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

УТВЕРЖДАЮ

Директор ИКНТ
_____ В.С. Заборовский
«29» 09 2017 г.

ПРОГРАММА

вступительного испытания для поступающих в магистратуру

по направлению подготовки/ образовательной программе

10.04.01 Информационная безопасность

10.04.01_01 Математические методы компьютерной безопасности

Код и наименование направления подготовки / образовательной программы

Санкт-Петербург

2017

Программа содержит перечень тем по основным дисциплинам учебного плана, формирующим профессиональные компетенции бакалавров по направлению 10.03.01 Информационная безопасность, вошедших в содержание тестовых заданий вступительных испытаний в магистратуру.

Составители:

профессор, д.т.н. Е.Б. Александрова

доцент, к.т.н. А.И. Печенкин

Руководитель ОП, д.т.н., проф. Д.П. Зегжда

Программа рассмотрена и рекомендована к изданию Ученым советом института компьютерных наук и технологий (протокол № 7 от «29» сентября 2017 г.).

1. ДИСЦИПЛИНЫ, ВКЛЮЧЁННЫЕ В ПРОГРАММУ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ В МАГИСТРАТУРУ

1.1. Математическая логика и теория алгоритмов.

1.2. Теория вероятностей и математическая статистика.

1.3. Алгебра и теория чисел.

1.4. Методы программирования.

1.5. Объектно-ориентированное программирование.

1.6. Операционные системы.

1.7. Компьютерные сети.

1.8. Основы информационной безопасности.

1.9. Модели безопасности компьютерных систем.

1.10. Теоретико-числовые методы в криптографии.

1.11. Программно-аппаратные средства обеспечения информационной безопасности.

2. СОДЕРЖАНИЕ УЧЕБНЫХ ДИСЦИПЛИН

2.1. Математическая логика и теория алгоритмов.

1. Основные логические операции, их приоритет.
2. Представление произвольной булевой функции в виде формулы алгебры логики.
3. Дизъюнктивная и конъюнктивная нормальные формы.
4. Многочлены Жегалкина.
5. Теорема Поста. Ее назначение и применение.
6. Минимизация нормальных форм. Метод Куайна.
7. Основы k-значной логики. Построение аналога многочлена Жегалкина.
8. Вывод из совокупности формул исчисления высказываний. Теорема дедукции.
9. Операции и множества истинности логики предикатов.
10. Предваренная нормальная форма.
11. Исчисление предикатов. Стандартная форма Скулема.
12. Унификация формул исчисления предикатов. Метод резолюций.
13. Базисные рекурсивные функции и операторы рекурсивных функций.
14. Алгоритмическая система Тьюринга. Тезис Черча–Тьюринга.
15. Временная и емкостная сложность алгоритмов.

Литература для подготовки:

1. Герасимов, А.С. Курс математической логики и теории вычислимости / А.С. Герасимов – https://www.mccme.ru/free-books/gerasimov-3ed-mccme.pdf.

2. Игошин, В.И. Математическая логика и теория алгоритмов: учеб. пособие для студ. высш. учеб. заведений / В.И. Игошин – http://vmate.ru/load/uchebniki/matematicheskaja_logika_i_teorija_algoritmov/igoshin_v_i_matematicheskaja_logika_i_teorija_algoritmov_ucheb_posobie_dlja_stud_vyssh_ucheb_zavedenij_v_i_igoshin_2_e_izd_ster/31-1-0-139.

3. Шапорев, С.Д. Математическая логика. Курс лекций и практических занятий / С.Д. Шапорев – https://eknigi.org/nauka_i_ucheba/176523-matematicheskaya-logika-kurs-lekciy-i-prakticheskih-zanyatiy.html.

2.2. Теория вероятностей и математическая статистика.

