МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут»

|  |  |  |
| --- | --- | --- |
|  |  | **ЗАТВЕРДЖЕНО** |
|  |  | вченою радоюНаціонального аерокосмічного університету ім. М.Є. Жуковського«Харківський авіаційний інститут»Заступник голови вченої ради \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_22 лютого 2017 р., протокол № 11 |

**ПРОГРАМА**

**ВСТУПНОГО ВИПРОБУВАННЯ**

для здобуття освітнього ступеня магістра

за освітньо-професійного програмою

зі спеціальності

**125 - Кібербезпека**

(шифр та найменування)

(спеціалізація **Безпека інформаційних і комунікаційних систем**)

(найменування)

**у 2017 році**

Харків

2017

**ВСТУП**

 Вступне випробування для здобуття освітнього ступеня магістра за освітньо-професійного програмою зі спеціальності

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_125 - Кібербезпека\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (код та найменування)

(спеціалізації Безпека інформаційних та комунікаційних систем\_\_\_\_\_\_\_\_\_\_\_\_)

відбувається відповідно до «Правил прийому до Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут» у 2017 році» у формі індивідуального письмового фахового іспиту, який приймає екзаменаційна комісія з певної спеціальності (спеціалізації), склад якої затверджується наказом ректора Університету.

До фахового іспиту входять питання за темами:

### – Мікропроцесорні системи;

### – Комп'ютерні мережі;

### – Захист інформації;

### – Організація баз даних;

### – Системне програмування.

 Перелік питань за темами наведений у програмі.

 Результат критерію оцінювання знань фахового іспиту визначається за 100-бальною шкалою згідно з розділом VII, п. 2 Правил прийому до Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут».

Іспит проводиться в вигляді тестів, що складається з 20 завдань з переліку питань, що входять до програми фахового випробування для здобуття освітнього ступеня магістра за освітньо-професійною програмою зі спеціальності 125 - Кібербезпека (спеціалізації Безпека інформаційних та комунікаційних систем).

Кожне завдання тесту оцінюється в 5 балів від загальної кількості балів згідно правил прийому. Тест може містити в собі завдання в яких потрібно вибрати одну або декілька вірних відповідей (якщо це зазначається в умові завдання) з запропонованого переліку варіантів відповідей до кожного завдання. Для завдань в яких потрібно вибрати декілька варіантів відповідей бали будуть зараховані лише в тому випадку, якщо всі відповіді на запитання вибрані абітурієнтом будуть вірними. За виправлення відповіді в випадку якщо виправлена відповідь виявиться вірною абітурієнту знімається один або два бали в залежності від умов завдання (одна або декілька вірних відповідей).

1. **Питання за темою «Мікропроцесорні системи»**
	1. Мікропроцесори. Основні визначення. Архітектура мікропроцесора. Основні вузли.
	2. Класифікація мікропроцесорів. RISC і CISC архітектури. Архітектура Фон-Неймана. Гарвардська архітектура.
	3. Система команд мікропроцесора. Арифметичні команди. Логічні команди. Команди розгалуження (переходу).
	4. Адресація в мікропроцесорах. Адресація пам'яті. Види адресації. Адресація зовнішніх пристроїв.
	5. Периферійні пристрої мікропроцесорів. Організація роботи з периферійними пристроями.
	6. Інтерфейси мікропроцесорних систем. Системні інтерфейси. Інтерфейси розширення. Інтерфейси ISA. PCL РСІН.
	7. Інтерфейси периферійного обладнання мікропроцесорних систем. Інтерфейси USB, CAN. SATA ...
	8. Організація стека в мікропроцесорних системах. Робота зі стеком.
	9. Переривання в мікропроцесорних системах. Вектор переривання. Контролер переривання. Маскування запитів. Пріоритетна обробка.
	10. Прямий доступ до пам'яті в мікропроцесорних системах. Контролер ПДП. Організація роботи. Пріоритети.
	11. Задатчики в мікропроцесорній системі. Види задатчиків. Пріоритети. Організація передачі управління.
	12. Задавальний генератор в мікропроцесорній системі. Види ЗГ. Розподіл і множення частоти ЗГ.
	13. Управління енергоспоживанням в мікропроцесорної системі. Способи зниження енергоспоживання. Реалізація.
	14. Сховище в мікропроцесорній системі. Класифікація. ОЗП, ПЗП. Регенерація ОЗП динамічного типу.
	15. Робота мікропроцесорної системи в режимі реального часу. Таймери. Лічильники. Процесориподій.
	16. Аналого-цифрові підсистеми мікропроцесорних систем. АЦП. Види АЦП. Організація АЦП. ЦАП. Масштабуючі підсилювачі. Компаратори аналогових сигналів. НОН. Мультиплексори аналогових сигналів.
	17. Мультимікропроцесорні системи. Класифікація. Способи організації. Синхронізація. Скидання. Взаємодія.
	18. Зовнішні запам'ятовуючі пристрої МПС. CD / DVD, вінчестер, FLASH ЗП.
	19. Відеосистема МПС. Архітектура відеосистеми. Класифікація пристроїв. Відображення інформації (ПВІ). Принципи роботи ПВІ.
	20. Принтери. Сканери. Плотери. Принципи роботи. Організація взаємодії у мікропроцесорній системі.

