Міністерство освіти і науки України
Навчально-науковий інститут фінансів, економіки, управління та права
Національного університету
«Полтавська політехніка імені Юрія Кондратюка» (Україна)
Українська асоціація з розвитку менеджменту та бізнес освіти (Україна)
Білостоцький технологічний університет (Польща)
Університет Ґренландії (Ґренландія)
«1 грудня 1918 р» Університет Альба Юлія (Румунія)
Вільнюський університет прикладних наук (Литва)
Сучавський університет імені Штефана Маре (Румунія)
Університет прикладних наук (Австрія)
Харківський національний університет імені В.Н. Каразіна (Україна)
Київський національний університет будівництва та архітектури (Україна)
Національний університет «Запорізька політехніка» (Україна)
Київський національний університет технологій та дизайну (Україна)
Львівській державний університет фізичної культури імені Івана Боберського (Україна)
Черкаський національний університет імені Богдана Хмельницького (Україна)
Сумський державний аграрний університет (Україна)

СУЧАСНІ ІННОВАЦІЙНО-ІНВЕСТИЦІЙНІ МЕХАНІЗМИ РОЗВИТКУ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

06 листопада 2025 року

Co-funded by the European Union

Полтава
2025

використанню електротранспорту та інтеграції енергозберігаючих технологій у складські й дистрибуційні процеси, що зменшує витрати ресурсів і підвищує екологічну стійкість.

Цифрові інструменти також забезпечують постійний моніторинг ключових показників ефективності, автоматизований контроль витрат і своєчасну корекцію процесів, що дозволяє оперативно реагувати на зміни зовнішнього середовища та ринкових умов. Це формує прозорі, прогнозовані та гнучкі логістичні операції, сприяє розвитку стійких конкурентних переваг та стимулює інноваційний розвиток підприємства.

Широке впровадження цифрових технологій сприяє формуванню адаптивних і стійких систем управління, ефективному управлінню транспортними потоками, раціональному розподілу складських ресурсів, автоматизації планування та контролю виконання замовлень, а також швидкому реагуванню на коливання попиту й ринкової кон'юнктури. Це забезпечує інтеграцію економічної, соціальної та екологічної ефективності, що є ключовим чинником довгострокової конкурентоспроможності підприємств у глобальній економіці.

Таким чином, інноваційні цифрові рішення виступають не лише засобом підвищення ефективності логістичних потоків, але й стратегічним механізмом реалізації цілей сталого розвитку. Вони забезпечують комплексне управління матеріальними ресурсами, мінімізують ризики дисбалансу запасів, оптимізують використання транспортних і складських потужностей та формують конкурентні переваги на основі високої адаптивності, оперативності й соціально-екологічної відповідальності підприємств.

Список використаних джерел

1. Крикавський Є. В., Похильченко О. А., Фертч М. Логістика та управління ланцюгами поставок. Львів: Видавництво Львівської політехніки, 2019. 848 с.

2. Петренко О. І. Інформаційні технології в управлінні ланцюгами постачання. Київ: Кондор, 2020. 200 с.

УДК 004.65:004.056

Шапошник Н.С., студент
Науковий керівник: Кудінов О.М., старший викладач
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(м. Полтава, Україна)

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ТА БЕЗПЕКИ БАЗ ДАНИХ

У сучасних умовах цифрової трансформації та глобалізації інформаційні ресурси стають ключовим елементом ефективного управління. Організації, установи та підприємства дедалі більше залежать від швидкого та безпечного доступу до даних. Саме тому питання забезпечення цілісності та безпеки баз даних посідає центральне місце серед інноваційних напрямів розвитку інформаційно-комунікаційних технологій управління.

Цілісність бази даних означає її узгодженість, правильність і достовірність. Вона гарантує, що всі дані зберігаються без суперечностей і відповідають встановленим правилам. Порушення цілісності може призвести до помилкових управлінських рішень, втрати довіри до інформаційної системи або неефективного функціонування організації. Тому при проєктуванні баз даних застосовуються механізми контролю достовірності − унікальні ключі, зв'язки між таблицями, обмеження введення даних та автоматичні перевірки. Нормалізація даних також відіграє важливу роль, оскільки усуває дублювання і забезпечує логічну структурованість інформації [1].

