УДК 004.056.53:004.652.1 DOI https://doi.org/10.35546/kntu2078-4481.2025.3.2.22

Є. А. ДРОЗДОВА
старший викладач кафедри комп'ютерних систем та мереж
Херсонський національний технічний університет
ORCID: 0000-0003-0276-6387

В. М. КОЗЕЛ
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних систем та мереж
Херсонський національний технічний університет
ORCID: 0000-0002-2627-2499

СУЧАСНІ МЕТОДИ ЗАХИСТУ БАЗ ДАНИХ В УМОВАХ КІБЕРЗАГРОЗ ТА ВІЙНИ

У дослідженні розглядаються актуальні виклики для інформаційної інфраструктури України в умовах зростання кіберзагроз і воєнних дій. Показано, що бази даних державних установ, об'єктів критичної інфраструктури, освітніх та медичних закладів, а також малого й середнього бізнесу є одними з найбільш уразливих цілей для кібератак. Встановлено, що кількість кіберінцидентів в Україні постійно зростає, що підтверджують дані CERT-UA за 2022–2025 роки. Виявлено тенденції до поширення атак із застосуванням шкідливого програмного забезпечення класу wiper, фішингових кампаній, атак на ланцюги постачання та спроб несанкціонованого доступу до SCADA-систем.

Метою роботи є систематизація сучасних методів захисту баз даних і створення практичного алгоритму, який може бути використаний малими та середніми підприємствами без значних витрат ресурсів. Запропонований алгоритм передбачає аудит інформаційних активів, впровадження багатофакторної автентифікації, організацію резервного копіювання, використання сучасних методів шифрування, навчання персоналу, моніторинг подій безпеки та формування комплексної політики захисту даних. Для практичного використання наведено приклад політики інформаційної безпеки та розроблено чекліст аудиту кіберзахисту.

Результати дослідження демонструють, що навіть за обмежених фінансових і кадрових можливостей можливо досягти достатнього рівня кіберстійкості. Ефективність забезпечується завдяки структурованому підходу, що включає як технічні рішення (SIEM, TDE, AES, системи виявлення вторгнень), так і організаційні заходи (навчання персоналу, контроль доступу, аудит). Проведений порівняльний аналіз українських та зарубіжних досліджень виявив, що у вітчизняних умовах акцент робиться на прикладних рішеннях і адаптації до воєнних викликів, тоді як зарубіжні праці зосереджені на стандартизації та регуляторних аспектах.

Практична значимість полягає у можливості використання запропонованих рекомендацій у МСП, державних установах та приватних компаніях, що працюють з конфіденційними даними, але не мають розгалужених відділів кібербезпеки. Захист баз даних розглядається не лише як технічне завдання, а як ключова складова економічної та національної безпеки.

Ключові слова: *кібербезпека, база даних, МСП, фішинг, резервне копіювання, SIEM, APT, політика безпеки, ISO/IEC 27001, кіберзагрози.*

YE. A. DROZDOVA
Senior Lecturer at the Department of Computer Systems and Networks
Kherson National Technical University
ORCID: 0000-0003-0276-6387

V. M. KOZEL
Candidate of Engineering Sciences (PhD), Associate Professor,
Associate Professor at the Department of Computer Systems and Networks
Kherson National Technical University
ORCID: 0000-0002-2627-2499

MODERN METHODS OF DATABASE PROTECTION UNDER CYBER THREATS AND WARTIME CONDITIONS

The study addresses the urgent challenges facing Ukraine's information infrastructure under escalating cyber threats and wartime conditions. It highlights that databases of government agencies, critical infrastructure, education and healthcare institutions, as well as small and medium-sized enterprises, have become the primary targets of cyberattacks.

CERT-UA data from 2022–2025 confirm a steady increase in incidents, reflecting the growing militarization of cyberspace. The main threats identified include wiper malware, phishing campaigns, supply-chain attacks, and unauthorized intrusions into SCADA systems.

The research aims to systematize modern approaches to database protection and to design a practical algorithm suitable for SMEs with limited resources. The proposed framework consists of asset auditing, multi-factor authentication, backup implementation, modern encryption methods, staff awareness training, security event monitoring, and comprehensive security policy development. A sample security policy and an audit checklist are provided to facilitate practical application.

The findings demonstrate that even resource-constrained organizations can achieve sufficient levels of cyber resilience if they apply structured and sequential measures. Effectiveness is ensured through the integration of technical tools such as SIEM platforms, TDE, AES, intrusion detection systems, along with organizational practices including personnel training, access control, and audits. A comparative review of Ukrainian and international studies shows that local works emphasize applied solutions and adaptation to wartime conditions, while international research prioritizes regulatory compliance and standardization.

The practical value of the study lies in the usability of the proposed recommendations by SMEs, public institutions, and private companies handling sensitive information without dedicated cybersecurity departments. Database protection is thus positioned not only as a technical challenge but also as a fundamental component of national and economic security.