1. Вероятностное пространство. Свойства вероятностей.
2. Испытания Бернулли. Теорема Пуассона, теоремы Муавра–Лапласа.
3. Случайная величина. Дискретное и непрерывное распределение. Функция распределения.
4. Математическое ожидание. Дисперсия. Ковариация. Коэффициент корреляции.
5. Производящая и характеристическая функции.
6. Закон больших чисел.
7. Центральная предельная теорема.
8. Цепи Маркова. Классификация состояний цепи Маркова.
9. Оценивание неизвестных параметров. Свойства оценок.
10. Метод моментов. Метод максимального правдоподобия.
11. Доверительные интервалы.
12. Проверка статистических гипотез: основные определения. Уровень значимости. Мощность статистического критерия.
13. Проверка статистических гипотез. Критерии согласия. Критерии однородности. Ранговые критерии.
14. Критерий отношения правдоподобия.

Литература для подготовки:

1. Бочаров, П.П. Теория вероятностей. Математическая статистика / П.П. Бочаров, А.В. Печинкин. 2-е изд. – М.: Физматлит, 2005. – 296 с.

2. Вентцель, Е.С. Теория вероятностей / Е.С. Вентцель. – 10-е изд., стер. – М.: «Академия», 2005. — 576 с.

3. Гмурман, В.Е. Теория вероятностей и математическая статистика: Учеб. пособие / В.Е. Гмурман. 12-е изд., перераб. – М.: Высшее образование, 2006. – 479 с.

4. Гнеденко, Б.В. Курс теории вероятностей / Б.В. Гнеденко. – 8-е изд., испр. и доп. – М.: Едиториал УРСС, 2005. – 448 с.

2.3. Алгебра и теория чисел.

1. Группа. Абелева группа. Основные свойства групп.
2. Подгруппа. Собственная/несобственная подгруппа. Смежный класс.
3. Порождающая система. Конечнопорожденная группа. Циклическая группа.
4. Порядок элемента. Порядок группы. Теорема Лагранжа.
5. Нормальная подгруппа. Факторгруппа.
6. Гомоморфизмы групп. Теорема о гомоморфизмах групп.
7. Симметрическая группа. Знакопеременная группа. Цикловая структура подстановки.
8. Кольцо. Целостное кольцо. Мультипликативная группа кольца. Характеристика кольца.
9. Подкольцо и идеал. Главный идеал.
10. Факторкольцо (кольцо классов вычетов). Теорема о гомоморфизмах колец.
11. Поле. Подполе. Простое поле. Характеристика поля.
12. Конечное поле. Структура мультипликативной группы конечного поля.

Литература для подготовки:

1. Лузгарев, А. Алгебра и теория чисел / А. Лузгарев – http://mahalex.net/151-153/algebra.pdf.

2. Курош, А.Г. Курс высшей алгебры / А.Г. Курош – 17-е изд., Стереотипное. – СПб. [и др.] Лань, 2008. – 432 с.

3. ван дер Варден, Б.Л. Алгебра / Б.Л. ван дер Варден – М.: Физматлит, 2004. – 272 с.

2.4. 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.

2.5. Объектно-ориентированное программирование.

1. Различие подходов к программированию: процедурное, функциональное, объектно-ориентированное.
2. Понятие класса, объекта.
3. Инкапсуляция, наследование и полиморфизм.
4. Основные понятия объектно-ориентированного программирования: метод, поле, виртуальный метод, скрытие методов, перегрузка методов, перегрузка операторов, конструктор, деструктор.
5. Основы технологии COM. Необходимость интерфейса IUnknown и каждого из его методов.
6. Технология .NET. CLR, JIT, CLS.
7. Технология .NET. Классификация типов. Метаданные. Boxing/unboxing.
8. Шаблонное программирование. Generics/C++ шаблоны. Модификаторы области видимости для C++ и C#.
9. Базовые диаграммы UML: Классов, объектов, последовательности.
10. Дополнительные диаграммы UML: состояний, деятельности, пакетов.
11. Шаблоны проектирования: Delegation pattern, Builder, Factory method, Lazy initialization, Multiton/Singleton.
12. Шаблоны проектирования: Prototype, RAII, Adapter, Bridge, Façade.
13. Шаблоны проектирования: Proxy, Composite, Decorator, Command, Iterator.
14. Шаблоны проектирования: Null object, State, Template method, Visitor, Event listener.

