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

подписано электронно-цифровой подписью

Программа дисциплины

Основы информационной безопасности Б3.Б.1

Направление подготовки: 090900.62 - Информационная безопасность
Профиль подготовки: Математические и программные средства защиты информации
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 940414

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.Б.1 Профессиональный" основной образовательной программы 090900.62 Информационная безопасность и относится к базовой (общепрофессиональной) части. Осваивается на 2 курсе, 3 семестр.

Данная дисциплина относится к профессиональным дисциплинам.

Читается на 2 курсе в 1 семестре для студентов обучающихся по направлению "Информационная безопасность".

Изучение основывается на результатах изучения дисциплин "Информатика", "Языки программирования".

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-11 (общекультурные компетенции)	способность к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства
ОК-12 (общекультурные компетенции)	способность критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков
ОК-2 (общекультурные компетенции)	способность осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм
ПК-13 (профессиональные компетенции)	способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности
ПК-3 (профессиональные компетенции)	способность использовать нормативные правовые документы в своей профессиональной деятельности
ПК-4 (профессиональные компетенции)	способность формирования комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-6 (профессиональные компетенции)	способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов
ПК-7 (профессиональные компетенции)	способность использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий

В результате освоения дисциплины студент:

1. должен знать:

- сущность и актуальность проблемы информационной безопасности;
- концептуальные подходы к обеспечению информационной безопасности;
- сервисы информаицонной безопасности;
-угрозы информации, средства и методы обеспечения информационной безопасности

2. должен уметь:

- свободно ориентироваться в проблемах ИБ,
- основные методы и средства защиты информации.

3. должен владеть:

- теоретическими знаниями о принципах построения безопасных ИС;
- навыками представление о проблемах информационной безопасности, способах, методах и средств их решения

4. должен демонстрировать способность и готовность:

-применять полученные знания в своей профессиональной деятельности

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 5 зачетных(ые) единиц(ы) 180 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 3 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	
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.	3		6	0	6	домашнее задание
2.	Тема 2. Методы контроля доступа к информации.	3		8	0	8	домашнее задание
3.	Тема 3. Организационно-правовые средства защиты	3		8	0	8	домашнее задание
4.	Тема 4. Криптографические средства защиты информации.	3		8	0	8	домашнее задание
5.	Тема 5. Эллиптические кривые.	3		6	0	6	домашнее задание
.	Тема . Итоговая форма контроля	3		0	0	0	экзамен
	Итого			36	0	36	

4.2 Содержание дисциплины

Тема 1. Сущность, задачи и проблемы информационной безопасности.

лекционное занятие (6 часа(ов)):

1.1. Введение в защиту информации. 1.2. Современная постановка задачи защиты информации. 1.3. Угрозы безопасности информационным системам и их классификация. 1.4. Меры противодействия угрозам безопасности ИС.

лабораторная работа (6 часа(ов)):

Математические основы информационной безопасности. Решение задач.

Тема 2. Методы контроля доступа к информации.

лекционное занятие (8 часа(ов)):

2.1. Методы идентификации и аутентификации пользователей, технических средств обработки, программ и баз данных. 2.2. Классификация информационных систем по степени защищенности. 2.3. "Общие критерии" стран Европейского сообщества, их основные положения. 2.4. Парольная идентификация и аутентификация в сетевых операционных системах.

лабораторная работа (8 часа(ов)):

Обсуждение моделей информационных систем и их систем защиты.

Тема 3. Организационно-правовые средства защиты

лекционное занятие (8 часа(ов)):

3.1. Законодательный уровень защиты информации. 3.2. Основные положения закона "Об информации, информационных технологиях и о защите информации 2006 года, определение понятий информации, документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов. 3.3. Закон "О лицензировании отдельных видов деятельности" от 8 августа 2001 г

лабораторная работа (8 часа(ов)):

Обсуждение основных законодательных аспектов информационной безопасности.

Тема 4. Криптографические средства защиты информации.

лекционное занятие (8 часа(ов)):

4.1. Криптографические средства защиты информации. 4.2. Криптосистемы с секретным ключом. 4.3. Математические основы современной криптологии. 4.4. Хэш-функции. 4.5. Открытое распределение ключей

лабораторная работа (8 часа(ов)):

Методы криптографии. Решение задач.

Тема 5. Эллиптические кривые.

лекционное занятие (6 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 (6 часа(ов)):

Решение задач на построение ЭК. Разбор основных свойств.

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.	3		подготовка домашнего задания	12	домашнее задание
2.	Тема 2. Методы контроля доступа к информации.	3		подготовка домашнего задания	16	домашнее задание
3.	Тема 3. Организационно-правовые средства защиты	3		подготовка домашнего задания	16	домашнее задание
4.	Тема 4. Криптографические средства защиты информации.	3		подготовка домашнего задания	16	домашнее задание
5.	Тема 5. Эллиптические кривые.	3		подготовка домашнего задания	12	домашнее задание
	Итого				72	

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. Конспект лекцийсодержит частичное изложение материала. 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.

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.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Обсуждение. Решение задач.

Тема 2. Методы контроля доступа к информации.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Обсуждение. Решение задач.

Тема 3. Организационно-правовые средства защиты

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Обсуждение. Решение задач.

Тема 4. Криптографические средства защиты информации.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Обсуждение. Решение задач.

Тема 5. Эллиптические кривые.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Обсуждение. Решение задач.

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

По данной дисциплине предусмотрено проведение экзамена. Примерные вопросы для экзамена - Приложение1.

ВОПРОСЫ К ЭКЗАМЕНУ

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

Приложение 2. Вариант контрольной работы.

Контрольная работа 1. Шифрование RSA.

1. Проверить число n=57 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=29, e=239, m=24.

3. Выполнить шифрование данных в системе RSA при заданных начальных данных.

7.1. Основная литература:

1. Расторгуев, С. П. Основы информационной безопасности: учебное пособие / С.П. Расторгуев.?Москва: Академия, 2007.?186 с.

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

3. 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

4. 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

5. 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. 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

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

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

Учебник по математическим основам защиты информации - 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:

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.

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 090900.62 "Информационная безопасность" и профилю подготовки Математические и программные средства защиты информации .

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

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