МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"

УТВЕРЖДАЮ

Проректор по научной деятельности КФУ

Проф. Д.К. Нургалиев ____________

"12" ______09______ 2014 г.

Программа дисциплины

Б1.В.ДВ.1 Избранные вопросы информационной безопасности

Направление подготовки: 02.06.01 Компьютерные и информационные науки

Направленность (профиль) подготовки: 05.13.11. Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Квалификация выпускника «Исследователь. Преподаватель-исследователь»

Форма обучения: очная

Язык обучения: русский

Казань 2014

1. КРАТКАЯ АННОТАЦИЯ

Дисциплина посвящена вопросам информационной безопасности сложных вычислительных систем и комплексов, проблемам безопасного хранения, обработке и передаче информации по информационным сетям. Также предложены нормативные документы в области информационной безопасности, постановления правительства и Госдумы РФ.

Дисциплина должна дать общее представление об основных задачах информационной безопасности, ее методах и средствах, вопросах прикладного построения безопасных информационных систем.

1.1. Цели освоения дисциплины

В рамках дисциплины рассматриваются основные математические модели, связанные с распределением ресурсов в сложных системах, прежде всего в телекоммуникации и компьютерных сетях. Рассматриваются общие подходы к информационной безопасности, условия надежного хранения и алгоритмы безопасной обработке информации. Рассматриваются общие задачи, возникающие при проектировании вычислительных сетей с фиксированными и мобильными абонентами, и основные подходы к их решению. Изучаются современные законодательные методы защиты данных, основные законы и постановления в области ИБ.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

Дисциплина относится к дисциплинам по выбору в программе обучения аспирантов по направлению 02.06.01 Компьютерные и информационные науки, по профилю 05.13.11 «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей». Дисциплина рекомендуется для выбора тем аспирантам, тема исследований которых связана с применением математических методов обработки данных, передачей их по сетям, работе с конфиденциальной информацией.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Аспирант, завершивший изучение дисциплины, должен
знать:
- основные математические модели, связанные с распределением ресурсов в сложных системах, в телекоммуникации и компьютерных сетях;

уметь:
- применять методы защиты данных для конкретных задач и выбирать алгоритмы поиска их решений;
- понимать основные подходы к построению безопасных моделей в сложных системах и их приложениях;

владеть:
- навыками построения безопасных сложных информационных систем;
- навыками практического применения методов защиты данных для решения прикладных задач;

демонстрировать способность и готовность:
- применять результаты освоения дисциплины в профессиональной деятельности.

В результате освоения дисциплины формируются компетенции:

Профессиональные:

ПК-3-способность к преподаванию дисциплин и учебно-методической работе в областях профессиональной деятельности, в том числе, на основе результатов проведенных теоретических и экспериментальных исследований;

Владение широким кругом знаний и навыков в области математического моделирования, применения математического аппарата исследования операций и методов принятия решений, особенно для решения задач разработки математического и программного обеспечения вычислительных машин, комплексов и компьютерных сетей.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

4.1. Распределение трудоёмкости дисциплины (в часах) по видам нагрузки обучающегося и по разделам дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов (лекции 18 ч., практика 18 ч., самостоятельная работа 72 ч.).

Форма промежуточной аттестации по дисциплине: зачет в 4-м семестре.

	Раздел дисциплины	**Семестр**	**Лекции**	**Практические занятия**	**Лабораторные работы**	**Самостоятельная работа**
1.	Задачи и методы информационной безопасности.	4	4	4	0	16
2.	Современное законодательство в области информационной безопасности.	4	4	4	0	16
3.	Системы шифрования с двумя ключами: RSA, эллиптические кривые.	4	4	4	0	16
4.	Математические проблемы построения защищенных информационных комплексов.	4	6	6	0	24
	Итого:		18	18	0	72

4.2 Содержание дисциплины

Тема 1. Задачи и методы информационной безопасности.
Лекционные занятия (4 часа):

Сущность и задачи информационной безопасности. Введение в защиту информации. Угрозы безопасности информационным системам и их классификация. Меры противодействия угрозам безопасности ИС. Классификация средств и методов защиты.

Практические занятия (4 часа):

Практика построения безопасных информационных систем. Аудит системы безопасности. Классификация классов защиты. Разбор методов защиты и условий их применения.

Тема 2. Современное законодательство в области информационной безопасности.
Лекционные занятия (4 часа):

Основные федеральные законы РФ в области информационной безопасности: "Об информации, информационных технологиях и о защите информации 2006 года, определение понятий информации, документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов. Закон № 63-ФЗ «Об электронной подписи» 2011 года о свойствах электронной подписи, условиях ее применения, алгоритме построения и юридической силе. Российские стандарты в области информационной безопасности. Доктрина национальной безопасности РФ.

