НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«Київський політехнічний інститут імені Ігоря Сікорського»

Затверджую

Голова Приймальної комісії
Ректор

Анатолій МЕЛЬНИЧЕНКО

28.03.2025 р.
дата

ПРОГРАМА
вступного іспиту зі спеціальності
для вступу на освітньо-наукову програму підготовки доктора філософії
«Інформаційні системи та технології»

за спеціальністю F6 Інформаційні системи та технології

Програму ухвалено:
Науково-методичною комісією за спеціальністю
Інформаційні системи та технології
Протокол № 2 від 20 березня 2025 р.
Голова НМКУ
Олександр РОЛІК

Київ – 2025

ВСТУП

Програма вступного іспиту визначає форму організації, зміст та особливості проведення вступного іспиту зі спеціальності на освітньо-наукову програму підготовки докторів філософії «Інформаційні системи та технології» за спеціальністю F6 Інформаційні системи та технології.

Освітня програма «Інформаційні системи та технології» відповідає місії та стратегії КПІ ім. Ігоря Сікорського, за якою стратегічним пріоритетом університету є формування якісного людського капіталу для відновлення та стійкого розвитку України, створення засад поставання соціально-відповідальних фахівців, готових вирішувати глобальні проблеми та змінювати світ. Особливості освітньої програми враховані шляхом обрання відповідних розділів програми вступного іспиту. Проведення вступного випробування має виявити рівень підготовки вступника з обраної для вступу спеціальності.

Метою програми є перевірка набуття вступником компетентностей та результатів навчання, що визначені стандартом вищої освіти за спеціальністю F6 Інформаційні системи та технології для другого (магістерського) рівня вищої освіти.

Програма проведення вступного іспиту для спеціальності F6 «Інформаційні системи та технології охоплює предметне коло питань із проєктування та розроблення інформаційних систем та технологій, управління ризиками інформаційної безпеки, інженерії даних та великих даних, методів надання інформаційних сервісів.

За своєю структурою зміст програми поділяється на такі розділи:

1) проєктування та розроблення інформаційних систем та технологій;
2) управління ризиками інформаційної безпеки;
3) інженерія даних та великі дані;
4) методи надання інформаційних сервісів.

Питання, що входять до тем розділів, розташовані у логічній послідовності та відповідають змісту навчальних дисциплін, що викладаються для студентів другого (магістерського) рівня вищої освіти за спеціальністю F6 «Інформаційні системи та технології».

1. ОСНОВНИЙ ВИКЛАД

1.1. Перелік розділів та тем, які виносяться на іспит зі спеціальності

Розділ 1

ПРОЄКТУВАННЯ ТА РОЗРОБЛЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

1.1 Архітектура систем
- 1.1.1 Архітектурні стилі
  - 1.1.1.1 Монолітна архітектура
    - 1.1.1.1.1 Однорівневі додатки
    - 1.1.1.1.2 Тісно пов'язані компоненти
    - 1.1.1.1.3 Проблеми розгортання
  - 1.1.1.2 Архітектура мікросервісів
    - 1.1.1.2.1 Принципи декомпозиції сервісів
    - 1.1.1.2.2 Міжсервісний зв'язок (REST, gRPC)
    - 1.1.1.2.3 Контейнеризація та оркестрація
  - 1.1.1.3 Безсерверна архітектура
    - 1.1.1.3.1 Функція як послуга (FaaS)
    - 1.1.1.3.2 Моделі виконання, керовані подіями

