КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015

ЗАТВЕРДЖЕНО
Голова приймальної комісії
_____ Анатолій МАЗАРАКІ
"20" січня 2022 р.

ПРОГРАМА
фахового вступного випробування для здобуття освітнього ступеня магістра на основі здобутого освітнього ступеня бакалавра, магістра (освітньо-кваліфікаційного рівня спеціаліста)

галузь знань	**12 «Інформаційні технології»**
спеціальність	**125 «Кібербезпека»**
освітня програма	**«Безпека систем електронних комунікацій в економіці»**

Київ 2022

ВСТУП

Програма вступного випробування з фахових дисциплін для здобуття освітнього ступеня «магістр» галузь знань – 12 «Інформаційні технології» спеціальність – 125 «Кібербезпека» (на базі освітнього ступеня «бакалавр» та «спеціаліст») підготовлена на основі освітньо-професійної програми, є науково-методичним документом, який забезпечує комплексний підхід до оцінки рівня теоретичної та практичної підготовки вступників до професійної діяльності.

Мета вступного випробування – визначити обсяг та рівень теоретичних знань, практичних навичок та вмінь з профілюючих дисциплін у галузі інформаційних технологій, які пов'язані з усіма аспектами виробництва програмного продукту від початкових стадій створення специфікації до супроводу системи після здачі в експлуатацію.

Вступні випробування проводяться у формі письмового тестування, що дозволяє перевірити теоретичні знання вступників, їх уміння логічно мислити та вирішувати проблемні ситуації з комплексу дисциплін які пов'язані з інформаційними технологіями.

Програма вступних випробувань містить такі розділи:

1.Основи кібербезпеки.

2. Архітектура комп'ютера.

3. Операційні системи.

4. Організація комп'ютерних мереж.

5. Бази даних.

6. Безпека інформаційних систем та мереж.

7. Криптографічні методи захисту інформації.

До програми додається список рекомендованих джерел, який допоможе у підготовці до вступного випробування.

ЗМІСТ ПРОГРАМИ ВСТУПНИХ ВИПРОБУВАНЬ

Розділ 1. Основи кібербезпеки

Роль криптографії у захисті даних. Поняття шифру. Шифр простої замінитайого аналіз. Шифри перестановки таїх аналіз. Варіанти ускладнення шифру простої заміни. Шифр багатоалфавітної замінитайого аналіз. Вимогидо шифрів - принцип Керхгоффса.

Вимоги до сучасних криптографічних систем. Шифри на основі мережі Фейстеля.. Шифри на основі SP-мережі. Стандарт AES. Схеми електронного цифрового підпису. Надійність цифрового підпису. Хеш-функції, призначення та їх основні властивості. Класифікація функцій хешування.

Основні методи криптоаналізу. Методи генерації псевдовипадкових числових послідовностей. Модулярна арифметика. Односторонні функції та їх властивості. Отримання великих простих чисел. Сучасні асиметричні криптосистеми.

Основні етапи аутентифікації та авторизації. Чинники аутентифікації. Аутентифікація суб'єктів доступа. Аутентифікація на основі знань. Аутентифікація на основі володіння. Аутентифікація на основі ознак та дій.

Сутність управління ключами. Стандарти генерації ключів. Накопичення, розподілення, оновлення, зберігання, резервування ключів. Генерація ключів. Модифікація ключа. Зберігання ключів. Розподіл ключів.

Основні поняття стеганографії. Стеганографічна система. Стеганографічний контейнер. Стеганографічний канал. Основні загрози безпеки стеганографічних систем. Виявлення стеганографічного каналу. Типи порушників безпеки стеганографічних систем. Сфера використання методів стеганографічного захистуінформації.

Розділ 2. Архітектура комп'ютера

Поняття архітектури ПК. Архітектура фон Неймана. Складові частини ПК та їх взаємодія. Основні показники та характеристики комп'ютерів.

Представлення даних у комп'ютері. Типи, форми та формати подання інформації у ПК. Логічні операції, логічні операції з двійковими числами. Логічні елементи. Елементи пам'яті, тригери, регістри. Лічильники. Оперативна пам'ять.

