УДК 004.056.5:004.65:334.716-021.412.1(477) DOI: 10.31673/2409-7292.2026.028416

Якименко Юрій Михайлович
кандидат військових наук, доцент, доцент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційних та комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-6848-852X
E-mail: y.yakymenko@duikt.edu.ua

Поляков Дмитрій Андрійович
аспірант кафедри комп'ютерних наук
Державний університет інформаційних та комунікаційних технологій, Київ, Україна
ORCID: 0009-0002-5321-2448
E-mail: mitiagod121@gmail.com

ОПТИМІЗАЦІЯ УПРАВЛІНСЬКИХ ПРОЦЕСІВ ЗАХИСТУ БАЗИ ДАНИХ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У статті розглянуто проблему забезпечення захисту баз даних інформаційних систем об'єктів критичної інфраструктури України в умовах зростання кіберзагроз та інтенсивної цифровізації управлінських процесів. Проведено аналіз сучасних підходів до організації захисту баз даних та визначено основні обмеження традиційних механізмів контролю доступу, що базуються на статичних політиках безпеки. Запропоновано підхід до оптимізації управлінських процесів захисту баз даних, який ґрунтується на використанні адаптивної моделі оцінки ризику доступу до інформаційних ресурсів. Розроблено математичну модель інтегрального показника ризику, що враховує сукупність факторів інформаційної безпеки, зокрема рівень привілеїв користувача, тип SQL-операції, часові характеристики доступу та обсяг оброблюваних даних. На основі запропонованої моделі розроблено прототип системи Adaptive Secure Database Management System, призначеної для автоматизованого моніторингу доступу до баз даних та підтримки прийняття управлінських рішень у сфері інформаційної безпеки. Архітектура системи включає модулі збору подій доступу, аналізу поведінки користувачів, оцінки ризику та формування рекомендацій для адміністратора безпеки. Результати експериментального дослідження показали ефективність запропонованого підходу у виявленні потенційно небезпечних операцій доступу до баз даних та підвищенні рівня захисту інформаційних ресурсів об'єктів критичної інфраструктури. Отримані результати можуть бути використані для підвищення ефективності управління інформаційною безпекою у державних інформаційних системах, енергетичній галузі, телекомунікаційних мережах та інших сферах критичної інфраструктури.

Ключові слова: база даних, об'єкти критичної інфраструктури, моделі, модулі, безпека, ризики.

Вступ

У сучасних умовах цифрової трансформації державних та промислових систем значна частина критично важливої інформації зберігається у базах даних (БД) інформаційних систем об'єктів критичної інфраструктури (ОКІ). До таких об'єктів належать енергетичні системи, транспортні мережі, системи зв'язку, банківська інфраструктура та державні інформаційні реєстри. Надійність функціонування цих систем безпосередньо залежить від рівня захисту інформаційних ресурсів, що зберігаються та обробляються у БД.

На сьогодні в Україні діють різні нормативно-правові акти, які визначають порядок ідентифікації, категоризації та паспортизації об'єктів критичної інфраструктури (ОКІ). Документи встановлюють детальні процедури, які забезпечують системний підхід до управління та захисту критичної інфраструктури. Розробка і введення в практичне використання методологічних підходів для оцінки ризиків і загроз є необхідним і допомагає визначити, які саме аспекти безпеки потребують посилення, вдосконалення чи оптимізації.

Постановка проблеми

Аналіз сучасних кіберінцидентів свідчить, що більша частина атак на ОКІ спрямована на несанкціонований доступ до інформації, що зберігається в БД, є проблемою у вигляді загрози для нанесення значної шкоди інформаційним ресурсам. Для вирішення проблеми необхідно проведення дослідження, яке зводиться до завдань: проаналізувати сучасні заходи до забезпечення безпеки БД, визначити реальність адаптивних методів управління захистом даних, запропонувати модель оцінки ризику доступу до БД, побудувати і реалізувати модель

оптимізації захисту БД на прикладі створеної системи Adaptive Secure Database Management System для моніторингу доступу до даних та автоматизації оцінки ризику виконуваних операцій, провести експериментальну перевірку працездатності запропонованого підходу - на прикладі моделі інформаційної системи енергетичного підприємства з метою підвищення ефективності управління інформаційною безпекою БД. Це буде сприйматися , як зменшення ризику несанкціонованого доступу до критичних даних і підвищення рівня захисту інформаційних ресурсів ОКІ.