1.1.1.3.3 Проблеми холодного старту
1.1.2 Патерни масштабованості
1.1.2.1 Горизонтальне масштабування
1.1.2.1.1 Стратегії балансування навантаження
1.1.2.1.2 Проектування додатків без стану
1.1.2.2 Вертикальне масштабування
1.1.2.2.1 Апаратні обмеження
1.1.2.2.2 Вартісні наслідки
1.1.2.2.3 Ризики єдиної точки відмови
1.2 Розроблення програмного забезпечення
1.2.1 Парадигми та найкращі практики програмування
1.2.1.1 Об'єктно-орієнтоване програмування
1.2.1.1.1 Принципи SOLID (єдина відповідальність (SRP), принцип відкритості/закритості (OCP), заміщення Лісков (LSP), розділення інтерфейсу (ISP), інверсії залежності (DIP)
1.2.1.1.2 Патерни проєктування (твірні (factory, singleton), структурні (adapter, decorator), поведінкові (observer, strategy)
1.2.1.2 Функціональне програмування
1.2.1.2.1 Чисті функції
1.2.1.2.2 Функції вищих порядків
1.2.1.2.3 Рекурсія
1.2.2 Розроблення API
1.2.2.1 RESTful API
1.2.2.1.1 HATEOAS
1.2.2.1.2 Стратегії керування версіями
1.2.2.2 gRPC/GraphQL
1.2.2.3 Безпека API (JWT, OAuth2)
1.2.3 Архітектура програмного забезпечення
1.2.3.1 Багаторівнева архітектура
1.2.3.2 Гексагональна архітектура
1.2.3.3 Мікросервіси
1.2.3.3.1 Межі сервісів (Bounded Contexts)
1.2.3.3.2 Міжсервісна комунікація
1.2.4 Екосистема Java
1.2.4.1 Ядро Java
1.2.4.1.1 Concurrency (Threads, CompletableFuture)
1.2.4.1.2 Collection Framework
1.2.4.2 Spring Framework
1.2.4.2.1 Ін'єкція залежностей
1.2.4.2.2 Spring Boot Auto-Configuration
1.2.4.2.3 Spring Data JPA
1.2.5 Прототипування UI/UX
1.2.5.1 Wireframing Tools
1.2.5.2 Стандарти доступності
1.2.6 Практики розробки
1.2.6.1 Тестова розробка (TDD)
1.2.6.2 Методи рефакторингу
1.2.6.3 Пайплайнери CI/CD
1.3 Системи баз даних
1.3.1 Проектування реляційних баз даних
1.3.1.1 ER-моделювання (ER-діаграма, сутності, атрибути, зв'язки)
1.3.1.2 Нормалізація

1.3.1.2.1 1NF (Атомарні значення атрибутів, первинні ключі)
1.3.1.2.2 2NF (Усунення часткових функціональних залежностей)
1.3.1.2.3 3NF (Усунення транзитивних залежностей)
1.3.1.2.4 BCNF (Посилена 3NF)
1.3.1.2.5 4NF (Нетривіальні багатозначні залежності)
1.3.1.2.6 5NF (Складні залежні сполуки)
1.3.1.3 Фізичне моделювання
1.3.1.3.1 Фізичне проєктування схеми бази даних (перетворення сутностей у таблиці, введення обмежень цілісності)
1.3.1.3.2 DDL та DML скрипти для створення структури бази даних та тестових записів
1.3.1.4 Розширений SQL
1.3.1.4.1 Аналіз запиту з метою знаходження «вузьких місць» (EXPLAIN PLAN, COST оптимізація)
1.3.1.4.2 Методи підвищення ефективності відпрацювання запитів (індексування, оптимізація SQL запиту, денормалізація)
1.3.2 Проектування баз даних NoSQL
1.3.2.1 Сховища документів (проектування схем MongoDB)
1.3.2.2 Часові ряди (політика зберігання даних у InfluXDB)

Розділ 2

УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Організація управління ризиками інформаційної безпеки
2.1.1 Системний підхід до управління ризиками. Показники ризику
2.1.2 Процесна модель менеджменту ризиків інформаційної безпеки
2.1.3 Методи обробки ризиків інформаційної безпеки
2.2 Методологічне та нормативне забезпечення аналізу та оцінювання ризиків. Міжнародні стандарти в галузі аналізу та оцінювання ризиків
2.2.1 Серія стандартів ДСТУ(ISO/IEC) 270xx
2.2.2 Серія стандартів ДСТУ (ISO/IEC) 310xx
2.3.3 Стандарти NIST 800-xx
2.3 Аналіз загроз і вразливостей
2.3.1 Системи класифікації і оцінювання вразливостей
2.3.1.1 Класифікація вразливостей CVSS
2.3.1.2 Класифікації вразливостей CVE та CWE
2.3.1.4 Вразливості веб-додатків OWASP-10
2.3.1 Моделювання загроз інформаційної безпеки
2.3.1.1 Типи та джерела кіберзагроз. APT-атаки
2.3.1.2 Моделі кібератак ATT&CK та CAPEC
2.3.1.3 Методологія STRIDE
2.3.1.4 Методологія DREAD
2.4 Методи аналізу і загального оцінювання ризиків інформаційної безпеки
2.4.1 Кількісні та якісні методи аналізу ризиків
2.4.2 Методи ідентифікації ризиків
2.4.3 Методи аналізу засобів управління ризиками (метод Bow Tie)
2.4.4 Методи визначення джерел і факторів ризику (метод Ishikawa)
2.5 Управління інцидентами інформаційної безпеки
2.5.1 Ознаки інциденту інформаційної безпеки
2.5.2 Порядок обробки інцидентів інформаційної безпеки