Класифікація материнських плат по форм-фактору. Чипсети. Північний та південний міст. Зведена таблиця параметрів чипсетів для сучасних процесорів. Програмні засоби тестування чипсет.

Послідовні та паралельні порти уводу/виводу. COM-порт. LTP-порт. PS/2. Шини ISA, PCI. Специфікація шини PCI. Стандартні модифікації шини PCI. Інтерфейси бездротового підключення периферійних пристроїв.

Комп'ютерний блок живлення. Системна шина (FSB). Шина даних. Шина адресу. Кешування оперативної пам'яті. Конвеєрна архітектура. Суперскалярна архітектура. Багатоядерні процесори. Паралельна архітектура.

Види RAM. Способи та програмні засоби тестування оперативної пам'яті.

Відеоадаптер: принципи роботи, пристрої, технічні характеристики. Основні компоненти графічної плати. Відеопам'ять. Монітор. Основи та принципи BIOS.

Програма самотестування комп'ютерів POST. Усунення помилок та обслуговування комп'ютерів. Методика обслуговування комп'ютерів та її особливості.

Розділ 3. Операційні системи

Поняття операційної системи, її призначення та функції. Історія розвитку операційних систем. Класифікація сучасних операційних систем. Функціональні компоненти операційних систем.

Поняття архітектури операційних систем. Взаємодія операційної системи з апаратним забезпеченням. Взаємодія операційної системи з програмним забезпеченням. Підходи до реалізації архітектури операційних систем. Архітектура системи UNIX. Архітектура системи Linux. Архітектура системи Windows.

Базові поняття процесів і потоків. Багатопотоковість та її реалізація. Стани процесів і потоків. Опис процесів і потоків. Загальні принципи планування. Види планування. Стратегії планування. Витісняюча та невитісняюча багатозадачність. Алгоритми планування. Реалізація планування в Linux. Реалізація планування у Windows.

Основні принципи взаємодії потоків. Взаємодія потоків у Linux. Взаємодія потоків у Windows.

Основи технології віртуальної пам’яті. Сегментація пам’яті. Сторінкова організація пам’яті. Сторінково-сегментна організація пам’яті. Реалізація керування основною пам’яттю у Linux. Реалізація керування основною пам’яттю у Windows.

Динамічна ділянка пам’яті процесу. Особливості розробки розподілювачів пам’яті. Послідовний пошук підходящого блоку. Ізольовані списки вільних блоків. Системи двійників. Підрахунок посилань і збирання сміття. Реалізація динамічного керування пам’яттю в Linux. Реалізація динамічного керування пам'яттю в Windows.

Поняття файлу і файлової системи. Організація інформації у файловій системі. Зв’язки. Атрибути файлів. Операції над файлами і каталогами. Налагодження взаємодії між процесами на основі інтерфейсу файлової системи.

Базові відомості про дискові пристрої. Розміщення інформації у файлових системах. Продуктивність файлових систем. Надійність файлових систем.

Файлові системи ext2fs і ext3fs. Файлові системи лінії FAT. Файлова система NTFS. Особливості кешування у Windows. Системний реєстр Windows.

Розділ 4. Організація комп’ютерних мереж

Основні етапи розвитку комп’ютерних мереж. Тенденції розвитку та структура апаратних та програмних засобів ранніх локальних та глобальних мереж. Відмінності від сучасних мереж.

Основні поняття та визначення, що використовуються у сучасних комп’ютерних мережах, їх класифікація та призначення. Концепції

побудови комп'ютерних мереж: локальні та глобальні комп'ютерні мережі. Типи локальних комп'ютерних мереж: однорангові мережі та мережі побудовані на основі клієнт / сервер-технологіях. Особливості і доцільність використання.

Поняття та порівняння комутації пакетів та комутації каналів.

Топологія комп'ютерних мереж. Базові топології комп'ютерних мереж. Еталонна мережна модель OSI як глобальний стандарт для визначення функціональних рівнів, необхідних для підтримки з'єднання між комп'ютерами. Поняття мережних стеків. Розподіл процесу з'єднання комп'ютерів на сім функціональних рівнів та взаємодія між ними.