Литература для подготовки:

1. Маконнел, С. Совершенный код. Мастер-класс / С. Маконнел. – Пер. с англ. – М. : Издательство «Русская редакция», 2010. – 896 с.

2. Страуструп, Б. Язык программирования C++ / Б. Страуструп. – Бином, 2015. – 1136 с.

3. Рихтер, Дж. CLR via C#. Программирование на платформе Microsoft .NET Framework 2.0 на языке C# / Дж. Рихтер. – Русская Редакция, Питер, 2007. – 656 с.

4. Брукс, Ф. Мифический человеко-месяц, или Как создаются программные системы / Фредерик Брукс. – Символ-Плюс, 2010. – 304 с.

5. Саттер, Г. Новые сложные задачи на C++ / Г. Саттер. – Вильямс, 2015. – 272 с.

6. Саттер, Г. Стандарты программирования на C++ / Г. Саттер, А. Александреску. – Вильямс, 2016. – 224 с.

7. Саттер, Г. Решение сложных задач на C++ / Г. Саттер. – Вильямс, 2008. – 400 с.

8. Бокс, Д. Сущность технологии COM. Библиотека программиста / Д. Бокс. – http://www.e-reading.club/book.php?book=7113.

2.6. 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.

2.7. 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.

2.8. 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.

2.9. 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. – http://www.imkn.ru/KIB/Nissenbaum/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2FKIB%2FNissenbaum%2FShared%20Documents%2F%D0%9A%D0%9E%D0%98%D0%91%D0%90%D0%A1%2D%D0%98%D0%91%D0%90%D0%A1%2F%D0%A2%D0%9E%D0%9A%D0%91.

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

2.10. Теоретико-числовые методы в криптографии.

1. Понятие сложности вычислительного алгоритма и вычислительной задачи. Сложность основных арифметических операций.
2. Отношение делимости. Норма. Деление с остатком. Наибольший общий делитель. Взаимно простые числа.
3. Алгоритм Евклида для целых чисел. Бинарный алгоритм Евклида. Расширенный алгоритм Евклида.
4. Сравнения и их свойства. Кольцо классов вычетов. Полная и приведенная система вычетов. Системы наименьших неотрицательных и абсолютно наименьших вычетов.
5. Функция Эйлера. Теорема Эйлера. Малая теорема Ферма.
6. Сравнения первой степени. Китайская теорема об остатках.
7. Символ Лежандра, его свойства. Символ Якоби, его свойства.
8. Сравнения второй степени. Решение сравнения второй степени.
9. Вероятностные алгоритмы проверки чисел на простоту. Свойства псевдопростых чисел. Числа Кармайкла. Свойства эйлеровых псевдопростых чисел.
10. Детерминированные алгоритмы проверки чисел на простоту. Теорема Поклингтона.
11. Непрерывные дроби. Подходящие дроби. Бесконечные непрерывные дроби.
12. Задача разложения числа на множители. Методы решения задачи разложения числа на множители. Парадокс дней рождения. Теорема Ферма о делителях составного числа.

13. Задача дискретного логарифмирования в простом поле. Методы решения задачи дискретного логарифмирования.

Литература для подготовки:

1. Банникова, Т.М. Основы теории чисел / Т.М. Банникова, Н.А. Баранова // http://elibrary.udsu.ru/ xmlui/bitstream/handle/123456789/3761/2009142.pdf.

2. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко // http://www.ict.edu.ru/ft/002416/book.pdf.

