Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
«Санкт-Петербургский политехнический университет Петра Великого»

Институт компьютерных наук и кибербезопасности

УТВЕРЖДАЮ

Директор ИКНК

_____ Д.П. Зегжда

«28» ноября 2024 г.

ПРОГРАММА

вступительного испытания для поступающих в магистратуру по направлению подготовки / образовательной программе

10.04.01 «Информационная безопасность»

10.04.01_03 «Искусственный интеллект в кибербезопасности»

10.04.01_04 «Кибербезопасность нефтегазовой отрасли»

10.04.01_05 «Безопасность и киберпсихология интернет-коммуникаций»

10.04.01_06 «Кибербезопасность беспилотных систем»

Код и наименование направления подготовки / образовательной программы

Санкт-Петербург
2024

АННОТАЦИЯ

Программа содержит перечень дисциплин, включенных в программу междисциплинарного вступительного экзамена в магистратуру, перечень тем (вопросов) по дисциплинам направления **10.03.01 «Информационная безопасность»**, рекомендуемую литературу для подготовки к экзамену и пример экзаменационного теста.

Вступительное испытание оценивается по стобалльной шкале и состоит из междисциплинарного экзамена в объеме требований, предъявляемых государственными образовательными стандартами высшего образования к уровню подготовки бакалавра по направлению, соответствующему направлению магистратуры, проводимого очно в письменной форме или дистанционно **(максимальный балл – 100).**

Минимальное количество баллов, подтверждающее успешное прохождение междисциплинарного экзамена – **50 баллов (50%)**.

Руководители ОП

Профессор ВШК ИКНК, д.т.н. Е.Б. Александрова

Доцент ВШК ИКНК, к.т.н. Д.В. Иванов

Профессор ВШК ИКНК, д.т.н М.А. Полтавцева

Составители:

Доцент ВШК ИКНК, к.т.н. Е.Ю. Павленко

Доцент ВШК ИКНК, к.т.н. В.В. Платонов

Программа рассмотрена и рекомендована к изданию Ученым советом ИКНК (протокол № 9/24 от «28» ноября 2024 г.).

1. ДИСЦИПЛИНЫ, ВКЛЮЧЁННЫЕ В ПРОГРАММУ МЕЖДИСЦИПЛИНАРНОГО ЭКЗАМЕНА

1.1. Методы программирования.

1.2. Операционные системы.

1.3. Компьютерные сети.

1.4. Основы информационной безопасности.

1.5. Модели безопасности компьютерных систем.

1.6. Криптографические методы защиты информации.

1.7. Программно-аппаратные средства обеспечения информационной безопасности.

2. СОДЕРЖАНИЕ УЧЕБНЫХ ДИСЦИПЛИН

2.1. Методы программирования.

1. Основные алгоритмы поиска и сортировки. Сортировка массивов и файлов, поиск в глубину и в ширину.
2. Рекурсивные алгоритмы. Виды и характеристики рекурсии.
3. Рекурсивные структуры данных и их применение.
4. Деревья как структуры данных. Основные виды деревьев, их сравнительные характеристики.
5. Поиск с помощью хэширования. Хэш-функции в программировании.
6. Методы оптимизации программ. Машинно-зависимая и машинно-независимая оптимизация.
7. Методы тестирования и отладки. Тестирование черного и белого ящика.
8. Переносимость программ. Правила написания переносимых программ.
9. Параллельное программирование. Особенности программирования параллельных программ на GPU.

Литература для подготовки:

1. Вирт, Н. Алгоритмы и структуры данных / Никлаус Вирт – СПб. Невский Диалект, 2008.
2. Кнут, Д. Искусство программирования / Дональд Э. Кнут – М. Вильямс, 2015.

3. Бентли, Дж. Жемчужины программирования / Дж. Бентли – СПб. Питер, 2002.

4. Боресков, А. Основы работы с технологией CUDA / А. Боресков, А. Харламов. – М., ДМК, 2010.