Література

1. Полупроводниковые БИС ЗУ. Справочник. Под ред. Гордонова А. Ю. И Дьякова Ю.Н .М. : Радио и связь, 1987.
2. БИС ЗУ. Справочник. Под ред. Гордонова А. Ю. И Дьякова Ю.Н. М.: Радио и связь, 1990.
3. Логические ИС КР1533. КР1 1554. Справочник. Петровский И. И. и др. Бином. 1993.
4. Однокристальные микро - ЭВМ. Липовецкий Г. П. и др. Бином. 1992.
5. Технические средства микропроцессорных систем. Дж. Коффрон М. Мир, 1983.

Питання склав

доцент кафедри 503 О.О. Галькевич

 (науковий ступень, посада) (ініціали та прізвище)

**2 Питання за темою "Комп'ютерні мережі"**

2.1. Класифікація, основні характеристики комп'ютерних мереж. Визначення і

класифікація комп'ютерних мереж. Основні характеристики і вимоги, що висуваються до комп'ютерних мереж.

2.2. Топології комп'ютерних мереж. Логічна і фізична топології комп'ютерних мереж. Топологія шина, кільце, зірка, змішана топологія.

2.3. Методи спільного доступу. Методи спільного доступу до середовища передачі даних. Комутація потоку даних і встановлення з'єднань. Призначення і загальна структура мережних кадрів/пакетів.

2.4. Протоколи і моделі взаємодії комп'ютерних мереж. Еталонна модель взаємодії відкритих систем ISO/OSI. Рівні моделі ISO/OSI та їхнє призначення. Інкапсуляція. Протоколи комп'ютерних мереж. Стек протоколів ТСР/ІР.

2.5. Гарантована передача інформації. Принципи гарантованої передачі інформації по комп'ютерних мережах. Забезпечення захисту від утрати, перекручування і дублювання.

2.6. Устаткування комп'ютерних мереж. Концентратори та комутатори: призначення, різниця у функціонуванні, недоліки. Комутатори та маршрутизатори: призначення, різниця у функціонуванні, недоліки.

2.7. Характеристики кабельних ліній зв'язку. Типи кабелів: коаксіальний кабель,

„кручена пара", оптичний кабель. Амплітудно-частотна характеристика. Затухання. Завадостійкість. Смуга пропускання та її зв'язок з пропускною здатністю. Формули Шенона та Найквіста.

2.8. Кабельна система комп'ютерних мереж. Структурована кабельна система: структура, підсистеми, вимоги щодо протяжності кабельних сегментів. Стандарти СКС. Адміністрування СКС.

2.9. Модуляція та спектральна характеристика сигналів. Види модуляції, частотна, амплітудна, фазова. Спектр модульованого сигналу. Спектр прямокутного синхро-сигнала. Цифрова модуляція аналогових сигналів: імпульсно-кодова модуляція, дельта-модуляція.

2.10. Фізичне та логічне кодування. Необхідність фізичного кодування інформації в комп'ютерних мережах. Коди: NRZ або потенційний, AMI. NRZI, 2B1Q, Manchester-Ii.

2.11. Сучасні технології локальних комп'ютерних мереж. Базові технології сучасних комп'ютерних мереж і їхня характеристика: Fast/GigabitEthernet, 1 OOVG-AnyLAN, FDDI, ATM, Організація абонентського доступу до глобальної мережі Internet: сімейство технологій xDSL.

2.12. Технології локальних мереж сімейства Ethernet. Метод доступу CSMA/CD. Особливості побудови локальних обчислювальних мереж Fast-. Gigabit- та 10G-Ethernet: специфікації фізичного рівня. Принципи високошвидкісної передачі інформації по кабелю „кручена пара".

