МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Челябинский государственный университет»
(ФГБОУ ВО «ЧелГУ»)

УТВЕРЖДАЮ
Проректор по научной работе
_____ И.В. Бычков
«31» _____ 2022 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ ПО СПЕЦДИСЦИПЛИНЕ

Группа научных специальностей
2.3. Информационные технологии и телекоммуникации

Научная специальность
2.3.6. Методы и системы защиты информации, информационная безопасность

Уровень образования
Высшее образование – подготовка кадров высшей квалификации

Форма обучения
очная

Челябинск, 2022

1. ОБЩИЕ ПОЛОЖЕНИЯ

Программа вступительного испытания по научной специальности (2.3.6. Методы и системы защиты информации, информационная безопасность), относящейся к группе научных специальностей – 2.3. Информационные технологии и телекоммуникации, составлена на основе федеральных государственных образовательных стандартов высшего образования соответствующих уровней образования (специалитет, магистратура).

Вступительное испытание нацелено на оценку знаний поступающих лиц, полученных ими в ходе освоения программ высшего образования и на отбор среди поступающих лиц наиболее способных и подготовленных к освоению программ подготовки научных и научно-педагогических кадров в аспирантуре.

Вступительное испытание проводится в рамках нескольких конкурсов и сдается однократно.

Вступительное испытание принимает экзаменационная комиссия.

Вступительное испытание проводится на русском языке.

Вступительное испытание проводится очно или с использованием дистанционных технологий в случаях, предусмотренных Правилами приема.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

Разделы и темы

1. Научные основы защиты информации:

1. основы информационной безопасности;
2. теоретические основы компьютерной безопасности.

2. Основы современных информационных технологий:

3. аппаратные средства вычислительной техники;
4. методы программирования;
5. языки программирования;
6. электроника и схемотехника;
7. системы и сети передачи информации.

3. Методы и средства обеспечения информационной безопасности:

8. безопасность операционных систем;
9. безопасность вычислительных сетей;
10. безопасность систем баз данных;
11. криптографические методы защиты информации;
12. технические средства и методы защиты информации;
13. программно-аппаратные средства обеспечения информационной безопасности.

4. Организационно-правовое обеспечение защиты информации:

14. организационное обеспечение информационной безопасности;
15. правовое обеспечение информационной безопасности.

5. Проектирование защищенных автоматизированных систем:

16. комплексное обеспечение информационной безопасности автоматизированных систем;
17. технология построения защищенных автоматизированных систем.

3. ПРОЦЕДУРА ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА

Вступительное испытание проводится в устной форме по билетам (приложение 1). Каждый билет содержит 2 вопроса. На подготовку вопроса отводится 30 минут. Записи при подготовке к ответу поступающие делают на учтенном комиссией листе, где указывается фамилия, номер билета и время его получения.

Во время вступительного испытания комиссией могут быть заданы дополнительные или уточняющие вопросы. После ответа черновые записи и билет сдаются председателю комиссии. Записи должны быть подписаны с указанием даты вступительного экзамена. При подготовке к ответу разрешается пользоваться программой вступительного испытания, выдаваемой комиссией.

Программа вступительного экзамена содержит 109 вопросов. Экзамен проводится по билетам, каждый из которых содержит два теоретических вопроса.

Вступительное испытание поступающий сдаёт один раз. Пересдача вступительного испытания не допускается, за исключением случаев удовлетворения апелляции о нарушении процедуры вступительного испытания.

Во время испытания не разрешается пользоваться словарями и справочными материалами на бумажных или электронных носителях.

4. ВОПРОСЫ К ВСТУПИТЕЛЬНОМУ ИСПЫТАНИЮ

1. Понятие национальной безопасности; виды безопасности; информационная безопасность (ИБ) в системе национальной безопасности Российской Федерации.
2. Общеметодологические принципы теории ИБ, анализ угроз ИБ.
3. Проблемы информационного противоборства; государственная политика в информационной сфере; региональные проблемы информационной безопасности.
4. Виды категорий информации; классификация методов и средств обеспечения ИБ.
5. Классификация угроз конфиденциальности, целостности и доступности информации; классификация каналов утечки и искажения информации.
6. Архитектура электронных систем обработки данных; формальные модели.
7. Модели безопасности.
8. Политика безопасности.
9. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
10. Характеристика стандартов по оценке защищенных систем.

