МИНОБРНАУКИ РОССИИ



Федеральное государственное бюджетное образовательное учреждение

высшего образования

# «Российский государственный гуманитарный университет»

# (ФГБОУ ВО «РГГУ»)

Институт информационных наук и технологий безопасности

Факультет информационных систем и безопасности

Кафедра комплексной защиты информации

**Методы и системы защиты информации, информационная безопасность**

Программа вступительного испытания в аспирантуру

2.3. Информационные технологии и телекоммуникации

(Шифр и наименование группы научных специальностей)

2.3.6. Методы и системы защиты информации,

информационная безопасность

(Шифр и наименование научной специальности)

Москва 2023

Методы и системы защиты информации, информационная безопасность

Программа вступительного испытания в аспирантуру

2.3. Информационные технологии и телекоммуникации.

2.3.6. Методы и системы защиты информации, информационная безопасность

Составитель**:** к.т.н. Д.А. Митюшин

Программа утверждена

на заседании кафедры комплексной защиты информации

\_\_23 марта\_\_\_\_ 2023 г., протокол № 8

Программа утверждена

на заседании Ученого совета ИИНТБ

30 марта 2023 г., протокол № 8

Программа утверждена

на заседании Научно-методического совета

по аспирантуре и докторантуре

20.04.2023 г., протокол № 1

© Российский государственный

 гуманитарный университет, 2023

# Введение

Настоящая программа предназначена для поступающих на обучение по программам подготовки научно-педагогических кадров в аспирантуре по группе научных специальностей 2.3. Информационные технологии и телекоммуникации, по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Программа включает содержание профилирующих учебных дисциплин, входящих в основную образовательную программу высшего профессионального образования, по которой осуществляется подготовка студентов, в соответствии с требованиями государственного образовательного стандарта. Поступающий в аспирантуру должен продемонстрировать высокий уровень практического и теоретического владения материалом вузовского курса. Обязательным предметом обсуждения на испытании являются реферат или представленные соискателем публикации.

# Содержание программы

1. Общий теоретический раздел программы по направлению подготовки

Основные понятия и принципы теории информационной безопасности. Угрозы информационной безопасности. Виды информации, методы и средства обеспечения информационной безопасности. Методы нарушения конфиденциальности, целостности и доступности информации. Основы комплексного обеспечения информационной безопасности. Модели, стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Лицензирование и сертификация в области защиты информации. Правовые основы защиты информации. Организационные основы защиты информации.

Локальные и глобальные вычислительные сети, типовые конфигурации, маршрутизация. Основные протоколы обмена данными в вычислительных сетях. Системы управления базами данных, реляционная, иерархическая и сетевая модели, распределенные БД. Деревья и графы, их представление в ЭВМ, обходы графов. Алгоритмы на графах, выделение компонент связности. Кратчайшие пути в графе, минимальный остов графа. Задача сортировки и основные алгоритмы сортировки. Поиск информации методом хеширования. Контрольно-испытательные и логико-аналитические методы анализа безопасности программ. Методы и средства хранения ключевой информации в ЭВМ. Защита программ от изучения, защита от изменения, контроль целостности. Защита от разрушающих программных воздействий.

2. Общий теоретический раздел по направленности программы

Шифры замены и перестановки, их свойства, композиции шифров. Криптостойкость шифров, основные требования к шифрам. Теоретическая стойкость шифров, совершенные и идеальные шифры. Блоковые шифры. Потоковые шифры. Криптографические хеш-функции, их свойства и использование в криптографии. Методы получения случайных последовательностей, их использование в криптографии. Системы шифрования с открытыми ключами. Криптографические протоколы. Протоколы распределения ключей. Протоколы идентификации. Парольные системы разграничения доступа. Цифровая подпись. Стойкость систем с открытыми ключами.

Методы решения систем линейных уравнений. Методы интерполяции. Методы численного интегрирования. Методы численного решения дифференциальных уравнений. Численные методы нахождения экстремумов функций. Элементы комбинаторики: перестановки, выборки, сочетания и размещения без повторений. Сочетания и размещения с повторениями, биномиальные коэффициенты, их свойства. Алгебра логики, формулы алгебры логики, высказывания и операции, построение формул. Случайные величины, математическое ожидание и дисперсия. Основные законы распределения случайной величины. Центральная предельная теорема. Цепи Маркова. Система массового обслуживания без очереди и с очередью.

