




**Федеральное агентство морского и речного транспорта**  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
**«Государственный университет морского и речного флота  
имени адмирала С.О. Макарова»**

---

УТВЕРЖДАЮ

Директор департамента высшего  
образования

  
\_\_\_\_\_ М.Н. Савельева  
31 » Мер 2024

**ПРОГРАММА  
ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ  
«Комплексное обеспечение информационной безопасности  
автоматизированных систем»**

для поступающих на обучение по образовательным программам  
высшего образования – программам магистратуры  
по направлению подготовки

**10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**  
направленность (профиль)  
**ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ОБЪЕКТОВ  
ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ**

Санкт-Петербург  
2024



Программа вступительного экзамена в магистратуру по направлению подготовки 10.04.01 «Информационная безопасность» разработана с учетом требований федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» (уровень бакалавриата) и утверждена на заседании кафедры «Комплексное обеспечение информационной безопасности».

## I. Методические указания к программе вступительного экзамена.

Цель программы вступительного испытания в магистратуру по направлению подготовки 10.04.01 «Информационная безопасность» заключается в регламентации порядка проведения вступительного испытания.

Целью вступительного испытания в магистратуру является проверка готовности поступающих освоить основную образовательную программу.

Поступающий в магистратуру должен:

– **знать** требования нормативно-методических документов Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю по защите государственной тайны и конфиденциальной информации, правовые основы аттестации объектов информатизации, основы построения защищенных ОС, основные современные криптографические алгоритмы и протоколы, программные средства системного, прикладного и специального назначения, принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;

– **уметь** производить аудит безопасности автоматизированных систем различного назначения, разработать комплекс мер по обеспечению заданного уровня защищенности информации, анализировать и оценивать угрозы информационной безопасности объекта, организовывать защищенную обработку информации, осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;

– **владеть** навыками разработки политики безопасности организации, навыками разработки технической и организационно-распорядительной документации, навыками оценивания безопасности информации автоматизированных систем, основными методами криптографической защиты информации, методами и средствами выявления угроз безопасности



автоматизированным системам, навыками выявления и уничтожения компьютерных вирусов.

## **II. Содержание программы**

### **Тема 1. Основы государственной информационной политики и информационной безопасности Российской Федерации**

1. Место информационной безопасности в системе национальной безопасности.
2. Современная концепция информационной безопасности.
3. Цели и концептуальные основы защиты информации.
4. Доктрина информационной безопасности РФ о состоянии информационной безопасности РФ, основных задачах и общих методах ее обеспечения.
5. Критерии, условия и принципы отнесения информации к защищаемой.
6. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.

### **Тема 2. Организационно–правовые методы защиты информации**

7. Правовые основы защиты информации ограниченного доступа, не составляющей государственную тайну.
8. Правовой режим государственной тайны.
9. Основные нормативные правовые акты в области информационной безопасности и защиты информации.
10. Отечественные и зарубежные стандарты в области компьютерной безопасности.
11. Принципы и методы организационной защиты информации.
12. Лицензирование и сертификация в области защиты информации.
13. Система контроля состояния защиты и юридическая ответственность за нарушение правового режима защиты.
14. Законодательство РФ об авторском праве и смежных правах.
15. Правовые проблемы защиты информации в Интернете.
16. Правовая регламентация лицензионной деятельности в области защиты информации.
17. Правовые основы применения ЭЦП.
18. Признаки и общая характеристика правонарушений в информационной



сфере.

### **Тема 3. Техническая защита информации**

19. Основные каналы утечки защищаемой информации.
20. Причины образования технических каналов утечки информации, их основные характеристики и факторы, способствующие их возникновению.
21. Технические средства негласного съема защищаемой информации.
22. Методы и средства перехвата сигнала в проводных и сотовых линиях связи.
23. Методы и средства выявления закладных устройств в помещениях и сетях коммуникации.
24. Аппаратура контроля и средства защиты проводных линий связи.
25. Аппаратура защиты помещений и сетей коммуникаций от технических средств негласного съема информации по акустическому каналу.
26. Криптографические методы и средства защиты линий связи, применяемые для борьбы с промышленным шпионажем.

