаля. 5.3. Реализации системы Эль-Гамаля на ЭК. 5.4. Алгоритм электронной подписи на ЭК

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. Сущность, задачи и проблемы информационной безопасности	6		Домашняя работа	6	Домашняя работа
2.	Тема 2. Методы контроля доступа к информации	6		Домашняя работа	8	Домашняя работа
3.	Тема 3. Организационно-правовые средства защиты	6		Домашняя работа	8	Домашняя работа
4.	Тема 4. Криптографические средства защиты информации	6		подготовка к контрольной работе	8	контрольная работа

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
5.	Тема 5. Эллиптические кривые.	6		Домашняя работа	6	Домашняя работа
	Итого				36	

5. Образовательные технологии, включая интерактивные формы обучения

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

Изучение курса подразумевает получение практических навыков для более глубокого понимания разделов дисциплины, 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, 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. Сущность, задачи и проблемы информационной безопасности

Домашняя работа , примерные вопросы:

Углубленное изучение литературы по теме. Обсуждение. Решение задач: 1. Разработать список объектов информационной системы, подлежащих защите. 2. Провести аудит задач информационной безопасности ИС. конфиденциальность, целостность и доступность информации.

Тема 2. Методы контроля доступа к информации

Домашняя работа , примерные вопросы:

Углубленное изучение литературы по теме. Решение задач: 1. Изучить мандатную и дискреционную системы защит. 2. Рассмотреть принципы организации защиты системы Kerberos.

Тема 3. Организационно-правовые средства защиты

Домашняя работа , примерные вопросы:

Углубленное изучение литературы по теме. Изучить: 1. Федеральный закон РФ 2011 года "Об электронной подписи" с поправками 2014 года. 2. Федеральный закон РФ 2006 года "Об информации, информационных технологиях и о защите информации" с поправками 2011 года. 3. Федеральный закон РФ 2006 года "О персональных данных".

Тема 4. Криптографические средства защиты информации

контрольная работа , примерные вопросы:

Решение задач: 1. Разработать систему шифрования на основе блочных и потоковых методов. 2. Изучить метод RSA и рассмотреть проблему выбора параметров RSA.

Тема 5. Эллиптические кривые.

Домашняя работа , примерные вопросы:

Подготовка к контрольной работе по теме. Решение задач на вычисление сумм точек эллиптической кривой, оценке числа точек и порядков точек. Шифрование на основе ЭК.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

Задачи к контрольным работам. 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

Вопросы на зачет:

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, технические, 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 положения.

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. Реализации системы Эль - Гамаля на эллиптических кривых.
42. Алгоритм электронной подписи на эллиптических кривых.

7.1. Основная литература:

1. 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
2. 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
3. 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:

1. Иванов К. В. Марковские модели защиты автоматизированных систем управления специального назначения / К. В. Иванов, П. И. Тутубалин.?Казань: [Республиканский центр мониторинга качества образования], 2012.?213 с.: ил.; 21.?(Серия "Современная прикладная математика и информатика").?Библиогр.: с. 185-199 (168 назв.).?ISBN 978-5-906158-15-4((в пер.)), 50.
2. Расторгуев, С. П. Основы информационной безопасности: учебное пособие / С.П. Расторгуев.?Москва: Академия, 2007.?186 с.

3. Партыка Т. Л. Информационная безопасность: учеб. пособие / Т.Л. Партыка, И.И. Попов.?Изд. 2-е, испр. и доп..?Москва: ФОРУМ: ИНФРА-М, 2007.?367 с

4. Бабаш, А. В. Информационная безопасность: лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников.?Москва: КноРус, 2012.?131 с.

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

6. Мельников, Владимир Павлович. Информационная безопасность и защита информации: учеб. пособие для студ.высш.учеб.заведений / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова.?М.: Академия, 2006.?336 с.

7.3. Интернет-ресурсы:

Библиотека интернет-ресурсов - http://engenegr.ru

Библиотека интернет-ресурсов - http://techlibrary.ru

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

Портал ресурсов по математике, алгоритмике и ИТ - http://algolist.manual.ru/

Справочник по компьютерной математике - http://www.users.kaluga.ru/math/

8. Материально-техническое обеспечение дисциплины(модуля)

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

Практические занятия по дисциплине проводятся в аудитории, оснащенной доской и мелом (маркером)

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010400.62 "Прикладная математика и информатика" и профилю подготовки Численные методы .

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

Рецензент(ы):
Рубцова Р.Г. _____
"__" _____ 201 __ г.