Мережний рівень, його призначення. Поняття дейтаграми.

Рівень маршрутизації, його зв'язок з мережними протоколами, поняття протоколів з установленим з'єднанням та без встановленого з'єднання.

Архітектура Ethernet. Сучасні стандарти Ethernet: Fast Ethernet та Gigabit Ethernet. Архітектура Token Ring. Перспективи розвитку Token Ring. Технологія FDDI. Місце технології FDDI на сучасному ринку технологій комп'ютерних мереж. Технологія ATM. Перспективи впровадження технології ATM.

Апаратні засоби комп'ютерних мереж: призначення та їх класифікація. Типи апаратних засобів, критерії вибору, співвідношення між їх функціями та рівнями моделі OSI. Вплив топології на вибір апаратних засобів.

Мережева операційна система – основа функціонування комп'ютерних мереж. Історія розвитку мережних операційних систем. Функціональна структура та стандартні служби мережевої операційної системи.

Технології мобільного доступу в Інтернеті. Базові технології мобільного зв'язку: першого покоління – GPRS, EGPRS; другого покоління – CDMA – 2000.

Розділ 5. Бази даних

Визначення, основні поняття та призначення баз даних та систем управління базами даних. Місце БД в сучасних інформаційних системах. Структура автоматизованого банку даних. Вимоги до сучасних баз даних. Види та класифікація баз даних. Персональні та багато користувальні бази даних. Типи моделей даних та різновиди БД: ієрархічні, сітьові та реляційні.

Архітектура системи баз даних. Три рівні архітектури: зовнішній, концептуальний, внутрішній. Архітектура клієнт-сервер. Утиліти. Розподілена обробка.

Реляційні бази даних та її об’єкти. Реляційна модель. Оптимізація. Каталог. Базові таблиці і представлення. Мова SQL. Цілісність реляційних даних. Потенційні ключі. Первинні та альтернативні ключі. Зовнішні ключі. Посилкова цілісність.

Проектування бази даних. Введення в функціональні залежності. Основні визначення. Тривіальні та нетривіальні залежності. Замкнення множини залежності. Замкнення множини атрибутів. Незведена множина залежності. Нормалізація відношень. Нормальні форми. Декомпозиція без втрат та функціональні залежності. Збереження залежності. Нормальна форма Бойса-Кодда.

Структури збереження та методи доступу.

Індексування.

Хешування.

CASE – технології розробки моделей даних. Призначення та функції CASE-технології ERWin компанії Computer Associates. Створення логічної моделі даних. Рівні логічної моделі даних. Сутності та атрибути. Генерація SQL-опису БД на основі фізичної моделі.

Основи архітектури бази даних MySQL.

Функціональна мова SQL. Категорії операторів SQL. Прості та складні запити мови SQL для вибірки даних. Запити мови SQL для визначення та обробки даних. Збережені процедури, тригери та представлення СУБД MySQL.

Технічний огляд інтерфейсу з базами даних ODBC (Open Database Connectivity). Пакет XAMPP. Доступ до MySQL з використанням PHP. Програмне забезпечення необхідне для створення Java-сервлетів, які використовують БД MySQL. Інтерфейс доступу до БД MySQL на мові Java.

Розділ 6. Безпека інформаційних систем та мереж

Види можливих порушень в роботі інформаційної системи. Розголошування. Витік інформації. Несанкціонований доступ до системи або мережі. Загрози інформації. Основні поняття і класифікація загроз. Основні загрози доступності. Основні загрози цілісності. Основні загрози конфіденційності. Порушники інформаційної безпеки. Класифікація порушників. Методика вторгнення. Умови, що сприяють неправомірному оволодінню інформацією. Канали витоку інформації та перехоплення даних. Модель безпеки: структура і компоненти. Засоби забезпечення безпеки інформаційних систем і мереж. Призначення і завдання у сфері забезпечення інформаційної безпеки на рівні держави. Міжнародні стандарти інформаційної безпеки. Державний стандарт України із захисту інформації.