### **Тема 4. Криптографические методы защиты информации**

27. Основные типы криптографических протоколов и задач.
28. Системы открытого распределения ключей и их инфраструктура.
29. Открытое шифрование.
30. Системы цифровой подписи на основе сложности факторизации чисел специального вида.
31. Системы цифровой подписи на основе сложности дискретного логарифмирования.
32. Слепая подпись и ее применение.
33. Свойства блочных шифров и режимы их использования.
34. Управляемые подстановочно-перестановочные сети как криптографический примитив.
35. Управление ключами в криптосистемах.
36. Хэш-функции: основные требования к ним и их применение.
37. Механизмы жеребьевки через Интернет.

### **Тема 5. Безопасность проводных и беспроводных сетей**

38. Модель взаимодействия открытых систем (OSI).
39. Стек протоколов TCP/IP



40. Логическая архитектура компьютерных сетей.
41. Особенности архитектуры интранет сетей
42. Классическая архитектура «клиент-сервер».
43. Коммутация каналов. Коммутация пакетов
44. Преимущества использования коммутаторов в сетях
45. Функции межсетевое экранирования.
46. Определение схемы подключения межсетевого экрана
47. Понятие, основные задачи и функции защищённых виртуальных сетей.
48. Построение защищенных виртуальных сетей.
49. Режимы соединений, организуемые в сетях стандарта IEEE 802.11, и их особенности.
50. Угрозы и риски безопасности беспроводных сетей.
51. Механизм шифрования WEP и краткая характеристика его уязвимостей.
52. Принципы аутентификации абонентов в стандарте IEEE 802.11 и краткая характеристика уязвимостей.
53. Стандарт безопасности WPA, его основные составляющие и улучшения по сравнению с WEP.
54. Стандарт сети 802.11i с повышенной безопасностью (WPA2), режимы работы и их краткая характеристика.
55. Стандарт IEEE 802.1X, назначение, особенности его применения для аутентификации абонентов в беспроводной сети.
56. Назначение и архитектура протокола WPS, известные уязвимости и реализация атаки на беспроводные сети с включенным WPS.

### **Тема 6. Управление информационной безопасностью**

57. Задачи службы информационной безопасности предприятия.
58. Принципы и направления инвентаризации информационных систем.
59. Постановка задачи классификации информационных систем.
60. Сопоставление ролей субъектов информационных систем их функциональным обязанностям.
61. Общие вопросы работы службы информационной безопасности с персоналом.
62. Количественная модель оценки информационных рисков.
63. Построение модели нарушителя информационной безопасности.
64. Порядок и методика тестирования аварийного плана.



65. Организационно-административные методы защиты информации.
66. Методика работы службы информационной безопасности с оборудованием информационных систем.
67. Структура аварийного плана предприятия.

### **Тема 7. Информационная безопасность транспортных объектов**

68. Способы контроля физического доступа на предприятие.
69. Методика выбора устройств видеонаблюдения.
70. Возможные варианты информационного нападения на цифровую АТС предприятия.
71. Специальные технические средства защиты речевой информации.
72. Задачи и организация системы управления доступом на предприятие.
73. Типовая схема охраны периметра предприятия.
74. Организация конфиденциальных переговоров.
75. Организация противопожарной защиты информационных систем.

### **III. Содержание, структура и форма проведения вступительного испытания**

Вступительные испытания по направлению подготовки 10.04.01 «Информационная безопасность» проводятся в письменной форме в виде тестирования, включающего 30 тестовых заданий. Продолжительность тестирования – один академический час. Для вступительного испытания установлена шкала оценивания и минимальное количество баллов, подтверждающее успешное прохождение вступительного испытания.

Структура вступительного испытания:

- 25 тестовых заданий предполагают «открытую форму» вопроса, т.е. выбор правильного ответа из четырех возможных вариантов. За правильный ответ начисляется 3 балла. За неправильный ответ баллы не начисляются;
- 5 тестовых заданий предполагают «закрытую форму» вопроса, т.е. краткий самостоятельный ответ. За полностью правильный ответ начисляется 5 баллов. За неправильный ответ баллы не начисляются. Возможно начисление баллов от 1 до 4 в случае, если дан ответ с ошибкой.

На вступительном испытании соискатель должен продемонстрировать основные компетенции, сформированные в результате освоения



фундаментальных технических дисциплин, по итогам обучения в высшем техническом учебном заведении по программам бакалавриата.

