МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮГО-ЗАПАДНЫЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ЮЗГУ)

УТВЕРЖДАЮ
Председатель
Приемной комиссии

_____ С.Г. Емельянов
(подпись)

« 28 » марта 2022 г.

ПРОГРАММА

К ВСТУПИТЕЛЬНОМУ ЭКЗАМЕНУ В АСПИРАНТУРУ

по научной специальности

2.3.6. Методы и системы защиты информации,

информационная безопасность

Курск 2022 г.

Программа вступительных испытаний формируется на основе соответствующих федеральных государственных образовательных стандартов высшего образования по программе специалитета и программе магистратуры.

Программа вступительных экзаменов в аспирантуру по направлению подготовки 10.06.01 – «информационная безопасность» по специальности 05.13.19 – «методы и системы защиты информации и информационной безопасности» составлена на основе общей части программы – минимума кандидатского экзамена по данной специальности.

Программа содержит три раздела:

- Избранные разделы математики;
- Вычислительная техника и программирование;
- Защита информации.

В основу программы положены следующие вузовские дисциплины: алгебра и геометрия, теория вероятностей и математическая статистика, математическая логика и теория алгоритмов, дискретная математика, системное программное обеспечение, организация ЭВМ и вычислительных систем, основы информационной безопасности, безопасность операционных систем, безопасность сетей ЭВМ, безопасность баз данных, криптографические методы защиты информации и др.

I. Избранные разделы математики

1. Линейная алгебра. Понятия группы, кольца, поля, их основные свойства. Основы теории конечных полей. Кольца вычетов. Кольцо многочленов над конечным полем. Поля Галуа.
2. Основные понятия теории вероятностей и математической статистики. Условная вероятность и независимость. Последовательность независимых испытаний. Цепи Маркова. Случайные величины и их характеристики: ; функция распределения, моменты, характеристические функции. Сходимость последовательностей случайных величин и сходимость распределений. Закон больших чисел. Центральная предельная теорема. Основные задачи математической статистики: точечная оценка, построение доверительного интервала, различение статистических гипотез.
3. Конечные автоматы. Граф перехода автомата. Графы и орграфы. Перечисление графов и отображений. Алгоритмические задачи на графах.

II. Вычислительная техника и программирование

1. Архитектура современной ЭВМ. Основные принципы работы ее отдельных компонент. Устройство персонального компьютера: центральный

процессор, структура памяти, структура ввода-вывода.

2. Программный интерфейс вычислительной системы. Языки программирования низкого и высокого уровня. Компиляторы и интерпретаторы. Технология объектно- ориентированного программирования.

3. Операционные системы. Функции ядра операционной системы. Функции защиты информации. ; Однопользовательская и многопользовательские многозадачные операционные системы.

4. Локальные и глобальные вычислительные сети. Типовые конфигурации сети. Протоколы обмена данными. Маршрутизация сообщений в сети.

5. Системы управления базами данных. Реляционная, иерархическая и сетевая модели. Распределенные базы данных в сетях ЭВМ.

III. Защита информации

1. Основные принципы современной концепции обеспечения защиты информации. Требования к защите с позиции пользователя. Основные методы защиты информации. Методология организации и проведении работ по разработке и анализу средств защиты информации.

2. Основные положения государственной политики обеспечения информационной безопасности. Современная нормативно-правовая база в области защиты информации, защиты информации. Понятие информации с ограниченным доступом. Цели защиты информации и степени секретности. Лицензирование в области защиты информации. Сертификации средств защиты информации. Аттестации объектов информатики. Правовая основа сертификации.

3. Понятие угрозы информационной безопасности системы. Классификация угроз информационной безопасности. Угрозы нарушения конфиденциальности, целостности информации, отказа служб, разведки параметров системы. Понятия непосредственных и опосредованных угроз. Основные уровни защиты информации в автоматизированных системах. Основные направления и методы реализации информационных угроз.

4. Понятие политики информационной безопасности. Каноническая модель управления доступом. Классификация каналов взаимодействия субъектов доступа. Основные модели управления доступом с взаимодействием субъектов доступа. Понятия дискреционного и мандатного механизмов

управления доступом. Метки безопасности, их назначение в разграничении прав доступа при реализации мандатной модели доступа. Правила разграничения доступа для полномочной модели управления доступом. Особенности использования мандатного механизма управления доступом при разграничении прав доступа субъектов. Правила назначения меток безопасности иерархическим объектам доступа. Анализ возможностей корректной реализации канонических моделей управления доступом в ОС с использованием дискреционного механизма. Анализ возможностей корректной реализации моделей управления доступом с каналом взаимодействия субъектов доступа для ОС UNIX. Исключение субъектов и объектов из схемы мандатного управления доступом. Принципы организации мандатного управления доступом к устройствам. Возможности разграничения доступа к системному диску для ОС Windows NT/2000/XP и Unix. Привилегированные процессы. Механизм обеспечения замкнутости программной среды и его роль в системе защиты. Реализация механизмов парольной защиты. Процедуры идентификации пользователя на рабочей станции и взаимной идентификации удаленных рабочих станций. Контроль целостности информации, основные схемы контроля. Аутентификация информации. Угрозы преодоления парольной защиты. Усиление парольной защиты. Стандарты в области защиты информации в вычислительной системе, "Оранжевая книга" США, российские стандарты.