Key words: *cybersecurity, database, SMEs, phishing, backup, SIEM, APT, security policy, ISO/IEC 27001, cyber threats.*

Постановка проблеми

В умовах повномасштабної війни в Україні питання інформаційної безпеки набуло критичного значення. Бази даних органів державної влади, освітніх закладів, медичних установ, підприємств критичної інфраструктури стали об'єктами кібератак з боку держави-агресора. У таких умовах особливої ваги набуває впровадження надійних, гнучких і відповідних до національного законодавства засобів захисту баз даних (БД).

Основними загрозами для баз даних є наступні:

– Масові кібератаки: DDoS, програми-здирники (ransomware), шкідливе ПЗ;

– Цілеспрямовані вторгнення: розвинена стала загроза (APT-групи, зокрема Sandworm – підрозділ кібервійни ГУ ГШ ЗС РФ, Gamaredon – кіберзлочинці, яких відносять до російського 18 центру інформаційної безпеки ФСБ, який діє в окупованому Криму);

– Інсайдерські витоки;

– Відсутність належного резервного копіювання;

– Атаки на фізичні дата-центри та електропостачання.

До основних груп засобів захисту баз даних належать:

– Шифрування (зокрема прозоре шифрування даних TDE, шифрування на рівні стовпців column-level encryption);

– Контроль доступу (модель управління доступом, заснована на ролях RBAC, метод автентифікації, який вимагає декількох способів підтвердження особистості MFA);

– Моніторинг (логування, SIEM – технологія, яка забезпечує централізований збір, аналіз та кореляцію даних про події безпеки з різних джерел в IT-інфраструктурі організації);

– Резервне копіювання;

– Захист на рівні прикладного програмного забезпечення.

Захист баз даних в Україні регулюється такими основними документами:

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (від 05.07.1994 № 80/94-ВР);

– Закон України «Про інформацію» (від 02.10.92 N 2657-XII), «Про захист персональних даних» (№ 2297-VI);

– Стандарти ДСТУ ISO/IEC 27001:2015, 27002:2015;

– Загальні рекомендації НКЦК (Національний координаційний центр кібербезпеки) та CERT-UA (Команда реагування на комп'ютерні надзвичайні події України) щодо захисту критичної IT-інфраструктури.

Аналіз останніх досліджень і публікацій

Вивчення джерел в українському інформаційному просторі засвідчує наявність комплексного підходу до проблем захисту баз даних, особливо в контексті адаптації до сучасних кіберзагроз. У низці праць акцент зроблено як на базових засобах захисту, так і на спеціалізованих інструментах з урахуванням технологічного середовища.

У роботі [1] проаналізовано основні проблеми захисту інформації в базах даних в умовах зростання ризиків кіберзлочинності. Автори класифікують загрози та описують механізми їх попередження на рівні архітектури БД. Окремо наголошено на необхідності відповідності міжнародним стандартам безпеки.

Дослідження [2] присвячено шифруванню даних у хмарних базах. Особливу увагу зосереджено на алгоритмах захисту під час зберігання й передавання, а також проблематиці автентифікації в умовах відкритого доступу до хмарних сервісів. Перевагою є практична складова – моделювання безпечної взаємодії клієнт-сервер.

Автори публікації [3] акцентують на безпеці СУБД PostgreSQL. Розглядається застосування вбудованих інструментів PostgreSQL, таких як контроль доступу, шифрування та політики SELinux. Висвітлено конкретні кейси впровадження у реальних проєктах.

У статті [4] наведено узагальнену класифікацію методів захисту в сучасних системах управління базами даних. Зроблено порівняння засобів на рівні архітектури, прикладного рівня та системної інфраструктури. Окремо підкреслено роль підсистеми моніторингу та логування.

Дослідження [5] присвячене аналізу програмного продукту DbProtect. Авторами надано оцінку ефективності цього інструменту виявлення вразливостей у корпоративному середовищі, зокрема в контексті попередження SQL-ін'єкцій, витоку даних та реалізації політик аудиту.

У роботі [6] здійснено систематизацію загроз для корпоративних баз даних з урахуванням нових тенденцій цифрової інфраструктури. Автори виокремлюють актуальні виклики, пов'язані з інтеграцією хмарних сервісів, а також пропонують концепцію багаторівневого підходу до безпеки.

У публікації [7] зроблено акцент на превентивних заходах щодо типових загроз для локальних БД. Розглядаються як класичні технічні рішення (антивірусні системи, фаєрволи), так і організаційні заходи, зокрема навчання персоналу.

Загалом, українські публікації підтверджують актуальність тематики безпеки баз даних в умовах цифровізації та гібридної загрози. Хоча в більшості праць акцент робиться на традиційних підходах, відчутною є тенденція до інтеграції рішень типу SIEM, застосування криптографічного захисту та орієнтація на відповідність міжнародним нормам (ISO/IEC 27001, NIST SP 80053).