Аналіз останніх досліджень і публікацій

На сьогодні проведена і продовжується велика кількість наукових досліджень, присвячених рішенню актуальних проблем захисту баз даних в ОКІ, що є актуальним із забезпеченням нормального функціонування всіх їх систем управління і виконання повсягденних задач діяльності.

Так в роботах авторів [2-10] для ОКІ визначено:

- загрози, які впливають на захищеність в умовах кібервійни і правового режиму воєнного стану;
- шляхи удосконалення вітчизняного законодавства з метою посилення стану забезпечення кібербезпеки;
- міжнародний досвід та стандарти, що демонструють ефективні практики забезпечення кібербезпеки;
- підвищення ролі штучного інтелекту у зниженні ризиків кіберзагроз, у автоматизації реакцій на інциденти, у прогнозуванні та запобіганні кіберзагрозам, у покращенні процедур ідентифікації, аутентифікації та авторизації користувачів;
- результативність заходів щодо забезпечення захисту даних в інформаційних системах;
- застосовність алгоритмів і створення моделей для підвищення рівня безпеки корпоративних БД;
- важливість інтеграції сучасних підходів та технологій у системи кіберзахисту;
- застосування рольової моделі захисту БД в сучасних СУБД.

Однак, не зважаючи на наявність значної кількості наукових праць, варто зазначити, що вони не вичерпують усіх аспектів проблеми забезпечення кіберзахисту (як ОКІ в цілому, так і їх БД) особливо при діяльності в умовах воєнного стану.

Метою статті є проведення дослідження методичних підходів до оптимізації управлінських процесів захисту баз даних на ОКІ України в умовах зростання кіберзагроз та підвищення рівня цифровізації інформаційних систем і використання адаптивних методів управління захистом баз даних.

Результати дослідження

Забезпечення кібербезпеки ОКІ є одним із ключових завдань державної політики будь якої країни, в тому числі і України – особливо в умовах триваючої військової агресії. [2,7]

Першечерговими задачами успішної діяльності організацій становлять забезпечення достатнього рівня їх загальної безпеки у кіберпростірі, а захист баз даних – критично важливим елементом інформаційної безпеки. Загроза кіберінцидентів значно зросла з 2022 року і на сьогодні залишається високою у сфері державного управління, ОКІ та приватного сектору. Для покращення рівня безпеки даних у БД пропонується застосовувати комплексні заходи [5,8], що включають як програмно-технічні засоби безпеки, так і адміністративні методи їх захисту, які враховують особливості конкретної організації.

Важливе призначення в організації займає управління доступом як баланс між безпекою (захист даних) та продуктивністю (швидкий доступ до інструментів управління процесами). Оптимізацію ресурсів адміністрування в управлінських процесах доступу виконує існуюча наявно **с**истема рольового управління доступом (RBAC- для розподілу прав на технічному рівні) або політика доступу на основі списків контролю доступу (ACL). Але вони не завжди

враховують поведінкові особливості користувачів, контекст виконання операцій та динаміку загроз (коли загрози змінюються щохвилини), тому класичного RBAC (стає вже недостатньо. З огляду на це актуальним виникає необхідність в застосуванні адаптивних методів управління захистом БД, які дозволяють аналізувати саме поведінку користувачів та автоматично оцінювати рівень ризику виконуваних ними операцій.

Концепція адаптивного управління захистом баз даних. Адаптивне управління захистом інформаційних систем передбачає використання механізмів, що здатні змінювати параметри системи безпеки залежно від поточного стану інформаційного середовища та характеру виконуваних операцій. Для цього потрібно виконувати основні принципи адаптивного захисту БД, якими є: безперервний моніторинг доступу до даних - здійснення постійного контролю усіх операцій доступу до БД, аналіз поведінки користувачів - визначення типових сценаріїв роботи користувачів та виявлення відхилень від нормальної поведінки, оцінка ризику виконуваних операцій - визначення рівня потенційної загрози для кожного SQL-запиту і автоматичне формування управлінських рішень - пропонування або автоматична реалізація заходів реагування на інциденти інформаційної безпеки. Ролі призначаються не назавжди, а на запит для виконання конкретної операції (наприклад, вивантаження бекапу). Динаміка загроз вимагає також постійного перегляду ролей – при цьому використовуються рішення з аналітики поведінки від UEBA. Щоб покращіти рівень виконання концепці адаптивного управління захистом баз даних треба переходити до такого методичного прийому як оптимізації управлінських процесів.