3. Раздел программы по областям исследований (профилю кафедры)

Структура, классификация и основные характеристики технических каналов утечки информации. Побочные электромагнитные излучения и наводки. Классификация средств технической разведки, их возможности. Концепция и методы инженерно-технической защиты информации. Методы скрытия речевой информации в каналах связи. Методы обнаружения и локализации закладных устройств. Методы подавления опасных сигналов акустоэлектрических преобразователей. Методы подавления информативных сигналов в цепях заземления и электропитания. Виды контроля эффективности защиты информации. Методы расчета и инструментального контроля показателей защиты информации. Утечка информации от мощной офисной аппаратуры. Упрощенная методика определения дальности, на которой возможен перехват ПЭМИ. Утечка информации от вспомогательной аппаратуры и кабелей, проходящих через помещение. Привести примеры. Несанкционированный съем информации с помощью радиозакладок. Достоинства радиозакладок. Основные характеристики радиозакладок. Прослушивание информации от пассивных закладок. Достоинства и недостатки. Структурная схема полуактивного микрофона. Приемники информации с радиозакладок. Деконспирационные признаки радиозакладок. Методы пассивной защиты от утечки по электромагнитному каналу. Технические средства для поиска работающих радиозакладок. Поиск радиозакладок нелинейными радиолокаторами. Нелинейные радиолокаторы с непрерывным режимом работы. Нелинейные радиолокаторы с импульсным режимом работы.

# Примерные темы рефератов

1. Модели и методы анализа эффективности систем защиты информации.
2. Модели и алгоритмы оценки эффективности программных систем защиты информации.
3. Методы и средства защиты программного обеспечения информационных систем.
4. Защищенные информационные технологии на основе сервисов безопасности.
5. Модели противодействия угрозам нарушения информационной безопасности при эксплуатации баз данных в защищенных корпоративных информационных системах.
6. Управление информационными рисками организации.
7. Риски информационной безопасности открытых систем.
8. Методы верификации и анализа защищенности баз данных.
9. Защита персональных данных в информационных системах.
10. Способы выявления угроз информационной безопасности в компьютерных сетях.
11. Методы защиты компьютерных систем от удаленных атак.
12. Методы обеспечения информационной безопасности компьютерных систем с использованием деревьев атак.
13. Адаптивное управление межсетевым экранированием информационно-телекоммуникационных сетей на этапе обнаружения вторжений.
14. Методы обеспечения защищенности документов от подделки.
15. Современные методы и средства защиты информации от утечки по техническим каналам.

# Вопросы для подготовки к вступительному испытанию

1. Основные понятия и принципы теории информационной безопасности.
2. Угрозы информационной безопасности.
3. Виды информации, методы и средства обеспечения информационной безопасности.
4. Методы нарушения конфиденциальности, целостности и доступности информации.
5. Основы комплексного обеспечения информационной безопасности.
6. Модели, стратегии и системы обеспечения информационной безопасности.
7. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
8. Лицензирование и сертификация в области защиты информации.
9. Правовые основы защиты информации.
10. Организационные основы защиты информации.
11. Локальные и глобальные вычислительные сети, типовые конфигурации, маршрутизация.
12. Основные протоколы обмена данными в вычислительных сетях.
13. Системы управления базами данных, реляционная, иерархическая и сетевая модели, распределенные БД.
14. Деревья и графы, их представление в ЭВМ, обходы графов.
15. Алгоритмы на графах, выделение компонент связности. Кратчайшие пути в графе, минимальный остов графа.
16. Задача сортировки и основные алгоритмы сортировки. Поиск информации методом хеширования.
17. Контрольно-испытательные и логико-аналитические методы контроля безопасности программ.
18. Методы и средства хранения ключевой информации в ЭВМ.
19. Защита программ от изучения, защита от изменения, контроль целостности.
20. Защита от разрушающих программных воздействий.
21. Шифры замены и перестановки, их свойства, композиции шифров.
22. Криптостойкость шифров, основные требования к шифрам.
23. Теоретическая стойкость шифров, совершенные и идеальные шифры.
24. Блоковые шифры. Потоковые шифры.
25. Криптографические хеш-функции, их свойства и использование в криптографии.
26. Методы получения случайных последовательностей, их использование в криптографии.
27. Системы шифрования с открытыми ключами. Криптографические протоколы.
28. Протоколы распределения ключей. Протоколы идентификации.
29. Парольные системы разграничения доступа.
30. Цифровая подпись. Стойкость систем с открытыми ключами.
31. Методы решения систем линейных уравнений.
32. Методы интерполяции. Методы численного интегрирования.
33. Методы численного решения дифференциальных уравнений.
34. Численные методы нахождения экстремумов функций.
35. Элементы комбинаторики: перестановки, выборки, сочетания и размещения без повторений.
36. Сочетания и размещения с повторениями, биномиальные коэффициенты, их свойства.
37. Алгебра логики, формулы алгебры логики, высказывания и операции, построение формул.
38. Случайные величины, математическое ожидание и дисперсия. Основные законы распределения случайной величины.
39. Центральная предельная теорема. Цепи Маркова.
40. Система массового обслуживания без очереди и с очередью.
41. Структура, классификация и основные характеристики технических каналов утечки информации.
42. Побочные электромагнитные излучения и наводки.
43. Классификация средств технической разведки, их возможности.
44. Концепция и методы инженерно-технической защиты информации.
45. Методы скрытия речевой информации в каналах связи.
46. Методы обнаружения и локализации закладных устройств.
47. Методы подавления опасных сигналов акустоэлектрических преобразователей.
48. Методы подавления информативных сигналов в цепях заземления и электропитания.
49. Виды контроля эффективности защиты информации.
50. Методы расчета и инструментального контроля показателей защиты информации.
51. Утечка информации от мощной офисной аппаратуры. Упрощенная методика определения дальности, на которой возможен перехват ПЭМИ.
52. Утечка информации от вспомогательной аппаратуры и кабелей, проходящих через помещение. Привести примеры.
53. Несанкционированный съем информации с помощью радиозакладок. Достоинства радиозакладок. Основные характеристики радиозакладок.
54. Прослушивание информации от пассивных закладок. Достоинства и недостатки. Структурная схема полуактивного микрофона.
55. Приемники информации с радиозакладок. Деконспирационные признаки радиозакладок.
56. Методы пассивной защиты от утечки по электромагнитному каналу.
57. Технические средства для поиска работающих радиозакладок.
58. Поиск радиозакладок нелинейными радиолокаторами.
59. Нелинейные радиолокаторы с непрерывным режимом работы.
60. Нелинейные радиолокаторы с импульсным режимом работы.

