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.

подписано электронно-цифровой подписью

Программа дисциплины

Информационная безопасность Б3.Б.12

Направление подготовки: 080500.62 - Бизнес-информатика
Профиль подготовки:
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Автор(ы):
Латыпов Р.Х.
Рецензент(ы):
Миссаров М.Д.

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 919916

Казань
2016

Содержание

Программу дисциплины разработал(а)(и) заведующий кафедрой, д.н. (профессор) Латыпов Р.Х. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Roustam.Latypov@kpfu.ru

1. Цели освоения дисциплины

В курсе "Информационная безопасность" 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.Б.12 Профессиональный" основной образовательной программы 080500.62 Бизнес-информатика и относится к базовой (общепрофессиональной) части. Осваивается на 2 курсе, 4 семестр.

Данная дисциплина проводится на 2 курсе в 4 семестре. Знания, полученные при изучении этой дисциплине, потребуются далее при изучении таких дисциплин как "Проектирование информационных систем", "Вычислительные системы, сети и телекоммуникации" и других дисциплин. Также эти знания могут быть использованы при написании выпускных работ бакалавра.

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-12 (общекультурные компетенции)	осознает сущность и значение информации в развитии современного общества; владеет основными методами, способами и средствами получения, хранения, переработки информации;
ОК-13 (общекультурные компетенции)	имеет навыки работы с компьютером как средством управления информацией, способен работать с информацией в глобальных компьютерных сетях;имеет навыки работы с компьютером как средством управления информацией, способен работать с информацией в глобальных компьютерных сетях;
ОК-15 (общекультурные компетенции)	владеет основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;
ПК-12 (профессиональные компетенции)	проектировать и внедрять компоненты ИТ-инфраструктуры предприятия, обеспечивающие достижение стратегических целей и поддержку бизнес-процессов.

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. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) 108 часа(ов).

Форма промежуточного контроля дисциплины зачет в 4 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. Тема: Сущность, задачи и проблемы информационной безопасности.	4	1-4	4	0	6	домашнее задание
2.	Тема 2. Тема: Методы контроля доступа к информации.	4	5-8	4	0	6	тестирование домашнее задание
3.	Тема 3. Тема: Организационно-правовые средства защиты.	4	9-12	4	0	6	контрольная работа домашнее задание
4.	Тема 4. Тема: Криптографические средства защиты информации.	4	13-15	3	0	5	тестирование 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	
5.	Тема 5. Тема: Эллиптические кривые.	4	16-18	3	0	5	домашнее задание контрольная работа
.	Тема . Итоговая форма контроля	4		0	0	0	зачет
	Итого			18	0	28	

4.2 Содержание дисциплины

Тема 1. Тема: Сущность, задачи и проблемы информационной безопасности.

лекционное занятие (4 часа(ов)):

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.

лабораторная работа (6 часа(ов)):

Изучение на лабораторном занятии основных составляющих информационной безопасности: конфиденциальности, целостности и доступности информации.

Тема 2. Тема: Методы контроля доступа к информации.

лекционное занятие (4 часа(ов)):

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

лабораторная работа (6 часа(ов)):

Подробный разбор на лабораторном занятии различных методов идентификации и аутентификации пользователей, технических средств обработки, программ и баз данных. Практическое изучение метода паролей и метода биометрической аутентификации. Разбор примеров способов разграничения доступа, методов и средств их реализации.

Тема 3. Тема: Организационно-правовые средства защиты.

лекционное занятие (4 часа(ов)):

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.

лабораторная работа (6 часа(ов)):

Изучение организационно-правовых средств защиты.

Тема 4. Тема: Криптографические средства защиты информации.

лекционное занятие (3 часа(ов)):

Тема: 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, подстановки, гаммирование. Блочные и потоковые криптосистемы. Проблема распределения ключей.