Оптимізація процесів в Україні має відповідати вимогам Держспецзв'язку та Закону [1]. Адаптивне управління перетворює захист БД ОКІ на активну систему, яка розпізнає загрозу за поведінковими ознаками ще до того, як відбудеться витік даних. При впровадженні адаптивного управління оптимізація процесів відбувається через чотири безперервні етапи виконання: прогнозування, запобігання, виявлення і реагування (табл.1).

Таблиця 1

Оптимізація процесів адаптивного управління

Етапи виконання	**Процеси виконання**
Прогнозування	Аналіз специфічних для України загроз (наприклад, атаки угруповань Sandworm або загрози інсайдерів). Оцінка вразливостей БД до того, як ними скористаються.
Запобігання	Використання динамічного маскування даних та посилення RBAC через контекстні перевірки (звідки і коли підключається адмін).
Виявлення	Моніторинг аномалій у запитах до БД. Якщо бухгалтер зазвичай читає 10 записів, а сьогодні завантажив 10 000 — система повинна реагувати миттєво.
Реагування	Автоматична ізоляція скомпрометованого облікового запису або тимчасове обмеження доступу до таблиць під час активної атаки.

Відповідно до постанови [19] визначено, що кіберзахист критичної інфраструктури переходить на ризик-орієнтовану модель. Це вимагатиме від організацій більш глибокого аналізу власних ризиків та побудови адаптивної системи безпеки.

В ризико-орієнтованому підході його реалізація спрямована на безперервний аудит інформаційної безпеки ОКІ – в заміні щорічних перевірок на автоматизований щоденний контроль відповідності вимогам нормативних і законодавчіх документах. Для оцінки адаптивності системи захисту БД ОКІ визначені ключові показники ефективності (KPI), що вимірюють швидкість, гнучкість та точність реакції захисту від загроз і інцидентів. Система захисту БД ОКІ повинна бути здатною адаптуватися до загроз завдяки цим показникам і в першу чергу – процесам управління доступом (оцінювання динамічності рольової моделі – RBAC/ABAC) і стійкості (вимірювання здатності системи продовжувати роботу під час атаки). Для звітності від ОКІ в наказі [20] рекомендована форма у вигляді інформаційної панелі (Dashboard), як інструмент для прийняття рішень у реальному часі. Вона має бути

структурованою за рівнями: від технічних метрик до бізнес-ризиків. Для побудови такої панелі в Україні зазвичай використовують: SIEM-системи (Wazuh, Splunk, Sentinel) – як фундамент для збору логів, моніторинг активності баз даних DAM (Database Activity Monitoring), для глибокого аналізу запитів до БД (IBM Guardium, Imperva) – та Grafana / Kibana – для візуалізації даних у реальному часі. На сайті Grafana описано сотні прикладів побудови Dashboard для моніторингу безпеки інфраструктури в реальному часі. Відповідно до наказу Держспецзв'язку та СБУ в рекомендаціях [21] для ОКІ враховані сучасні виклики у сфері інформаційної безпеки: оновлені шаблони планів, обов'язкова оцінка ризиків, врахування залежностей між об'єктами інфраструктури та адаптація до нових загроз.

Відповідно до Постанови КМУ України захист БД в ОКІ в Україні базується на ризик-орієнтованому та процесному підходах (PDCA), які включають 6 основних етапів, серед них вказані : Оцінка ризиків та Вибір і оптимізація засобів захисту.

