

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

Криптографические методы защиты информации БЗ.ДВ.4

Направление подготовки: 010400.62 - Прикладная математика и информатика

Профиль подготовки: Математическое и программное обеспечение вычислительных машин и сетей

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Автор(ы):

Разинков Е.В.

Рецензент(ы):

Ишмухаметов Ш.Т.

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 9110414

Казань
2014

Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Программу дисциплины разработал(а)(и) ассистент, к.н. Разинков Е.В. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Evgenij.Razinkov@kpfu.ru

1. Цели освоения дисциплины

В курсе защиты информации рассмотрены как основы информационной безопасности, так и некоторые специальные темы, например, скрытая передача данных.

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

Данная учебная дисциплина включена в раздел " Б3.ДВ.4 Профессиональный" основной образовательной программы 010400.62 Прикладная математика и информатика и относится к дисциплинам по выбору. Осваивается на 4 курсе, 8 семестр.

Данная дисциплина относится к профессиональным дисциплинам.

Читается на 4 курсе в 7 семестре для студентов обучающихся по направлению "Фундаментальная информатика и информационные технологии".

Изучение основывается на результатах изучения дисциплин "Алгебра и геометрия", "Дискретная математика", "Теория кодирования информации и криптография".

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-9 (общекультурные компетенции)	способность осознать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности
ПК-13 (профессиональные компетенции)	способность использовать основы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий и применения современных средств поражения, основных мер по ликвидации их последствий, способность к общей оценке условий безопасности жизнедеятельности
ПК-14 (профессиональные компетенции)	способность владеть методикой преподавания учебных дисциплин

В результате освоения дисциплины студент:

1. должен знать:

- важность обеспечения информационной безопасности

2. должен уметь:

- применять подбирать аппаратные и программные средства защиты информации

3. должен владеть:

- теоретическими знаниями об основных принципах защиты информации, ориентироваться в современных технологиях;

- навыками применения теоретических знаний при решении прикладных задач

4. должен демонстрировать способность и готовность:

- 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 8 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. Введение в защиту информации.	8		0	0	5	домашнее задание
2.	Тема 2. Контроль доступа.	8		0	0	5	домашнее задание
3.	Тема 3. Анализ рисков.	8		0	0	5	домашнее задание
4.	Тема 4. Вредоносное программное обеспечение.	8		0	0	5	домашнее задание
5.	Тема 5. Сетевая безопасность.	8		0	0	6	домашнее задание
6.	Тема 6. Безопасность программного обеспечения.	8		0	0	7	домашнее задание
7.	Тема 7. Скрытая передача информации.	8		0	0	7	домашнее задание
	Тема . Итоговая форма контроля	8		0	0	0	зачет
	Итого			0	0	40	

4.2 Содержание дисциплины

Тема 1. Введение в защиту информации.

лабораторная работа (5 часа(ов)):

Введение в защиту информации. Основные понятия защиты информации: конфиденциальность, целостность, доступность. Роль защиты информации в современном обществе.

Тема 2. Контроль доступа.

лабораторная работа (5 часа(ов)):

Контроль доступа. Аутентификация, основные способы аутентификации, их достоинства и недостатки. Авторизация. Основные модели безопасности: многоуровневая модель, модель Белла-ЛаПадулы.

Тема 3. Анализ рисков.

лабораторная работа (5 часа(ов)):

Анализ рисков. Понятие риска. Основные составляющие риска. Этапы анализа и управления рисками.

Тема 4. Вредоносное программное обеспечение.

лабораторная работа (5 часа(ов)):

Вредоносное программное обеспечение. Классификация вредоносного программного обеспечения. Компьютерные вирусы. Антивирусные техники, их сравнительный анализ.

Тема 5. Сетевая безопасность.

лабораторная работа (6 часа(ов)):

Сетевая безопасность. Протокол IPSec: протоколы AH и ESP. Виртуальные частные сети (VPN).

Тема 6. Безопасность программного обеспечения.

лабораторная работа (7 часа(ов)):

Безопасность программного обеспечения. Атака на переполнение буфера, ее возможности и условия успешного применения.

Тема 7. Скрытая передача информации.

лабораторная работа (7 часа(ов)):

Скрытая передача информации Цифровая стеганография. Понятие стеганографической стойкости. Стегоанализ. Виды стегоанализа, их сравнительная характеристика.

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. Введение в защиту информации.	8		подготовка домашнего задания	5	домашнее задание
2.	Тема 2. Контроль доступа.	8		подготовка домашнего задания	5	домашнее задание
3.	Тема 3. Анализ рисков.	8		подготовка домашнего задания	5	домашнее задание
4.	Тема 4. Вредоносное программное обеспечение.	8		подготовка домашнего задания	5	домашнее задание
5.	Тема 5. Сетевая безопасность.	8		подготовка домашнего задания	5	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
6.	Тема 6. Безопасность программного обеспечения.	8		подготовка домашнего задания	3	домашнее задание
7.	Тема 7. Скрытая передача информации.	8		подготовка домашнего задания	4	домашнее задание
	Итого				32	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лабораторных занятий, а также самостоятельной работы студентов.

