МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Сибирский государственный университет геосистем и технологий»

«УТВЕРЖДАЮ»
Ректор СГУГиТ
_____А.П. Карпик
«06» октября 2020 г.

ПРОГРАММА
КОМПЛЕКСНОГО МЕЖДИСЦИПЛИНАРНОГО
ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ В МАГИСТРАТУРУ

ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направленность (профиль)
«Организация и управление информационной безопасностью»

Поступающие в магистратуру по направлению подготовки 10.04.01 Информационная безопасность, образовательная программа «Организация и управление информационной безопасностью», должны продемонстрировать свои знания, умения и компетенции по следующим разделам:

– организация и управление информационной безопасностью;

– отечественные и зарубежные стандарты в области информационной безопасности;

– проектирование защищенных телекоммуникационных систем;

– технические, организационные и кадровые аспекты управления информационной безопасностью;

– контроль защищенности информации от утечки по техническим каналам.

Примерные вопросы для подготовки к экзамену.

1. Понятие СУИБ.
2. Требования к СУИБ.
3. Ключевые процессы СУИБ.
4. Цели обеспечения информационной безопасности.
5. Методы реализации программы информационной безопасности.
6. Меры обеспечения информационной безопасности.
7. Управление информационной безопасностью.
8. Процессы управления и обеспечения информационной безопасности.
9. Стандарт 9001–рекомендуемая база-ИСО/МЭК 27001.
10. Угрозы ИБ. Основные понятия. Классификация угроз. Классификация источников угроз. Виды удалённых атак. Методы анализа уязвимости информационной системы.
11. Государственная информационная политика. Основные положения государственной информационной политики РФ. Первоочередные мероприятия по реализации государственной политики обеспечения ИБ.
12. Органы защиты государственной тайны. Организация режима защиты государственной тайны. Допуск предприятий, учреждений и организации к проведению работ, связанных с использованием сведений, составляющих государственную тайну. Основные положения допуска должностных лиц и граждан к государственной тайне: получение и прекращение допуска.
13. Поясните осуществление контроля и надзора за обеспечением защиты государственной тайны. Охарактеризуйте виды правовой ответственности за нарушения законодательства РФ «О государственной тайне». Перечислите и охарактеризуйте виды посягательств на государственную тайну
14. Охарактеризуйте положения ФЗ-152 «О персональных данных». Источники права. Основные термины. Документы, содержащие персональные данные. Регуляторы и их основные области деятельности в рамках исполнения ФЗ-152.. Ответственность за нарушение требований закона ФЗ-152.
15. Раскройте основные принципы и условия обработки персональных данных согласно ФЗ-152.
16. Институты правовой защиты конфиденциальной информации. Коммерческая тайна как объект права. Режим коммерческой тайны. Охрана конфиденциальности информации, составляющей коммерческую тайну. Ответственность за нарушение законодательства о коммерческой тайне.
17. Законодательство РФ по лицензированию и сертификации в области информационной безопасности. Дайте определение терминам «лицензия» и «лицензирование»

18. Поясните назначение сертификационно–испытательных центров и лабораторий. Поясните работу структуры сертификации средств защиты информации.

19. Основные нормативно-правовые акты в области лицензирования деятельности по технической защите конфиденциальной информации.

20. Раскройте суть термина «интеллектуальная собственность». Какие из существующих институтов права и какие субъекты интеллектуальной собственности занимаются регулированием вопросов интеллектуальной собственности?

21. Основные виды вредоносных программ. VirWare (классические вирусы и сетевые черви). TrojWare (троянские программы). Спам. Технологии рассылки спама. Технологии борьбы со спамом. Методы борьбы с вредоносными программами.

22. Условия существования вредоносных программ в конкретной ОС. Способы проникновения в вредоносных программ в ОС. Правила именования вредоносных программ. Способы защиты от вредоносных программ. Классификация вредоносных программ.

23. Назначение стандарта ГОСТ Р ИСО/МЭК 15408-2002. Основные определения, структура, применение.

24. Достоинства и недостатки симметричных и асимметричных методов шифрования

25. Управление рисками. Этапы управления рисками.

26. Процедура управления рисками нарушения информационной безопасности в коммерческих организациях.

27. Аудит информационной безопасности - цели, принципы, типы организации, требования к аудитору.

28. Приведите определения относящихся к процессу регистрации пользователей в информационной системе. Опишите компоненты аутентификации и их содержание. Поясните термин «Фактор аутентификации».

29. Дайте определения терминам - объект, субъект, монитор безопасности обращений. Математические модели используются для описания моделей доступа. Поясните основные свойства и элементы избирательного управления доступом. Достоинства и недостатки избирательного управления доступом.

30. Основные свойства и элементы полномочного управления доступом. Достоинства и недостатки полномочного управления доступом. Суть модели Белла-ЛаПадула.