Оцінка ризиків є важливою складовою управління безпекою та стійкістю критичної інфраструктури. Використання такого підходу дозволяє реалізувати цикл безперервного вдосконалення системи кіберзахисту. Систематичний підхід до оцінки ризиків дозволяє не лише виявляти потенційні загрози та вразливі місця в інфраструктурних системах, але і забезпечувати своєчасне реагування на можливі негативні події. Індикатори у вигляді кількісних показників оцінювання будуть слугувати базисом для оцінки і моніторингу діяльності та збереження високого рівня вимог нормативних документів в сфері безпеки, а також допомагають виявляти слабкі місця у вже реалізованих заходах захисту.

Вибір і оптимізація засобів захисту. Ризик-орієнтований підхід, в зв'язку зі зростанням витоків корпоративних даних , спрямований на захист найбільш критичної інформації в напрямах шифрування фінансових транзакцій і обмеження доступу до клієнтських БД. Оптимізація засобів захисту БД — це безперервний процес і полягає в усуненні надлишкових контролів та захистів критичних БД . Найефективніший підхід реалізації ризик-орієнтованого підходу - в його об'єднанні з автоматизованим. Українські дослідження [10] підтверджують необхідність цієї автоматизації, в тому числі і з використанням штучного інтелекту (UEBA-вивчає поведінку користувача і автоматично виконує кроки захисту при виявленні витоку даних з БД) . Методика оптимізації управлінських процесів. Для підвищення ефективності захисту БД пропонується застосування процесної моделі управління, етапи оптимізації якої представлені в табл. 2.

Таблиця 2

Етапи оптимізації управління захистом БД

Етапи оптимізації	Основні заходи
Аналіз ризиків	оцінка загроз та вразливостей
Планування	розробка політик безпеки
Реалізація	впровадження засобів захисту
Моніторинг	контроль подій безпеки
Оптимізація	коригування політик

Математична модель оптимізації захисту баз даних включає нижче наведені етапи.

1. Постановка задачі. Фактори ризику доступу до баз даних. Для оцінки ризику доступу до інформаційних ресурсів БД необхідно враховувати сукупність факторів, що впливають на управління інформаційними процесами. До таких основних факторів ризику слід розглядати наступні:

- рівень привілеїв користувача. Значна увага повинна бути націлена на облік того, що чим вищі права доступу користувача, тим більший потенційний ризик для інформаційної системи у разі компрометації облікового запису [7];
- тип SQL-операції. Різні типи запитів мають різний рівень критичності, наприклад, операції SELECT пов'язані лише з читанням даних, тоді як DELETE або DROP можуть призвести до втрати інформації [5];

© Якименко Ю.М., Поляков Д.А. Оптимізація управлінських процесів захисту бази даних на об'єктах критичної інфраструктури. Сучасний захист інформації, 2(66), 191–200. https://doi.org/10.31673/2409-7292.2026.028416

- час виконання операції. Нетипове використання часу доступу до системи (наприклад, у нічний час), що може свідчити про потенційний інцидент безпеки [14];
- обсяг оброблюваних даних. Масове вилучення або модифікація великих обсягів інформації може бути ознакою несанкціонованих дій;
- поведінкові характеристики користувача (найслабша ланка в системі безпеки). Фокусування на регулярному навчанні користувачів та створенні «культури безпеки», де їх помилка не карається, а стає приводом для покращення системи.

Аналіз історії доступу дозволяє сформувати модель типової поведінки користувача та виявляти аномальні операції. [18]

2. Математична модель оцінки ризику доступу. Для формалізації процесу оцінки ризику доступу до БД пропонується використовувати інтегральний показник ризику, що враховує сукупність факторів безпеки. [1, 14]

Інтегральний показник ризику визначається як:

$$R = \sum nw\_if\_i ,$$

де R – інтегральний показник ризику; f_i – значення і-го фактора ризику; w_i – ваговий коефіцієнт відповідного фактора; n – кількість факторів ризику.

3. Оптимізація управлінських процесів інформаційної безпеки. У традиційних системах ІБ управлінські рішення щодо реагування на інциденти приймаються адміністраторами безпеки на основі аналізу журналів поді безпекий. Такий підхід має ряд недоліків: значний час реагування, залежність від людського фактора, складність аналізу великих обсягів журналів подій. [17]

Використання автоматизованих систем підтримки управлінських рішень дозволяє значно підвищити ефективність управління ІБ. Основними перевагами автоматизованих систем є: скорочення часу виявлення інцидентів, підвищення точності аналізу подій, автоматизація процесів реагування на загрози.