5. Основные понятия криптографии. Понятие симметричной и ассиметричной криптосистем. Основные типы криптоаналитических атак. Шифрование методом простой замены. Алгоритм простой замены. Шифрование методом полиалфавитной замены. Алгоритм полиалфавитной замены с использованием таблицы Вижинера. Аддитивные методы шифрования. Шифрование методом перестановки. Карты Гамильтона. Аналитические методы шифрования. Система открытого распространения ключей. Использование схемы открытого шифрования для создания цифровых подписей. Применение хэш-функции для создания цифровых подписей. Алгоритм цифровой подписи с использованием хэш-функции.

6. Защита информации от технической разведки. Основные физические канаты утечки информации о функционировании информационной системы. Узлы и блоки оборудования информационной системы, уязвимые для технической разведки. Технические параметры современных средств перехвата побочных сигналов. Методы и средства зашиты от инженерно-технической разведки. Методика оценки качества инженерно-технической защиты.

7. Разрушающие, программные воздействия. Компьютерные вирусы как особый класс разрушающих программных воздействий. Классификация вирусов. Методы выявления и защиты от вирусов. Методика анализа алгоритмов защиты программных реализаций информационных систем. Методы восстановления алгоритмов защиты в программных продуктах Оценка уровня криптографической защиты типовых программных продуктов.

Литература

1. Ахо А., Допкрофт Дж., Ульман Дне. Построение и анализ вычислительных алгоритмов.
2. Берж С. Теория графов и ее применения.
3. Ван дер Варден Б. Л. Алгебра.
4. Гнеденко Б.В. Курс теории вероятностей.
5. Карлин С. Основы теории случайных процессов.
6. Крамер Г. Математические методы статистики.
7. Курош А.Г. Курс высшей алгебры.
8. Ленг С. Алгебра;
9. Рейнгольд Э., Нивергельт Ю., Део Н. Комбинаторные алгоритмы: теория и практика.
10. Романовский В.И. Дискретные цепи Маркова.
11. Сачков В.Н. Комбинаторные методы дискретной математики.
12. Сачков В.Н. Вероятностные методы в комбинаторном анализе.
13. Трахтенброт Б.А., Барздинь Я.М. Конечные автоматы (поведение и синтез).
14. Феллер В. Введение в теорию вероятностей и ее приложения, тт. 1,2.
15. Абель П. Язык Ассемблера для IBM PC и программирования.
16. Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции.
17. Блейк Ю. Сети ЭВМ: протоколы, стандарты, интерфейсы.
18. Буг Г. Объектно-ориентированное программирование с примерами применения.
19. Данкан Р. Профессиональная работа в MS-DOS.
20. Дейтел Г. Введение в операционные системы, тт. 1,2.
21. Дунаев С. UNIX SYSTEM V Release 4.2. Общее руководство.
22. Зайцева Л.В. Алгоритмические языки и программирование.
23. Кастер Х. Основы Windows NT и NTRS.