11. Построение парольных систем, примеры практической реализации.
12. Особенности применения криптографических методов; способы реализации криптографической подсистемы.
13. Особенности реализации систем с симметричными и несимметричными ключами; концепция защищенного ядра.
14. Классификация методов верификации и исследования корректности систем защиты.
15. Классификация методов построения защищенных автоматизированных систем.
16. Методология обследования и проектирования систем защиты.
17. Особенности управления процессами функционирования систем защиты.
18. Определение и место проблем информационной безопасности в общей совокупности информационных проблем современного общества. Анализ развития подходов к защите информации. Современная постановка задачи защиты информации.
19. Особенности и состав научно-методологического базиса решения задач защиты информации. Общеметодологические принципы формирования теории защиты информации. Основное содержание теории защиты информации. Модели систем и процессов защиты информации.
20. Определение и содержание понятия угрозы информации в современных системах ее обработки. Системная классификация угроз. Система показателей уязвимости информации. Методы и модели оценки уязвимости информации.
21. Постановка задачи определения требований к защите информации. Методы оценки параметров защищаемой информации. Факторы, влияющие на требуемый уровень защиты информации.
22. Определение и общеметодологические принципы построения систем защиты информации. Основы архитектурного построения систем защиты. Типизация и стандартизация систем защиты.
23. Основные выводы из истории развития теории и практики защиты информации. Перспективы развития теории и практики защиты. Трансформация проблемы защиты информации в проблему обеспечения информационной безопасности.
24. Организация и структура памяти, системы прерывания; системы ввода-вывода; периферийные устройства.
25. Архитектура ПЭВМ, рабочих станций и серверов, системная магистраль, буферизация шин, управление системной магистралью, подключение дополнительных и интерфейсных схем.
26. Универсальные и специализированные ЭВМ высокой производительности; архитектура специализированных вычислительных комплексов, ориентированных на программное обеспечение, машины баз данных, объектно-ориентированная архитектура.
27. Оценка качества программного обеспечения.
28. Общие принципы методы и средства проектирования архитектуры и структуры, проектирования логики, тестирования и отладки,

документирования и сопровождения программного обеспечения с учетом повышенных требований к надежности программ и их защищенности от несанкционированного доступа.

29. Особенности разработки и сопровождения программного обеспечения для рабочих групп.
30. CASE-технологии, технологии виртуального программирования и объектно-ориентированного программирования.
31. Применение математических методов в проектировании надежного и защищенного программного обеспечения: функциональное программирование, логическое программирование.
32. Структуры данных и абстракции данных; элементарные и простые структуры данных; сложные структуры данных.
33. Оценка сложности алгоритмов; модели вычислений.
34. Алгоритмы сортировки, алгоритмы поиска, Алгоритмы на графах.
35. Общие принципы построения и использования языков программирования; средства описания данных; средства описания действий.
36. Абстрактные типы данных: инкапсуляция, спецификация, реализация, параметризация, классы и объекты.
37. Обработка файлов; обработка исключительных ситуаций.
38. Параллельная обработка данных.
39. Общая характеристика языков ассемблера: назначение, принципы построения и использования; структура языка, основные группы команд, операторы, средства взаимодействия с операционной системой.
40. Общая характеристика операционных систем; назначение и возможности систем клона UNIX, систем группы Windows.
41. Управление ресурсами: управление процессорами; управление памятью; управление устройствами.
42. Классификация, общая характеристика файловых систем.
43. Управление процессами: состояния процессов, синхронизация процессов, обмен сообщениями, стратегии и дисциплины планирования, наследование ресурсов, тупиковые ситуации, обработка исключений, сохранение и восстановление процессов.
44. Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей; основы организации и функционирования сетей.
45. Сетевые операционные системы; основные сетевые стандарты.
46. Средства взаимодействия процессов в сетях.
47. Распределенная обработка информации в системах клиент-сервер; одноранговые сети.
48. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа.
49. Общие принципы построения баз данных: реляционная, иерархическая и сетевая модели.
50. Распределенные базы данных в сетях ЭВМ.