Стандарти інформаційної безпеки. Критерії оцінювання захищеності інформаційної системи. «Критерії оцінки довірених комп'ютерних систем» («Помаранчева книга»). Міжнародний стандарт побудови ефективної системи безпеки ISO 17799. Аналіз засобів порушення інформаційної безпеки. Інженерно-технічний рівень інформаційної безпеки. Технічні засоби для несанкціонованого доступу до інформації. Засоби протидії несанкціонованому доступу до інформації. Канали витоку інформації. Захист інформації від витоку по технічним каналам. Апаратні засоби захисту. Програмні засоби захисту.

Основні терміни та поняття криптографії. Одноалфавітні системи шифрування Віженера, Плейфейра та інші. Багатоалфавітні системи шифрування: Бьюфорта, Віженера та інші Основні типи алгоритмів шифрування. Електронний цифровий підпис. Управління ключами та сертифікація ключів. Стеганографічні методи захисту інформації. Поняття і класифікація комп'ютерних вірусів. Коротка характеристика вірусів. Програмні закладки. Програми – шпигуни і логічні бомби. Антивірусні програми. Корпоративні антивіруси. Правила використання стороннього програмного забезпечення. Спам і засоби боротьби з ним. Фішинг.

Правила безпечної роботи в мережах. Захист на мережевому рівні. Системи виявлення вторгнення в безпроводові мережі.

Розділ 7. Криптографічні методи захисту інформації

Базові поняття криптографії. Поняття та види шифрів: шифр простої заміни, шифри перестановки, шифр багатоалфавітної заміни. Роль криптографії у захисті даних. Поняття та види шифрів. Вимоги до шифрів - принцип Керхгоффса. Шифрувальні машини та підходи до їх аналізу. Ідеальний шифр і класи стійкості шифрів.

Основні види криптографічних методів. Реалізація криптографічних методів. Симетричні і асиметричні методи шифрування. Шифри на основі мережі Фейстеля. Мережа Фейстеля. Американський шифр DES. Шифри на основі SP-мережі.

Сучасні блокові шифри. Компоненти сучасного блокового шифру. Розгляд відомих блокових шифрів (ГОСТ 28147, DES, AES, ДСТУ 7624 і т.д.). Переваги недоліки. Складені шифри. Режими роботи блокових шифрів.

Криптографічне перетворення. Симетричні криптографічні перетворення. Методи генерації псевдовипадкових числових послідовностей. Модулярна арифметика. Створення комбінованих криптографічних засобів та нові підходи до побудови шифрів.

Криптосистема Ель–Гамаля. Шифрування та розшифрування в криптосистемі Ель–Гамаля. Коректність, ефективність та надійність криптосистем Рабіна та Ель-Гамаля. Криптосистема Діфі-Хелмана.

Шифрування та розшифрування в криптосистемі Діфі-Хелмана. Коректність, ефективність та надійність криптосистем Діфі-Хелмана.

Принципи еліптичної криптографії. Методи шифрування в еліптичній криптографії. Алгебраїчні операції в скінчених полях. Особливості програмної реалізації операції над точками еліптичної кривої.

Поняття криптографічних протоколів. Їх опис. Класифікація криптографічних протоколів. Властивості, що визначають безпеку криптографічних протоколів. Атаки на протоколи. Аналіз та моделювання криптографічних протоколів. Протоколи електронного цифрового підпису.

Принцип Керкгоффса. Стандарти генерації ключів. Накопичення, розподілення, оновлення, зберігання, резервування ключів. Генерація та модифікація ключа. Зберігання та розподіл ключів. Протоколи обміну ключами. Протоколів, що ґрунтуються на симетричних криптосистемах. Протоколи, що ґрунтуються на асиметричних криптосистемах.

Типи та класи порушників безпеки стеганографічних систем. Типи атак на стеганографічні системи. Атака з відомим контейнером. Атака з вибором контейнера. Атака з відомим повідомленням. Атака з вибором повідомлення. Атака, що направлена на руйнування повідомлення.