3. Герман, О.Н. Теоретико-числовые методы в криптографии / О.Н. Герман, Ю.В. Нестеренко // http://new.math.msu.su/department/number/dw/lib/exe/fetch.php?media=%D1%82%D1%87%D0%BC%D0%BA.pdf

4. Ишмухаметов, Ш.Т. Методы факторизации натуральных чисел / Ш.Т. Ишмухаметов // http://old.kpfu.ru/f9/bibl/Monograph_ishm.pdf.

2.11. 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

ВСТУПИТЕЛЬНОЕ ИСПЫТАНИЕ

по направлению подготовки/образовательной программе

10.04.01 Информационная безопасность

Код и наименование направления подготовки / образовательной программы

УТВЕРЖДАЮ

Руководитель ОП

_____ Д.П. Зегжда

«___» _____ 20__ г.

ВАРИАНТ № 1

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). В смежном классе $x^4 - 2x^2 + 3x + 3 + (x^2 - 3)$ из факторкольца $\mathbf{Q}[x]/(x^2 - 3)$ представитель наименьшей возможной степени равен:

1) $3x + 6$; 2) $3x + 3$; 3) $x^2 + 1$; 4) $x^2 - 3$.

Задание 4 (2 балла). Ядро гомоморфизма колец — это:

1) множество элементов прообраза, отображающихся в 0; 2) множество элементов прообраза, отображающихся в 1; 3) множество образов; 4) нормальная подгруппа аддитивной группы кольца.

Задание 5 (2 балла). Какое из колец $\mathbf{F}_2[t]$, $\mathbf{F}_2[t]/(t^3 + t + 1)$ является конечным полем?

1) ни одно из колец; 2) $\mathbf{F}_2[t]$; 3) $\mathbf{F}_2[t]/(t^3 + t + 1)$; 4) оба кольца.

Задание 6 (2 балла). Сколько различных подгрупп в группе корней 6-й степени из единицы?

1) 1; 2) 2; 3) 3; 4) 4.

Задание 7 (2 балла). Какой набор логических операций является полным?

1) &, ¬; 2) ∨, ¬; 3) →; 4) |.

Задание 8 (2 балла). Совершенной дизъюнктивной нормальной формой (ДНФ) формулы *A* называется:

1) минимальная по числу переменных и операций ДНФ формулы *A*; 2) ДНФ формулы *A*, для которой выполнены свойства совершенности; 3) ДНФ формулы *A*, которая не является тождественно ложной; 4) ДНФ формулы *A*, которая является тождественно ложной.

Задание 9 (2 балла). Главным плюсом механизма полиморфизма вирусов со стороны злоумышленника является:

1) легкость внедрения такой вредоносной программы в WinPE; 2) невозможность создания универсальной сигнатуры для данного образца вредоносной программы; 3) легкость внедрения такой вредоносной программы в файл; 4) такая программа не определяется с помощью сканирования.

Задание 10 (2 балла). Переключение контекста процесса осуществляется:

1) при исполнении в режиме ядра; 2) при исполнении в режиме задачи; 3) при переходе из режима задачи в режим ядра; 4) при переходе из режима ядра в режим задачи.

Задание 11 (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 12 (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 13 (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 14 (2 балла). Архитектура системы обнаружения вторжений включает в себя:

1) модуль работы с источником информации; 2) модуль обнаружения; 3) модуль реагирования; 4) модуль передачи данных.

Задание 15 (2 балла). Полной системой вычетов по модулю 4 является множество:

1) {1, –2, 3, 8}; 2) {0, 1, 3, 5}; 3) {2, 4, 6, 8}; 4) {2, 3, 5, 8}.

Задание 16 (2 балла). Чему равен символ Якоби (5/25)?

1) 0; 2) –1; 3) 1; 4) (1/5).

Задание 17 (2 балла). Экземпляр класса, представляющий собой совокупность переменных и связанных с ними методов (операций), — это:

1) класс; 2) метод; 3) объект; 4) структура.