51. Общая характеристика, назначение и возможности систем управления базами данных (СУБД).
52. Информация, данные, сигналы. Источники информации и ее носители. Количество информации и энтропия. Формулы Хартли и Шеннона.
53. Характеристики процесса передачи информации. Математические модели каналов связи и их классификация.
54. Помехоустойчивость передачи информации. Пропускная способность каналов связи. Теорема Шеннона для каналов без помех и с ними.
55. Типы сигналов, их дискретизация и восстановление. Спектральная плотность сигналов. Частота Найквиста, теорема Котельникова.
56. Частотное представление дискретных сигналов. Ортогональные преобразования дискретных сигналов. Задачи интерполяции и прореживания сигналов.
57. Классификация кодов. Линейные коды. Оптимальное кодирование.
58. Геометрический подход к кодированию. Неравномерные коды Хемминга.
59. Циклические коды. Помехоустойчивое кодирование. Корректирующие коды.
60. Аналого-цифровые и цифро-аналоговые преобразователи; быстрые преобразования. Цифровые фильтры.
61. Нелинейное и параметрическое преобразование сигналов; модуляция и демодуляция; преобразование частоты.
62. Классификация систем связи; кодирование информации в системах связи.
63. Методы модуляции в системах связи; основные типы модемов; уплотнение информации в системах связи; дискретные вокодеры.
64. Шифры и их свойства; композиции шифров; системы шифрования.
65. Модели шифров; основные требования к шифрам; совершенные шифры, криптографические хеш-функции.
66. Теоретико-информационный подход к оценке криптостойкости шифров; имитостойкость и помехоустойчивость шифров; принципы построения криптографических алгоритмов; различие между программными и аппаратными реализациями.
67. Криптографические параметры узлов и блоков шифраторов; синтез шифров.
68. Методы получения случайных и псевдослучайных последовательностей; программные реализации шифров.
69. Особенности использования вычислительной техники в криптографии; организация сетей засекреченной связи; ключевые системы.
70. Криптографические протоколы и основные требования к ним; протоколы «рукопожатия»; протоколы установления подлинности; протоколы идентификации и аутентификации.
71. Парольные системы разграничения доступа.
72. Протоколы генерации ключей; протоколы распределения ключей; рекомендации X.509.
73. Протоколы разделения секретов; протоколы с нулевым разглашением; доказательства нулевого разглашения; протоколы "игры в покер".

74. Сложность основных целочисленных алгоритмов в кольце целых чисел, кольцах вычетов и конечных полях; дискретное преобразование Фурье для кольца целых чисел.
75. Квадратичные вычеты и невычеты, квадратичный закон взаимности Гаусса; цепные дроби.
76. Асимптотический закон распределения простых чисел; проверка чисел на простоту; построение больших простых чисел.
77. Методы разложения чисел на множители; алгоритмы дискретного логарифмирования в конечном поле, криптографическая система RSA, протокол Диффи-Хеллмана.
78. Суть криптографических методов защиты информации (ЗИ). Основ-ные задачи по ЗИ, решаемые с использованием криптографических методов. Значение криптографических методов в комплексной системе ЗИ. Базовые понятия криптологии (шифр, ключи, протоколы, шифрсистема).
79. Этапы развития криптологии. Криптография с секретным (симметричная) и открытым ключом (асимметричная). Основные различия. Криптографические примитивы и криптографические протоколы по защите информации.
80. Криптографическая стойкость шифров. Активные и пассивные атаки на шифрсистемы, задачи криптоаналитика. Теоретически стойкие шифры. Практическая стойкость шифров, её основные характеристики (трудоёмкость и надёжность дешифрования, количество необходимого материала). Связь между временной и вычислительной сложностью дешифрования. Классификация методов криптографического анализа.
81. Виды, источники и носители защищаемой информации; демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники.
82. Побочные электромагнитные излучения и наводки; структура, классификация и основные характеристики технических каналов утечки информации; классификация технической разведки; основные этапы и процедуры добывания информации технической разведкой; возможности видов технической разведки.
83. Методы и средства инженерной защиты и технической охраны объектов; скрытие объектов наблюдения.
84. Организация и обеспечение ограничения доступа, пропускного и внутри объектового решения, охрана объектов в процессе транспортировки.
85. Защита информации при авариях, экстремальных ситуациях и в условиях чрезвычайного положения.
86. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности, концепция диспетчера доступа.
87. Методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации.