Практические занятия (4 часа):
Подготовка рефератов и их разбор по теме российского законодательства в области информационной безопасности.

Тема 3. Системы шифрования с двумя ключами: RSA, эллиптические кривые.
Лекционные занятия (4 часа):
Классические защиты шифрования информации на основе одного ключа. Криптографические примитивы. Подстановки и перестановки. Математические основы современной криптологии. Открытое распределение ключей. Конечные поля. Эллиптические кривые в конечных полях. Групповые свойства множеств точек эллиптических кривых. Задача вычисления кратного точки ЭК.

Практические занятия (4 часа):
Решение задач на шифрование с использованием перестановок, подстановок, метода RSA, эллиптических кривых.

Тема 4. Математические проблемы построения защищенных информационных комплексов.
Лекционные занятия (6 часов):
Построение систем шифрования на основе эллиптических кривых. Вычисление кратного точки ЭК в афинных и проективных координтатах. Методы факторизации натуральных чисел. Метод Ферма и ро-метод Полларда. Методы вычисления дискретного логарифма в конечном поле. Метод больших и малых шагов Шенкса.

Практические занятия (6 часов):
Выполнение лабораторной работы на компьютерах по разработке программ факторизации по методам Ферма и Полларда. Построение экспериментальных оценок сходимости и криптостойкости RSA и метода Эль-Гамаля.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Основными формами занятий по дисциплине являются лекционные и практические занятия, а также самостоятельная работа аспирантов, которая включает самостоятельное изучение передовой учебной и научной литературы в области исследований операций. Аудиторные занятия практического типа проводятся в активной, дискуссионной форме, включая совместное решение задач, доклады, подготовленные студентами в процессе самостоятельной работы, дискуссии и обсуждения различных методом математического моделирования и методов исследования операций.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Вопросы к практическим занятиям

Тема 1. Задачи и методы информационной безопасности.

1. Сформулировать сущность и задачи информационной безопасности, угрозы информационной безопасности, методы и средства защиты.
2. В чем заключается комплексная система информационной безопасности?
3. Сформулировать задачи физической системы защиты информации.
4. Сформулировать задачи технической системы защиты информации.
5. Сформулировать задачи организационной системы защиты информации.
6. Что такое золотые сервисы информационной безопасности?
7. В чем заключается принцип разумной достаточности построения комплексной системы ИБ?

Тема 2. Современное законодательство в области информационной безопасности.

1. Сформулировать основные понятия ФЗ "Об информации, информационных технологиях и о защите информации 2006 года, определение понятий информации, документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов.

2. Сформулировать основные понятия ФЗ № 63-ФЗ «Об электронной подписи» 2011 года о свойствах электронной подписи, условиях ее применения, алгоритме построения и юридической силе.

3. Сформулировать основные понятия Доктрины национальной безопасности РФ.

4. Сформулировать определение и свойства хеш-функций, алгоритм построения электронной цифровой подписи.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

7.1. Регламент дисциплины

Цикл аудиторных занятий по предмету составляет 18 лекционных часов, 18 часов практических занятий и 72 часа самостоятельной работы, всего 3 зачетные единицы.

7.2. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы аспирантов

Оценочные средства текущего контроля состоят из проверки домашних заданий, подготовки аспирантами ответов по вопросам программы, подготовки рефератов и защиты их в аудитории.

Возможные темы рефератов:

1. Основные федеральные законы РФ в области информационной безопасности. ФЗ 2006 года "Об информации, информационных технологиях и о защите информации.

2. Закон № 63-ФЗ «Об электронной подписи» 2011 года о свойствах электронной подписи, условиях ее применения, алгоритме построения и юридической силе.

3. Российские стандарты в области информационной безопасности.

4. Доктрина национальной безопасности РФ.

7.3. Вопросы к зачету.

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, технические, 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 положения.

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 Федерального Закона «Об информации, информационных технологиях и о защите информации» (в редакции от 27.07.2006), определение понятий информации, документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов.

22. Основные положения закона Федерального Закона «О персональных данных» от 27

июля 2006 г.

23. Основные положения закона РФ "Об электронной подписи" (от 4 апреля 2011 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. Примеры шифров замены и перестановки. Методы их дешифрования.

27. Криптографические примитивы: перестановки, подставки, гаммирование.

28. Блочные и потоковые криптосистемы.

29. Математические основы современной криптологии.

30. Криптосистемы с открытым ключом (ассиметричные).

31. Система RSA.

32. Хэш-функции. Их свойства.

33. Использование хэш-функций для защиты паролей, целостности и конфиденциальности информации.

34. Открытое распределение ключей.

35. Прямые и обратные операции в конечных полях.

36. Система шифрования Эль-Гамаля.

