

**Министерство науки и высшего образования Российской Федерации
Калужский филиал
федерального государственного бюджетного
образовательного учреждения высшего образования
«Московский государственный технический университет
имени Н.Э. Баумана» (национальный исследовательский университет)
(КФ МГТУ им. Н.Э. Баумана)**

Кафедра «Защита информации» (ИУК6)

ПРОГРАММА

вступительного экзамена в аспирантуру

по научной специальности

**2.3.6 «Методы и системы защиты информации, информационная
безопасность»**

Калуга, 2024 г.

Содержание программы

1. Информационная безопасность. Основные понятия и структура проблемы обеспечения информационной безопасности.
2. Доктрина информационной безопасности РФ.
3. Национальные интересы РФ в информационной сфере.
4. Основные категории требований к средствам обеспечения информационной безопасности.
5. Государственная система обеспечения информационной безопасности в РФ. Основные правовые акты, регулирующие вопросы информационной безопасности
6. Федеральный закон №187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры».
7. Структура и задачи Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).
8. Требования к средствам обеспечения безопасности и организации контроля обеспечения безопасности значимых объектов критической информационной инфраструктуры.
9. Информационное противоборство и информационно психологические мероприятия.
10. Система защиты государственной тайны в Российской Федерации
11. Основные принципы отнесения сведений к государственной тайне и засекречивания этих сведений. Порядок отнесения сведений к государственной тайне.
12. Порядок допуска должностных лиц и граждан к государственной тайне.
13. Защита конфиденциальной информации.
14. Угрозы безопасности информации в автоматизированных системах.
15. Формирование модели угроз безопасности информации. Выявление и анализ угроз.
16. Организация защиты информации на объектах информатизации.

17. Общие критерии и гармонизированные стандарты Российской Федерации ГОСТ Р ИСО/МЭК 15408.
18. Функциональные уровни Общих критериев.
19. Уровни доверия Общих критериев.
20. Оценочные уровни доверия Общих критериев. Классификация и общая характеристика.
21. Гармонизированные стандарты информационной безопасности ГОСТ Р ИСО/МЭК 15446. Основные положения и назначение.
22. Основные правовые акты и организация деятельности по защите персональных данных.
23. Концепция информационной безопасности автоматизированных систем.
24. Основные задачи защиты информации в операционных системах.
25. Основные задачи защиты информации в базах данных и информационных системах(ИС).
26. Сущность процедур аутентификации, идентификации и авторизации.
27. Типы процедур аутентификации пользователей ИС.
28. Функции системы обнаружения вторжений при обеспечении защиты информации в базах данных и ИС.
29. Методы контроля целостности данных.
30. Цели и организация аудита ИС на соответствие требованиям стандарта защищенности системы.
31. Уязвимость ИС. Классификация уязвимостей информационных систем по ГОСТ Р 56546.
32. Основные задачи обеспечения информационной безопасности облачных вычислений.
33. Криптография с секретным ключом: области применения и основные алгоритмы.
34. Методы передачи ключевой информации.
35. Криптография с открытым ключом: области применения и основные

алгоритмы.

36. Информационная безопасность технологии блокчейн. Защита информации для криптовалют.
37. Хэш-функции. Основные понятия и методы реализации.
38. Стеганография. Основные понятия и направления использования для обеспечения информационной безопасности автоматизированных систем.
39. Методы стеганографии для звуковых файлов и изображений.
40. Методы анализа социальных графов для своевременного выявления потенциально опасных мероприятий в обществе.
41. Защита информации в мобильных устройствах.
42. Сущность и методы реализации электронной цифровой подписи.
43. Современное состояние сертификационной деятельности в области информационной безопасности в России.
44. Политика безопасности и ее структура.
45. Угрозы безопасности информации и их классификация.
46. Структура угрозы безопасности информации.
47. Идентификация угроз безопасности информации.
48. Методика определения угроз безопасности информации в информационных системах ФСТЭК.
49. Оценка вероятности реализации угрозы безопасности информации.
50. Технические каналы утечки информации. Классификация и причины возникновения.
51. Защита информации в информационных технологиях и АС от угроз, реализуемых с использованием скрытых каналов.
52. Конфликт, базовые понятия и структура конфликта.
53. Государственные стандарты Российской Федерации серии 34.ххх.
54. Понятие класса защищенности, определяемого руководящими документами ФСТЭК.
55. Классификация информации (по доступу к ней).