Аналіз зарубіжних наукових праць свідчить про високий рівень формалізації, стандартизації та практичної спрямованості у тематиці захисту баз даних. Частина публікацій фокусується на криптографічному захисті, деякі на системах виявлення загроз у великих інфраструктурах або захисті даних у хмарних системах.

У роботі Fuller et al. [8] представлено глибоке порівняння криптографічних механізмів захищеного пошуку по БД. Автори класифікують методи за рівнем безпеки, продуктивності та сферами застосування. Робота цінна з точки зору балансу між захистом і зручністю для користувача.

Kamran & Farooq [9] присвятили дослідження захисту БД за допомогою водяних знаків, що особливо актуально у випадках розповсюдження комерційних наборів даних або підтвердження авторства. Автори систематизують підходи за типами структурованості даних.

Bauskar [10] розглядає проблеми безпеки хмарних баз даних. В роботі виокремлено фактори ризику, притаманні публічним і приватним хмарам, та детально проаналізовано застосування таких засобів, як шифрування на стороні клієнта, багатофакторна автентифікація, VPN-тунелювання.

У статті Ankur Mahida [11] надано критичний огляд юридичних та етичних аспектів захисту даних у хмарних БД. Робота інтегрує технічний і правовий підходи до забезпечення приватності в інформаційних системах.

Загалом, в українських та зарубіжних джерелах, які вивчають захист баз даних, виявлені деякі відмінності в підходах, що продемонстровано в таблиці 1.

Таблиця 1

Порівняння підходів до захисту БД в українських та зарубіжних джерелах

Критерій	Українські джерела	Англомовні джерела
Основна увага	Базовий захист, аудит, впровадження локальних засобів	Криптографія, хмарні технології, машинне навчання
Прикладна база	Практичні кейси (PostgreSQL, DbProtect)	Переважно теоретично-прикладні моделі, стандарти NIST
Рівень формалізації	Обмежене застосування формальних моделей	Висока формалізація, структурні моделі безпеки
Методи шифрування	TDE, AES-256, VPN	Order-preserving encryption, searchable encryption
Регуляторна база	ДСТУ, КСЗІ, законодавство України	ISO/IEC 27001, GDPR, HIPAA, NIST
Інструменти моніторингу	Логування, SIEM (зазначено частково)	Повноцінні системи SIEM, IDS/IPS
Інноваційність	Обмежене згадування ШІ або адаптивних систем	Активне використання AI, privacy-preserving ML
Ризики в хмарі	Часткове згадування	Повна класифікація загроз та рішень
Фокус на інсайдерів	Так, у контексті RBAC/DLP	Так, у контексті поведінкової аналітики (UEBA)
Юридичний супровід	Посилання на закони України	Юридичний аналіз (GDPR, ePrivacy)

Українські публікації надають цінну інформацію щодо практичного впровадження захисту у реальних умовах воєнного часу та обмежених ресурсів, у той час як міжнародні дослідження пропонують глибше теоретичне обґрунтування, детальну стандартизацію та увагу до перспективних технологій (AI, гомоморфне шифрування). Оптимальною стратегією для національного рівня є поєднання локального досвіду з міжнародними підходами.

Формулювання мети дослідження

Аналіз актуальних статистичних даних показав вплив війни РФ проти України на рівень загроз для баз даних в Україні в порівнянні з довоєнним періодом.

Так, зросло загальне число кібератак. У 2022 році – перший рік повномасштабної війни – CERT-UA зареєструвала понад 2 194 інциденти, що значно перевищило рівень 2021 р. (1350 зафіксованих атак) [12].

У 2023 р. кількість інцидентів зросла на 16 %, до 2 543 випадків, проти 2 194 у 2022 р. [13].

У 2024 р. зафіксовано 4 315 інцидентів, що на 70 % більше, ніж у попередньому році, причому а другій половині року команда CERTUA опрацювала 2 576 інцидентів – це на 48 % більше, ніж у першому півріччі. Проте кількість випадків високої чи критичної важкості зменшилась на 77 % (з 48 до 11) [14].

За перші 77 днів 2025 року CERTUA зафіксувала 1 384 кібератаки, що на 50 % більше, ніж у ту саму пору 2024 року [15]. Якщо темп збережеться, кількість атак може сягнути 10 000 інцидентів у 2025 році.

Отже, зростання виявлених інцидентів складає від 50 % до 70 % щорічно (рис. 1), демонструючи стабільне домінування кіберзагрози під час війни.

