МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт компьютерных технологий и информационной безопасности

УТВЕРЖДАЮ
Директор Института компьютерных технологий и информационной безопасности
_____ Г.Е. Веселов
«__» _____ 2018 г.

Программа вступительного экзамена в аспирантуру по специальной дисциплине

Направление подготовки
10.06.01 Информационная безопасность

Направленность образовательной программы
Методы и системы защиты информации, информационная безопасность

Уровень высшего образования
подготовка кадров высшей квалификации (аспирантура)

Таганрог 2018

Программа отражает современное состояние знаний по направлению «Информационная безопасность» отрасли «Технические науки» и включает важнейшие профессиональные разделы, знание которых необходимо высококвалифицированному специалисту. Программа содержит также важнейшие естественнонаучные разделы и разделы по смежным областям информационных технологий, знание которых необходимо специалисту по направлению «Информационная безопасность».

Сдающий вступительное испытание по данной программе должен показать высокий уровень теоретической и профессиональной подготовки, знание основ теории, методов и средств защиты информации в современных системах ее обработки, путей и способов организации защиты с учетом текущего состояния и перспектив информатизации общества.

СОДЕРЖАНИЕ ПРОГРАММЫ

1. Избранные разделы математики

1. Методы решения систем линейных уравнений.
2. Методы интерполяции.
3. Методы численного интегрирования.
4. Методы численного решения дифференциальных уравнений.
5. Численные методы нахождения экстремумов функций.
6. Элементы комбинаторики: перестановки, выборки, сочетания и размещения без повторений и с повторениями, биномиальные коэффициенты и их свойства.
7. Элементы теории графов: определение графа, способы представления.
8. Изоморфизм графов, элементы графов, валентность, маршруты, цепи, циклы.
9. Связность графов, подграфы, виды графов и операции над ними.
10. Алгебра логики, формулы алгебры логики, высказывания и операции, построение формул.
11. Булевы функции алгебры логики, способы представления булевых функций, нормальные формы.
12. Карты Карно, минимизация булевых функций с помощью карт Карно.
13. Случайные события, полная группа событий, зависимые и независимые случайные события, вероятность случайного события.
14. Теоремы сложения и умножения вероятностей.
15. Формула полной вероятности. Вероятность гипотез. Формулы Байеса.
16. Случайные величины, виды случайных величин, характеристики случайных величин: математическое ожидание, дисперсия.
17. Функция распределения и плотность распределения вероятностей случайной величины.
18. Основные законы распределения случайной величины: равномерный, нормальный, показательный.
19. Многомерные случайные величины. Совместные распределения случайных величин.
20. Основные задачи математической статистики: статистические оценки параметров распределения, доверительные интервалы, расчет сводных характеристик распределения.
21. Метод Монте-Карло. Основные определения и понятия. Оценка погрешности.
22. Генерирование значений дискретных случайных величин.
23. Цепи Маркова. Марковские процессы с дискретным временем, матрицы перехода дискретной цепи Маркова, предельные вероятности.
24. Случайные процессы. Классификация случайных процессов. Стационарные и нестационарные случайные процессы.
25. Основные характеристики случайных процессов: среднее квадратичное

отклонение, дисперсия, плотность распределения, автокорреляционная функция, спектральная плотность.

26. Совместные характеристики случайных процессов: совместная плотность распределения, взаимная корреляционная функция, взаимная спектральная плотность.

2. Структуры данных и прикладные алгоритмы

1. Понятие данных и информации. Семантика данных. Моделирование данных.
2. Структуры данных. Множества: домены и атрибуты. Отношения: сущности и связи. Представление и реализация: таблицы и графы.
3. Элементарные и линейные данные и их хранение. Целые и вещественные числа. Символьные данные, логические данные, указатели, массив, стек, очередь, таблица.
4. Нелинейные структуры данных и их хранение. Графы и деревья. Типы деревьев. Хранение древовидных структур. Списковые структуры. Деревья поиска и их применение. Кратчайшие пути в графе.
5. Алгоритмы. Понятие и определение алгоритма. Требования к алгоритмам. Понятие сложности алгоритма. Машина Тьюринга. Способы описания алгоритмов.
6. Способы упорядочивания информационных массивов. Основные понятия и принципы сортировки. Внутренняя и внешняя сортировки. Основные алгоритмы сортировки.
7. Поиск информации в массивах. Основные принципы информационного поиска. Последовательный поиск. Ускоренные методы поиска. Поиск по двоичному дереву. Особенности многоаспектного поиска. Хеширование.
8. Справочники. Общий справочник, единый справочник, справочник, основанный на структуре сбалансированного дерева.