88. Защита программ от изучения, способы встраивания средств защиты в программное обеспечение.
89. Защита от разрушающих программных воздействий, защита программ от изменения и контроль целостности, построение изолированной программной среды.
90. Программно-аппаратные средства защиты информации в сетях передачи данных.
91. Организация управления доступом и защиты ресурсов ОС; основные механизмы безопасности: средства и методы аутентификации в ОС.
92. Модели разграничения доступа, организация и использование средств аудита.
93. Администрирование ОС: задачи и принципы сопровождения системного программного обеспечения, генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС; основные стандарты ОС.
94. Анализ и оценка угроз информационной безопасности объекта управления. Методология оценки ущерба от злоумышленных и неумышленных противоправных нарушений безопасности информации.
95. Цели и задачи службы безопасности объекта информации. Организационная структура. Особенности функционирования структурных подразделений.
96. Организация и обеспечение ограничения доступа, пропускного и внутри объектового решения, охрана объектов в процессе транспортировки, защита информации при авариях, экстремальных ситуациях и в условиях чрезвычайного положения.
97. Понятие секретного (конфиденциального) делопроизводства. Общие принципы его организации. Механизм и процедуры установления степени секретности (конфиденциальности).
98. Правила оформления документов с ограниченным доступом. Правила и формы регистрации документов. Размножение, правила приема и передачи.
99. Обеспечение сохранности документов с ограниченным доступом. Организация хранения. Требования к помещениям и хранилищам. Правила и порядок уничтожения документов с ограниченным доступом.
100. Контроль и методы проверки состояния делопроизводства с ограниченным доступом. Порядок проведения служебных расследований случаев нарушения порядка специального делопроизводства.
101. Особенности организации электронного документооборота. Система удостоверения ЭЦП. Цели, задачи и особенности функционирования удостоверяющих центров.
102. Особенности организации системы мониторинга и сетевого аудита. Взаимодействие с правоохранительными органами.
103. Постановка проблемы комплексного обеспечения информационной безопасности автоматизированных систем; состав компонентов комплексной системы обеспечения информационной безопасности

(КСИБ), функциональные и обеспечивающие подсистемы, технология, управление.

104. Методология формирования задач защиты; интеграция средств информационной безопасности в технологическую среду; этапы проектирования КСИБ и требования к ним: предпроектное обследование, техническое задание, техническое проектирование, рабочее проектирование, испытания и внедрение в эксплуатацию, сопровождение.
105. Особенности проектирования на современном уровне и синтез КСИБ; типовая структура комплексной системы защиты информации от несанкционированного доступа (НСД).
106. Методы и методики проектирования: методика выявления возможных каналов НСД, последовательность работ при проектировании комплексной системы защиты информации от НСД и утечки за счет ПЭМИН, моделирование как инструментарий проектирования.
107. Методы и методики оценки качества КСИБ: методы нормативного функционального наполнения, метод экспертных структурных вопросников, метод оценки уязвимости информации Хоффмана, метод оценки риска Фишера.
108. Аттестация автоматизированных систем по требованиям безопасности информации.
109. Особенности эксплуатации КСИБ на объекте защиты, организационно-функциональные задачи службы безопасности, управление информационной безопасностью объекта.

5. КРИТЕРИИ ОЦЕНКИ РЕЗУЛЬТАТОВ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Максимальное количество баллов за вступительное испытание – 100 баллов.

Минимальное количество баллов за успешное прохождение вступительного испытания, независимо от условия поступления, соответствует минимальным баллам, утверждённым Правилами на текущий год.

«Отлично» (от 91 до 100) – поступающий обнаружил всестороннее, систематическое и глубокое знание учебно-программного материала, исчерпывающе, последовательно, грамотно и логически стройно его излагает, не затрудняется с ответом при видоизменении задания, свободно справляется с поставленными задачами, показывает знания монографического материала, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических работ, обнаруживает умение самостоятельно обобщать и излагать материал, не допуская ошибок, уяснил взаимосвязь основных понятий дисциплины и их значение для приобретения профессии.

«Хорошо» (от 76 до 90) – поступающий твердо знает учебно-программный материал, грамотно и по существу излагает его, не допускает существенных

неточностей в ответе на вопрос, может правильно применить теоретические положения и владеет необходимыми навыками при выполнении практических задач.

«Удовлетворительно» (от 40 до 75) – поступающий усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий.

«Неудовлетворительно» (от 0 до 39) – поступающий не знает значительной части программного материала, допускает существенные ошибки, с большим затруднением выполняет практические работы.