Безпека баз даних − це ще один важливий аспект, який охоплює захист інформації від несанкціонованого доступу, втрати чи спотворення. В епоху глобальних викликів, таких як зростання кількості кібератак, розвиток дистанційних технологій та хмарних сервісів, захист інформації стає ключовим елементом стабільності систем управління. Основними методами

забезпечення безпеки є аутентифікація користувачів, авторизація, контроль доступу, резервне копіювання, ведення журналів транзакцій та шифрування даних. Використання цих методів гарантує не лише збереження інформації, а й підвищує рівень довіри до системи з боку користувачів і керівництва.

У сучасних системах керування базами даних, таких як MySQL, PostgreSQL, Oracle чи Microsoft SQL Server, впроваджено вбудовані механізми цілісності й безпеки, що дозволяють автоматизувати процеси контролю. Однак ефективність цих рішень залежить не лише від технологій, а й від політики управління даними. Організації повинні регулярно оновлювати системи безпеки, впроваджувати багаторівневий контроль доступу та навчати персонал правилам безпечного користування інформаційними системами [2].

Отже, забезпечення цілісності та безпеки баз даних є невід'ємною складовою інноваційних інформаційно-комунікаційних технологій управління. У світі, де інформація стала головним стратегічним ресурсом, саме надійність і захищеність даних визначають ефективність управлінських процесів. Постійне вдосконалення методів безпеки, адаптація до нових загроз і використання сучасних технологій дозволяють організаціям не лише захищати свої дані, а й забезпечувати конкурентоспроможність в умовах глобальних викликів.

Список використаних джерел

1. Ситник Р., Гнатушенко В. Метод забезпечення достовірності та цілісності персональних даних, що обробляються в блокчейн-системі. *Системні технології*. 2025. №3. С. 158.

2. Teimoor R. A. A Review of Database Security Concepts, Risks, and Problems. *UHD Journal of Science and Technology*. 2021. №5. С. 38–46.

УДК 005.21:658

Шумілова А.Ю., студент
Науковий керівник: Кудінов О.М., старший викладач
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(м. Полтава, Україна)

ПРОЄКТУВАННЯ БАЗ ДАНИХ ЯК ОСНОВА КІБЕРСТІЙКОЇ АРХІТЕКТУРИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

У сучасному цифровому середовищі інформаційно-комунікаційні системи стають дедалі більш уразливими до кіберзагроз, що обумовлено як технічною складністю інфраструктур, так і зростанням кількості цілеспрямованих атак. У центрі більшості інформаційно-комунікаційних систем знаходяться бази даних, які забезпечують зберігання, обробку, передачу та аналітику інформації, необхідної для функціонування державних, корпоративних та критичних систем. У цьому контексті саме етап проєктування бази даних визначає потенціал кіберстійкості всієї архітектури інформаційно-комунікаційної системи.

Проєктування баз даних, орієнтоване на кіберстійкість, виходить за межі традиційного підходу, що зосереджений на логічній структурі, нормалізації та продуктивності. Сучасна архітектура має передбачати здатність бази даних витримувати вплив різноманітних загроз, забезпечувати безперервність обслуговування, цілісність та конфіденційність даних у надзвичайних ситуаціях: під час кібератак, фізичних інцидентів або системних збоїв. Тобто, бази даних мають бути спроєктовані з урахуванням вимог до відмовостійкості, захищеності, моніторингу та адаптивності [1].

Одним із ключових напрямів забезпечення кіберстійкості на етапі проєктування є правильна організація доступу до даних. Необхідно реалізовувати принцип найменших привілеїв, що передбачає надання користувачам і процесам лише тих прав, які є необхідними для виконання їхніх функцій. Рольова модель доступу (RBAC) та атрибутна модель (ABAC)