56. Роль компьютерной разведки при построении системы защиты АС. Правовое обеспечение компьютерной разведки.
57. Распространение объектно-ориентированного подхода на информационную безопасность.
58. Понятие угрозы. Наиболее распространенные угрозы. Классификация угроз.
59. Законодательный уровень информационной безопасности. Обзор зарубежного законодательства в области ИБ. Назначение и задачи в сфере обеспечения информационной безопасности.
60. Российские стандарты защищенности автоматизированных систем.
61. Основные положения теории информационной безопасности. Модели безопасности и их применение.
62. Особенности обеспечения информационной безопасности в условиях функционирования в России глобальных сетей.
63. Сущность и содержание проблемы перехвата данных в распределенной информационной системе.
64. Модель нарушителя. Виды нарушителей по классификации ФСТЭК.
65. Классификация различных видов компьютерных вирусов
66. Система охраны объектов компьютерных систем.
67. Организация работы с конфиденциальными информационными ресурсами.
68. Защита от злоумышленных действий обслуживающего персонала и пользователей.
69. Задача определения инсайдера в организации. Основные методы решения.
70. Квантовый компьютер. Основные отличия от стандартного.
71. Нанесение меток на технические и программные изделия. Классификация меток.
72. Квантовый компьютер. Основные модели и отличия от традиционного компьютера.
73. Основы квантовой криптографии.
74. Использование меток для решения задач защиты информации. Классификация меток технических и программных изделий.

Рекомендуемая литература

а) основная литература:

1. В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе Защита информации. - М.: Издательский центр «Академия», 2021. - 304 с. (Сер. Бакалавриат).
2. Смирнов С. Н. Безопасность систем баз данных: учеб. пособие для вузов /М.: Гелиос, 2007. - 350 с.
3. Смирнова Е. В., Пролетарский А. В., Ромашкина Е. А. [и др.]. Технологии коммутации и маршрутизации в локальных компьютерных сетях: учеб. пособие для вузов / - М.: Изд-во МГТУ им. Н. Э. Баумана, 2013. - 389 с.
4. Безопасность операционных систем: учеб. пособие для студ. учреждений высш. образования /[А.М. Сычев, Б.Н. Коробец, С.Н. Смирнов и др.] ; под ред. С.В. Скрыля. - М.: Издательский центр «Академия», 2021. - 256 с. (Сер. Бакалавриат).
5. Родичев Ю. А. Нормативная база и стандарты в области информационной безопасности. : учеб. пособие для вузов /. - 2-е изд. - СПб. : Питер, 2017. - 256 с.. - ISBN 978-5-496-02434-1.
6. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. учеб. пособие / 2-е изд., перераб. и доп. - М. : МГТУ им. Н. Э. Баумана, 2016. - 252 с. : ил. - ISBN 978-5-70384414-4.
7. Вострецова Е. В. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд- во Урал. ун-та, 2019.— 204 с.
8. Галатенко В. А. Основы информационной безопасности. Курс лекций : учеб. пособие для вузов / Галатенко В. А. ; ред. Бетелин В. Б. - 2-е изд., испр. - М. : Интернет- Университет Информационных Технологий, 2004. - 261 с. - (Основы информационных технологий). - Библиогр.: с. 255-260. - ISBN 5-9556-0015-9.
9. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1.
10. Вайц Е. В., Грачева Ю. В. Разработка комплекса организационных и технических мероприятий по защите информации от утечки по техническим каналам на объекте информатизации : метод. указания к выполнению курсовой работы / МГТУ им. Н. Э. Баумана. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2016. - 15 с. : ил. - Библиогр. в конце брош.
11. Стрельцов А. А., Горбатов В. С., Полякова Т. А. [и др.]. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для вузов / ред. Стрельцов А. А. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность). - Библиогр.: с.

242-245. - ISBN 978-57695-4240-4.

б) дополнительная литература:

1. Емельянов В.В., Курейчик В.М., Курейчик В.В. Теория и практика эволюционного моделирования. «ФИЗМАТЛИТ», 2003. - 432 с.
2. Меньшаков Ю. К. Теоретические основы технических разведок : учеб. пособие для вузов / Меньшаков Ю. К. ; ред. Лаврухин Ю. Н. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2008. - 535 с. : ил. - Библиогр.: с. 529-532.
3. Теория информации: учеб. пособие для студ. учреждений высш. образования / [А.И. Куприянов, С.Н. Смирнов, Б.Н. Коробец и др.] ; под ред. С.В. Скрыля. - М.: Издательский центр «Академия», 2021. - 240 с. (Сер. Бакалавриат).
4. Введение в теоретико-числовые методы криптографии: учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург : Лань, 2021. — 400 с. — ISBN 9785-8114-1116-0.
5. Аттетков А.В., Галкин С.В., Зарубин В.С. Методы оптимизации. Учебное пособие. Изд. МГТУ им. Н.Э. Баумана, 2001. - 440 с.
6. Лю Б. Теория и практика неопределенного программирования. // «БИНОМ», 2005. - 416 с.: ил.
7. Talib, Amir Mohamed Towards a Comprehensive Security Framework of Cloud Data Storage Based on Multi Agent System Architecture / R. Atan, R. Abdullah, M.A.A. Murad // Journal of Information Security. — 2012. — № 3. — P. 295—306.

Заведующий кафедрой

ИУК6 «Защита информации»



Мазин А. В.