КРИТЕРІЇ
оцінювання знань на вступному фаховому випробуванні для здобуття освітнього ступеня магістра

1. Загальні положення:

Мета фахового випробування – оцінити відповідність знань, умінь та навичок вступників згідно з вимогами програми вступного фахового випробування.

2. Структура екзаменаційного білета:

Екзаменаційний білет з фахового випробування складається з 50-ти закритих тестових завдань.

3. Критерії оцінювання:

- Рівень знань оцінюється за 200-баловою шкалою.
- Серед відповідей на тестове завдання вступнику слід обрати одну правильну.
- Правильна відповідь на тестове завдання оцінюється у 4 бали, а неправильна – у 0 балів.
- Особи, які отримали менше 100 балів до наступних випробувань не допускаються та участі у конкурсі не беруть.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Ducket, Jon (2014). HTML and CSS: Design and Build Websites. Indianapolis: John Wiley & Sons.
2. ISO/IEC 15288 Systems and software engineering - System life cycle processes. – [Чинний від 2008-03-18] – 70 с. (міжнародний стандарт).
3. Nixon, Robin (2015). Learning PHP, MySQL &JavaScript: With jQuery, CSS & HTML5. USA, Sebastopol: O'Reilly Media, Inc.
4. Андон Ф. И. Основы инженерии качества программных систем / Ф. И. Андон, Г. И. Коваль., Т. М. Коротун, Е. М. Лаврищева, В. Ю.Суслов. – К. : Академпериодика, 2017. – 672 с.
5. Анісімов А.В. Інформаційні системи та бази даних: Навчальний посібник / А.В. Анісімов, П.П. Кулябко. – Київ: КНУ, 2017. – 110 с.
6. Берко А. Ю. Системи баз даних та знань. Книга 2. Системи управління базами даних та знань / А. Ю. Берко, О. М. Верес, В. В. Пасічник – Львів: «Магнолія-2006», 2015. – 470 с.
7. Бурлаков А. А. Об'єктно-орієнтований аналіз і проектування. Методичні рекомендації з самостійного вивчення дисципліни студентами напрямку підготовки «Програмна інженерія» / А. А. Бурлаков. – Хмельницький: ХНУ, 2017. – 136 с.
8. Буров Є. В. Комп'ютерні мережі: підручник / Є. В. Буров.– Львів: «Магнолія 2006», 2015. – 262с.
9. Бушуєв С. Д. Методологія управління бюджетними проектами: Посібник / С. Д. Бушуєв, С. В. Цюцюра, О. В. Криворучко та ін. – К.: КНУБА, 2016. – 196 с.
10. Вонтинг Ларс Бо. Oracle Enterprise Manager 101 : пер. з англ. / Ларс Бо Вонтинг, Дирк Щепанек – К. : «Лори», 2005. – 480с.
11. Гончарова Л. Л., Возненко А. Д., Стасюк О. І., Коваль Ю. О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013. – 435 с.
12. Грабер М. «SQL. Справочное руководство» / М. Грабер – М. : «Лори», 2000, – 291с.
13. Ебби Майкл. Oracle 9i: Первое знакомство : пер. з англ. / Майкл Ебби, Майкл Кори, Йен Амбросон – К. : «Лори», 2003. – 506с.
14. Кавун С. В. Архітектура комп'ютерів. Особливості використання комп'ютерів в ІС : навчальний посібник / С. В. Кавун, І. В. Сорбат. – Харків : Вид. ХНЕУ, 2010. – 256с.
15. Кунгурце А. Б. Основи програмування на мові Java. Середовище Net Beans. Навч. Посібник для студентів вищих навчальних закладів / А. Б. Кунгурцев, Т. В. Ковалюк. – Одеса, 2016. – 183 с.
16. Микитишин А. Г. Комп'пютерні мережі, кн. 2. Навчальний посібник для технічних спеціальностей ВНЗ / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк. – Львів: «Магнолія 2006», 2018. – 328 с.

17. Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99
18. С. В. Кавун Системне програмування та операційні системи Д. Ю. Голубничий, С. В. Кавун, В. Ф. Третяк: навч.посібник. Ч.2 Харків : ХНЕУ, 2015.
19. Ткаченко О. М. Об'єктно-орієнтоване програмування мовою Java. Навчальний посібник. / О. М. Ткаченко. – Вінниця: ВНТУ, 2016. – 107с.
20. Цюцюра С. В. Системи управління інвестиційними проектами. Навчальний посібник/ С. В. Цюцюра, О. В. Криворучко, М. І. Цюцюра. – К.: КНУБА, 2013. – 152 с.
21. Шеховцев В. А. Операційні системи / В. А. Шеховцев. – К. : BHV, 2015. – 576 с.
22. Шклярський С. М. Прикладний Інтернет для економістів : навч. посіб. – Київ : КНТЕУ, 2009. – 121с.
23. Энсор Дейв. Oracle. Проектирование баз даних: Пер. С англ. / Дейв Энсор, Йен Стивенсон – К.: Издательская група BHV, 2000. – 560 с.

Додатковий

1. Delisle, Marc (2014). Mastering phpMyAdmin 3.3.x for Effective MySQL Management. Packt Publishing. p. 359
2. Бурк Р. UNIX для системных администраторов. Р. Бурк, Б. Хорват. Энциклопедия пользователя Київ : ДиаСофт, 2017.
3. Гайна Г.А. Основи проектування баз даних: Навчальний посібник. − К.: КНУБА, 2016. – 204 с.
4. Кантор М. Управление программными проектами. Практическое руководство по разработке успешного программного обеспечения.: Пер. с англ. – М.: Издательский дом «Вильямс», 2002. – 176с.
5. M.C. Paulk, C.V. Weber, B. Curtis, M.B. Chrissis et al The Capability Maturity Model: Guidelines for Improving the Software Process. AddisonWesley, Boston. 2015. – 456 p.
6. Мельник А. О. Архітектура комп'ютера. Підручник :/ А. О. Мельник: Волинська обласна друкарня , 2008. – 471с.
7. Полянська, В. Кібернетична безпека України в умовах розвитку глобальної інформаційної системи [Текст] / В. Полянська // Підприємництво, господарство і право. – Київ, 2013. – No 7 (211).
8. Пономаренко Л. А. Комп'ютерні технології управління інноваційними проектами. – К.: КНТЕУ, 2001. – 453с.
9. Рибалов Б. О. Архітектура комп'ютерів: Посібник до виконання лабораторних робіт./ Б. О. Рибалов; Одеська національна академія харчових технологій, 2015. – 43с.
10. Схемотехніка електронних систем. У 3 кн. Кн. 3. Мікропроцесори та мікроконтролери: Підручник / В. І. Бойко, А. М. Гуржий, В. Я. Жуйков та ін.. – К.: Вища шк., 2004. – 399с.
11. Троян С.О. Програмування мовою Java: навч. посіб. / С. О. Троян. – Умань: ФОП Жовтий О. О., 2017. – 132 с.

12. Форкун Ю. В.– Об’єктно-орієнтоване програмування: лабораторний практикум для студентів напрямів освіти «Програмна інженерія» та «Комп’ютерні науки»/ Ю. В. Форкун, Р. В. Сорокатий, С.С. Блащук.. – Хмельницький: ХНУ, 2014. – 143 с.
13. Цюцюра С. В. Управління інноваційними проектами модернізації підприємств енергоємних галузей. – К.: Наук. світ, 2016. – 219 с.
14. Чернега В. Безпровідні локальні комп’ютерні мережі / В. Чернега, Б. Платтнер. – К.: «Кондор», 2015. – 238 с.

Інтернет-ресурси

1. Журнал «Информационные технологии. Аналитические материалы». – Режим доступу: http://it.ridne.net
2. http://litrus.net/book/read/3455?p=1 – книги по БД
3. http://ua.bookfi.org/ – книги по БД
4. http://www.citforum.ru – ресурс комп’ютерних технологій
5. http://www.w3c.org/– сайт консорціума WWW