Саме з цією метою пропонується розробка системи Adaptive Secure Database Management System, що реалізує механізми адаптивного управління захистом БД. [11, 12]. Необхідність впровадження такої різновидності інтелектуальних систем управління ІБ, як один з сучасних підходів до захисту БД на ОКІ [15,], дозволить автоматично оцінювати ризики доступу до даних та формувати управлінські рішення щодо протидії кіберзагрозам.З урахуванням зазначених вище перелічених вимог було розроблено прототип системи Adaptive Secure Database Management System, що забезпечує автоматизований моніторинг доступу до БД та оцінку ризику виконуваних операцій, опис архітектури та програмної реалізації наведено нижче.

4. Практична реалізація Adaptive Secure Database Management System (ASDBMS), призначеного для оптимізації управлінських процесів захисту БД на ОКІ. [15]

Можливості запропонованої системи для проведення дослідження:

- моніторинг доступу до БД у режимі реального часу;
- автоматичне визначення аномальних SQL-запитів;
- оцінка ризику доступу до критичних даних;
- формування управлінських рекомендацій для адміністратора безпеки.

Розроблений методичний підхід для використання в ОКІ у таких сферах критичної інфраструктури:

- енергетичні системи;
- телекомунікаційні мережі;
- транспортні інформаційні системи;
- державні реєстри.

5. Архітектура запропонованої системи. Архітектура системи оптимізації управлінських процесів захисту БД на ОКІ складається з п’яти функціональних модулів (табл.3).

Таблиця 3

Система оптимізації управлінських процесів захисту БД на ОКІ

Функціональні модулі	**Призначення модулів**
Модуль збору подій доступу	Здійснює фіксацію всіх SQL-запитів до БД, включаючи: • ідентифікатор користувача; • тип операції; • час доступу; • обсяг оброблюваних даних.
Модуль аналізу поведінки користувачів	Формує профіль типової поведінки користувачів на основі: • історії доступів; • типів виконуваних запитів; • часових патернів роботи.
Модуль оцінки ризику	обчислює інтегральний показник ризику операції доступу до БД .
Модуль управлінської підтримки	Формує рекомендації для адміністратора безпеки: • блокування сесії; • запит додаткової аутентифікації; • обмеження доступу до даних.
Модуль аудиту та журналювання	Забезпечує ведення журналу інцидентів інформаційної безпеки.

Найважливішим для отримання кількісних значень в процесах оптимізації управлінських процесів захисту БД є модель оцінки ризику доступу- у вигляді інтегрального показника ризику, який визначається за формулою:

$$R = w1U + w2T + w3Q + w4D ,$$

де R – інтегральний показник ризику; U – рівень довіри до користувача; T – час доступу; Q – тип SQL-запиту; D – обсяг запитуваних даних; w – вагові коефіцієнти факторів ризику (рівнів в табл. 4).

Таблиця 4

Оцінка факторів ризику

Фактор	Значення	Рівень ризику
Роль користувача	Адміністратор	1
	Оператор	2
	Гість	4
Тип SQL-запиту	SELECT	1
	UPDATE	2
	DELETE	4
	DROP	5
Час доступу	Робочий час	1
	Нічний доступ	3
Обсяг даних	<1000 записів	1
	1000–10000	2
	>10000	3

6. Приклад програмної реалізації. Для перевірки працездатності запропонованої технології було розроблено експериментальний програмний модуль мовою Python.

```
import datetime

class DatabaseSecurityMonitor:

    def calculate_risk(self, role, query, data_volume, time):
```

```
        risk = 0

        role_weight = {
            "admin": 1,
            "operator": 2,
            "guest": 4
        }

        query_weight = {
            "SELECT": 1,
            "UPDATE": 2,
            "DELETE": 4,
            "DROP": 5
        }

        risk += role_weight.get(role, 3)
        risk += query_weight.get(query, 3)

        if data_volume > 10000:
            risk += 3
        elif data_volume > 1000:
            risk += 2
        else:
            risk += 1

        if time.hour < 6 or time.hour > 22:
            risk += 2

        return risk


monitor = DatabaseSecurityMonitor()

risk = monitor.calculate_risk(
    role="operator",
    query="DELETE",
    data_volume=8000,
    time=datetime.datetime.now()
)

print("Risk score:", risk)
```

7. Експериментальні результати. Для перевірки ефективності запропонованої системи було змодельовано роботу БД енергетичного підприємства.