3. Вычислительная техника и программирование

1. Архитектура современных ЭВМ, принципы работы отдельных компонент.
2. Языки программирования высокого и низкого уровня, компиляторы и интерпретаторы.
3. Технология объектно-ориентированного программирования.
4. Операционные системы: функции ядра, функции защиты информации, основные типы ОС.
5. Локальные и глобальные вычислительные сети, типовые конфигурации, маршрутизация.
6. Основные протоколы обмена данными в вычислительных сетях, их информационная безопасность.
7. Методы и средства хранения высокочувствительной информации в ЭВМ (криптографических ключей, паролей).
8. Защиты программ от изучения, защита от изменения и контроль целостности.
9. Защита от разрушающих программных воздействий.

4. Теоретические основы информационной безопасности

1. Понятие угрозы информационной безопасности. Виды угроз, взаимосвязь угроз, атак и уязвимостей. Системы классификации и оценки уязвимостей.
2. Основные методы реализации угроз информационной безопасности. Основные

принципы обеспечения информационной безопасности в компьютерных системах.

3. Методы оценки угроз информационной безопасности. Модель угроз. Модель нарушителя. Модели анализа рисков информационной безопасности.
4. Причины, виды и каналы утечки информации.
5. Построение систем защиты от угрозы нарушения конфиденциальности информации.
6. Построение систем защиты от угрозы нарушения целостности информации.
7. Построение систем защиты от угрозы отказа доступа к информации.
8. Политика безопасности. Понятие политики безопасности. Понятия доступа и монитора безопасности. Основные типы политик безопасности. Основные подходы к разработке политик безопасности.
9. Модели безопасности. Модель матрицы доступа HRU.
10. Модель системы безопасности Белла-Лападула.
11. Основные критерии защищенности автоматизированных систем. Классификация систем защиты автоматизированных систем. Руководящие документы ФСТЭК России.
12. Общие критерии. Основные положения общих критериев.

5. Основы криптографической защиты информации

1. Криптографические методы зашиты информации. Основные понятия криптографии.
2. Шифры и их свойства. Композиции шифров. Системы шифрования. Теоретическая, практическая и временная стойкость шифров.
3. Шифры замены и перестановки, их свойства. Блочные шифры. Потоковые шифры.
4. Криптографические хеш-функции, их свойства и использование.
5. Методы получения псевдослучайных последовательностей и их использование в криптографии.
6. Шифрсистемы с секретным ключом. Классификация шифрсистем с секретным ключом. Шифрсистемы поточного шифрования (синхронные и асинхронные).
7. Итерационные системы блочного щифрования (шифры Фейстеля, IDEA, RIJNDAEL). Режимы шифрования. Автоматные модели шифров.
8. Криптография с открытым ключом. Однонаправленные функции с секретом и их применение. Схемы шифрования с открытым ключом. Схемы шифрования и подписи RSA и Рабина. Схемы открытого шифрования Эль Гамаля.
9. Электронная цифровая подпись. Схемы цифровой подписи RSA и Рабина и их применение. Схема цифровой подписи Эль Гамаля и ее модификации. Стандарты цифровой подписи США (DSA) и России (ГОСТ Р 34.10). Методы генерации секретных параметров для стандартов цифровой подписи. Разновидности схем электронной цифровой подписи и их применение.
10. Вопросы генерации и распределения ключей. Протоколы генерации и распределения ключей.
11. Криптографическая стойкость шифров. Активные и пассивные атаки на шифрсистемы. Теоретически стойкие шифры. Практическая стойкость шифров, её основные характеристики. Связь между временной и вычислительной сложностью дешифрования. Классификация методов криптографического анализа.

6. Защита информации в компьютерных сетях

1. Классификация сетей по способам распределения данных. Сравнительная характеристика различных типов сетей. Основы организации и функционирования сетей.
2. Средства взаимодействия процессов в сетях.
3. Распределенная обработка информации в системах клиент-сервер. Одноранговые сети.
4. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа. Межсетевые экраны (МЭ). Типы, классы, основные свойства МЭ. Создание демилитаризованных зон с помощью МЭ.
5. Понятие о средствах адаптивной безопасности. Классификация средств адаптивной безопасности. Сетевые и хостовые системы обнаружения атак.
6. Сканеры уязвимостей. Ложные информационные объекты (обманные системы). Аудит информационной безопасности.
7. Средства повышения надежности функционирования сетей.
8. Интеграция локальных сетей в региональные и глобальные сети.
9. Эталонная модель взаимодействия открытых систем. Общие сведения о протоколах эталонной семиуровневой модели.
10. Глобальные и локальные сети: особенности современных сетевых архитектур, архитектурные особенности локальных сетей, протоколы физического и канального уровней.