Розділ 3

ІНЖЕНЕРІЯ ДАНИХ ТА ВЕЛИКІ ДАНІ

3.1 Архітектура та життєвий цикл даних

3.1.1 Джерела, потоки й споживачі даних

3.1.2 Data Lineage, Data Governance, метадані

3.1.3 Порівняння ETL, ELT, Lambda- та Kappa-архітектур

3.2 Моделювання та схеми даних

3.2.1 Концептуальне → логічне → фізичне моделювання

3.2.2 Нормалізація / денормалізація, зіркова та сніжинка-схеми

3.2.3 Партиціювання, шардінг, індекси (B-tree, bitmap, inverted)

3.3 Реляційні СУБД і оптимізація запитів

3.3.1 Глибинний розбір плану виконання (EXPLAIN/EXPLAIN ANALYZE)

3.3.2 Індексація, матеріалізовані представлення, кластеризація таблиць

3.3.3 Транзакції, блокування, ізоляційні рівні

3.4 NoSQL-підходи

3.4.1 Key-Value, Document, Wide-Column, Graph

3.4.2 CAP-теорія та вибір бази під конкретну бізнес проблему

3.4.3 Універсальні патерни моделювання NoSQL-даних

3.4.3.1 One-to-Many та Many-to-Many у денормалізованих сховищах

3.4.3.2 Time-series та подієві журнали (append-only)

3.4.3.3 Handling hot partitions, TTL, soft-deletes

3.5 Файлові формати та серіалізація

3.5.1 CSV, JSON, XML — переваги та обмеження

3.5.2 Колончаті формати (Parquet, ORC)

3.5.3 Стиснення (gzip, zstd, Snappy) та вплив на продуктивність

3.6 Побудова ETL/ELT-конвеєрів

3.6.1 Оркестратори: Airflow, Prefect, Dagster

3.6.2 Інкрементальне завантаження, CDC (Change Data Capture)

3.6.3 Обробка помилок, idempotency, SLA/SLO для пайплайнів

3.7 Обробка потоків (stream processing)

3.7.1 Apache Kafka / Pulsar: топологія, partition keys, at most once / at least once / exactly-once

3.7.2 Spark Streaming / Flink: window функції, watermark, stateful ops

3.8 Big Data та розподілені обчислення

3.8.1 Hadoop HDFS, YARN, MapReduce

3.8.2 Apache Spark: RDD vs DataFrame, Catalyst, Tungsten

3.8.3 Оптимізація Spark завдань: broadcast join, partition pruning, caching

3.9 Хмарні сервіси та Data Lake / Data Warehouse

3.9.1 S3 / GCS як шар зберігання; формати + partition layout

3.9.2 Snowflake, BigQuery, Redshift — відмінності архітектур

3.9.3 Delta Lake / Iceberg / Hudi (ACID у Data Lake)

3.10 Моніторинг та спостережуваність

3.10.1 Метрики (latency, throughput, SLA, SLO)

3.10.2 Логи й трасування (ELK / OpenTelemetry)