У рамках експерименту було проаналізовано 5000 SQL-запитів, серед яких:

- 4200 – легітимні операції;
- 800 – потенційно небезпечні.

Результати експерименту наведено в табл.5.

Таблиця 5

Результати оцінки факторів ризику

Показник	**Значення**
Кількість проаналізованих запитів	5000
Виявлені аномальні операції	764
Точність виявлення	95.5%
Хибні спрацювання	3.2%
Час аналізу одного запиту	0.012 с

8. Приклад сценарію інциденту. На енергетичному підприємстві було зафіксовано запит:

DELETE FROM power_control_nodes

Оскільки: користувач мав роль оператора, операції виконувались у нічний час і обсяг змін перевищував 5000 записів, то система визначила високий рівень ризику (R = 9) та автоматично виконала: блокування SQL-сесії, створення запису у журналі обліку інцидентів і повідомлення адміністратора безпеки.

Підтверджено, що перевагами запропонованої технології оптимізації захисту баз даних є те, що вони забезпечують:підвищення ефективності управління ІБ, автоматизацію контролю доступу до БД, зниження ризику інсайдерських атак, оптимізацію роботи адміністраторів безпеки.

Наукова новизна роботи полягає у: розробці моделі адаптивного управління доступом до БД, формуванні інтегрального показника ризику доступу і інтеграції алгоритмів поведінкового аналізу у систему захисту БД критичної інфраструктури.

Висновки

У статті досліджено проблематику оптимізації управлінських процесів захисту БД на ОКІ України в умовах зростання кіберзагроз та підвищення рівня цифровізації інформаційних систем. Проведений аналіз сучасних підходів до забезпечення безпеки БД показав, що традиційні механізми контролю доступу, засновані на статичних політиках безпеки, не забезпечують достатнього рівня захисту у складних інформаційних середовищах критичної інфраструктури. У роботі обґрунтовано доцільність використання адаптивних методів управління захистом БД, які передбачають аналіз поведінки користувачів, оцінку ризику виконуваних операцій та автоматизацію процесів прийняття управлінських рішень у сфері ІБ.

У рамках дослідження запропоновано модель оцінки ризику доступу до БД, що базується на інтегральному показнику ризику та враховує ключові фактори ІБ, зокрема рівень привілеїв користувача, тип SQL-операції, час виконання запиту та обсяг оброблюваних даних. Використання даної моделі дозволяє формалізувати процес прийняття управлінських рішень щодо реагування на потенційні інциденти безпеки. На основі запропонованої моделі розроблено прототип системи Adaptive Secure Database Management System, призначеної для моніторингу доступу до БД та автоматизованої оцінки ризику виконуваних операцій. Архітектура системи включає модулі збору подій доступу, аналізу поведінки користувачів, оцінки ризику та підтримки прийняття управлінських рішень. Експериментальна перевірка працездатності запропонованого підходу на моделі інформаційної системи енергетичного підприємства показала високу ефективність системи у виявленні потенційно небезпечних операцій доступу до БД. Отримані результати свідчать про можливість підвищення рівня захисту інформаційних ресурсів ОКІ та зменшення ризику несанкціонованого доступу до критичних даних.

Практична цінність роботи полягає у можливості використання запропонованої технології для підвищення ефективності управління інформаційною безпекою БД у державних інформаційних системах, енергетичній галузі, телекомунікаційній інфраструктурі та інших сферах критичної інфраструктури. Перспективи подальших досліджень пов’язані з

розширенням функціональних можливостей запропонованої системи шляхом використання методів машинного навчання для більш точного виявлення аномальної поведінки користувачів, а також інтеграції розробленого підходу з сучасними системами моніторингу інформаційної безпеки (SIEM) та платформами управління кіберінцидентами.