24. Кейслер С. Проектирование операционных систем для малых ЭВМ.
25. Керниган Б.В., Пайк Р. UNIX - универсальная среда программирования.
26. Мартин Дж. Организация баз данных в вычислительных системах.
27. Подбельский В.В. Язык С++.
28. Пол И. Объектно-ориентированное программирование с использованием С++.
29. Ульман Дж. Основы систем баз данных.
30. Фигурнов В.Э. IBM PC для пользователя.
31. Флинт Д. Локальные сети ЭВМ: архитектура, принципы построения, реализация.
32. Шилдт Г. Программирование на С и С++ для Windows 95.
33. Вартанесян В. А. Радиоэлектронная разведка.
34. Волчин М.Л. Паразитные процессы в радиоэлектронной аппаратуре.
35. Диффи У., Хэллмэн М.Э. Защищенность и имитостойкость в криптографии. ТИИЭР. т. 67, N3, март 1979 г.
36. Дмитриевский Н.Н. Информационная безопасность. Борьба с компьютерными вирусами и другими вредоносными программами.
37. Дориченко С.А., Ященко В.В. "25 этюдов о шифрах.
38. Жельников В. Криптография от папируса до компьютера.
39. Законы РФ "О государственной тайне", "Об информации, информатизации и защите информации", "О стандартизации". Положения о лицензировании Гостехкомисссии и ФАПСИ.
40. Зегжда Д.П., Ивашко А.М Как построить защищенную информационную систему.
41. Касперский Е. Компьютерные вирусы в MS DOS.
42. Кнут Д. Искусство программирования для ЭВМ, т. 2, получисленные алгоритмы.
43. Клиффорд. Яйцо кукушки.
44. Мафтик С. Механизмы защиты в сетях ЭВМ.
45. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через INTERNET.
46. Правиков Д.И. Ключевые дискеты. Разработка элементов систем защиты от несанкционированного копирования.
47. Прелов А.В. Проблемы защиты обрабатываемой средствами ЭВТ информации об утечке за счет перехвата побочных электромагнитных излучений и наводок и общие пути их решения.
48. Прокофьев И.В. Защита информации в телекоммуникационных системах

(учебное пособие).
49. Проскурин В.Г., Проскурин Г.В Типовые программные средства защиты информации и оценка их надежности, (учебное пособие).
50. Проскурин Г.В. Принципы и методы защиты информации, (учебное пособие).
51. Расторгуев С.П. Программные методы защиты информации в компьютерных сетях.
52. Расторгуев С.П., Дмитриевский Н.Н. Искусство защиты и "раздевания" программ.
53. Соболева Т. А. Тайнопись в истории России (История криптографической службы России XVIII - начало XX века)
54. Спесивцев А.В., Вегнер В. А.. Кругяков А.Ю., Серегин В.В., Сидоров В. А. Защита информации в персональных ЭВМ.
55. Хоффман Л. Дж. Современные методы защиты информации.
56. Фролов Г. Тайны тайнописи.
57. Шеннон К. Работы по теории информации и кибернетике.
58. Щербаков А. Зашита от копирования.
59. Щербаков А, Разрушающие программные воздействия.
60. Щербаков А. Введение в проблему защиты информации криптографическими методами.
61. Халяшш Д.Б. Технические средства, используемые для промышленного шпионажа.
62. Ярочкин В.И. Лазерные системы подслушивания.
63. Ярочкин В.И. Подслушивание телефонных переговоров и меры борьбы с подслушиванием.
64. Ярочкин В.И. Радиосистемы акустического подслушивания.
65. Ярочкин В.И. Способы несанкционированного доступа к объектам и источникам конфиденциальной информации.
66. Ярочкин В.И. Технические каналы утечки информации.
67. Ярочкин В.И., Халяшш Д.Б. Основы защиты информации. Служба безопасности предприятия.
68. Konheim A.G. A Primer Cryptography, John Wiiey&Sons, 1981.
69. Russell D., G.T. Gangemi Sr, Computer Security Basics, O'Reilly & Associates, Inc., 1991.
70. Sebery J., Pieprzyk J. Cryptography: An Introduction to Computer Security. Prentice Hall of Australia, New York, London. Toronto, Sydney, Tokio/1989.

Шкала оценивания и минимальное количество баллов, подтверждающее успешное прохождение вступительного испытания (для каждого вступительного испытания)
Шкала оценивания

(критерии выставления баллов)

49 баллов и менее	50-65 баллов	66-84 баллов	85-100 баллов
Минимальное количество баллов, подтверждающее успешное прохождение вступительного испытания – 50 баллов			
Поступающий:	Поступающий:	Поступающий:	Поступающий:
- изложил менее 25% материала, требуемого федеральным государственным стандартом подготовки аспиранта по направлению;	- изложил от 50% до 75% материала, требуемого федеральным государственным стандартом подготовки аспиранта по направлению;	- изложил от 75% до 100% материала, требуемого федеральным государственным стандартом подготовки аспиранта по направлению;	- продемонстрировал владение материалом, как по полноте, так и по глубине полностью соответствующим требованиям федеральным государственным стандартом подготовки аспиранта по направлению;
- продемонстрировал низкий уровень глубины изложения материала по направлению	- продемонстрировал уровень глубины изложения материала по направлению выше среднего	- продемонстрировал высокий уровень изложения материала по направлению.	- владеет системой научных понятий, культурой мышления; фактами научных теорий; методами и процедурами профессиональной деятельности; умение поставить цель и сформулировать задачи, связанные с реализацией профессиональных функций.

Программа обсуждена и рекомендована для вступительного экзамена в аспирантуру по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность на заседании кафедры информационной безопасности протокол №5 от «23» марта 2022 г.