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
30 05 2023

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
2023

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 межсетевого 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. 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).
5. 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.
6. 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.
7. Морозова Е.В., Нырков А.П. Информационная безопасность и защита информации (Часть I). – СПб.: СПГУВК, 2006. – 34 с.
8. 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).
9. 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.

10. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. СПб.: НИУИТМО, 2012.
11. Каторин Ю.Ф., Кривцова И.Е. Инженерно-техническая защита информации. Руководство к практическим занятиям. СПб.: НИУИТМО, 2013.
12. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Техническая защита информации. Лабораторный практикум. СПб.: НИУИТМО, 2014.
13. Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа. – СПб.: ООО «Издательство Полигон», 2000. – 856 с.
14. Юрин И.В. Основы безопасности передачи информации по сотовым сетям связи. СПб.: Издательство СПГУВК, 2009.
15. Юрин И.В., Малов С.С. Теоретические основы организации работы службы информационной безопасности с информационными активами. СПб.: Издательство СПГУВК, 2009.
16. Сикарев И.А., Гаскаров В.Д. Помехозащищенность информационных каналов телекоммуникационных систем речного транспорта. СПб.: Издательство СПГПУ, 2010.
17. Гаскаров В.Д., Сикарев А.А. Электромагнитная защищённость инфокоммуникационных систем речного транспорта. СПб.: Издательство СПГПУ, 2010.
18. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. СПб.: БХВ –Петербург, 2010.
19. Зуров Е.В. Теоретические основы компьютерной безопасности (Способы разграничения доступа в системах защиты информации от несанкционированного доступа). СПб.: Издательство СПГУВК, 2010.
20. Башмаков А.В., Зуров Е.В. Информационная безопасность. СПб.: Издательство СПГУВК, 2011.
21. Башмаков А.В., Зуров Е.В. Безопасность беспроводных сетей. СПб.: Издательство СПГУВК, 2011.
22. Башмаков А.В., Зуров Е.В., Ныркov А.П. Дискретная математика. Методы кодирования и обработки дискретных структур данных. СПб.: Издательство СПГУВК, 2012.

Дополнительная литература:

1. Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2006. — 264 с.

2. Домарев В. В. Безопасность информационных технологий. Системный подход . - К.: ООО ТИД Диа Софт, 2004. - 992 с.
3. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008. - 176 с.
4. 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).
5. Петренко С. А., Курбатов В. А. Политики информационной безопасности. - М.: Компания АйТи, 2006. - 400 с.
6. . 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).
7. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации» .
8. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. - 544 с.
9. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. - М.: Книжный мир, 2009. - 352 с.
10. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие: - М.: Форум, Инфра-М, 2008 – 416 с.

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

ДЕМОНСТРАЦИОННАЯ ВЕРСИЯ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

«Комплексное обеспечение информационной безопасности автоматизированных систем»

(Приложение к программе вступительного испытания)

Санкт-Петербург
2023

Тест вступительного испытания

1. **К основным непреднамеренным искусственным угрозам автоматизированной системы обработки информации (АСОИ) относится?**
   а) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы;
   б) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
   в) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
   г) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;

2. **К посторонним лицам – нарушителям информационной безопасности, относятся?**
   а) персонал, обслуживающий технические средства;
   б) технический персонал, обслуживающий здание;
   в) сотрудники службы безопасности;
   г) представители конкурирующих организаций;

3. **Антивирус, который запоминает исходное состояние программ, каталогов и системных областей диска, когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным это?**
   а) ревизор;
   б) детектор;
   в) доктор;
   г) сканер;

4. **Антивирус, который представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов это?**
   а) сторож;
   б) ревизор;
   в) сканер;
   г) детектор;

5. **К конфиденциальной информации не относится?**
   а) коммерческая тайна;
   б) персональные данные о гражданах;
   в) государственная тайна;
   г) "ноу-хау";

6. **Государственные информационные ресурсы не могут принадлежать?**
   а) коммерческим предприятиям;
   б) негосударственным учреждениям;
   в) физическим лицам;
   г) всем перечисленным;