Задание 18 (2 балла). Механизм, позволяющий объектам класса приобретать характеристики (данные и методы) более простых и общих типов (классов), называется:

1) инкапсуляцией; 2) абстракцией; 3) полиморфизмом; 4) наследованием.

Задание 19 (2 балла). Если класс имеет ассоциацию с самим собой, то такую ассоциацию называют:

1) транзитивной; 2) рефлексивной; 3) коммутативной; 4) ассоциативной.

Задание 20 (2 балла). Какой тип структурной связи изображен на диаграмме классов?

1) агрегация; 2) ассоциация; 3) обобщение; 4) композиция.

Задание 21 (2 балла). Поведенческий шаблон проектирования, предоставляющий способ последовательного доступа к элементам множества, независимо от его внутреннего устройства, называется:

1) Visitor; 2) Proxy; 3) Iterator; 4) Event Listener.

Задание 22 (2 балла). Что такое деструктор?

1) специальная функция-элемент, которая должна отслеживать данные в экземпляре класса в процессе работы; 2) специальная функция-элемент, которая должна уничтожать экземпляр класса после завершения его работы; 3) функция, которая должна открывать динамическую область для экземпляра класса; 4) указатель на удаленный объект.

Задание 23 (2 балла). События A и B являются независимыми, если:

1) $P(AB) = 0$; 2) $P(A|B) = P(A)$; 3) $P(A|B) = P(B)$; 4) 2) $P(AB) = P(A)P(B)$.

Задание 24 (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 25 (2 балла). Временная сложность наиболее быстрого метода сортировки равна:

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

Задание 26 (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.

Задание 27 (2 балла). Компиляторы выполняют:

1) машинно-зависимую оптимизацию; 2) машинно-независимую оптимизацию; 3) оптимизацию на уровне ассемблера; 4) все указанные виды оптимизаций.

Задание 28 (2 балла). Транспортный протокол, требующий установления соединения:

1) UDP; 2) ARP; 3) TCP; 4) ICMP.

Задание 29 (2 балла). Какие типы прав доступа для базовых классов доступа к файлам поддерживаются в операционной системе Unix?

1) Read (r), write (w), execute (e); 2) Read (r), write (w), execute (e), grant (g) ; 3) Read (r), write (w); 4) Read (r), write (w), grant (g).

Задание 30 (2 балла). На каком уровне модели OSI располагается подуровень управления доступом к среде (Media Access Control)?

1) физический; 2) канальный; 3) прикладной; 4) сеансовый.

Задание 31 (2 балла). Наивысшим быстродействием обладает межсетевой экран:

1) фильтрации пакетов; 2) уровня соединения; 3) прикладного уровня; 4) «глубокого изучения пакетов».

Задание 32 (2 балла). Протокол разрешения адресов ARP предназначен для:

1) преобразования фиктивных IP-адресов в реальные IP-адреса; 2) преобразования адресов сетевого уровня модели OSI в адреса канального уровня модели OSI; 3) динамического получения IP-адреса; 4) получения email-адреса отправителя письма.

Задание 33 (2 балла). Какие из следующих утверждений описывают недостатки одноранговых сетей (выберите все верные ответы)?

1) неисправность одного узла выводит из строя всю сеть; 2) существенное увеличение стоимости в связи с необходимостью в выделенном оборудовании и специализированном программном обеспечении; 3) при доступе к разделенным ресурсам наблюдается снижение производительности рабочей станции; 4) для управления сложным серверным программным обеспечением требуется квалифицированный сотрудник.

Задание 34 (2 балла). Динамическая трансляция адреса — это

1) операция при которой физически последовательным страницам виртуальной памяти при поддержке ОС и аппаратуры ставятся в соответствие определенные логические страницы ОЗУ: 2) операция при которой логически последовательным страницам виртуальной памяти при поддержке ОС и аппаратуры ставятся в соответствие определенные физические страницы ОЗУ; 3) копирование памяти с жесткого диска в оперативную память; 4) сохранение данных из оперативной памяти на жесткий диск.