37. Реализации системы Эль - Гамаля на ЭК.

38. Алгоритм электронной подписи на эллиптических кривых.

7.4. Таблица соответствия компетенций, критериев оценки их освоения и оценочных средств

Индекс компетенции	**Расшифровка компетенции**	**Показатель формирования компетенции для данной дисциплины**	**Оценочное средство**
ПК-3	ПК-3-способность к преподаванию дисциплин и учебно-методической работе в областях профессиональной деятельности, в том числе, на основе результатов проведенных теоретических и экспериментальных исследований;	Аспирант овладел специальным материалом по предмету в степени достаточной для преподавания дисциплины в ВУЗе	Защита реферата по теме.
		Аспирант способен к выполнению научных исследований в области защиты информации.	Зачет по темам лекционных и практических занятий.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПРИ ОСВОЕНИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для подготовки к зачету по дисциплине рекомендуется сочетание разных форм самостоятельной работы аспирантов:

1. Чтение основной и дополнительной литературы. Самостоятельное изучение материала по литературным источникам.

2. Работа с библиотечным каталогом, самостоятельный подбор необходимой литературы.

3. Работа со словарем, справочником.

4. Поиск необходимой информации в сети Интернет.

5. Конспектирование источников.

6. Реферирование источников.

7. Составление аннотаций к литературным источникам.

8. Составление рецензий и отзывов на прочитанный материал.

9. Составление обзора публикаций по теме.

10. Составление и разработка словаря (глоссария).

11. Составление или заполнение таблиц.

12. Составление библиографии (библиографической картотеки).

13. Работа по трансформации учебного материала, перевод его из одной формы в другую.

14. Ведение дневника (дневник практики, дневник наблюдений, дневник самоподготовки и т.д.)

15. Прослушивание учебных аудиозаписей, просмотр видеоматериала.

16. Выполнение аудио - и видеозаписей по заданной теме.

17. Подготовка к различным формам промежуточной и итоговой аттестации (к тестированию, контрольной работе, зачету, экзамену).

18. Выполнение домашних контрольных работ.

19. Самостоятельное выполнение практических заданий репродуктивного типа (ответы на вопросы, тренировочные упражнения, опыты, задачи, тесты).

20. Выполнение творческих заданий.

21. Проведение опыта и составление отчета по нему.

22. Подготовка устного сообщения для выступления на занятии.

23. Написание реферата. Подготовка к защите (представлению) реферата на занятии.

24. Подготовка доклада и написание тезисов доклада.

25. Выполнение комплексного задания или учебного проекта по учебной дисциплине. Подготовка к его защите на семинарском или практическом занятии.

26. Подготовка к участию в деловой игре, конкурсе, творческом соревновании.

27. Подготовка к выступлению на конференции.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

9.1. Основная литература.

1. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел/ Ш.Т.Ишмухаметов. - Казань: Казан. гос. ун-т, 2011.- 187 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

9.2. дополнительная литература:

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш .— 2-е изд. — Москва : РИОР : ИНФРА-М, [2014] .— 254, [1] с.

2. Кандаурова, Н. В. Вычислительные системы, сети и телекоммуникации. (Курс лекций и лабораторный практикум) [Электронный ресурс]: учеб. пособие / Н. В. Кандаурова, С. В. Яковлев, В. П. Яковлев и др. - 2-е изд., стер. - М.: ФЛИНТА, 2013. - 344 с.

http://znanium.com/bookread.php?book=466100
3. Расторгуев, С. П. Основы информационной безопасности: учебное пособие / С.П. Расторгуев.-Москва: Академия, 2007.,186 с.

9.3. Программное обеспечение и Интернет-ресурсы:

- Интернет-ресурсы по математике: http://exponenta.ru;
- Портал математических интернет-ресурсов: http://www.math.ru;
- Портал математических интернет-ресурсов: http://www.allmath.com;
- Портал ресурсов по математике и ИТ: http://algolist.manual.ru;
- Научный портал по математическим наукам: http://www.mathnet.ru;
- Электронная библиотечная система «Лань»: http://e.lanbook.com;
- Электронная библиотечная система «Знаниум»: http://znanium.com

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитории, оборудованные мультимедийным оборудованием, компьютерные классы.

Программа составлена в соответствии с требованиями ФГОС ВО аспирантуры (Приказ Минобрнауки РФ от 30.07.2014 № 872)

Автор(ы): д.ф.-м.н., профессор Ишмухаметов Ш.Т.

Рецензенты: д.т.н., профессор Латыпов Р.Х.
к.ф.-м.н., доцент Андрианова А.А.,

Программа одобрена на заседании Учебно-методической комиссии Института ВМ и ИТ КФУ от 11 сентября 2014 г. протокол № 1.