лабораторная работа (5 часа(ов)):

Изучение криптографических средств защиты информации. Подробный разбор примеров шифров замены и перестановки и методов их дешифрования. Практическое изучение на примерах криптосистем с секретным ключом (симметричных). Рассмотрение криптографических примитивов, блочных и потоковых криптосистем. Изучение проблемы распределения ключей.

Тема 5. Тема: Эллиптические кривые.

лекционное занятие (3 часа(ов)):

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

лабораторная работа (5 часа(ов)):

Разбор на лабораторном занятии математических основы построения эллиптических кривых. Изучение системы шифрования Эль-Гамаля и реализации её на эллиптических кривых. Подробный разбор алгоритма электронной подписи на эллиптических кривых.

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. Тема: Сущность, задачи и проблемы информационной безопасности.	4	1-4	подготовка домашнего задания	12	домашнее задание
2.	Тема 2. Тема: Методы контроля доступа к информации.	4	5-8	подготовка домашнего задания	6	домашнее задание
				подготовка к тестированию	6	тестирование
3.	Тема 3. Тема: Организационно-правовые средства защиты.	4	9-12	подготовка домашнего задания	6	домашнее задание
				подготовка к контрольной работе	6	контрольная работа
4.	Тема 4. Тема: Криптографические средства защиты информации.	4	13-15	подготовка домашнего задания	6	домашнее задание
				подготовка к тестированию	6	тестирование
5.	Тема 5. Тема: Эллиптические кривые.	4	16-18	подготовка домашнего задания	6	домашнее задание
				подготовка к контрольной работе	8	контрольная работа
	Итого				62	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекционных и лабораторных 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 на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать 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 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. Тема: Сущность, задачи и проблемы информационной безопасности.

домашнее задание , примерные вопросы:

Изучение лекционного материала, основной и дополнительной литературы по теме. Доработка заданий, выполняемых на лабораторных занятиях.

Тема 2. Тема: Методы контроля доступа к информации.

домашнее задание , примерные вопросы:

Изучение лекционного материала, основной и дополнительной литературы по теме: Методы контроля доступа к информации. Доработка заданий, выполняемых на лабораторных занятиях.

тестирование , примерные вопросы:

Подготовка к тестированию. Вопросы к тестированию: - Определение информационной безопасности. - Современная постановка задачи защиты информации. - Основные составляющие информационной безопасности. - Методы контроля доступа к информации. - Методы идентификации и аутентификации пользователей. - Методы технических средств обработки, программ и баз данных. .- - Метод паролей. - Биометрическая аутентификация. - Способы разграничения доступа, методы и средства их реализации. - Дискреционный и мандатный методы доступа.

Тема 3. Тема: Организационно-правовые средства защиты.

домашнее задание , примерные вопросы:

Изучение лекционного материала, основной и дополнительной литературы по теме: -Организационно-правовые средства защиты. Доработка заданий, выполняемых на лабораторных занятиях.

контрольная работа , примерные вопросы:

Подготовка к контрольной работе (выполнению индивидуальных заданий) по пройденным темам.

Тема 4. Тема: Криптографические средства защиты информации.

домашнее задание , примерные вопросы:

Изучение лекционного материала, основной и дополнительной литературы по теме: -Криптографические средства защиты. Доработка заданий, выполняемых на лабораторных занятиях.

тестирование , примерные вопросы:

Подготовка к тестированию. Вопросы к тестированию: -Криптографические средства защиты информации. - Основные понятия и задачи криптологии (криптографии). - Примеры шифров замены и перестановки. Методы их дешифрования. - Криптосистемы с секретным ключом (симметричные). - Криптографические примитивы: перестановки, подставки, гаммирование. - Блочные и потоковые криптосистемы. - Проблема распределения ключей.

Тема 5. Тема: Эллиптические кривые.

домашнее задание , примерные вопросы:

Изучение лекционного материала, основной и дополнительной литературы по теме: -Эллиптические кривые. Доработка заданий, выполняемых на лабораторных занятиях.

контрольная работа , примерные вопросы:

Подготовка к контрольной работе (выполнению индивидуальных заданий) по пройденным темам.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

По данной дисциплине предусмотрено проведение зачета.