# Рекомендуемая литература

**Основная литература**

1. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1865598 (дата обращения: 18.03.2023). – Режим доступа: по подписке.
2. Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714 (дата обращения: 18.03.2023). – Режим доступа: по подписке.
3. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н. В. Гришина. - Москва : ИНФРА-М, 2021. - 216 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016534-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178150 (дата обращения: 18.03.2023). – Режим доступа: по подписке.
4. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843022 (дата обращения: 18.03.2023). – Режим доступа: по подписке.

**Дополнительная литература**

1. Аппаратные и программные средства защиты информации: Учебное пособие / Душкин А.В., Кольцов А., Кравченко А. - Воронеж:Научная книга, 2016. - 232 с. ISBN 978-5-4446-0746-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/923168 (дата обращения: 18.03.2023). – Режим доступа: по подписке.
2. Молдовян, А. А. Протоколы аутентификации с нулевым разглашением секрета : учебное пособие / А. А. Молдовян, Д. Н. Молдовян, А. Б. Левина. — Санкт-Петербург : НИУ ИТМО, 2016. — 55 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/91498 (дата обращения: 18.03.2023). — Режим доступа: для авториз. пользователей.
3. Торокин Анатолий Алексеевич. Инженерно-техническая защита информации : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности / А. А. Торокин. - М. : Гелиос АРВ, 2005. - 958 с. : рис.,табл. - Библиогр.: с. 934-949. - ISBN 5-85438-140-0. - ISBN 5-85438-140-0(ошибоч.) : 275.
4. Глухарев, М. Л. Технические средства защиты информации : учебное пособие / М. Л. Глухарев, М. Ф. Исаева. — Санкт-Петербург : ПГУПС, 2018. — 55 с. — ISBN 978-5-7641-112-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111736 (дата обращения: 18.03.2023). — Режим доступа: для авториз. пользователей.
5. Горбачев, А. А. Техническая защита информации. Поисковые приборы : учебное пособие / А. А. Горбачев, С. И. Алешников. — Калининград : БФУ им. И.Канта, 2022. — 148 с. — ISBN 978-5-9971-0696-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/310139 (дата обращения: 18.03.2023). — Режим доступа: для авториз. пользователей.
6. Галатенко В.А. Стандарты информационной безопасности : курс лекций : для студентов вузов, обучающихся по специальности 351400 "Прикладная информатика" / В.А. Галатенко ; под ред. В.Б. Бетелина ; Интернет-Ун-т информ. технологий. - Москва : Интернет-Ун-т информ. технологий, 2004. - 326 с. - (Серия "Основы информационных технологий"). - Библиогр.: с.316-322 (101 назв.). - ISBN 5-9556000-7-8 : 200..
7. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Технические средства и методы защиты информации : учебник для студентов высших учебных заведений, обучающихся по группе специальностей - "Информационная безопасность" / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. - 7-е изд., [испр.]. - Москва : Горячая линия-Телеком, 2014. - 442 с. : рис., табл. ; 21 см. - Библиогр.: с. 408-410. - ISBN 978-5-9912-0233-6 : 300.00..
8. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вешах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 18.03.2023). – Режим доступа: по подписке.