31. Аутентификация пользователей информационных систем. Базовые понятия. Факторы аутентификации. Виды аутентификации. One-time password. Хэш-функция (практ. использование). Криптография с открытым ключом (практ. использование).

32. Методы идентификации и аутентификации в ОС. Механизм управления доступом в ОС.

33. Принцип парольной аутентификации. Стойкость парольной аутентификации? Процесс парольной аутентификации на основе хешированного пароля. Недостатки методов аутентификации с запоминаемым паролем и способы защиты.

34. Дайте определения биометрическим характеристикам. Какие коэффициенты показывают эффективность биометрических методов аутентификации? Приведите достоинства и недостатки биометрических методов аутентификации.

35. Поясните процесс аутентификации на основе OTP-токенов. Поясните процесс аутентификации с помощью метода «запрос-ответ» при использовании OTP-токенов. Недостатки методов аутентификации с помощью OTP и способы защиты.

36. Парольная аутентификация. Достоинства и недостатки. Меры, позволяющие повысить надежность парольной аутентификации.

37. Охарактеризуйте виды правовой ответственности за нарушения законодательства РФ «О государственной тайне».

38. Ответственность за нарушение требований закона ФЗ-152.

39. Определения параметров ИБ согласно ГОСТ Р ИСО/МЭК 15408-2002

40. В чем суть понятия защита информации? Какие бывают угрозы и меры защиты?

41. Какие существуют основные виды атак? Что такое сетевые атаки?

42. Какие виды политик информационной безопасности Вы знаете?

43. Какие существуют технологии аутентификации?

44. Как организована защита информации в сети? В чем суть семиуровневой модели OSI? Что такое стек TCP/IP?

45. Что такое протокол IPSec?Каковы его режимы работы?

46. Как построена стратегия безопасности протокола IPSec?

47. Что такое система отслеживания вторжений?

48. В чем суть понятия защищенности (безопасности) компьютерной информации? Что такое конфиденциальность, целостность и доступность информации?

49. Что такое угроза безопасности компьютерной информации? Как строится классификация угроз?

50. Какие основные принципы проектирования современных сетей связи?

51. Какие существуют принципы проектирования абонентских сетей?

52. Какие существуют современные и перспективные средства доступа пользователей к сетям электросвязи?

53. Опишите принцип применения сенсоров сетевого трафика ids/ips на сетях связи передачи данных.

54. Как организуются защищенные каналы передачи данных с применением криптографических средств?

55. Как проводится оценка стойкости криптосистем?

56. В чем суть понятия утечки информации?

57. В чем особенности электромагнитного канала утечки информации?

58. В чем особенности индукционного канала утечки информации?

59. В чем особенности оптикоэлектронного канала утечки информации?

60. В чем особенности виброакустического канала утечки информации?

61. В чем особенности параметрического канала утечки информации?

62. Каковы основные задачи систем защиты информации?

63. Каковы структура и классификация технических каналов утечки информации?

64. Каковы основные характеристики технических каналов утечки информации?

65. В чем особенности технических каналов утечки речевой информации?

66. Каковы основные способы технической защиты?

67. В чем заключаются концепция и методы инженерно-технической защиты информации?

Критерии оценивания вступительного испытания.

Экзаменационный билет состоит из двух вопросов, ответ на каждый вопрос оценивается максимально в 50 баллов. Максимально возможное количество баллов – 100.

Оценка в **50 баллов** выставляется студенту, если он показал системность изложения материала, исчерпывающие знания всего вопроса, понимание сущности и взаимосвязи рассматриваемых явлений и процессов, технологий и методов, твердое знание основных положений смежных дисциплин. Ответ логически последователен, содержателен, конкретен и полон.

Оценка в **40 баллов** выставляется студенту, если он показал твердые и достаточно полные знания всего вопроса, правильное понимание сущности и взаимосвязи рассматриваемых явлений и процессов, технологий и методов. Последовательный, правильный, конкретный ответ. Но при этом отсутствует целостный подход к проблеме и заметны логические нарушения изложения материала.

Оценка в **30 баллов** выставляется студенту, если он показал твердые знания и понимание основных вопросов. Ответ правильный и конкретный, но неполный, допущение негрубых ошибок. Изложение материала не всегда логично и последовательно.

Оценка в **20 баллов** выставляется студенту, если он показал фрагментарные (частичные) знания вопроса. Изложенный материал правильный, но не систематизирован, нет взаимосвязи рассматриваемых явлений и процессов, технологий и методов.

Оценка в **10 баллов** выставляется студенту, если он демонстрирует свое понимание основных положений рассматриваемых явлений и процессов, технологий и методов, но не излагает материал. Ответ содержит грубые ошибки.

Оценка в **0 баллов** выставляется студенту, если он дал неправильный ответ, показал непонимание сущности излагаемых вопросов.

