МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Отделение менеджмента

подписано электронно-цифровой подписью

Программа дисциплины

Информационная безопасность Б3.Б.16

Направление подготовки: 080500.62 - Бизнес-информатика
Профиль подготовки: Информационно-аналитические системы в бизнесе
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Ишмухаметов Ш.Т.

Рецензент(ы):

Миссаров М.Д.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 201__г

Учебно-методическая комиссия Института управления, экономики и финансов (отделение менеджмента):
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 94993214

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

Целями освоения дисциплины "Информационная безопасность" являются систематизация наиболее важных понятий в сфере информационной безопасности АИС, БД и БнД, изучение моделей, механизмов и технологий обеспечения конфиденциальности, целостности и правомерной доступности информации в АИС, БД и БнД, методов обеспечения безопасности функций АИС и БнД.

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

Данная учебная дисциплина включена в раздел " Б3.Б.16 Профессиональный" основной образовательной программы 080500.62 Бизнес-информатика и относится к базовой (общепрофессиональной) части. Осваивается на 4 курсе, 7 семестр.

Дисциплина " Информационная безопасность " изучается на четвертом году обучения. Данная дисциплина является логическим продолжением ряда курсов, изученных студентами по программе бакалавриата направления "Бизнес-информатика", включая "Автоматизация бухгалтерского учета", "Вычислительные системы, сети и телекоммуникации", "Информационные системы управления производственной компанией" и ряда других.

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
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:

- понятие, виды и структуру автоматизированных информационных систем;
- систематику методов и механизмов обеспечения информационной безопасности АИС;
- основные политики, дискреционные и мандатные модели разграниченияоступа к информации в АИС;
- идеологию и общую характеристику критериев оценки безопасности информационных технологий ("Общие критерии");
- порядок разработки и структуру профилей защиты СУБД.

2. должен уметь:

- планировать и анализировать структуру индивидуально-группового доступак разделяемым ресурсам;

- анализировать и применять политику тематико-иерархического разграничения доступа в документальных АИС;

- анализировать и обосновывать политику и механизмы обеспечения информационной безопасности, ее аудита в распределенных АИС.

3. должен владеть:

- навыками работы с нормативно-методическими документами в сфере информационной безопасности автоматизированных информационных систем;

- навыками использования и разработки систем анализа рисков и аудита информационных систем.

4. должен демонстрировать способность и готовность:

- анализировать функциональную и системную архитектуру АИС в контексте обеспечения информационной безопасности.

4. Структура и содержание дисциплины/ модуля

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

Форма промежуточного контроля дисциплины зачет в 7 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.	7	1-4	2	0	2	домашнее задание
2.	Тема 2. Тема: Методы контроля доступа к информации.	7	5-8	2	0	2	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	
3.	Тема 3. Тема: Организационно-правовые средства защиты информации.	7	9-12	4	0	2	контрольная точка
4.	Тема 4. Тема: Криптографические средства защиты информации.	7	13-15	2	0	2	домашнее задание
5.	Тема 5. ТТема 6: Системы шифрования с двумя ключами. Метод RSA.	7	16-18	2	0	4	контрольная работа
6.	Тема 6. Тема: Электронная подпись на основе эллиптических кривых.	7	2	0	0	4	домашнее задание
6.	Тема 6. Тема: Системы шифрования с двумя ключами. Метод RSA.	7		0	0	4	домашнее задание
.	Тема . Итоговая форма контроля	7		0	0	0	зачет
	Итого			12	0	20	

4.2 Содержание дисциплины

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

лекционное занятие (2 часа(ов)):

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. Современная постановка задачи защиты информации. Основные составляющие информационной безопасности: конфиденциальность, целостность и доступность информации.

лабораторная работа (2 часа(ов)):

Методы, модели и механизмы обеспечения конфиденциальности данных.

Тема 2. Тема: Методы контроля доступа к информации.

лекционное занятие (2 часа(ов)):

Методы идентификации и аутентификации пользователей, технические средства обработки. Метод паролей. Биометрическая аутентификация. Способы разграничения доступа, методы и средства их реализации. Краткая характеристика современных средств разграничения доступа. Дискреционный и мандатный методы доступа.

лабораторная работа (2 часа(ов)):

Методы, модели и механизмы обеспечения целостности данных.

Тема 3. Тема: Организационно-правовые средства защиты информации.

лекционное занятие (4 часа(ов)):

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 (2 часа(ов)):

Методы, механизмы и технологии обеспечения сохранности и правомерной доступности информации в АИС, БД и БнД.

Тема 4. Тема: Криптографические средства защиты информации.

