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

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Минзарипов Р.Г.
_____
"___"_____20___ г.

Программа дисциплины

Информационная безопасность Б3.Б.12

Направление подготовки: 080500.62 - Бизнес-информатика
Профиль подготовки: не предусмотрено
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):
Латыпов Р.Х.
Рецензент(ы):
Миссаров М.Д.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой:
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института управления и территориального развития:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No

Казань
2014

Содержание

Программу дисциплины разработал(а)(и) директор института вычислительной математики Латыпов Р.Х. Директорат Института ВМ и ИТ Институт вычислительной математики 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:

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 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.	4	1-4	0	0	0	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
2.	Тема 2. Тема: 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.	4	5-8	0	0	0	
3.	Тема 3. Тема: 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.	4	9-12	0	0	0	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
4.	Тема 4. 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, подставки, гаммирование. Блочные и потоковые криптосистемы. Проблема распределения ключей.	4	13-15	0	0	0	
5.	Тема 5. Тема: 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	16-18	0	0	0	
.	Тема . Итоговая форма контроля	4		0	0	0	зачет
	Итого			0	0	0	

4.2 Содержание дисциплины

Тема 1. Тема: 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. Тема: 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. Тема: 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. 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, подставки, гаммирование. Блочные и потоковые криптосистемы. Проблема распределения ключей.

Тема 5. Тема: 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

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

Тема 5. Тема: 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

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

По данной дисциплине предусмотрено проведение зачета и промежуточных тестов. Примерные вопросы для зачета - Приложение 1. Примерные тестовые вопросы для текущего контроля успеваемости - Приложение 2.

7.1. Основная литература:

1. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и защита - М.: ДМК Пресс, 2008. - 544 с.

2. Девянин П.Н. Модели безопасности компьютерных систем: Уч. Пособие для студентов ВУЗов. - М.: Издательский центра "Академия", 2005.

3. 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", 2008.

4. Расторгуев С.П. Программные методы защиты информации. Пенза, 2000, 100 с.

5. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, протоколы. СПб.: "Piter-press", 2001, 668 с.

7.2. Дополнительная литература:

1. Герасименко В.А., Малюк А.А. "Основы защиты информации" М.: МИФИ. /Учебник (рекомендован Минобразованием России в качестве учебника для студентов вузов). 1997 - 538 с.

2. Малюк А.А., Пазизин С.В., Погожин Н.С. "Введение в защиту информации в автоматизированных системах" М.: "Горячая Линия-Телеком". 2001 - 148 с.

3. Ярочкин В.И. "Информационная безопасность". М.: "Международные отношения". 2000 - 400 с.

4. Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации. М.: Издательская группа "Юрист", 2001 - 415с.

7.3. Интернет-ресурсы:

8. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Освоение дисциплины "Информационная безопасность" предполагает использование следующего материально-технического обеспечения:

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

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

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