Перелік посилань

1. Закон України «Про основні засади забезпечення кібербезпеки України». №2163-VIII.

2. Гарасимчук О., Бужович О. Стратегії та інноваційні підходи до захисту баз даних в епоху зростаючих кіберзагроз. Безпека інформації. 2024. DOI: 10.18372/2225-5036.30.18618.

3. Мануїлов Я. С. Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни. Інформація і право. 2023. DOI: https://doi.org/10.37750/2616-6798.2023.1(44).287780.

4. Ільєнко, А., Телющенко, В., Дубчак , О. (2025). Сучасні кіберзагрози критичної інфраструктури україни та світу. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(27), 150–164. https://doi.org/10.28925/2663-4023.2023.27.719.

5. Будзинський О.В. (2025). Метод виявлення вразливостей та автоматизованого реагування в системах захисту корпоративних баз даних.Сучасний захист інформації, 2(62), 180–186. DOI: 10.31673/2409-7292.2025.029259, https://doi.org/10.31673/2409-7292.2025.029259180.

6. Щавінський, Ю., & Будзинський, О. (2025). Аналіз актуальних проблем безпеки корпоративних баз даних в умовах сучасної інфраструктури та шляхи їх вирішення. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(27), 390–405. https://doi.org/10.28925/2663-4023.2025.27.726.

7. Казьмірук С.Д, Леонов Б.Д. Забезпечення кібербезпеки об'єктів критичної інфраструктури на основі використання штучного інтелекту в умовах воєнного стану. Юридичний науковий електронний журнал. № 6/2024.- с. 201-206. DOI https://doi.org/10.32782/2524-0374/2024-6/49.

8. Антоненко Н. В., Граболюк М. С., Семенченко Н. О.(2021). Проблеми захисту інформації в сучасних базах даних. Науковий вісник Полтавського університету економіки і торгівлі. Серія «Економічні науки». 2021. Випуск № 2–1 (103), с.106–110. https://doi.org/10.37734/2409-6873-2021-2-18.

9. Гайдур Г. І., Гахов С. О., Скибун О. Ж. Оцінка стану кібербезпеки критичної інфраструктури з використанням штучного інтелекту. Сучасний захист інформації. 2025. DOI: https://doi.org/10.31673/2409-7292.2025.020831.

10. Легомінова, С. В., Щавінський, Ю. В., & Будзинський, О. В. (2024). Аналіз сучасних підходів до забезпечення кібербезпеки корпоративних баз даних. Сучасний захист інформації, 2(58), 50–58. https://doi.org/10.31673/2409-7292.2024.020006.

11. Bertino E., Sandhu R. Database security – concepts, approaches and challenges. IEEE Transactions on Dependable and Secure Computing. 2005. Vol. 2, No. 1. P. 2–19. URL: https://doi.org/10.1109/TDSC.2005.9.

12. Hu V., Ferraiolo D., Kuhn D. Assessment of access control systems. NIST Special Publication 800-192. 2018. URL: https://doi.org/10.6028/NIST.SP.800-192.

13. Sandhu R., Coyne E., Feinstein H., Youman C. Role-based access control models. IEEE Computer. 1996. Vol. 29. No. 2. P. 38–47. URL: https://doi.org/10.1109/2.485845.

14. Peltier T. Information Security Risk Analysis. Auerbach Publications, 2016.

15. ENISA. Securing critical infrastructures in the digital age. European Union Agency for Cybersecurity. 2022. URL: https://www.enisa.europa.eu.

16. NIST Cybersecurity Framework Version 2.0. National Institute of Standards and Technology. 2024. URL: https://www.nist.gov/cyberframework.

17. Scarfone K., Mell P. Guide to intrusion detection and prevention systems (IDPS). NIST Special Publication 800-94. 2007. URL: https://doi.org/10.6028/NIST.SP.800-94.

18. Garcia-Teodoro P., Diaz-Verdejo J., Macia-Fernandez G., Vazquez E. Anomaly-based network intrusion detection: techniques, systems and challenges. Computers & Security. 2009. Vol. 28. P. 18–28. URL: https://doi.org/10.1016/j.cose.2008.08.003.