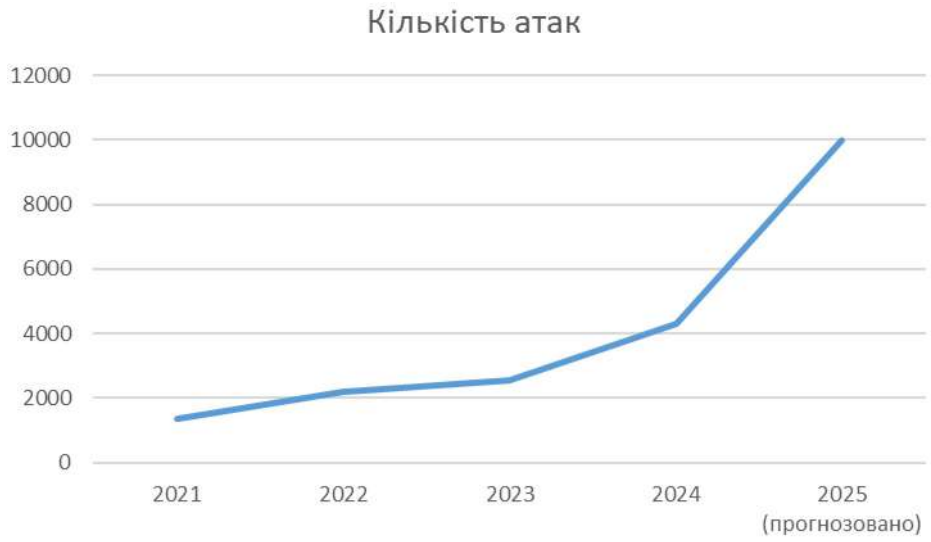

Рис. 1. Зростання кількості кіберінцидентів в роки війни

Аналіз також показує зміну характеру атак. Якщо в довоєнний період спостерігалися переважно локальні DDoS атаки, а також традиційний фішинг, то в 2022 р. окрім DDoS на держструктури та військовий сектор (зростання в перші дні на 196 %), поширилось масштабне розповсюдження шкідливого програмного забезпечення, а також wiper (Malware з функціями знищення даних). У 2022 р. вперше зареєстровано 16 різних сімейств атомарних wiper-вірусів – найвищий рівень в історії. Wiper-атаки – це тип кібернападу, що спрямований на пошкодження або знищення даних на комп'ютерах, серверах чи інших пристроях. Вони призначені не для витоку інформації, а для її деструкції, що може призвести до значних втрат для постраждалих.

Помітним стало зростання загальної кількості атак, що вказує на масштабну кібероперацію проти національної кібербезпеки України. Ціль атак змістилася в бік критичної інфраструктури, що робить питання захисту баз даних і IT-систем стратегічним. Спостерігається підвищення складності атак, паралельно з пониженням кількості надзвичайно критичних випадків, що, можливо, вказує на кращу стійкість або адаптивність систем захисту.

Стійке інтелектуальне шпигунство відображає зростання тригерів APT-груп (наприклад, Gamaredon/Trident Ursa) у 2024–25 роках.

Кібернапади супроводжують фізичні атаки (cyber-kinetic warfare). Cyber-kinetic warfare – це новий тип війни XXI століття, в якому знищення інформаційної інфраструктури (БД, телеком, SCADA) служить підготовкою або підтримкою реального фізичного нападу. Яскравим прикладом може бути атака на Київстар в грудні 2023 р, коли спочатку відбулась масштабна кібератака, яка спричинила знищення серверів та інфраструктури, а далі – ракетні удари по об'єктах зв'язку. Результатом була повна втрата зв'язку в частині країни. Аналогічній атаці піддавався енергетичний сектор в 2022–2023рр. Попередньо кібероперації на SCADA-системи електромереж спричиняли відключення, потім наносилися удари по підстанціях або мережах – подвійний удар. Це лягло в основу тенденції подальших кібератівностей. Захист баз даних у таких умовах – не просто кібербезпека, а елемент національної оборони.

Викладення основного матеріалу дослідження

Ми проаналізували кібератаки під час війни в розрізі типів об'єктів, на які вони були спрямовані. Так, за даними CERTUA (національна команда реагування) в 2023 р. статистика нападів була наступною (табл. 2) [16, 17].

Проаналізовано також, атакам якого виду піддавалися ті або інші об'єкти (таблиця 3).

Типи атак різняться залежно від об'єкта, але фішинг і шкідливе ПЗ – універсальні загрози. Найбільше під загрозою знаходяться держструктури та критична інфраструктура, які разом складають понад 50–60 % атак.

Таблиця 2

Розподіл кількості кіберінцидентів за типом об'єктів (на 2023 р.)