лекционное занятие (2 часа(ов)):

Основные понятия и задачи криптологии (криптографии). Краткий исторический экскурс развития. 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.

лабораторная работа (2 часа(ов)):

Критерии и стандарты информационной безопасности (защищенности) АИС

Тема 5. ТТема 6: Системы шифрования с двумя ключами. Метод RSA.

лекционное занятие (2 часа(ов)):

Математические основы построения ЭК. Прямые и обратные операции в конечных полях. Система шифрования RSA. Система шифрования Эль-Гамаля. Реализации системы Эль - Гамаля на ЭК.

лабораторная работа (4 часа(ов)):

Программная реализация методов построения электронной подписи ЭЦП.

Тема 6. Тема: Электронная подпись на основе эллиптических кривых.

лабораторная работа (4 часа(ов)):

Изучение методов шифрования на эллиптических кривых.

Тема 6. Тема: Системы шифрования с двумя ключами. Метод RSA.

лабораторная работа (4 часа(ов)):

Программная реализация RSA.

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.	7	1-4	подготовка домашнего задания	4	домашнее задание
2.	Тема 2. Тема: Методы контроля доступа к информации.	7	5-8	подготовка домашнего задания	4	домашнее задание
3.	Тема 3. Тема: Организационно-правовые средства защиты информации.	7	9-12	подготовка к контрольной точке	4	контрольная точка
4.	Тема 4. Тема: Криптографические средства защиты информации.	7	13-15	подготовка домашнего задания	4	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
5.	Тема 5. ТТема 6: Системы шифрования с двумя ключами. Метод RSA.	7	16-18	подготовка к контрольной работе	4	контрольная работа
				подготовка к контрольной точке	4	контрольная точка
6.	Тема 6. Тема: Электронная подпись на основе эллиптических кривых.	7	2	подготовка домашнего задания	8	домашнее задание
6.	Тема 6. Тема: Системы шифрования с двумя ключами. Метод RSA.	7		подготовка домашнего задания	8	домашнее задание
	Итого				40	

5. Образовательные технологии, включая интерактивные формы обучения

В соответствии с требованиями ФГОС удельный вес занятий, проводимых в активных и интерактивных формах, составляет не менее 40% аудиторных занятий. Так, в процессе изучения дисциплины " Информационная безопасность" студенты разбирают практические примеры в компьютерном классе, решают предлагаемые кейсы, выступают со стендовыми докладами. До 50% лекционных и практических занятий проходят с использованием презентаций MS PowerPoint.

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 литературы. Подготовка к занятию.

Тема 2. Тема: Методы контроля доступа к информации.

домашнее задание , примерные вопросы:

Изучение литературы. Подготовка к занятию.

Тема 3. Тема: Организационно-правовые средства защиты информации.

контрольная точка , примерные вопросы:

1. Международные стандарты информационного обмена. 2. Понятие угрозы. 3. Информационная безопасность в условиях функционирования в России глобальных сетей. 4. Виды нарушений ИБ 5. Понятия о видах вирусов. 6. Три вида возможных нарушений информационной системы. Защита. 7. Основные нормативные руководящие документы. Стандарт шифрования данных ГОСТ 28147-89

Тема 4. Тема: Криптографические средства защиты информации.

домашнее задание , примерные вопросы:

Изучение литературы. Подготовка к занятию.

Тема 5. TTема 6: Системы шифрования с двумя ключами. Метод RSA.

контрольная работа , примерные вопросы:

Подготовка к контрольной работе

контрольная точка , примерные вопросы:

1. Системы с открытым ключом 2. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. 3. Основные положения теории информационной безопасности информационных систем. 4. Модели безопасности и их применение. 5. Методы защиты информации с использованием голографии являются актуальным и развивающимся направлением 6. Анализ способов нарушений информационной безопасности. 7. Криптографические методы

Тема 6. Тема: Электронная подпись на основе эллиптических кривых.

домашнее задание , примерные вопросы:

Изучение литературы. Подготовка к занятию.

Тема 6. Тема: Системы шифрования с двумя ключами. Метод RSA.

домашнее задание , примерные вопросы:

Изучение литературы. Подготовка к занятию.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

Приложение 1. Примерный перечень вопросов к зачету.

1. Дать определение понятия "Информационная безопасность". Основные методологические и нормативно-правовые документы по информационной безопасности.

2. Основные понятия по защите компьютерных данных. Доступ к информации, санкционированный доступ, несанкционированный доступ, конфиденциальность данных, субъект и объект информационных технологий, доступность компонента или ресурса системы, угроза безопасности автоматизированной информационной системе, ущерб безопасности, уязвимость АСОИ, атака на компьютерную систему, политика безопасности.

