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. Таюрский Д.А.
_____
"___"_____20___ г.

Программа дисциплины

Основы информационной безопасности Б1.В.ДВ.21

Направление подготовки: 01.03.02 - Прикладная математика и информатика
Профиль подготовки: Системное программирование
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

Казань
2016

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 " Б1.В.ДВ.21 Дисциплины (модули)" основной образовательной программы 01.03.02 Прикладная математика и информатика и относится к дисциплинам по выбору. Осваивается на 3 курсе, 6 семестр.

Данная дисциплина относится к профессиональным дисциплинам.

Читается на 3 курсе в 6 семестре для студентов обучающихся по направлению "Прикладная математика и информатика".

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

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-4 (профессиональные компетенции)	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-1 (профессиональные компетенции)	способностью собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям
ПК-3 (профессиональные компетенции)	способностью критически переосмысливать накопленный опыт, изменять при необходимости вид и характер своей профессиональной деятельности

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

-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. Сущность, задачи информационной безопасности.	6	1-3	0	6	0	письменное домашнее задание
2.	Тема 2. Методы контроля доступа к информации.	6	4-6	0	6	0	письменное домашнее задание
3.	Тема 3. Организационно-правовые средства защиты.	6	7-9	0	6	0	письменное домашнее задание
4.	Тема 4. Криптографические средства защиты информации. Метод RSA.	6	10-12	0	6	0	письменное домашнее задание
5.	Тема 5. Сертификаты X.509. Аутентификация на основе сертификатов.	6	13-15	0	6	0	письменное домашнее задание

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
6.	Тема 6. Системы шифрования на основе эллиптических кривых.	6	16-18	0	6	0	контрольная работа
.	Тема . Итоговая форма контроля	6		0	0	0	зачет
	Итого			0	36	0	

4.2 Содержание дисциплины

Тема 1. Сущность, задачи информационной безопасности.

практическое занятие (6 часа(ов)):

Введение в защиту информации. Современная постановка задачи защиты информации. Угрозы безопасности информационным системам и их классификация. Меры противодействия угрозам безопасности ИС.

Тема 2. Методы контроля доступа к информации.

практическое занятие (6 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. Изучение методов аутентификации пользователей в сети. Аутентификация на основе процедуры "Вызов-ответ". Хеш-функции и их использование в криптографии.

Тема 3. Организационно-правовые средства защиты.

практическое занятие (6 часа(ов)):

Законодательный уровень защиты информации. Основные положения закона "Об информации, информатизации и защите информации" от 2006 года, определение понятий информации, документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов. ФЗ "О персональных данных " 2006 года. ФЗ 063 "Об электронной подписи" от 2011 г. с дополнениями 2014 г.

Тема 4. Криптографические средства защиты информации. Метод RSA.

практическое занятие (6 часа(ов)):

Классические и современные криптографические средства защиты. Криптосистемы с открытым ключом. Хэш-функции. Открытое распределение ключей. Алгоритм шифрования и цифровой подписи RSA.

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

практическое занятие (6 часа(ов)):

Сертификаты электронной цифровой подписи X.509, их назначение. Состав сертификата. Виды сертификатов и порядок их получения. Процедура аутентфикации на основе сертификатов.

Тема 6. Системы шифрования на основе эллиптических кривых.

практическое занятие (6 часа(ов)):

Математические основы построения эллиптические кривых. Прямые и обратные операции в конечных полях. Система шифрования Эль-Гамаля. Реализации системы Эль -Гамаля на ЭК. Алгоритм электронной подписи Эль-Гамаля 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 информационной безопасности.	6	1-3	подготовка домашнего задания	6	домашнее задание
2.	Тема 2. Методы контроля доступа к информации.	6	4-6	подготовка домашнего задания	6	домашнее задание
3.	Тема 3. Организационно-правовые средства защиты.	6	7-9	подготовка домашнего задания	6	домашнее задание
4.	Тема 4. Криптографические средства защиты информации. Метод RSA.	6	10-12	подготовка домашнего задания	6	домашнее задание
5.	Тема 5. Сертификаты X.509. Аутентификация на основе сертификатов.	6	13-15	подготовка домашнего задания	6	домашнее задание
6.	Тема 6. Системы шифрования на основе эллиптических кривых.	6	16-18	подготовка к контрольной работе	6	контрольная работа
	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. Сущность, задачи информационной безопасности.

домашнее задание , примерные вопросы:

Решение задач. Изучить понятия сервисов информационной безопасности, разобрать угрозы ИБ и возможные методы защиты на примере.

Тема 2. Методы контроля доступа к информации.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Разобрать достоинства и недостатки дискреционного и мандатного подхода к управлению доступом.

Тема 3. Организационно-правовые средства защиты.

домашнее задание , примерные вопросы:

Разобрать понятия электронной подписи, сертификата открытого ключа, права и обязанности удостоверяющего центра по ФЗ "Об электронной подписи" 2011 года.

Тема 4. Криптографические средства защиты информации. Метод RSA.

домашнее задание , примерные вопросы:

Разобрать особенности метода RSA шифрования с открытым ключом. Решить задачи на шифрование тектов и построение подписи на основе RSA.

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

домашнее задание , примерные вопросы:

Разобрать структуру PKI, состав и назначение сертификатов X.509, достоинства и недостатки аутентификации на основе сертификатов

Тема 6. Системы шифрования на основе эллиптических кривых.

контрольная работа , примерные вопросы:

1. Задано конечное поле Fp. Найти наименьшее число g>=2, являющееся генератором поля, вычислить открытый ключ y по заданному x. Зашифровать сообщение m и выполнить обратную расшифровку, используя заданный параметр k. p=29, x=5, m=13, k=11 2. Хакер Вася перехватил зашифрованное сообщение (p,g,y,a,b)=(47,5,7,11,45). Помогите Васе расшифровать сообщение, используя метод Шенкса больших и малых шагов(ответ m<=10). 3. Заданы параметры поля Fp p=37, g=2, открытый ключ y=17 и сообщение m=9. Установить цифровую подпись на сообщение m и выполнить проверку, используя секретный ключ x=7.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

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 ЭК

7.1. Основная литература:

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

2. 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

3. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. URL:http://znanium.com/bookread2.php?book=495249

4. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие. - Электрон. дан. - СПб. : Лань, 2016. - 324 с. - Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=75515

5. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: НИЦ ИНФРА-М, 2016. - 118 с. http://znanium.com/bookread2.php?book=507334

7.2. Дополнительная литература:

1. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. - ЭБС 'Знаниум': http://znanium.com/bookread.php?book=491597

2. Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с. - ЭБС 'Знаниум': http://znanium.com/bookread.php?book=169345

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

4. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с. ЭБС 'Знаниум': http://znanium.com/bookread2.php?book=508381

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 01.03.02 "Прикладная математика и информатика" и профилю подготовки Системное программирование .

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

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