Категорія	Кількість інцидентів у 2023	% від загальної кількості (2 543)
Урядові структури	347	~13.6 %
Місцева влада	276	~10.8 %
Сектор безпеки/оборони	175	~6.9 %
Комерційні організації	127	~5.0 %
Енергетика	92	~3.6 %
Телеком	81	~3.2 %
Освітні заклади	38	~1.5 %
Транспорт	32	~1.3 %
Фінансовий сектор	30	~1.2 %
IT-сектор	25	~1.0 %
ЗМІ	15	~0.6 %
Медичний сектор	12	~0.5 %

Таблиця 3

Види атак по категоріям об'єктів

Категорія об'єкта	Основні атаки	Коментар
Державні установи	DDoS, фішинг, компрометація облікових даних, знищення реєстрів	Атаки мають на меті дестабілізацію систем
Критична інфраструктура	Wiper-ПЗ, APT, supply-chain, SCADA атаки	Спрямовані на паралізування інфраструктури
Великі підприємства	Фішинг, compromise через постачальників	Вразливі через ланцюги постачання
Освіта	Ransomware, внутрішні загрози (здобувачі)	Значні ризики від внутрішніх користувачів
Малі та середні підприємства	Фішинг, крадіжка пристроїв, вкрадені облікові дані	Викликані недостатнім рівнем захищеності

Заклади освіти стикаються з унікальними ризиками внутрішніх загроз (наприклад, джерелом інцидентів можуть бути здобувачі освіти). Малий бізнес переживає численні атаки фішингу та соціальної інженерії, але зазвичай не мають ресурсів для захисту.

Малий та середній бізнес (МСП) є однією з найбільш вразливих цілей кібератак в Україні, особливо під час війни. Попри те, що державні установи, об'єкти критичної інфраструктури (КІ), а також великий бізнес набагато частіше піддаються ворожим атакам, вони мають вищий рівень кіберзахисту, ніж МСП, з кількох системних причин.

Ці структури не можуть функціонувати без відповідності регламентам, тому зобов'язані впроваджувати захист на системному рівні. Їхня діяльність в сфері кіберзахисту повинна задовольняти вимогам, які викладені в обов'язкових документах (КСЗІ – Комплексна система захисту інформації, затверджена Держспецзв'язку, Закон України «Про основні засади забезпечення кібербезпеки», Стратегія кібербезпеки, ISO/IEC 27001 та інш.). Великі компанії мають відокремлені бюджети на кібербезпеку, IT-відділи, підрядників з ISMS – системи управління інформаційною безпекою, консалтингові компанії. Державні об'єкти фінансуються з бюджету, в т.ч. у рамках проєктів, що підтримують кіберзахист сектору безпеки. У КІ передбачено фінансування на відновлення та стійкість (resilience) – один із KPI згідно з ISO/IEC 27031. У структурі держорганів і КІ створено підрозділи інформаційної безпеки, які відповідають за побудову політик безпеки, аудит доступу, логування, відповідність регламентам, взаємодію з CERT-UA. У великому бізнесі діє: SOC (Security Operation Center) – постійний моніторинг подій, а також SIEM-системи, інструменти аналізу інцидентів.

Державні установи, підприємства КІ та великий бізнес підлягають регулярному аудиту в сфері кіберзахисту. В разі порушення вимог регламенту настають наслідки у вигляді адміністративної або дисциплінарної відповідальності, а також втрати ліцензій, штрафи, санкції регуляторів та інш. МСП таких перевірок не проходять, а отже, не мають системної мотивації будувати ефективну безпеку.

Отже, МСП є слабкою ланкою в кіберпросторі. Більшість МСП не мають IT-відділу або користуються послугами зовнішніх підрядників без чітких вимог до безпеки. Інвестиції в кіберзахист часто відкладаються, особливо у кризових умовах. Працівники не проходять навчання з кібергігієни, відкривають фішингові листи, використовують слабкі паролі. Використання безкоштовного або застарілого ПЗ має наслідком відсутність оновлень, легких засобів шифрування та моніторингу. Залежність від хмарних або сторонніх рішень спричиняє недостатній контроль над даними, використання слабко захищених API.

За оцінкою фахівців, середня сума втрат для малого бізнесу після інциденту становить від 5 000 до 50 000 доларів (включаючи відновлення, простої, втрату клієнтів), а 82 % постраждалих МСП не відновлюються повністю протягом 6 місяців після інциденту [18]. Типовими втратами внаслідок кібератак є:

– втрати конфіденційної клієнтської інформації (CRM, рахунки);
– вимушене припинення операцій через зламаний сайт чи систему автоматизації бізнес-процесів ERP;
– репутаційні ризики, наслідком яких є відтік клієнтів;
– санкції, якщо підприємство мало справу з персональними даними і не виконало Закон «Про захист персональних даних»).

Зважаючи на унікальний профіль загроз, ресурсні можливості та нормативні обмеження, можна рекомендувати для МСП засоби, які забезпечують баланс між безпекою та простотою впровадження. Метою є забезпечити мінімально достатній рівень кіберзахисту, який дозволить захистити дані клієнтів, партнерів і фінансів, уникнути простоїв бізнесу через атаки, а також виконати вимоги Закону України «Про захист персональних даних».