3. Основные виды угроз безопасности компьютерных систем, Угрозы нарушения целостности информации, угрозы нарушения работоспособности АСОИ и отказы в работе.

4. Структурные составляющие гипотетической модели нарушителя, Преднамеренные потенциальные угрозы. Классификация каналов несанкционированного доступа.

5. Наиболее распространенные способы несанкционированного доступа в компьютерных технологиях. Перехват паролей, маскарад, незаконное использование привилегий, пассивное вторжение в АСОИ, активное вторжение.

6. Основные подходы для парирования и нейтрализации угроз информационной безопасности: фрагментарный подход и комплекный подход.

7. Политика безопасности. Виды политики безопасности: избирательная политика безопасности, полномочная политика безопасности.

8. Этапы построения системы защиты автоматизированных информационных систем. Составляющие отдельных этапов.

9. Основные задачи методов защиты информации в автоматизированных информационных системах. Принципы системы защиты информации в АСОИ.

10. Принципы криптографической защиты информации. Криптология, криптография, стеганография, криптоанализ. Три класса криптографических систем.

11. Традиционные сиссметричные криптографические системы. Ключ шифрования данных, шифры криптографической защиты данных: шифры перестановок, шифры замены, шифры гаммирования, шифры, основанные на аналитических преобразованиях шифруемых данных.

12. Шифрующие таблицы без ключевого слова.

13. Табличное шифрование методов перестановки по ключевому слову или фразе, задающими перестановку.

14. Табличное шифрование методом двойной перестановки.

15. Шифр Цезаря.

16. Система шифрования Вернама.

17. Шифрование методом гаммирования.

18. Современные симметричные криптосистемы.

19. Стандарт шифрования DES.

20. Алгоритм шифрования IDEA.

21. Отечественный стандарт шифрования данных ГОСТ 28147-89.

22. Концепция криптографической системы с открытым ключом.

23. Однонаправленные Хэш-функции.

24. Криптографическая система шифрования данных RSA.

25. Процедура шифрования и расширения данных в криптографической системе RSA.

26. Схема шифрования Эль Гамаля.

27. Комбинированный метод шифрования данных.

28. Электронная цифровая подпись. Правовые основы электронной цифровой подписи. Федеральный закон РФ "Об электронной цифровой подписи.

29. Проблема аутентификации данных и электронная цифровая подпись.

30. Однонаправленные Хэш-функции. Алгоритмы электронной цифровой подписи.

31. Положения Конституции РФ в области защиты информации.

32. Закон РФ 2011 года "Об электронной подписи".

Приложение 2. Вариант контрольной работы.

Тема: Шифрование RSA.

7.1. Основная литература:

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

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

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

7.2. Дополнительная литература:

Жукова М.Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с.// http://www.znanium.com/bookread.php?book=463061

Васильков А.В. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с.// http://www.znanium.com/bookread.php?book=405313

Черников Б.В. Информационные технологии управления: Учебник / Б.В. Черников. - 2-е изд., перераб. и доп. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 368 с.// http://www.znanium.com/bookread.php?book=373345

Журнал "Информатика и ее применения" // http://elibrary.ru/title_about.asp?id=26694

Журнал "Информатика и образование" // http://elibrary.ru/title_about.asp?id=8739

Журнал "Вычислительные технологии" // http://elibrary.ru/title_about.asp?id=8610

7.3. Интернет-ресурсы:

Борисенко В. Лекции по программированию. Материалы к курсу программирования на мех-мат. ф-те МГУ . - http://mech.math.msu.su/~vvb/2course/Borisenko/lectRus.html

Борисенко В. Материалы по курсу: Алгоритмы и структуры данных? - http://mech.math.msu.su/~vvb/HSE/

Официальный сайт Интернет-университета информационных технологий. - http://www.intuit.ru

Полнотекстовая база данных по общественным и гуманитарным наукам - http://www.ebiblioteka.ru/

Электронная библиотека Elibrary - http://elibrary.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 "КнигаФонд", доступ к которой предоставлен студентам. Электронно-библиотечная система "КнигаФонд" реализует легальное хранение, распространение и защиту цифрового контента учебно-методической литературы для вузов с условием обязательного соблюдения авторских и смежных прав. КнигаФонд обеспечивает широкий законный доступ к необходимым для образовательного процесса изданиям с использованием инновационных технологий и соответствует всем требованиям новых ФГОС ВПО.

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" и профилю подготовки Информационно-аналитические системы в бизнесе .

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

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