6. СПИСОК РЕКОМЕНДУЕМЫХ ИСТОЧНИКОВ ДЛЯ ПОДГОТОВКИ К ВСТУПИТЕЛЬНОМУ ИСПЫТАНИЮ

Источники, отмеченные знаком «*», имеются в научной библиотеке ЧелГУ в печатном или электронном виде в ЭБС «Университетская библиотека онлайн» и «ЛАНЬ», к которым имеется подписка по договорам с правообладателями на текущий учебный год.

Основные источники:

1. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206279 (дата обращения: 17.03.2022)
2. Потерпеев, Г. Ю. Безопасность операционных систем : учебное пособие / Г. Ю. Потерпеев, В. С. Нефедов, А. А. Криулин. — Москва : РТУ МИРЭА, 2021. — 93 с. — ISBN 978-5-7339-1393-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182416 (дата обращения: 17.03.2022)
3. Федин, Ф. О. Информационная безопасность баз данных : учебное пособие / Ф. О. Федин, О. В. Трубиенко, С. В. Чискидов. — Москва : РТУ МИРЭА, 2020 — Часть 1 — 2020. — 133 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167605 (дата обращения: 17.03.2022)
4. Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва : РТУ МИРЭА, 2020. — 136 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167606 (дата обращения: 17.03.2022)

Дополнительные источники:

1. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. А. Гатчин, В. В. Сухостат, А. С. Куракин, Ю. В. Донецкая. — 2-е изд., испр. и доп. — Санкт-Петербург : НИУ ИТМО, 2018. — 100 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/136476 (дата обращения: 17.03.2022)
2. Булычев, Г. Г. Программно-аппаратные средства обеспечения информационной безопасности : методические указания / Г. Г. Булычев. — Москва : РТУ МИРЭА, 2020 — Часть 2 — 2020. — 46 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163812 (дата обращения: 17.03.2022)
3. Рацеев, С. М. Математические методы защиты информации : учебное пособие для вузов / С. М. Рацеев. — Санкт-Петербург : Лань, 2022. — 544 с. — ISBN 978-5-8114-8589-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/193323 (дата обращения: 17.03.2022)
4. 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. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 (дата обращения: 17.03.2022)

Рекомендуемые ресурсы информационно-коммуникационной сети «Интернет»:

Средством доступа к системе собственных электронных ресурсов является сайт библиотеки www.lib.csu.ru. Электронный каталог обеспечивает полное и оперативное представление о библиотечном фонде, повышает качество и эффективность поиска информации – более 1,5 млн. записей.

1. Электронный каталог. Библиографические базы данных. Книги, электронные ресурсы, диссертации и авторефераты.
2. Электронная библиотека. Издания ЧелГУ, УМК; диссертации, защищенные в советах ЧелГУ, резервные коллекции, фонд редких книг, электронный справочник «Информио», статистические издания России и стран СНГ.
3. Реферативные базы данных ИНИОН РАН, базы данных ВИНИТИ, Scopus (http://www.scopus.com), Science (архив).
4. Полнотекстовые базы данных диссертаций РГБ, АРБИКОН, SIGLA, научная электронная библиотека http://elibrary.ru, подписка на полнотекстовую коллекцию российских научных журналов (148 наименований), издательств: Taylor&Francis, Sage Publications (архив научных журналов); Springer, American Physical Society (http:www.journals.aps.org/about), American Mathematical Society (http:www.ams.org/mathscinet), Wiley (http://onlinelibrary.wiley.com).

5. Электронно-библиотечные системы с возможностью пользования лицензионными материалами из любой точки, имеющей доступ к сети Интерент (регистрация из сети университета персонального аккаунта): Университетская библиотека онлайн (www.biblioclub.ru), Лань (www.e.lanbook.com)
6. Программный комплекс «Эталон» [Электронный ресурс] (полнотекстовая база данных по действующему российскому законодательству). – Режим доступа: http:// www.scli.ru/ , свободный (Дата обращения: 22.02.2022).

Приложение 1
Образец билета

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования «Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)

Уровень образования
Высшее образование – подготовка кадров высшей квалификации

ВСТУПИТЕЛЬНОЕ ИСПЫТАНИЕ ПО СПЕЦДИСЦИПЛИНЕ

Группа научных специальностей
2.3. Информационные технологии и телекоммуникации

Научная специальность
2.3.6. Методы и системы защиты информации, информационная безопасность

БИЛЕТ № 1

1. Методология обследования и проектирования систем защиты.
2. Безопасность систем баз данных

Председатель предметной комиссии ФИО