Примерные вопросы для зачета:

1. Сущность, задачи и проблемы информационной безопасности

2. Введение в защиту информации. Роль информации в жизнедеятельности современного общества. Влияние информации на современное общество и повышение в связи с этим интереса к ней.

3. Определение информационной безопасности. Современная постановка задачи защиты информации.

4. Основные составляющие информационной безопасности: конфиденциальность, целостность и доступность информации.

5. Методы контроля доступа к информации

6. Методы идентификации и аутентификации пользователей, технических средств обработки, программ и баз данных.

7. Метод паролей.

8. Биометрическая аутентификация.

9. Способы разграничения доступа, методы и средства их реализации.

10.Краткая характеристика современных средств разграничения доступа.

11.Дискреционный и мандатный методы доступа.

12.Организационно-правовые средства защиты.

13. 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.

14.Криптографические средства защиты информации.

15.Основные понятия и задачи криптологии (криптографии).

16.Краткий исторический экскурс развития.

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

18.Криптосистемы с секретным ключом (симметричные).

19.Криптографические примитивы: перестановки, подставки, гаммирование.

20.Блочные и потоковые криптосистемы.

21.Проблема распределения ключей.

22.Эллиптические кривые. Математические основы построения ЭК.

23.Прямые и обратные операции в конечных полях.

24.Система шифрования Эль-Гамаля. Реализации системы Эль - Гамаля на ЭК.

25.Алгоритм электронной подписи на ЭК

7.1. Основная литература:

1.Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2

http://www.znanium.com/bookread.php?book=405000

2.Баранова, Е. К. Основы информатики и защиты информации [Электронный ресурс] : Учеб. пособие / Е. К. Баранова. - М. : РИОР : ИНФРА-М, 2013. - 183 с. + Доп. материалы. - (Высшее образование: Бакалавриат). - ISBN 978-5-369-01169-0 (РИОР), ISBN 978-5-16-006484-0 (ИНФРА-М).

http://www.znanium.com/bookread.php?book=415501

3.Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-91134-353-8, 1500 экз.

http://www.znanium.com/bookread.php?book=169345

7.2. Дополнительная литература:

1. Мельников В.П. Информационная безопасность и защита информации; учеб. пособие для студентов высш. учеб. заведений/ Мельников В.П., Клейменов С.А., Петраков А.М.; под ред. Мельникова В.П. М.: Издательский центра "Академия", 2006. - 336с.

2.Основы информационной безопасности : учебное пособие для студентов высших учебных заведений, обучающихся по специальностям "Компьютерная безопасность", "Комплексное обеспечение информационной безопасности автоматизированных систем" и "Информационная безопасность телекоммуникационных систем" / С.П. Расторгуев .? Москва : Академия, 2007 .? 186,[1] с.

3. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш .? 2-е изд. ? Москва : РИОР : ИНФРА-М, [2014] .? 254, [1] с. : ил. ; 22 .? (Высшее образование, Бакалавриат) (Соответствует Федеральному государственному образовательному стандарту 3-го поколения) .? На обороте тит. л. авт.: Баранова Е. К. - доц., Бабаш А. В. - д.ф.-м.н., проф. ? Библиогр. в конце гл. и в подстроч. примеч. ? ISBN 978-5-369-01218-5 (РИОР) .? ISBN 978-5-16-006829-9 (ИНФРА-М) , 500

4.Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-91134-360-6, 500 экз.
http://znanium.com/bookread.php?book=405313

7.3. Интернет-ресурсы:

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

Интернет-сборник статей по безопасности - http://www.web-hack.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 "Информационная безопасность" 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 оборудованием 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.

Компьютерные классы лаборатории малой вычислительной техники Института ВМ и ИТ, оборудованные мультимедийным оборудованием.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 080500.62 "Бизнес-информатика" .

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

Рецензент(ы):
Миссаров М.Д. _____
"__" _____ 201 __ г.