Задание 35 (2 балла). К механизмам межпроцессного взаимодействия относятся:

1) тупики; 2) семафоры; 3) светофоры; 4) перекрестки.

Задание 36 (2 балла). Основная особенность абстрактного класса состоит в том, что он

1) изолирован, не наследуется; 2) может служить только базовым для других классов, нельзя создавать его экземпляры; 3) доступен только в текущем модуле; 4) содержит виртуальные методы.

Задание 37 (2 балла). Способ планирования, при котором момент переключения на другую задачу определяет сама текущая задача, называется:

1) вытесняющей многозадачностью; 2) невытесняющей многозадачностью; 3) обгоняющей многозадачностью; 4) самостоятельной многозадачностью.

Задание 38 (2 балла). Сколько итераций совершит цикл for(int x = 0; x = 3; x++);

1) 3; 2) 4; 3) это бесконечный цикл; 4) в коде содержится синтаксическая ошибка.

Задание 39 (2 балла). Преобразование первоначального текста программы перед тем, как он подвергается компиляции, производится:

1) компилятором; 2) препроцессором; 3) интерпретатором; 4) компоновщиком.

Задание 40 (2 балла). Какой документ, описывает задачи обеспечения защиты информации в терминах функциональных требований и требований гарантированности?

1) профиль защиты; 2) проект защиты; 3) пояснительная записка; 4) техническое задание.

Задание 41 (2 балла). Какая модель безопасности использует модель защищенного документооборота, переработанную для применения в сфере информационных технологий?

1) модель Белла и ЛаПадулы; 2) модель Харрисона–Руззо–Ульмана; 3) модель действий/сущностей; 4) модель Китайской стены.

Задание 42 (2 балла). К основным подходам к определению информационной безопасности относятся:

1) нормативный; 2) конструктивный; 3) интуитивный; 4) экспериментальный.

Задание 43 (2 балла). На какие этапы разделяют моделирование защищенной системы?

1) синтез; 2) анализ; 3) сопровождение; 4) утилизация.

Задание 44 (2 балла). Вирусы, которые постоянно находятся в памяти компьютера, называются:

1) резидентными; 2) нерезидентными; 3) загрузочными; 4) файловыми.

Задание 45 (2 балла). Пусть в директории C:\x\ находятся файлы target.bat, target.com и target.exe. Какой файл запустится при выполнении команды C:\x\target?

1) target.exe; 2) target.com; 3) target.bat; 4) команда не выполнится из-за отсутствия расширения файла.

Задание 46 (2 балла). Сигнатурой компьютерного вируса называется:

1) Уникальная последовательность байтов, принадлежащая конкретному известному компьютерному вирусу и не встречающаяся в других программах; 2) заголовок кода вируса; 3) любая последовательность байтов, записанная в коде программы вируса; 4) совокупность операций, произведенная вирусом.

Задание 47 (2 балла). Недостаток программного средства, которым может воспользоваться злоумышленник, называется:

1) уязвимостью; 2) просчетом; 3) ошибкой; 4) эксплойтом.

Задание 48 (2 балла). Проверка подлинности запросов и ответов не предусмотрена протоколом:

1) DNS; 2) ARP; 3) POP3; 4) HTTP.

Задание 49 (2 балла). Уязвимость, позволяющая атакующему передать серверу исполняемый код, который будет перенаправлен браузеру пользователя, это:

1) фиксация сеанса; 2) межсайтовая подделка запроса; 3) межсайтовое выполнение сценариев; 4) расщепление HTTP-запроса.

Задание 50 (2 балла). В чем основное отличие Blind SQL-инъекции от классической SQL-инъекции:

1) содержание запроса закодировано другой кодировкой; 2) отправляется неполный запрос; 3) результат инъекции невозможно получить; 4) результат инъекции не отображается на странице.