2.13. Технології бездротових мереж. Бездротові мережі Wi-Fi сімейства ІЕЕЕ802.11. Метод доступу CSMA/CA. Частотні канали. Режими роботи: Ad-hoc, Infrastructure. Принципи розгортання бездротових мереж.

2.14. ІР-адреси та ІР-протокол. ІР-адреса і маска підмереж. Типи підмереж. Оптимальний розподіл ІР-адресів за технологією CIDR. IPv4 та IPv6. Формат заголовку ІР-протоколу. Фрагментація ІР-пакетів

2.15. Протоколи маршрутизації. Дистанційно-векторні протоколи. Протоколи стану лінії зв'язку. Різниця у принципах роботи. Протоколи внутрішньої та зовнішньої маршрутизації. Особливості реалізації протоколів RIP. OSPF, EIGRP.

2.16. Система адресації в мережах ТСР/ІР. Адресація вузлів комп'ютерної мережі: доменні імена, фізичні та мережні адреси. Перетворення між різними типами адресів. Ідентифікація мережних програм. Порти транспортних протоколів.

2.17. Транспортний протокол TCP. Встановлення та розрив мережного з'єднання. Продуктивність протоколу TCP. Вікно передачі. Алгоритми керування потоком даних і контролю за перевантаженнями. Структура пакетів TCP. Флаги TCP.

2.18. Захист інформації у комп'ютерних мережах. Загрози безпеки інформації у комп'ютерних мережах. Мережні атаки. Етапи інформаційного вторгнення.

2.19. Методи та засоби захисту інформації. Брандмауери: proxy-сервери, фільтруючи маршрутизатори. Списки доступу. Види підключень брандмауерів. Екранована підмережа.

2.20. Віртуальні приватні мережі. Типи та протоколи віртуальних приватних мереж. Протокол IPSec. Користування VPN-з'єднанням для доступу до Internet.

Література

1. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд. / В. Г. Олифер, Н. А. ОлиферСПб.: Питер. 2009.- 864 с.
2. М. Кульгин. Технология корпоративных сетей. Энциклопедия. - СПб.: Питер, 2003. -704 с.
3. Таненбаум Э. Компьютерные сети. - СПб.: Питер, 2008. - 848 с.

Питання склав

к.т.н., доцент кафедри 503 Д.Д. Узун

(науковий ступень, посада) (ініціали та прізвище)

**3 Питання за темою "Організація баз даних"**

3.1. Теоретичні основи реляційних БД. Загальні поняття. Таблиці та зв'язки між ними. Типи зв'язків.

3.2. Проектування сховищ баз даних. Нормалізація. Приведення сховищ даних до нормальних форм та денормалізація.

3.3. OLAP та OLTP. Визначення та концептуальна різниця.

3.4. Інструментальний засіб MSSQL Server Management Studio.

Принципи роботи з інструментальним засобом MSSQL Server Management Studio та його основні функціональні можливості.

3.5. Архітектура MSSQL Express 2005.

Типи даних MSSQL Express 2005. Об'єкти баз даних (безпеки, програмні). Системні бази даних, та їх призначення. Ховання даних на фізичному рівні.

3.6. Засоби обмеження цілісності даних. Первинні ключі. Зовнішні ключі. Тригери.

3.7. Transact-SQL. Ідентифікатори. Оператори. Вирази. Змінні, умовні та циклічні конструкції.

3.8. Обробка помилок. Виключення. Функції роботи з виключеннями.

3.9. SQL. Підмножина DML. Select, insert, update, delete, truncate. Рекомендації оптимізатору запитів.

3.10. SQL. Підмножина DDL. Create, alter, drop (застосовано до таблиць, індексів, тригерів та процедур, що зберігаються).

3.11. Рекурсивні запити.Засоби реалізації ієрархічних сховищ у реляційній СКБД.

3.12.Індекси. Унікальні. Кластерні та некластерні. XML-індекси, повнотекстові індекси.

3.13. Уявлення. Призначення, функціональні можливості, особливості використання.

3.14. Функціональні блоки. Процедури, що зберігаються. Функції, що призначені для користувача. Передача та повернення параметрів у наслідок виклику.

3.15. Тригери DML. Принципи роботи з тригерами.

3.16. Курсори. Принципи роботи з курсорами. Синтаксис та параметри курсорів.

3.17. Транзакції. Загальні поняття. Властивості транзакцій (ACID). Рівні ізоляції, їх властивості та призначення. Програмування транзакцій. Вкладені транзакції.

3.18. Сучасні технології доступу до баз даних на стороні клієнта.