Пропонується наступний алгоритм впровадження кіберзахисту для МСП.

Крок 1. Призначення відповідального

Власник або менеджер повинен офіційно призначити відповідальну особу за інформаційну безпеку (навіть якщо це одна особа для IT і безпеки).

Створити реєстр відповідальностей (наприклад, у Google Docs або Excel).

Крок 2. Облік цифрових активів

Створити перелік:
– Облікових записів (пошта, CRM, банки);
– Пристроїв (ноутбуки, смартфони, касові апарати);
– Програмного забезпечення;
– Баз даних (які зберігаються локально або в хмарі).

Позначити:
– Хто має доступ;
– Які паролі використано;
– Чи є шифрування.

Крок 3. Налаштування базового захисту доступу

Запровадити двофакторну автентифікацію (2FA) в email, CRM, банкінг.

Змінити всі паролі на унікальні, згенеровані менеджером паролів.

Розподілити доступи за ролями (тільки до необхідної інформації).

Створити резервні облікові записи адміністратора.

Крок 4. Налаштування резервного копіювання

Забезпечити автоматичне щоденне інкрементне резервне копіювання.

Копії зберігати:
– локально (зовнішній SSD);
– у хмарі (Google Drive, Dropbox).

Тестовий відкат з резервної копії повинен відбуватися раз на 3 місяці.

Крок 5. Впровадження захисту даних

Активувати шифрування на рівні СУБД (AES/SSL).

Обмежити зовнішні підключення до БД (через VPN або IP-фільтрацію).

Увімкнути автоматичне оновлення ОС і ПЗ.

Крок 6. Навчання персоналу

Провести коротке навчання з кібергігієни (1 година, Zoom або PDF-презентація):
– як розпізнати фішинг;
– що робити при підозрі на атаку;
– як правильно створювати паролі.

Оформити інструкцію з безпечної роботи з даними.

Крок 7. Аудит кібербезпеки

Раз на півроку провести власний аудит за чеклістом (20–30 пунктів).

Перевіряти:
– чи оновлені ПЗ та ОС;
– чи доступна резервна копія;
– чи актуальні облікові записи.

Зафіксувати звіт в Excel або Word.

Крок 8. Реагування на інциденти

Створити план дій при інциденті:
– хто відповідає;
– куди звертатися (CERT-UA, IT-підрядник);

– як ізолювати уражений пристрій.

Зберегти копію плану офлайн (на папері).

Крок 9. Угода з IT-підрядником

Укласти договір з підрядником, з включенням:

– вимог до безпеки;
– відповідальності за витік даних;
– процедур аварійного відновлення.

Крок 10. Документація політики безпеки

Оформити коротку політику безпеки, яка включає:

– мету (захист персональних і комерційних даних);
– зони відповідальності;
– перелік заходів (резервування, доступи, навчання);
– відповідального за політику.

Зберігати документ в Google Drive та в надрукованому вигляді.

Стосовно безпеки бази даних можна запропонувати наступний чекліст (рис. 2), який може бути використаний при аудиті безпеки (власними силами чи за допомогою сторонніх спеціалістів з безпеки).

Категорія	Перевірка	Рекомендовані дії	Статус (✓/✗)	Примітки
Контроль доступу	Чи увімкнено двофакторну аутентифікацію (2FA)?	Увімкнути через Authenticator або SMS		
Контроль доступу	Чи використовуються складні унікальні паролі?	Застосувати менеджер паролів		
Контроль доступу	Чи обмежено доступ до БД лише необхідним користувач	Використати RBAC		
Захист БД	Чи оновлена СУБД до актуальної версії?	Оновити MySQL/PostgreSQL		
Захист БД	Чи активоване шифрування даних (TDE, SSL)?	Увімкнути шифрування		
Захист БД	Чи вимкнений зовнішній доступ до БД?	Дозволити доступ лише через VPN		
Бекап	Чи налаштовано регулярне резервне копіювання?	Налаштувати інкрементне копіювання		
Бекап	Чи зберігаються копії в іншому географічному місці або хм	Використати хмару/зовнішній диск		
Бекап	Чи перевірялося відновлення з бекапу протягом останніх	Провести тест відновлення		
Моніторинг	Чи ведуться логи доступу до бази даних?	Увімкнути логування у СУБД		
Моніторинг	Чи є механізм сповіщення про підозрілий вхід?	Налаштувати email-повідомлення		
Аудит	Чи проводився аудит безпеки протягом останніх 6 міс.?	Провести самостійний або зовнішній аудит		
Аудит	Чи задокументовані основні політики безпеки?	Оформити внутрішній документ		
Юридичний супровід	Чи оформлено згоду на обробку персональних даних?	Підготувати шаблон згідно ЗУ		
Юридичний супровід	Чи укладено договір з IT-підрядником?	Внести пункт про відповідальність за безпеку		

Рис. 2. Чекліст для аудиту безпеки бази даних

Отже, навіть без внутрішнього спеціаліста з кібербезпеки, ФОП та МСП можуть забезпечити базовий, але ефективний рівень захисту БД за допомогою правильного контролю доступу, регулярного резервного копіювання, простих інструментів моніторингу та періодичного самостійного або стороннього аудиту.