7. Безопасность систем баз данных

1. Концепция безопасности баз данных (БД). Интерпретация критериев оценки надежных компьютерных систем для надежных СУБД. Европейские критерии. Руководящие документы ФСТЭК России.
2. Модели безопасности в системах управления базами данных (СУБД). Дискреционный принцип разграничения доступа. Одноуровневая модель безопасности СУБД. Добровольное, принудительное и комбинированное управление доступом. Мандатный принцип разграничения доступа. Многоуровневая модель безопасности СУБД.
3. Идентификация и аутентификация субъектов в БД. Аутентификация объектов и процессов. Особенности процедур идентификации/аутентификации в СУБД.
4. Управление доступом в БД. Привилегии, группы, роли, представления. Соотношение прав доступа СУБД и ОС. Метки безопасности и принудительный контроль доступа.
5. Обеспечение целостности данных. Доменная целостность. Сущностная целостность. Ссылочная целостность. Ограничения. Правила.
6. Регистрация действий пользователей, влияющих на информационную безопасность. Регистрируемые события. Управление набором регистрируемых событий. Анализ регистрационной информации.
7. Угрозы, специфичные для СУБД. Логический вывод. Агрегатирование данных. Покушения на высокую готовность. Технология разрешенных процедур.
8. Обеспечение высокой доступности. Технологии постоянного дублирования. Технологии архивации. Кластерные системы высокой готовности. Тиражирование данных. Зеркальное отображение БД. Репликация БД. Способы обеспечения катастрофоустойчивости БД.

8. Технические средства и методы защиты информации

1. Структура, классификация и основные характеристики технических каналов утечки информации.
2. Побочные электромагнитные излучения и наводки.
3. Классификация средств технической разведки, их возможности.
4. Концепция и методы инженерно-технической защиты информации.
5. Методы скрытия речевой информации в каналах связи.
6. Методы обнаружения и локализации закладных устройств.
7. Методы подавления опасных сигналов акустоэлектрических преобразователей.
8. Методы подавления информативных сигналов в цепях заземления и электропитания.
9. Виды контроля эффективности защиты информации.
10. Методы расчета и инструментального контроля показателей защиты информации.

ЛИТЕРАТУРА

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учеб. Пособие для вузов. - М.: Гелиос АРИ, 2001 г. - 480 с.
2. Андерсон Дж. А. Дискретная математика и комбинаторика: Пер. с англ. - М.: Дом «Вильямс», 2003 г.
3. Аникин П.П., Балыбердин А.Л. и др. Государственная тайна в Российской Федерации, С-Петербургский университет, 2000 г.
4. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. курс. - М.: Горячая линия-телеком, 2002 г. - 175 с.
5. Бахвалов Н.С. Численные методы, 2003 г.
6. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учеб. пособие для вузов. - М.: Горячая линия- телеком, 2006 г. - 544 с.
7. Вьюкова Н.И., Галатенко В.А. Информационная безопасность систем управления базами данных. СУБД, 1996, № 1.
8. Галатенко В.А. Основы информационной безопасности // Интернет-университет информационных технологий - Интуит.ру, 2005 г.
9. Гмурман В.Е. Теория вероятностей и математическая статистика. - 2003 г.
10. Гостехкомиссия России. Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения. - М.: ГТК, 1992 г. - 13 с.
11. Гостехкомиссия России. Руководящий документ: Средства вычислительной техники. Межсетевые экраны. Показатели защищенности от несанкционированного доступа. - М.: ГТК, 1997 г. - 17 с.
12. Дейт К. Введение в системы баз данных. - М.: Изд-во: ИД Вильямс, 2001 г. - 1072 с.
13. Демидович Б.П., Марон И.А. Основы вычислительной математики. - 2006 г.
14. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000 г. - 452 с.
15. Золотарев В.В., Федорова Н.А. Анализ защищенности автоматизированных систем: Учебное пособие // СибГАУ. - Красноярск, 2007 г.
16. Кириллов В.В., Громов Г.Ю. Введение в реляционные базы данных (+CD): учебник для ВУЗов. - СПб.: БХВ-Петербург, 2009 г. - 464 с.
17. Кузин А.В., Левонисова С.В. Базы данных. - М.: Академия, 2008. - 320 с.
18. Кузнецов С.Д. Основы баз данных: учебное пособие. - М.: Интернет Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2007. - 484 с.

19. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия // Интернет-университет информационных технологий - ИНТУИТ.ру, 2005 г.
20. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. - М.: Горячая линия-Телеком, 2001 г. - 148 с.
21. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие. - М.: Горячая линия-Телеком, 2004 г. - 280 с.
22. Мандиа К., Просис К. Защита от вторжений. Расследование компьютерных преступлений // Изд. "Лори", 2005 г.
23. Марков А.С. Базы данных. Введение в теорию и методологию: Учебник / А.С. Марков, К.Ю. Лисовский. - М.: Финансы и статистика, 2006. - 512 с.
24. Милославская Н.Г., Толстой А.И. Интрасети: доступ в Internet, защита: Учеб.пособие для вузов. - М.: ЮНИТА-ДАНА, 2000 г. - 527 с.
25. Мэйволд Э. Безопасность сетей. Шаг за шагом. - М.: СП ЭКОМ, 2005 г. - 527 с.
26. Новиков Ф.А. Дискретная математика для программистов. - 2003 г.
27. Норткат С. и др. Анализ типовых нарушений безопасности в сетях. - М.: Издат. дом «Вильямс», 2001 г. - 460 с.
28. Петраков А.В., Лагутин В.С. Защита абонентского телетрафика: учеб. пособие. - М.: Радио и связь, 2004 г. - 499 с.
29. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. М.: ДМК, 2000 г.
30. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей // М.: Издательский центр «Академия», 2006 г.
31. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов / Проскурин В.Г., Крутов С.В., Мацкевич И.В. - М.: Радио и связь, 2000. - 168 с.
32. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Защита в операционных системах. Учеб. Пособие для вузов. - М.: Радио и связь, 2000 г. -168 с.
33. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях. - М.: изд-во агентства "Яхтсмен", 1993 г.
34. Романцев Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и стеях. М.: Радио и связь, 1999 г.
35. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: учеб. пособие для вузов. - М.: Горячая линия-телеком, 2005 г. - 229 с.
36. Самарский А.А. Введение в численные методы. - 2005 г.
37. Скиба В.Ю. Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. // СПб.: Питер, 2008 г.
38. Смирнов С.Н. Безопасность систем баз данных. - М.: «Гелиос», 2007 г. - 352 с.
39. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. - М.: ДМК Пресс, 2002 г.
40. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов / П.Н. Девянин, О.О. Михальский, Д.И. Правиков и др. - М.: Радио и связь, 2000 г. - 192 с.
41. Теория вероятностей. Учеб. для вузов. А.В. Печинкин, О.И. Тескин, Г.М. Цветкова и др. М.: МГТУ им Н.Э Баумана, 2004 г.
42. Теория вероятностей. Учеб. для вузов. Вентцель Е.С. - М.: Высшая школа, 1999 г. 575 с.
43. Торокин А.А. Основы инженерно-технической защиты информации. - М.: «Ось-89», 1998 г. - 336 с.
44. Фостер Дж., Лю В. Разработка средств безопасности и эксплойтов / Пер. с англ. // М.: Издательство «Русская Редакция»; СПб.: «Питер», 2007 г.
45. Фостер Дж., Прайс М. Защита от взлома: сокеты, эксплойты, shell-код: Пер. с англ.

Слинкина А. А. // М.: Издательский Дом ДМК-пресс, 2006 г.
46. Харрингтон Джен Л. Проектирование реляционных баз данных. - М.: Изд-во «Лори», 2006 г. - 230 с.
47. Хомоненко А.Д., Цыганков В.М., Мальцев М.Г. Базы данных: учебник для высших учебных заведений / Под ред. проф. А.Д. Хомоненко. - 6-е изд. - СПб.: изд-во "КОРОНА-Век", 2010 г. 736 с.
48. Хорев П.Б. Методы и средства защиты информации в компьютерных системах - М.: Академия, 2005 г. - 255 с.
49. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. - Феникс, 2008 г. - 173 с.
50. Чмора А.Л. Современная прикладная криптография. - М.: Гелиос АРВ, 2001 г.
51. Щербаков А.Ю. Компьютерная безопасность. - М.: издатель Молгачева С.В., 2001 г.
52. Эриксон Д. Хакинг: искусство эксплоита. Пер. с англ. // СПб.: Символ-Плюс, 2005 г.
53. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия. Учебное пособие. Из-воДашков и К 2006, -336 с.
54. Гриняев С.Н. Интеллектуальное противодействие информационному оружию. СИНТЕГ, Москва - 1999.
55. Цыгичко В.Н. и др. Информационное оружие как геополитический фактор и инструмент силовой политики. М,, ИСА РАН, 1997.
56. Издательство: Горячая Линия - Телеком. 2002 г. -336 с.
57. Майкл Далворт Социальные сети руководство по эксплуатации. Издательство: Добрая книга . 2010 г. -248 с.
58. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. М., 1991, с. 25 - 30