3.10.3 Data Quality Monitoring: дрейф схем, пропущені партіції

Розділ 4

МЕТОДИ НАДАННЯ ІНФОРМАЦІЙНИХ СЕРВІСІВ

4.1 Архітектура хмарних сервісів

4.1.1 Проєктування відмовостійких (fault-tolerant) архітектур

4.1.1.1 Горизонтальне масштабування

4.1.1.2 Обробка пікового навантаження
4.1.1.3 Резервування та зонування доступності
4.1.2 Архітектура сервісів з високою доступністю (HA)
4.1.2.1 Балансування навантаження між регіонами
4.1.2.2 Реплікація сервісів між дата-центрами
4.1.2.3 Побудова мульти-регіональних рішень
4.1.3 Моделі розгортання інформаційних сервісів
4.1.3.1 Порівняння IaaS, PaaS та SaaS
4.1.3.2 Trade-off між контрольованістю та зручністю
4.2 Хмарна інфраструктура і автоматизація
4.2.1 Інфраструктура як код (IaC)
4.2.1.1 Опис та управління ресурсами
4.2.1.2 Аудит і контроль змін
4.2.1.3 Ролі IaC у розгортанні ETL та сервісів
4.2.2 Побудова гібридних хмарних рішень
4.2.2.1 Інтеграція локальної інфраструктури з хмарною
4.2.2.2 Забезпечення уніфікованого моніторингу
4.3 Обчислювальні моделі і масштабування
4.3.1 Serverless-архітектура
4.3.1.1 Моделі подійної обробки
4.3.1.2 Холодний старт та затримки
4.3.1.3 Переваги і обмеження безсерверної моделі
4.3.2 Контейнеризація і автоскейлінг
4.3.2.1 Мікросервісна декомпозиція
4.3.2.2 Автоматичне масштабування на основі навантаження
4.3.2.3 Балансування навантаження в контейнерних кластерах
4.3.3 Оптимізація витрат у хмарі
4.3.3.1 Порівняння моделей ціноутворення
4.3.3.2 Прогнозування навантаження і резервування ресурсів
4.3.3.3 Капсуляція сервісів з урахуванням вартості
4.4 Безпека і управління доступом
4.4.1 Організація доступу до хмарних сервісів
4.4.1.1 Рольова модель доступу (RBAC)
4.4.1.2 Політики на рівні ресурсів
4.4.1.3 Ізоляція клієнтів у багатокористувацьких рішеннях
4.4.2 Забезпечення безпеки даних у публічній хмарі
4.4.2.1 Географічне розміщення даних
4.4.2.2 Шифрування і контроль доступу
4.4.2.3 Захист каналів обміну
4.5 Обробка подій і даних
4.5.1 Архітектури обробки подій
4.5.1.1 Системи повідомлень та черг
4.5.1.2 Семантика обробки подій (exactly-once, at-least-once)
4.5.1.3 Масштабування обробників подій
4.5.2 Оркестрація обробки даних
4.5.2.1 Побудова ETL-пайплайнів
4.5.2.2 Автоматизація трансформації даних
4.5.2.3 Інтеграція з багатьма джерелами і контроль доступу

1.2. Порядок проведення іспиту

Іспит проводиться у вигляді письмової роботи. Кожен білет містить чотири запитання. Для випробування передбачено 50 екзаменаційних білетів, сформованих з наведеного вище переліку тем.

Термін виконання іспиту становить 2 астрономічні години (120 хвилин – основна частина та 15 хвилин – організаційна частина) без перерви. Після написання роботи предметна комісія перевіряє її та виставляє оцінку згідно з критеріями оцінювання.

Методика проведення іспиту наступна. Члени комісії інформують вступників про порядок проведення та оформлення робіт з вступного іспиту зі спеціальності видають вступникам екзаменаційні білети з відповідними варіантами та заздалегідь роздруковані підписані листи для написання робіт. Надалі в ці листи вступники записують письмові відповіді на питання екзаменаційного білету і наприкінці зазначають дату та ставлять особистий підпис.

На організаційну частину іспиту (пояснення по проведенню, оформленню і критеріям оцінювання іспиту, видачі білетів і листів для написання роботи) відводиться 10 хвилин від усього часу іспиту, на відповіді на кожне з чотирьох питань екзаменаційного білету вступнику надається по 30 хвилин і на заключну частину (збір білетів і письмових робіт у вступників членами комісії) – 5 хвилин.

Після закінчення етапу написання іспиту, проводиться перевірка відповідей та їх оцінювання всіма членами комісії. Члени предметної комісії приймають спільне рішення щодо виставлення оцінки на відповідь до кожного з питань екзаменаційного білету. Ці оцінки виставляються на аркуші з відповідями студента.