Висновки

У контексті триваючої військової агресії проти України кіберпростір став невід'ємною складовою бойових дій, а захист баз даних – критично важливим елементом національної, корпоративної та інституційної безпеки. Загроза кіберінцидентів значно зросла з 2022 року, особливо у сфері державного управління, об'єктів критичної інфраструктури та приватного сектору. Основними видами атак залишаються фішинг, компрометація облікових даних, масове розповсюдження шкідливого ПЗ, supply-chain атаки та wiper-інструменти, APT-діяльність, спрямована на держоргани, КІ та оборонний сектор.

Малий та середній бізнес є однією з найуразливіших категорій у кіберпросторі. Це обумовлено браком фінансових і людських ресурсів, низькою кіберобізнаністю персоналу, відсутністю політик безпеки та регулярного аудиту, використанням незахищених хмарних сервісів.

Водночас держсектор, КІ та великий бізнес мають значно вищий рівень захисту, що забезпечується наявністю нормативних вимог, внутрішніх служб кібербезпеки, доступу до міжнародної системи обміну кіберзагрозами тощо.

У ході дослідження було розроблено класифікацію основних типів загроз і засобів протидії, практичний план впровадження кіберзахисту для МСП, який включає 10 кроків, чекліст перевірки стану захисту баз даних.

На підставі проведеного аналізу надано цільові рекомендації для МСП, що дозволяють навіть за обмежених умов суттєво підвищити кіберстійкість організації. Ключовими серед них є впровадження двофакторної автентифікації, резервного копіювання, обмеження доступів, навчання персоналу та проведення мінімального кібераудиту.

Отже, базовий рівень кіберзахисту цілком досяжний навіть для малих організацій за умов чіткого алгоритму дій та усвідомлення значущості цифрової безпеки як елемента загальної стійкості бізнесу та держави.

Список використаної літератури

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

2. Шербиніна Є., Марценюк Б., Філоненко А. Безпека бази даних і вивчення методів шифрування даних в хмарному сховищі // Системи управління, навігації та зв'язку. 2020. Т. 3, № 61. С. 104–106. DOI: https://doi.org/10.26906/SUNZ.2020.3.104

3. Баргилевич О. А., Найман Г. Г. Забезпечення безпеки системи управління базами даних PostgreSQL // Сучасний захист інформації. 2022. № 3(51). С. 24–31. DOI: https://doi.org/10.31673/2409-7292.2022.032431

4. Лисий Р. Ю. Технології забезпечення безпеки систем управління базами даних // Зв'язок (ДонДУТ). 2017. № 3. С. 27–29. Режим доступу: https://con.dut.edu.ua/index.php/communication/article/view/1630/1560

5. Хращевський Р. В., Нестеренко К. С., Козловський В. В., Ткаля О. І. Захист баз даних за допомогою програмного комплексу DbProtect // Наукоємні технології (НАУ). 2022. № 2(54). С. 86–93. DOI: https://doi.org/10.18372/2310-5461.54.16746

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

7. Пєвнєв В. Я. Безпека баз даних: загрози та превентивні заходи // Сучасні інформаційні системи. 2018. Т. 2, № 1. С. 69–72. DOI: https://doi.org/10.20998/2522-9052.2018.1.13

8. Fuller B., Mayberry T., Reynolds P., та ін. SoK: Cryptographically Protected Database Search // IEEE Symposium on Security and Privacy. 2017. С. 20. DOI: https://doi.org/10.48550/arXiv.1703.02014

9. Kamran M., Farooq M. A Comprehensive Survey Of Watermarking Relational Databases Research // Computers & Security. 2018. DOI: https://doi.org/10.48550/arXiv.1801.08271

10. Bauskar S. Navigating Database Security in Cloud Computing: Challenges and Solutions // International Journal of Computer Applications. 2024. Т. 186, № 51. DOI: http://dx.doi.org/10.5120/ijca2024924173

11. Mahida A. A comprehensive review on ethical considerations in cloud computing: privacy, data sovereignty and compliance [Електронний ресурс] // Journal of Artificial Intelligence & Cloud Computing. 2022. № 1(4). С. 1–4. ISSN 2754–6659. DOI: 10.47363/JAICC/2022(1)231. Режим доступу: https://www.researchgate.net/publication/379792762 Дата звернення: 25.07.2025.