Список основной литературы

1. Милославская, Н.Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Серия «Вопросы управления информационной безопасностью". Выпуск 3 [Электронный ресурс]: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва: Горячая линия-Телеком, 2013. — 170 с. — Режим доступа: https://e.lanbook.com/book/5180. — Загл. с экрана.
2. Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность [Электронный ресурс]: Пособие / Петренко С.А., Симонов С.В., - 2-е изд., (эл.) - М.:ДМК Пресс, 2018. - 396 с. — Режим доступа: http://znanium.com/bookread2.php?book=983162. — Загл. с экрана.
3. Барабанов, А.В. Семь безопасных информационных технологий [Электронный ресурс] : учебник / А.В. Барабанов, А.В. Дорофеев, А.С. Марков, В.Л. Цирлов ; под ред. Маркова А.С.. — Электрон. дан. — Москва: ДМК Пресс, 2017. — 224 с. — Режим доступа: https://e.lanbook.com/book/97352. — Загл. с экрана.
4. Баранова Е. К. Актуальные вопросы защиты информации [Электронный ресурс]: монография / А.В. Бабаш, Е.К. Баранова. — М.: РИОР: ИНФРА-М, 2018. — 111 с. — Режим доступа: http://znanium.com/bookread2.php?book=979073. — Загл. с экрана.
5. Золотухина Е. Б. Управление жизненным циклом информационных систем (продвинутый курс): Электронная публикация / Золотухина Е.Б., Красникова С.А., Вишня А.С. - М.:КУРС, НИЦ ИНФРА-М, 2017. - 119 с. — Режим доступа: http://znanium.com/bookread2.php?book=767219. — Загл. с экрана.
6. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс]: учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва: ДМК Пресс, 2014. — 702 с. — Режим доступа: https://e.lanbook.com/book/50578. — Загл. с экрана.
7. Международные и российские нормативные акты и стандарты по информационной безопасности: основы стандартизации и сертификации [Электронный ресурс] : учебно-метод. пособие / И. В. Минин, О. В. Минин ; СГГА. - Новосибирск: СГГА, 2013. - 34, [1] с. - Режим доступа: http://lib.sgugit.ru. - Загл. с экрана.
8. Ищукова Е. А. Криптографические протоколы и стандарты [Электронный ресурс]: Учебное пособие / Ищукова Е.А., Лобова Е.А. - Таганрог: Южный федеральный университет, 2016. - 80 с. - Режим доступа: http://znanium.com/bookread2.php?book=991903. - Загл. с экрана.
9. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей : учебное пособие / Е.Б. Алексеев, В.Н. Гордиенко, В.В. Крухмалев [и др.] ; под редакцией В.Н. Гордиенко, М.С. Тверецкого. — 2-е изд., испр. — Москва : Горячая линия-Телеком, 2017. — 392 с. — ISBN 978-5-9912-0254-3. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/111002 (дата обращения: 24.09.2019). — Режим доступа: для авториз. пользователей.

10. Милославская, Н.Г. Технические, организационные и кадровые аспекты управления информационной безопасностью. Серия «Вопросы управления информационной безопасностью". Выпуск 4 [Электронный ресурс]: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 214 с. — Режим доступа: https://e.lanbook.com/book/5181. — Загл. с экрана.

11. Левушкина С. В. Кадровая политика и кадровый аудит организаций [Электронный ресурс]: учебное пособие / сост. С.В. Левушкина; Ставропольский гос. аграрный ун-т. - Ставрополь, 2014. – 168 с. - Режим доступа: http://znanium.com/catalog.php?bookinfo=514173. — Загл. с экрана.

Дополнительная литература

1. Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управления информационной безопасностью". Выпуск 1. [Электронный ресурс] / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 244 с. — Режим доступа: http://e.lanbook.com/book/5178. — Загл. с экрана.

2. Милославская, Н.Г. Проверка и оценка деятельности по управлению информационной безопасностью. Серия «Вопросы управления информационной безопасностью". Выпуск 5 [Электронный ресурс] : учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 166 с. — Режим доступа: https://e.lanbook.com/book/5182. — Загл. с экрана.

3. Защита информации [Электронный ресурс]: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: РИОР: ИНФРА-М, 2018. - 392 с. — Режим доступа: http://znanium.com/bookread2.php?book=937469 — Загл. с экрана.

4. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности. [Электронный ресурс] — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 140 с. — Режим доступа: http://e.lanbook.com/book/5163. — Загл. с экрана.

5. Правовая защита информации [Электронный ресурс] : учеб. пособие / А. И. Маркеев ; СГГА. - Новосибирск : СГГА, 2011. - 180 с. - Режим доступа: http://lib.sgugit.ru. - Загл. с экрана.

6. Зайцев, А.П. Технические средства и методы защиты информации. [Электронный ресурс] / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. — Электрон. дан. — М : Горячая линия-Телеком, 2012. — 442 с. — Режим доступа: http://e.lanbook.com/book/5155. — Загл. с экрана.