Підведення підсумку іспиту зі спеціальності здійснюється шляхом занесення балів в екзаменаційну відомість. Ознайомлення студента з результатами іспиту проводиться згідно з правилами прийому до університету.

1.3. Допоміжні матеріали для складання іспиту

Під час складання іспиту заборонено використання допоміжної літератури та інших допоміжних матеріалів та засобів.

1.4. Рейтингова система оцінювання (РСО)

На іспиті студенти виконують письмову контрольну роботу. Кожний екзаменаційний білет містить чотири теоретичні питання. Усі чотири завдання рівнозначні.

В залежності від повноти і правильності відповіді на питання вступник отримує:

23…25	балів за	91…100 %	правильної відповіді
20…22	балів за	81…90 %	правильної відповіді
17…19	балів за	71…80 %	правильної відповіді
14…16	балів за	61…70 %	правильної відповіді
11…13	балів за	51…60 %	правильної відповіді
9…10	балів за	41…50 %	правильної відповіді
7…8	балів за	31…40 %	правильної відповіді
5…6	балів за	21…30 %	правильної відповіді
3…4	балів за	11…20 %	правильної відповіді
1…2	балів за	5…10 %	правильної відповіді
0	балів за	0…5 %	правильної відповіді

Правильною відповіддю в даному контексті вважається повне і адекватне висвітлення питання згідно з Програмою іспиту зі спеціальності.

У відповідях на завдання екзаменаційного білета оцінюють:

- повноту розкриття питання;
- уміння чітко формулювати визначення понять/термінів та пояснювати їх;
- здатність аргументувати відповідь;
- аналітичні міркування, порівняння, формулювання висновків;
- акуратність оформлення письмової роботи.

Загальна оцінка за іспит обчислюється як арифметична сума балів за всі чотири відповіді на запитання екзаменаційного білету. Таким чином, згідно з рейтинговою системою оцінювання, за результатами іспиту вступник може набрати від 0 до 100 балів.

З метою обчислення конкурсного балу вступника результат іспиту зі спеціальності перераховується з шкали від 0 до 100 балів до шкали, визначеної Порядком прийому на навчання для здобуття вищої освіти (100…200 балів) згідно з Таблицею відповідності:

Таблиця відповідності оцінок РСО (60…100 балів)
оцінкам 200-бальної шкали (100…200 балів)

шкала РСО	шкала 100…200	шкала РСО	шкала 100…200	шкала РСО	шкала 100…200	шкала РСО	шкала 100…200
60	100	70	140	80	160	90	180
61	105	71	142	81	162	91	182
62	110	72	144	82	164	92	184
63	115	73	146	83	166	93	186
64	120	74	148	84	168	94	188
65	125	75	150	85	170	95	190
66	128	76	152	86	172	96	192
67	131	77	154	87	174	97	194
68	134	78	156	88	176	98	196
69	137	79	158	89	178	99	198
						100	200

Вступники, результати іспиту яких за шкалою РСО складають від 0 до 59 балів, отримують оцінку "незадовільно" і не допускаються до участі в наступних вступних випробуваннях (за наявності) і в конкурсному відборі.

1.5. Приклад типового завдання іспиту зі спеціальності

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Освітній ступінь	доктор філософії
Спеціальність	F6 Інформаційні системи та технології
Освітня програма	Інформаційні системи та технології
Іспит	Вступний іспит зі спеціальності

ЕКЗАМЕНАЦІЙНИЙ БІЛЕТ № 1

1. Проєктування та розроблення інформаційних систем та технологій

Оптимізуйте неефективний SQL-запит для звіту про електронну комерцію (запит надається). Перепроєктуйте надану схему бази даних (нормалізація, індексація) та обґрунтуйте зміни.

2. Управління ризиками інформаційної безпеки

На порталі пацієнтів лікарні є незахищена кінцева точка API, яка розкриває ідентифікаційну інформацію. Ідентифікуйте потенційні загрози і запропонуйте методи пом'якшення наслідків атаки.

3. Інженерія даних та великі дані

Спроектуйте ETL конвеєр Kafka-to-Snowflake фондової біржі. Конвеєр має обробляти потокові дані у об'ємі 10 тис. подій/с та мати можливість відновлюватися після збою.