Изучение курса подразумевает овладение теоретическим материалом и получение практических навыков для более глубокого понимания разделов дисциплины "Защита информации" 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. Введение в защиту информации.

домашнее задание , примерные вопросы:

Программная реализация алгоритма RSA.

Тема 2. Контроль доступа.

домашнее задание , примерные вопросы:

Программная реализация алгоритма SHA-512.

Тема 3. Анализ рисков.

домашнее задание , примерные вопросы:

Программная реализация схемы Optimal Asymmetric Encryption Padding.

Тема 4. Вредоносное программное обеспечение.

домашнее задание , примерные вопросы:

Программная реализация криптографически стойкого генератора псевдослучайных чисел.

Тема 5. Сетевая безопасность.

домашнее задание , примерные вопросы:

Программная реализация алгоритма AES.

Тема 6. Безопасность программного обеспечения.

домашнее задание , примерные вопросы:

Программная реализация алгоритма DSA.

Тема 7. Скрытая передача информации.

домашнее задание , примерные вопросы:

Программная реализация алгоритма nsF5.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

Контрольная работа 1:

Построение системы аутентифицированного шифрования.

Контрольная работа 2:

Реализация стеганографического встраивания информации с нарушением квантования.

Вопросы к зачету:

1. Основная задача защиты информации.
2. Атаки.
3. Угрозы.
4. Аутентификация.
5. Вредоносное программное обеспечение.
6. Виды вредоносного программного обеспечения.
7. Антивирусные техники.
8. Модель безопасности Харрисона-Пуццо-Ульмана.
9. Матрица доступов (модель ХРУ).
10. Примитивные операторы (модель ХРУ).
11. Команды (модель ХРУ).
12. Утечка права (модель ХРУ).
13. Модель распространения прав доступа Take-Grant.
14. Граф доступов в модели Take-Grant.
15. Де-юре правила (правила преобразования графа доступов) в модели Take-Grant.
16. Предикат "возможен доступ" (модель Take-Grant).
17. Предикат "возможно похищение" (модель Take-Grant).
18. Остров, мост, начальный пролет моста, конечный пролет моста (модель Take-Grant).
19. Вирусное множество (абстрактная теория компьютерных вирусов).
20. Теорема об определении утечки права для монооперационных систем защиты информации.
21. Теорема об определении утечки права для произвольной системы защиты информации.
22. Необходимое и достаточное условие истинности предиката "возможен доступ" в случае, когда граф доступов состоит только из субъектов (модель Take-Grant).
23. Необходимое и достаточное условие истинности предиката "возможен доступ" (модель Take-Grant).
24. Необходимое и достаточное условие истинности предиката "возможно похищение".
25. Теорема о невозможности создания универсального антивируса.

Типовой билет:

1. Формулировка теоремы о необходимом и достаточном условии истинности предиката "возможно похищение".
2. Предикат "возможен доступ" (модель Take-Grant).

7.1. Основная литература:

1. Громкович, Ю. Теоретическая информатика: Введение в теорию автоматов, теорию вычислимости, теорию сложности, теорию алгоритмов, рандомизацию, теорию связи и криптографию. - Издание 3 - е. - СПб: БХВ - Петербург, 2010. - 336 с.
2. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с.
<http://znanium.com/catalog.php?bookinfo=441493>
3. 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://znanium.com/bookread.php?book=405000>
4. Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие, 2012. - URL: <http://kpfu.ru/docs/F366166681/mzi.pdf>

7.2. Дополнительная литература:

1. Применко Э. А. Алгебраические основы криптографии: М.: URSS: [ЛИБРОКОМ, 2013]..283 с
2. Латыпов, Р. Х. Математические основы кодирования информации и криптографии: учеб. Пособие./ Казан. гос. ун - т. - Казань: [КГУ], 2005. - 59 с.
3. Земор, Жиль. Курс криптографии / Жиль Земор; пер. с фр. В.В. Шуликовской. - М.; Ижевск: Ин - т компьютер. исслед.: Регуляр. и хаотич. динамика, 2006. - 255 с
4. Введение в теоретико-числовые методы криптографии : учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090101 "Криптография" / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин .? Санкт-Петербург [и др.] : Лань, 2011 .? 394 с.

7.3. Интернет-ресурсы:

Википедия - <http://ru.wikipedia.org>

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

Интернет-портал со статьями по алгоритмике и программированию - <http://algolist.manual.ru/>

Портал математических интернет-ресурсов - <http://www.math.ru/>

Портал ресурсов по информационной безопасности - <http://all-ib.ru/>

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Криптографические методы защиты информации" 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.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен студентам. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Лабораторные занятия по дисциплине проводятся в компьютерном классе.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010400.62 "Прикладная математика и информатика" и профилю подготовки Математическое и программное обеспечение вычислительных машин и сетей .

Автор(ы):

Разинков Е.В. _____

"__" _____ 201__ г.

Рецензент(ы):

Ишмухаметов Ш.Т. _____

"__" _____ 201__ г.