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

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)

є найбільш ефективними в реалізації такого підходу. Ці моделі дозволяють динамічно керувати доступом на основі рівнів довіри, політик безпеки або контексту користувача.

Додатково, на архітектурному рівні мають бути впроваджені технічні засоби для збереження цілісності та достовірності даних [2]. До таких засобів належать:

1) шифрування даних на рівні таблиць, полів або сховища для захисту від перехоплення і компрометації інформації;

2) цифрові підписи та хеш-функції, що дають змогу перевірити автентичність даних при читанні або передаванні;

3) контроль цілісності за допомогою тригерів, обмежень і перевірок, що знижує ризик випадкової або навмисної модифікації важливої інформації.

Проєктування кіберстійкої баз даних повинно включати системи логування та аудиту, які дають змогу контролювати дії користувачів і системних процесів.

Такі журнали мають зберігатися у середовищі, захищеному від несанкціонованого редагування, а також регулярно перевірятися засобами аналітики безпеки. Крім того, доцільно впроваджувати інтеграцію з системами виявлення вторгнень (IDS/IPS), що дозволяє в реальному часі виявляти аномалії в поведінці запитів до бази даних.

Не менш важливою є реалізація архітектурної відмовостійкості, яка забезпечується за допомогою таких рішень: реплікація баз даних для створення копій у реальному часі та перенаправлення запитів у разі збою, регулярне резервне копіювання зі збереженням копій у географічно розподілених середовищах і використання кластерів і контейнеризованих систем управління базами даних, що дозволяє автоматично масштабувати ресурси та перемикатися на резервні вузли без втрати доступу.

У реальному середовищі функціонування інформаційно-комунікаційних систем умови постійно змінюються: зростають навантаження, з’являються нові точки входу в систему, змінюються правила безпеки. Проєктування бази даних має враховувати ці виклики, закладаючи можливість динамічного оновлення конфігурацій, розгортання нових сервісів без зупинки основної системи та впровадження інструментів самовідновлення. Особливо важливо це для хмарних і гібридних систем управління, де ізольованість компонентів і відмовостійкість є важливою умовою функціонування.

Проєктування баз даних як основа кіберстійкої архітектури інформаційно-комунікаційних систем вимагає інтеграції концепцій інформаційної безпеки, гнучкого адміністрування, контролю доступу, аналітики поведінки та забезпечення безперервності обслуговування. Бази даних мають проєктуватися з урахуванням ключових принципів кіберстійкості –захищеності, ізоляції, моніторингу, відмовостійкості та адаптивності. Комплексний підхід, що включає технічні й організаційні заходи, сприяє формуванню архітектури, здатної протистояти сучасним кіберзагрозам і підтримувати стабільну роботу ІКС в умовах високої невизначеності.

Досягнення високого рівня кіберстійкості баз даних потребує впровадження на етапі проєктування таких рішень, як шифрування даних, аудит дій користувачів, автоматичне резервне копіювання, георозподіл та реплікація. Особливе значення має адаптивність системи до зміни загроз і навантажень, що є важливим для хмарних і розподілених середовищ. У перспективі доцільно орієнтуватися на розробку самонавчальних архітектур баз даних із проактивним захистом, здатних автоматично виявляти та локалізувати загрози, забезпечуючи підвищену стійкість до кіберінцидентів.

Список використаних джерел

1. Легомінова С. В., Щавінський Ю. В., Будзинський О. В. Аналіз сучасних підходів до забезпечення кібербезпеки корпоративних баз даних. Сучасний захист інформації, 2024, 2: 50-58.

2. Закон України Про захист інформації в інформаційно-комунікаційних системах URL:https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text