4. Методи надання інформаційних сервісів

Велика організація впроваджує сервіс, що має обслуговувати користувачів у різних країнах. Вимоги включають: високу доступність навіть при відмові одного з дата-центрів; можливість зберігати дані в найближчому до користувача регіоні; забезпечення ізоляції доступу до даних між підрозділами (рольова модель); можливість централізованого моніторингу стану компонентів системи.

Опишіть загальні архітектурні принципи побудови такого сервісу. У відповіді розгляньте: як забезпечити розподілене зберігання з можливістю реплікації; як організувати доступ на основі ролей; як реалізувати міжрегіональну відмовостійкість; які метрики або логи важливо збирати для підтримки стабільної роботи системи.

Затверджено на засіданні НМКУ
протокол № ____ від ___ березня 2025 р.

Гарант освітньої програми Вікторія Онищенко

2. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

1. Особи, які без поважних причин не з'явилися на вступні іспити у визначений розкладом час, особи, знання яких було оцінено балами нижче встановленого рівня, до участі в наступних вступних іспитах і в конкурсному відборі не допускаються.

2. Перескладання вступних випробувань не допускається.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

до розділу 1

1. Роберт Мартін. Чиста архітектура. Ранок, 2019. 368 с.
2. Роберт Мартін. Чистий код. Створення і рефакторинг за допомогою Agile. Фабула, 2019. 448 с.
3. Ерік Фрімен (2020). Head First. Патерни проєктування. Легкий для сприйняття довідник. ISBN: 978-6170961594.
4. Bruce Eckel. Thinking in Java. Prentice Hall, 2006. 1150 p. ISBN 978-0131872486
5. Craig Walls. Spring in Action, 6th edition (2022). ISBN 978-1617297571.
6. K. Siva Prasad Reddy, Sai Upadhyayula. Beginning Spring Boot 3, Build Dynamic Cloud-Native Java Applications and Microservices, Second Edition (2023). ISBN: 978-1484287910.
7. Herbert Schildt. Java: The Complete Reference, Twelfth Edition 12th Edition. McGraw Hill, 2022. 1280 p. ISBN 978-1-26-046342-2
8. Hugh Darwen, An Introduction to Relational Database Theory — ISBN 978-87-7681-500-4, 2010. — 231 p.
9. Ron McFadyen, Relational Databases and Microsoft Access, - Winnipeg, Manitoba, Canada R3B 2E9, 2016 – 221 p.
10. Serge Abiteboul, Rick Hull, Victor Vianu, Foundations of Databases, - ISBN-10: 0201537710, - Addison-Wesley Publishing, 2017 – 678 p.
11. Mastering Relational Databases: from Models to Querying., Libby Shoop Macalester College Saint Paul, MN, USA, — 2019 — 385 p.
12. Ролік О.І., Теленик С.Ф., Ясочка М.В. Управління корпоративною ІТ-інфраструктурою. - Київ: Видавництво «Наукова думка» НАН України, 2018. -577с.
13. Еталонні архітектури MSA.- К., Майкрософт Україна; К.: Видавнича група BHV, 2005.- 352с.
14. Бондарчук А. П. Основи інфокомунікаційних технологій: навчальний посібник [Електронний ресурс] / А. П. Бондарчук, Г. С. Срочинська, М. Г. Твердохліб // Київ, ДУТ. – 2015. – 76 с. – Режим доступу до ресурсу: http://www.dut.edu.ua/ua/lib/1/category/1090/view/840.
15. Жаріков Е.В. Інформаційні технології управління ІТ-інфраструктурою хмарного центру оброблення даних. Київ: НТУУ "КПІ імені Ігоря Сікорського, 2020.- 250 с.

до розділу 2

16. ISO/IEC 27004:2016 (E). Information technology — Security techniques — Information security management — Measurement.
17. ДСТУ ISO /IEC 31010:2013 (ISO /IEC 31010:2009, IDT) «Керування ризиком. Методи загального оцінювання ризику».
18. ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT) «Інформаційні технології. МЕТОДИ ЗАХИСТУ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ. Вимоги».