7. **К коммерческой тайне могут быть отнесены?**
   а) сведения, не являющиеся государственными секретами;
   б) сведения, связанные с производством и технологической информацией;
   в) сведения, связанные с управлением и финансами;

г) сведения, перечисленные в остальных пунктах;

8. Являются ли авторское право, патентное право и коммерческая тайна формами защиты интеллектуальной собственности?
а) да;
б) нет;
в) только авторское и патентное;
г) только коммерческая тайна;

9. К информации ограниченного доступа не относится?
а) государственная тайна;
б) размер золотого запаса страны;
в) персональные данные;
г) коммерческая тайна;

10. Действие Закона "О государственной тайне" распространяется?
а) на всех граждан и должностных лиц РФ;
б) только на должностных лиц;
в) на граждан, которые взяли на себя обязательство выполнять требования законодательства о государственной тайне;
г) на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения;

11. Основными составляющими информационной безопасности являются?
а) конфиденциальность;
б) целостность;
в) доступность;
г) все перечисленные;

12. Какой из нормативно-правовых документов определяет перечень объектов информационной безопасности и методы ее обеспечения?
а) Доктрина информационной безопасности РФ;
б) ФЗ РФ “Об информации, информационных технологиях и о защите информации”;
в) ФЗ РФ “О государственной тайне;
г) все перечисленные;

13. Какие органы осуществляют контроль и надзор за соблюдением требований ФЗ-152 “О персональных данных”?
а) ФСБ;
б) ФСТЭК;
в) Роскомнадзор;
г) все перечисленные;

14. Какие задачи информационной безопасности решаются на организационном уровне?
а) разработка документации;
б) обучение персонала;
в) ограничение доступа на объект;
г) все перечисленные;

15. К формам защиты информации не относятся?
а) правовая;
б) аналитическая;
в) организационная;

г) техническая;

16. Идентификация – это…?
а) распознавание информации;
б) присвоение какому-либо объекту или субъекту уникального имени или образа;
в) последовательность действий, приводящих к пониманию информации;
г) полное игнорирование информации;

17. Антивирусная программа может выполнять следующие функции?
а) обнаружение вируса;
б) уничтожение вируса;
в) “лечение” вируса;
г) все перечисленные;

18. Несуществующий вид сервера в иерархической сети - это ...?
а) почтовый сервер;
б) файловый сервер;
в) сервер баз данных;
г) архивный сервер;

19. Беспроводная связь между компьютерами - это ...?
а) BLUETOOTH;
б) WI-FI;
в) 3G;
г) все перечисленные;

20. Компьютер, подключенный к Интернету, обязательно имеет …?
а) электронную почту;
б) доменное имя;
в) IP-адрес;
г) WEB - страницу;

21. Начальным этапом при любом виде работ в глобальных сетях является ...?
а) соединение с провайдером;
б) отправка электронной почты;
в) формулировка запросов;
г) все перечисленные;

22. Модель сети равноправных компьютеров (рабочих станций), каждый из которых имеет уникальное имя - это ... сеть?
а) одноранговая;
б) двухранговая;
в) многоранговая;
г) иерархическая;

23. Сервер - это …?
а) компьютер сети, использующий ресурсы других компьютеров;
б) программа управления сетью;
в) сетевая операционная система;
г) компьютер сети, предоставляющий свои ресурсы другим компьютерам;

24. Каждая локальная сеть в сети Интернет - это?

а) провайдер;
б) узел;
в) домен;
г) хост;

25. Виды модемов?
а) односторонний;
б) циклический;
в) системный;
г) внешний;

26. Злонамеренный код обладает следующими отличительными чертами: не требует программы-носителя, вызывает распространение своих копий и их выполнение (для активизации вируса требуется запуск зараженной программы). Назовите тип этого злонамеренного кода?

_____

27. Свойство информационных ресурсов, заключающееся в их недоступности для неуполномоченных лиц, называется…?

_____

28. Преднамеренные дефекты, внесенные в программные средства для целенаправленного скрытого воздействия на автоматизированную или информационную систему, называются…?

_____

29. Присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения, называется …?

_____

30. Совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации – это …?

_____