19. Постанова КМУ України від 13 листопада 2025 р. № 1470 затверджено зміни постанови № 518 "Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури (ОКІ).

20. Наказ Адміністрації Держспецзв'язку від 30.08.2023 №773 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту систем електронного документообігу».

21. Держспецзв'язку та СБУ № 627/772 від 19 грудня 2024 року Нові рекомендації та форму плану захисту від кіберзагроз для ОКІ.

Yurii Yakymenko
Candidate of Military Sciences, Associate Professor, Associate Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-6848-852X
E-mail: y.yakymenko@duikt.edu.ua

Dmytryi Polyakov
Postgraduate student, Department of Computer Science
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0002-5321-2448
E-mail: mitiagod121@gmail.com

OPTIMIZATION OF DATABASE PROTECTION MANAGEMENT PROCESSES AT CRITICAL INFRASTRUCTURE FACILITIES

This paper addresses the problem of securing databases within information systems of critical infrastructure facilities in Ukraine under conditions of increasing cyber threats and ongoing digital transformation of management processes. An analysis of existing approaches to database protection is conducted, revealing the limitations of traditional access control mechanisms based on static security policies. An approach to optimizing management processes for database security is proposed, based on an adaptive risk assessment model for data access operations. A mathematical model of an integrated risk indicator is developed, taking into account key security factors such as user privilege level, SQL query type, access time, and volume of processed data. Based on the proposed model, a prototype system named Adaptive Secure Database Management System (ASDBMS) is developed. The system is designed to provide automated monitoring of database access and support decision-making processes in the field of information security. The architecture of the system includes modules for access event collection, user behavior analysis, risk assessment, and decision support. Experimental evaluation of the proposed approach demonstrates its effectiveness in detecting potentially malicious database operations and improving the overall level of protection of critical information resources. The results of the study can be applied to enhance information security management in government information systems, energy sector infrastructures, telecommunications networks, and other critical infrastructure domains.

Keywords: database, critical infrastructure objects, models, modules, security, risks.

Надійшла до редакції (Received): 13.05.2026
Прийнята до друку (Accepted): 12.06.2026
Опубліковано онлайн (Available online): 25.06.2026

УДК 004.056.53:004.58 DOI: 10.31673/2409-7292.2026.024917

Яковлев Максиміліан Миколайович
здобувач ступеня доктора філософії
Сумський державний університет, Суми, Україна
ORCID: 0000-0002-1196-4062
E-mail: maksimilianyakovlev@gmail.com

Довбиш Анатолій Степанович
доктор технічних наук, професор, лауреат Державної премії України в галузі освіти
Сумський державний університет, Суми, Україна
ORCID: 0000-0003-1829-3318
E-mail: a.dovbysh@cs.sumdu.edu.ua

КОМПЛЕКСНА КІБЕРЛАБОРАТОРІЯ ДЛЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ТА АНАЛІЗУ ЛОГІВ БЕЗПЕКИ

У статті розглянуто концепцію та практичну реалізацію комплексної кіберлабораторії для тестування на проникнення (penetration testing) та аналізу логів безпеки. Актуальність дослідження зумовлена зростанням кількості кіберінцидентів у світі, дефіцитом кваліфікованих фахівців і потребою в інтегрованих навчально-дослідницьких середовищах, які дозволяють безпечно моделювати сучасні кібератаки. У роботі проведено аналіз сучасних підходів до побудови тренувальних середовищ кібербезпеки, зокрема на основі віртуалізації, контейнеризації (Docker) та стеків обробки логів (ELK, Zeek). Запропонована архітектура лабораторії реалізована за принципом мікросервісної моделі, що забезпечує масштабованість, гнучкість та ізоляцію компонентів. Система складається з окремих шарів: frontend (React + TypeScript), backend (Node.js + Express), шару симуляції атак (Kali Linux, Metasploit, Hydra), цільового середовища (DVWA, MySQL, Vulnerable APIs) та шару

© Якименко Ю.М., Поляков Д.А. Оптимізація управлінських процесів захисту бази даних на об'єктах критичної інфраструктури. Сучасний захист інформації, 2(66), 191–200.
https://doi.org/10.31673/2409-7292.2026.028416