19. Загурський О. Управління ризиками. - К.: Університет Україна, 2016. - 244 с.
20. КорченкоО.Г. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. [Електронний ресурс] / [КорченкоО.Г., Гнатюк С.О., КазмірчукС.В. та ін.]. –К.: Центр навч.-наук. та наук.-пр. видань НАСБ України, 2014. – 190 с. – Режим доступу: http://193.178.34.24/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf
21. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.
22. Корченко О.Г., Казмірчук С.В., Ахметов Б.Б., Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія, Київ, ЦП «Компринт», 2017 – 435 с.

до розділу 3

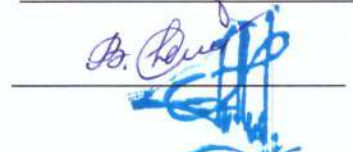
23. Литвин В. В. Методи та засоби інженерії даних та знань: Навч. посіб. – Львів: "Магнолія 2006", 2024. – 241 с.
24. Joe Reis, Matt Housley Fundamentals of Data Engineering, O'Reilly Media, Inc., 2022.
25. Kleppmann, M. Designing Data-intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems. O'Reilly Media, Inc., 2017.
26. Chambers, B. Zaharia, M. Spark: The Definitive Guide : Big Data Processing Made Simple. O'Reilly Media, Inc., 2018.
27. Crickard, P. Data Engineering with Python: Work with massive datasets to design data models and automate data pipelines using Python. Packt Publishing, 2020.
28. Kimball, R. Ross, M. The Data Warehouse Toolkit: The Definitive Guide to Dimensional Modeling. Wiley, 2013.
29. Chan Yupo, John Talburt, Terry M. Talley, eds. Data engineering: mining, information and intelligence. Vol. 132. Springer Science & Business Media, 2009.
30. Len Silverston, The data model resource book, Volume 1: A library of universal data models for all enterprises. John Wiley & Sons, 2011.
31. Hernandez, Michael James. Database design for mere mortals: a hands-on guide to relational database design. Pearson Education, 2013.
32. Genesereth, Michael. Data integration: The relational logic approach. Springer Nature, 2022.

до розділу 4

33. The Twelve-Factor App. Twelve-Factor, Inc. [Електронний ресурс]. – Режим доступу: https://12factor.net
34. Microsoft. Cloud Design Patterns: Prescriptive Architecture Guidance for Cloud Applications. Microsoft Learn, 2023. [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/azure/architecture/patterns/
35. HashiCorp. Terraform Documentation. Terraform by HashiCorp, 2024. [Електронний ресурс]. – Режим доступу: https://developer.hashicorp.com/terraform/docs
36. Google Cloud. Cloud Architecture Center. Google Cloud Platform, 2024. [Електронний ресурс]. – Режим доступу: https://cloud.google.com/architecture
37. Bolivar, A. Awesome Serverless: Curated list of resources. GitHub, 2023. [Електронний ресурс]. – Режим доступу: https://github.com/anaibol/awesome-serverless
38. Cloud Native Computing Foundation. Cloud Native Glossary. CNCF, 2024. [Електронний ресурс]. – Режим доступу: https://glossary.cncf.io
39. Open Guides Contributors. Open Guide to AWS. GitHub, 2023. [Електронний ресурс]. – Режим доступу: https://github.com/open-guides/og-aws

40. Навчально-методичні матеріали до вивчення дисципліни «Дослідження операцій і дискретний аналіз» для студентів усіх спеціальностей з напрямку «Економіка і підприємництво» освітньо-кваліфікаційного рівня бакалаврів усіх форм навчання / Уклад.: О. С. Катуніна, С. С. Савіна, Д. Є. Семьонов. — К.: КНЕУ, 2001. — 60 с.
41. Наконечний С. І., Савіна С. С. Математичне програмування: Навч. посіб. — К.: КНЕУ, 2003. — 452 с. ISBN 966–574–538–7

РОЗРОБНИКИ ПРОГРАМИ:

д.т.н., проф.каф. ІСТ ФІОТ		Богдан КОРНІЄНКО
д.т.н., проф.каф. ІСТ ФІОТ		Вікторія ОНИЩЕНКО
к.т.н., доц., каф.ІСТ ФІОТ		Андрій ПИСАРЕНКО
к.т.н., доц., каф.ІСТ ФІОТ		Максим БУКАСОВ
к.т.н., доц., каф.ІСТ ФІОТ		Ксенія УЛЬЯНИЦЬКА