### Список рекомендованной литературы

#### Основная литература:

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2006. – 544 с. (Гриф УМО по ИБ).
2. Нестеров С.А. Основы информационной безопасности: учеб. пособие. – СПб.: Изд-во Лань, 2022. – 324 с.
3. Рыданов А.А., Глебов Н.Б., Гурьянов Д.Ю. Организационно-правовое обеспечение информационной безопасности: правовые аспекты защиты информации. СПб.: Изд-во ГУМРФ, 2021. – 148 с.
4. Нырков А.П., Кузнецов А.Ю., Башмаков А.В., Зуров Е.В. Дискретная математика: кодирование и обработка дискретных структур данных. СПб.: Издательство ГУМРФ, 2022.
5. Соколов С.С., Нырков А.П., Лаута О.С. и др. Основы построения защищенных телекоммуникационных сетей с использованием оборудования на базе MikroTik RouterOS. СПб.: Изд-во ГУМРФ, 2023. – 160 с.
6. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М.: ДМК Пресс, 2023. - 594 с.
7. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. пособие для студентов вузов. Под ред. Зайцева А.П. и Шелупанова А.А. – М.: Горячая линия-Телеком, 2009. – 616 с. (Гриф УМО по ИБ).
8. Теплов Э.П. Гуманитарные аспекты информационной безопасности: основные понятия, логические основы и операции / Э. П. Теплов, Ю. А. Гатчин, А. П. Нырков, А. Г. Коробейников, В. В. Сухостат. – СПб: Университет ИТМО, 2016. – 122 с.
9. Теплов Э.П. Гуманитарные аспекты информационной безопасности: методология и методика поиска истины, построения доказательств и защиты от манипуляций / Э. П. Теплов, Ю. А. Гатчин, А. П. Нырков, В. В. Сухостат. – СПб: Университет ИТМО, 2016. – 120 с.



10. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2010.- 436 с. (Гриф УМО по ИБ).
11. Каторин Ю.Ф., Монахов А.Е., Нырков А.П. Техническая защита информации: поиск закладных устройств в помещениях. – СПб.: ГУМРФ имени адмирала С.О. Макарова, 2013. – 279 с.
12. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. СПб.: НИУИТМО, 2012.
13. Каторин Ю.Ф., Кривцова И.Е. Инженерно-техническая защита информации. Руководство к практическим занятиям. СПб.: НИУИТМО, 2013.
14. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Техническая защита информации. Лабораторный практикум. СПб.: НИУИТМО, 2014.
15. Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа. – СПб.: ООО «Издательство Полигон», 2000. – 856 с.
16. Юрин И.В. Основы безопасности передачи информации по сотовым сетям связи. СПб.: Издательство СПГУВК, 2009.
17. Юрин И.В., Малов С.С. Теоретические основы организации работы службы информационной безопасности с информационными активами. СПб.: Издательство СПГУВК, 2009.
18. Сикарев И.А., Гаскаров В.Д. Помехозащищенность информационных каналов телекоммуникационных систем речного транспорта. СПб.: Издательство СПГПУ, 2010.
19. Гаскаров В.Д., Сикарев А.А. Электромагнитная защищённость инфокоммуникационных систем речного транспорта. СПб.: Издательство СПГПУ, 2010.
20. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. СПб.: БХВ –Петербург, 2010.
21. Зуров Е.В. Теоретические основы компьютерной безопасности (Способы разграничения доступа в системах защиты информации от несанкционированного доступа). СПб.: Издательство СПГУВК, 2010.
22. Башмаков А.В., Зуров Е.В. Информационная безопасность. СПб.: Издательство СПГУВК, 2011.
23. Башмаков А.В., Зуров Е.В. Безопасность беспроводных сетей. СПб.: Издательство СПГУВК, 2011.





### Дополнительная литература:

1. Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2006. — 264 с.
2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие: - М.: Форум, Инфра-М, 2021 – 416 с.
3. Домарев В. В. Безопасность информационных технологий. Системный подход . - К.: ООО ТИД Диа Софт, 2004. - 992 с.
4. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008. - 176 с.
5. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: учеб. пособие для вузов. – 4-е издание, стереотип. – М.: Горячая линия–Телеком, 2011. – 146 с. (гриф УМО по ИБ).
6. Петренко С. А., Курбатов В. А. Политики информационной безопасности. - М.: Компания АйТи, 2006. - 400 с.
7. . Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: учеб. пособие для вузов. Изд. 4-е. стер. – М.: Изд. центр «Академия, 2006. – 240 с. (гриф УМО по ИБ).
8. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» .
9. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. - 544 с.
10. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. - М.: Книжный мир, 2009. - 352 с.