Загальні принципи роботи з базами даних із клієнтських додатків. Використання баз даних MSSQL Express із зовнішніх програм. Програмна модель підключення до СКБД. Виконання запитів та отримання результатів.

3.19. Бібліотека JDBC. Класи та методи бібліотеки JDBC. Приклади програм на Java.

3.20. Бібліотека ADO.NET. Класи та методи бібліотеки ADO.NET. Приклади програм на С#.

Література

1. Пирогов В. «SQL Server 2005. Программирование клиент-серверных приложений.» -СПб: БХВ-Петербург. 2006. ~336с.
2. ДейтК.Дж. «Введение в базы данных» - М.: Вильяме, 2006. -1328с.
3. Конноли Т.. Бегт К. Базы данных. Проектирование, реализация и сопровождение.Теория и практика. Москва: «Вильяме». 2001 г -1436с.

Питання склав

к.т.н., доцент кафедри 503 А.В. Шостак

(науковий ступень, посада) (ініціали та прізвище)

**4 Питання за темою "Захист інформації в комп'ютерних системах та мережах "**

4.1. Базові поняття криптографія та криптоаналіза. Поняття криптографії та криптоаналізу, криптографічної системи, криптографічного алгоритму, шифру, криптограми, ключа. Поняття про криптоаналіз як процес, принцип Кергхофа.

4.2. Принципи побудови симетричних та асиметричних криптосистем та їх порівняльна характеристика. Комбіновані криптосистеми.

4.3. Класифікація методів та засобів криптографічного захисту інформації. Моноалфавітні та поліалфавітні шифри підстановки.

4.4. Загальна характеристика методів криптоаналіза і класифікація криптографічних систем за рівнем стійкості. Показники криптографічної стійкості криптосистем. Умови реалізації абсолютно-стійких криптосистем на основі ентропійного підходу. Шифр Вернама.

4.5. Принципи побудови потокових криптосистем. Узагальнена структура потокової

криптосистеми. Принципи побудови потокової криптосистеми за принципом комбінування на базі лінійних рекурентних регістрів здвигу зі зворотнім зв'язком.

4.6. Принципи побудови блочних симетричних криптосистем Узагальнена структура блочної симетричної криптосистеми. Схема Фейстеля.

4.7. Загальна характеристика блочного симетричного криптоалгоритма DES. принципи його функціонування.

4.8. Загальна характеристика блочного симетричного криптоалгоритма ГОСТ 21847-89 та принципи його функціонування в режимі простої заміни.

4.9. Режими шифрування блочних симетричних шифрів. Порівняльна характеристика сучасних блочних симетричних алгоритмів.

4.10. Узагальнена структура несиметричної криптосистеми. принципи її побудови та теоретико-числова проблематика.

4.11. Характеристика процедур шифрування і розшифрування згідно з криптоалгоритмом RSA.

4.12. Характеристика процедур шифрування і розшифрування згідно з криптоалгоритмом Ель-Гамаля.

4.13. Принципи побудови сучасних криптографічних хеш-функцій та вимоги, що пред'являються до них.

4.14. Поняття про цифровий підпис та вимоги, що пред'являються до нього. Узагальнений протокол цифрового підпису.

4.15. Алгоритми цифрового підпису Ель-Гамаля і DSA.

4.16.Класифікація процесів автентифікації суб'єктів (автентифікація як елемент системи управління доступом до інформаційних ресурсів та взаємна мережева автентифікація). Паролювання як механізм автентифікації.

4.17. Протокол взаємної автентифікації з нулевою передачею знань Фейге-Фіата-Шаміра.

4.18. Загальна характеристика методів розподілу ключів.

4.19. Характеристика компонентів інфраструктура відкритих ключів. Склад цифрового сертифіката.

4.20. Протокол відкритого ключового обміну Діффі-Хеллмана.

Література

1. Столлингс В. Криптография и защита сетей. Принципы и практика. - К.: «Вильяме», 2001.-669 с.

2. Шнайер Б. Прикладная криптография: протоколы, алгоритмы, исходные тексты на языке Си. - М.: "Триумф". 2002. - 815 с.

3. Мамаев М. Петренко С. Технологии защиты информации в Интернете. Специальный справочник. - СПб: Питер. 2002. 848 с.

4. Конеев И.Р.. Беляев A.B. Информационная безопасность предприятия. - СПб.: БХВ -Петербург. 2003. - 752 с.