2.2. Операционные системы.

1. Функции операционных систем, архитектуры операционных систем.
2. Планирование процессов и потоков.
3. Взаимодействие процессов, взаимоисключения и синхронизация процессов.
4. Управление памятью. Виртуальная память.
5. Организация ввода/вывода.
6. Файловые системы.
7. Механизмы защиты операционных систем.
8. Системы реального времени.
9. Многопроцессорные системы.
10. Механизмы виртуализации операционных систем.
11. Операционная система UNIX. Архитектура, механизмы управления процессами и памятью.
12. Операционная система UNIX. Организация файловой системы.
13. Операционная система Windows. Архитектура, механизмы управления процессами и памятью.
14. Операционная система Windows. Файловые системы, сервисы, системный реестр.
15. Операционные системы Windows и UNIX. Подсистемы безопасности.
16. Служба каталога.

Литература для подготовки:

1. Таненбаум, Э. Современные операционные системы / Э. Таненбаум ; Х. Бос. – 4-е изд . – М. [и др.] : Питер, 2017 . – 1120 с.

2. Столлингс, В. Операционные системы : Внутреннее устройство и принципы проектирования: Пер. с англ. / В. Столлингс . – 4-е изд . – М. : Вильямс, 2002 . – 843 с.

3. Робачевский, А.М. Операционная система UNIX : Учеб. пособие для вузов / А.М. Робачевский . – СПб. : БХВ-Петербург, 2007 . – 656 с.

4. Соломон, Д. Внутреннее устройство Microsoft Windows Основные подсистемы ОС : / М. Руссинович, Д. Соломон, А. Ионеску. – СПб : Питер, 2014 . – 672 с.

2.3. Компьютерные сети.

1. Модель OSI ISO. Модель TCP\IP. Уровни моделей. Инкапсуляция данных.
2. Витая пара, виды. Коаксиальный кабель. Волоконная оптика.
3. Протоколы множественного доступа с контролем несущей. Кадр, структура. Адресация.
4. Ethernet. Уровень MAC. Типы адресов.
5. Протокол ARP. Взаимосвязь IP и MAC-адресов.
6. Протокол IP. Инкапсуляция данных. Заголовок.
7. Разделение сети на подсети. Схемы адресации. VLSM.
8. Транспортный уровень. Структура данных. Адресация.
9. Уровень приложений. Протоколы. Служба DNS.
10. VLAN. Назначение, типы. Транковые порты. Протокол DTP.
11. Статическая маршрутизация. Типы маршрутов.
12. Динамическая маршрутизация. Протоколы состояния канала. Алгоритм Дейкстра. Маршрутные обновления.
13. Протокол DHCP. Поддержка IPv6. Технология SLAAC.
14. NAT. Назначение, преимущества, типы.

Литература для подготовки:

1. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер – СПб. Питер, 2016.
2. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл – СПб. Питер, 2016.
3. Мэрфи, Н. IPv6. Администрирование сетей / Н. Мэрфи, Д. Мэлоун – СПб. КУДИЦ-Пресс, 2007.

2.4. Основы информационной безопасности.

1. Группы причин нарушения безопасности компьютерных систем.
2. Состояние правового обеспечения информационной безопасности, система стандартов в области информационной безопасности.
3. Лицензирование деятельности в области информационной безопасности.
4. Системы сертификации в области информационной безопасности.

5. Понятие угроз информационной безопасности, их систематизация.
6. Разрушающие программные средства.
7. Модель нарушителя.
8. Сценарий компьютерной атаки.
9. Функции защиты.
10. Виды и средства контроля безопасности.
11. Системы и средства обнаружения компьютерных атак.
12. Технология построения защищенных информационных систем.

Литература для подготовки:

1. Нестеров, С.А. Основы информационной безопасности. / С.А. Нестеров. – СПб. : Лань, 2016.— 324 с.
2. Партыка Т.В. Информационная безопасность / Т.В. Партыка. – 5-е изд . – М. : Форум, 2014 . – 432 с.
3. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие / Ю.А. Родичев. – СПб : Питер, 2017. – 256 с.