12. Державна служба спеціального зв'язку та захисту інформації України. [Електронний ресурс]. Режим доступу: https://scpc.gov.ua/en/articles/163 Дата звернення: 25.07.2025.

13. Українська правда. [Електронний ресурс]. Режим доступу: https://www.pravda.com.ua/eng/news/2024/01/31/7439720 Дата звернення: 25.07.2025.

14. CERT-UA. [Електронний ресурс]. Режим доступу: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv Дата звернення: 25.07.2025.

15. SPEKA. [Електронний ресурс]. Режим доступу: https://speka.media/kilkist-kiberatak-na-ukrayinu-zrosla-maize-vdvici-u-2024-zvidki-atakuyut-9g2nz8 Дата звернення: 25.07.2025.

16. UNN. [Електронний ресурс]. Режим доступу: https://unn.ua/en/news/in-2023-more-than-2500-cyber-incidents-were-recorded-in-ukraine Дата звернення: 25.07.2025.

17. Українська правда. [Електронний ресурс]. Режим доступу: https://www.pravda.com.ua/eng/news/2024/01/31/7439720 Дата звернення: 25.07.2025.

18. Astra Security. [Електронний ресурс]. Режим доступу: https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/ Дата звернення: 25.07.2025.

References

1. Antonenko, N. V., Hraboliuk, M. S., & Semenchenko, N. O. (2021). Problems of information protection in modern databases. *Scientific Bulletin of Poltava University of Economics and Trade. Series "Economic SciencesФ*, (2–1(103)), 106–110. https://doi.org/10.37734/2409-6873-2021-2-18

2. Sherbina, Y., Martsenyuk, B., & Filonenko, A. (2020). Database security and data encryption methods in cloud storage. *Control, Navigation and Communication Systems*, 3(61), 104–106. https://doi.org/10.26906/SUNZ.2020.3.104

3. Barhylevych, O. A., & Naiman, H. H. (2022). Security of PostgreSQL database management systems. *Modern Information Protection*, 3(51), 24–31. https://doi.org/10.31673/2409-7292.2022.032431

4. Lysyi, R. Yu. (2017). Technologies for ensuring database management systems security. *Communication (DonDUT)*, (3), 27–29. https://con.dut.edu.ua/index.php/communication/article/view/1630/1560

5. Khrashchevskyi, R. V., Nesterenko, K. S., Kozlovskyi, V. V., & Tkalia, O. I. (2022). Database protection using DbProtect software. *High Technologies (NAU)*, 2(54), 86-93. https://doi.org/10.18372/2310-5461.54.16746

6. Shchavinskyi, Yu., & Budzynskyi, O. (2025). Analysis of current issues in corporate database security and solutions. *Cybersecurity: Education, Science, Technology*, 3(27), 390-405. https://doi.org/10.28925/2663-4023.2025.27.726

7. Pievnev, V. Ya. (2018). Database security: threats and preventive measures. *Modern Information Systems*, 2(1), 69–72. https://doi.org/10.20998/2522-9052.2018.1.13

8. Fuller, B., Mayberry, T., Reynolds, P., et al. (2017). SoK: Cryptographically Protected Database Search. *IEEE Symposium on Security and Privacy*, 20. https://doi.org/10.48550/arXiv.1703.02014

9. Kamran, M., & Farooq, M. (2018). A comprehensive survey of watermarking relational databases research. *Computers & Security*. https://doi.org/10.48550/arXiv.1801.08271

10. Bauskar, S. (2024). Navigating database security in cloud computing: Challenges and solutions. *International Journal of Computer Applications*, 186(51). https://doi.org/10.5120/ijca2024924173

11. Mahida, A. (2022). A comprehensive review on ethical considerations in cloud computing: Privacy, data sovereignty and compliance. *Journal of Artificial Intelligence & Cloud Computing*, 1(4), 1–4. https://www.researchgate.net/publication/379792762

12. State Service of Special Communications and Information Protection of Ukraine. (n.d.). https://scpc.gov.ua/en/articles/163

13. Ukrainska Pravda. (2024, January 31). https://www.pravda.com.ua/eng/news/2024/01/31/7439720

14. CERT-UA. (2024). https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv

15. SPEKA. (2024). https://speka.media/kilkist-kiberatak-na-ukrayinu-zrosla-maize-vdvici-u-2024-zvidki-atakuyut-9g2nz8

16. UNN. (2023). https://unn.ua/en/news/in-2023-more-than-2500-cyber-incidents-were-recorded-in-ukraine

17. Ukrainska Pravda. (2024). https://www.pravda.com.ua/eng/news/2024/01/31/7439720

18. Astra Security. (2025). https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/

Дата першого надходження рукопису до видання: 17.09.2025
Дата прийнятого до друку рукопису після рецензування: 14.10.2025
Дата публікації: 28.11.2025