5. Шостак A.B. Программирование алгоритмов защиты информации в.NET Framework: лаб. практикум / A.B. Шостак, И.В. Лысенко. - X.: Нац. аэрокосм. ун-т «Харьк. авиац. ин-т», 2011.-74 с. [Электронное издание]

Питання склав

к.т.н., доцент кафедри 503 І.В. Лисенко

(науковий ступень, посада) (ініціали та прізвище)

**5 Питання за темою "Системне програмування"**

5.1. Що означає поняття Win32 АРІ? Які файли в системі входять до складу Win32 АРІ?

5.2. Типи даних Win32 та їх відповідність стандартним С / С + + типам.

5.3. Визначення статусу виконання системних АРІ. Отримання кодів помилок і рядків описуючих помилок.

5.4. Подання ANSI і Юникод рядків Win32. Конвертування рядків з одного кодування в іншу.

5.5. Робота з файлами через Win32 АРІ. Операції створення, відкриття, запису, читання та ін.

5.6. Символічні й жорсткі посилання в NTFS. Робота з символічними жорсткими посиланнями в Win32 АРІ.

5.7. Навігація по директоріях, отримання списків файлів і каталогів, маніпуляція файлів по імені (копіювання, видалення, переміщення і т.д) за допомогою Win32 АРІ.

5.8. Що таке File Mapping? Робота з File Mapping на Win32 АРІ.

5.9. Функції роботи з реєстром на Win32 АРІ.

5.10. Купи пам'яті. Звичайні та Low Fragmentation купи. АРІ роботи з пам'яттю через купи.

5.11. Механізм віртуальної пам'яті в ОС Windows. Менеджер віртуальної пам'яті та його алгоритм роботи. Файли підкачки. АРІ для роботи з пам'яттю за прямими віртуальним адресами.

5.12. Багаторівнева модель додатків Windows. Ресурси, пов'язані з процесами і потоками. Градація пріоритетів для процесів і потоків.

5.13. Створення дочірніх процесів на Win32 АРІ. Перенаправлення потоків вводу / виводу для дочірніх процесів.

5.14. Маніпуляція процесами за допомогою Win32 АРІ. Отримання списку процесів, зупинка і запуск процесів і т.д.

5.15. Створення багато потокових додатків на Win32 API. TLS пам'ять потоків.

5.16. Що таке Pipes? Робота с Pipes на Win32 АРІ.

5.17. Функції очікування процесів або потоків.

5.18. Об'єкти синхронізації Win32 АРІ. Що таке Event. Mutex. Semaphore. Waitable Timer та Critical Section.

5.19. Архітектура віконних додатків Windows. Цикли обробки віконних повідомлень. Віконні процедури та повідомлення Windows.

5.20. Створення віконного інтерфейсу на Win32 АРІ. Базові функції і структури.

Література

1. Харт, Джонсон, М. Системное программирование в среде Win32. 3-е изд.: Пер. с англ.: - М. : Издательский дом «Вильяме». 2005. - 592 с.

2. РихтерДж. Windows для профессионалов: создание эффективных Win32 приложений с учетом специфики 64-разрядной версии Windows/Пер, англ - 4-е изд. - СПб; Питер; М.: Издательско-торговый дом "Русская Редакция", 2001. - 752 с.

3. Дейтел Г. Введение в операционные системы: В 2-х т. Пер. с англ. - М: Мир, 1987. - 359 с.

Питання склав

Ст. викл.кафедри 503 О.С. Годунов

(науковий ступень, посада) (ініціали та прізвище)

 Завідувач кафедри 503 \_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.С.Харченко

 (підпис) (ініціали та прізвище)

Програму розглянуто й узгоджено на випусковій кафедрі 503\_\_\_\_\_\_\_\_

Протокол № 8 від «20» січня 2017 р.

Програму вступного випробування для здобуття освітнього ступеня магістра за освітньо-професійного програмою зі спеціальності 125 - Кібербезпека (спеціалізації Безпека інформаційних та комунікаційних систем) узгоджено науково-методичною комісією Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут» з галузей знань: «Математика та статистика», «Інформаційні технології», «Автоматизація та приладобудування», «Хімічна біоінженерія», «Електроніка та телекомунікації» (НМК 2).

Протокол № \_\_\_ від \_\_\_\_\_\_\_ лютого 2017 р.

Голова НМК 2

к.т.н., доц. О.В. Заболотний

погоджено науково-методичною комісією Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут»

Протокол № \_\_\_ від \_\_\_\_\_\_\_лютого 2017 р.

Голова НМК Університету

д.т.н., проф. В.М. Павленко