2.5. Модели безопасности компьютерных систем.

1. Дискреционный контроль доступа. Модель Харрисона–Руззо–Ульмана: основные определения. Теорема безопасности.
2. Модель Харрисона–Руззо–Ульмана. Теорема о разрешимости проблемы безопасности в частных и в общем случае. Монитор безопасности пересылок.
3. Модель типизированной матрицы доступа (ТМД), монотонная ТМД.
4. Мандатный контроль доступа. Модель Белла и ЛаПадулы: основные определения.
5. Модель Белла и ЛаПадулы: формальное описание. Основная теорема безопасности. Критика модели Белла и ЛаПадулы.
6. Модели целостности. Модель Биба: описание, теорема о пути передачи информации. Критика модели Биба.
7. Модель безопасных функций перехода. Теорема Мак-Лина.
8. Модель уполномоченных субъектов.
9. Модель совместного доступа. Критерий безопасности. Безопасная функция перехода для моделей совместного доступа.
10. Ролевой контроль доступа. Критерии безопасности. Достоинства и недостатки.

11. Модель Take-Grant. Основные определения. Разделение права доступа в терминах модели Take-Grant, необходимые и достаточные условия разделения права.

12. Модель Кларка-Вилсона: область применения, цели, описание.

13. Модель Китайской стены: область применения, цели, описание.

Литература для подготовки:

1. Гайдамакин, Н.А. Теоретические основы компьютерной безопасности / Н.А. Гайдамакин //Екатеринбург: Изд-во Урал. ун-та, 2008. – http://elar.urfu.ru/bitstream/10995/1778/5/1335332_schoolbook.pdf.

2. Зегжда, П.Д. Теоретические основы компьютерной безопасности: Курс лекций / Зегжда П.Д., Зегжда Д.П. – СПб., 2008.

3. Девянин, П.Д. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений / П.Д. Девянин. – М.: Издательский центр «Академия», 2005 – 144с.

2.6. Криптографические методы защиты информации.

1. Основные понятия симметричной криптографии. Понятие стойкости криптографического алгоритма. Простейшие шифры и их свойства.

2. Криптографические функции хэширования.

3. Основные понятия криптографии с открытым ключом. Вычислимая в одну сторону функция. Функция с лазейкой. Шифрование с открытым ключом. Цифровая подпись.

4. Протоколы на основе задачи разложения числа на множители. RSA. Методы решения задачи разложения числа на множители.

5. Протоколы на основе задачи дискретного логарифмирования. Схема Эль-Гамаля. Методы решения задачи дискретного логарифмирования.

Литература для подготовки:

1. Введение в криптографию / Под общ. ред. В. В. Ященко. - 4-е изд., доп. М.: МЦНМО, 2012.

2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 480 с.

3. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов // http://www.bnti.ru/dbtexts/ipks/old/analmat/1_2002/crypto.pdf.

4. Ишмухаметов, Ш.Т. Методы факторизации натуральных чисел / Ш.Т. Ишмухаметов.

2.7. Программно-аппаратные средства обеспечения информационной безопасности.

1. Основы сетевого и межсетевого взаимодействия.
2. Сущность и основные виды вредоносного программного обеспечения.
3. Основные методы защиты от вредоносного ПО.
4. Виды удаленных сетевых атак.
5. Основные механизмы обеспечения информационной безопасности.
6. Основные технологии межсетевого экранирования.
7. Системы обнаружения сетевых атак и вторжений.
8. Методы обнаружения сетевых аномалий.
9. Виртуальные частные сети. Удостоверяющие центры и сертификаты.
10. Технология IPSec.

Литература для подготовки:

1. Программно-аппаратные средства защиты информации / В.В. Платонов — М.: Издательский центр «Академия», 2013. — 336 с. — http://it-ebooks.ru/publ/it_secutity/programmno_apparatnye_sredstva_zashhity_informacii/15-1-0-745.

2. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин — М.: ИД ФОРУМ: ИНФРА-М, 2012. — 416 с. — http://znanium.com/bookread.php?book=335362.

3. Башлы, П.Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — М.: РИОР, 2013. — 222 с. — http://znanium.com/bookread.php?book=405000.

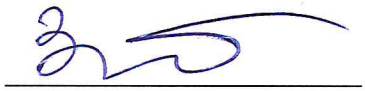
3. ПРИМЕР ТЕСТОВОГО ЗАДАНИЯ

Санкт-Петербургский политехнический университет Петра Великого

Институт компьютерных наук и кибербезопасности

УТВЕРЖДАЮ

Директор ИКНК



_____ Д.П. Зегжда

«28» ноября 2024 г.

ВСТУПИТЕЛЬНОЕ ИСПЫТАНИЕ

по направлению подготовки
10.04.01 «Информационная безопасность»

Междисциплинарный экзамен состоит из 50 тестовых заданий.
Максимальное количество баллов за каждое задание - 2
Примеры тестовых заданий:

Задание 1 (2 балла). Стеки – это подкласс:

1) **однонаправленных линейных списков**; 2) двунаправленных линейных списков; 3) очередей; 4) деревьев.

Задание 2 (2 балла). Наиболее существенное уменьшение времени выполнения дает следующая оптимизация:

1) понижение мощности; 2) размещение переменных в регистрах; 3) оптимизация вызовов процедур; 4) **развертка циклов**.

Задание 3 (2 балла). Отличие сетевого червя от вируса заключается в том, что он:

1) использует средства маскировки; 2) является многоплатформенным; 3) **является самостоятельной программой**; 4) распространяется через весь Интернет.

Задание 4 (2 балла). Операционную систему UNIX можно охарактеризовать как:

1) многопользовательскую систему пакетной обработки; 2) однопользовательскую систему разделения времени; 3) многозадачную

систему реального времени; 4) **систему разделения времени с вытесняющей многозадачностью**.

Задание 5 (2 балла). Текущий процесс операционной системы UNIX переходит в состояние останова, но в системе нет других процессов, готовых к исполнению. В такой ситуации:

1) **текущий процесс продолжает исполняться до появления процесса, готового к исполнению**; 2) происходит перезагрузка операционной системы; 3) планировщик уничтожает процесс, вызвавший тупиковую ситуацию; 4) ни один из ответов не верен.

Задание 6 (2 балла). Идентификация и аутентификация межсетевых экранов включает в себя:

1) **аутентификацию входящих и исходящих запросов**; 2) **идентификацию и аутентификацию всех субъектов прикладного уровня**; 3) идентификацию и аутентификацию администратора при его запросах на доступ; 4) препятствие доступу не идентифицированных субъектов.

Задание 7 (2 балла). Архитектура системы обнаружения вторжений включает в себя:

1) **модуль работы с источником информации**; 2) **модуль обнаружения**; 3) **модуль реагировани**я; 4) модуль передачи данных.

Задание 8 (2 балла). Организации выделена IP-сеть класса C, содержащая адрес 140.25.0.0. Какие из узлов принадлежат подсети этой организации?

1) 140.26.1.5; 2) 140.25.0.2; 3) 140.25.1.1; 4) **условие задачи неверно**.

Задание 9 (2 балла). Временная сложность наиболее быстрого алгоритма сортировки равна:

1) $O(n^2)$; 2) $O(n)$; 3) $\boldsymbol{O(n \log n)}$; 4) $O(\log n)$.

Задание 10 (2 балла). Деревья Фибоначчи – это:

1) самый лучший случай идеально сбалансированных деревьев; 2) самый худший случай идеально сбалансированных деревьев; 3) самый лучший случай АВЛ-сбалансированных деревьев; 4) **самый худший случай АВЛ-сбалансированных деревьев**.