NETWORK AND APPLICATION SECURITY

DOI 10.20535/2411-1031.2022.10.2.270412
УДК 004.056(53+57)

ІГОР СУБАЧ,
ОЛЕКСАНДР ВЛАСЕНКО

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЗАХИСТУ БАЗ ДАНИХ ВІД КІБЕРАТАК В ІНФОРМАЦІЙНИХ СИСТЕМАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

З початком широкомасштабного вторгнення російської федерації в Україну значно зросла кількість кібератак на органи державної влади, об'єкти критичної інфраструктури та підрозділи, діяльність яких передбачає обробку критично важливої інформації, зокрема, інформаційні системи Збройних Сил України. Сучасні інформаційні системи військового призначення є складовою частиною будь-якої системи управління сил оборони та безпеки держави і відіграють важливу роль в управлінні військами на полі бою. База даних являється невід'ємною частиною інформаційної системи військового призначення, а її кіберзахист є одним з найважливіших факторів забезпечення цілісності, конфіденційності та доступності даних. У статті представлено аналіз сучасного стану кіберзахисту баз даних в інформаційних системах військового призначення. Наведено порівняльний аналіз існуючих кіберзагроз та типів і видів кібератак на ресурси систем керування базами даних. Визначено рівні безпеки баз даних, а також класифіковано загрози безпеці баз даних відповідно до них. Розглянуто існуючі методи та сучасні програмні рішення захисту баз даних (систем керування базами даних) від кібератак різних видів, описано їх переваги та недоліки. Запропоновано перспективний напрям удосконалення існуючих систем виявлення кібератак у аспекті провадження захисту баз даних на всіх рівнях екосистеми систем керування базами даних, а також усіх складових архітектури кіберзахисту інформаційних систем військового призначення, суть якого полягає у інтелектуальній обробці отриманих консолідованих даних. Консолідація даних про базу даних (опрацювання інформації про події та кіберінциденти, пов'язані безпосередньо з базою даних), що підлягають аналізу дозволяє отримати підґрунтя для розробки нових підходів до виявлення кібератак, які базуються на відслідковуванні не типових сценаріїв (експлойтів) їх реалізації. Такий підхід надає можливість вирішення виявленого протиріччя в сфері кіберзахисту баз даних у контексті невідповідності вимог, які висуваються до методів кіберзахисту баз даних інформаційних систем військового призначення та можливостей щодо їх реалізації. До того ж, втілення запропонованого підходу у комплексі із теорією нечітких множин дозволить провадити ефективний кіберзахист баз даних в умовах неповноти та неточності інформації.

Ключові слова: база даних, кіберзахист, кіберзагроза, кібератака, система виявлення вторгнень, теорія нечітких множин.

Постановка проблеми. Активне впровадження та використання інформаційних систем військового призначення (ІСВП) в процесах діяльності Збройних Сил спричинило створення окремого виду бойових дій, який знаходиться в кіберпросторі. НАТО у 2016 році офіційно визнало кіберпростір ареною воєнних дій разом із традиційними: сушею, морем і повітрям. У реаліях повномасштабного вторгнення російської федерації в Україну відбувається перша в світі повномасштабна кібервійна за участю військових підрозділів, державних органів, спецслужб і хакерських угрупувань. Цілями атак, в основному, є об'єкти критичної інфраструктури: енергетичні та комунальні підприємства, лікарні, служби екстреного реагування, фінансова система, логістика та ІТ-інфраструктура країни.

Таким чином, кіберпростір є не менш важливим простором бойових дій, ніж безпосередні бойові зіткнення на суші, морі та у повітрі.

Відповідно до цього, забезпечення кіберзахисту ІСВП – є одним з найважливіших завдань будь-якого підрозділу кіберзахисту. Слід зауважити, що майже вся інформація ІВСП зберігається у базі даних (БД) і це робить її критичним об'єктом захисту. У свою чергу, захист безпосередньо самої БД є важливим питанням у контурі захисту ІСВП у цілому.

Аналіз останніх досліджень та публікацій. Аналіз джерел, показує що питанням захисту БД надається надзвичайно велике значення. Дана область являється дуже актуальною в сучасних наукових дослідженнях. У багатьох вітчизняних і закордонних публікаціях висвітлюється питання кіберзахисту БД. У [1] конкретизовано складність питання захисту БД, яке потребує окремої уваги. Чим складніше БД тим більше заходів безпеки потрібно застосовувати для її захисту. Підключення до мережі БД значно ускладнює ситуацію. Виділено та визначено основні аспекти кібератак на БД, способи протидії ним, а також розглянуто існуючі методи кіберзахисту БД. У [3] представлено короткий огляд деяких вразливостей, які можуть виникнути при роботі з сучасними БД. Пропонується певний набір правил і дій, які можуть знизити ризики, пов'язані з порушенням конфіденційності, доступності і цілісності даних. Зроблено акцент на те, що самим важливим моментом безпеки БД є персонал, якій відповідає за безпеку і розвиток БД. У [4] розглядаються основи БД, такі як її призначення, функції та роль з акцентом на різні питання безпеки. Крім цього в даній публікації особливу увагу приділено основам керування безпекою БД, а також відповідним технологіям, що їх реалізують. У [5] проведено огляд загроз безпеки для існуючих БД та "контрзаходи" щодо їх усунення. Зроблено наголос на забезпеченні конфіденційності даних. Розглянуто різні методи, за допомогою яких ланцюжки автентифікації користувачів можуть бути розширеними. У [6] розглянуто питання захисту БД з точки зору безпеки розроблювальних застосунків, які підключаються до БД. У даній статті представлено огляд двадцяти загроз безпеці БД, що реалізуються через вебсайти. Були розглянуті можливі заходи контролю для усунення таких атак, щоб привернути увагу розробників вебзастосунків, а також широкої наукової спільноти. У роботі висловлено думку про те, що розробники повинні прикладати значні зусилля, щоб включити всі необхідні функції кіберзахисту при розробці застосунку та прийняти міри застереження. Крім того, усі розробники повинні пройти навчання з питань кібербезпеки. Автор вважає, що адміністратор системи повинен розробити метод підтримки безперервного резервного копіювання БД за допомогою застосунків, доступних в мережі Інтернет у режимі онлайн. У [7] визначено, що БД є основою будь-якої інформаційної системи. Виходячи з цього необхідно підтримувати якість БД для забезпечення якості інформаційної системи в цілому. В останній час дуже важко визначити, що собою являє ефективна модель чи архітектура БД. У результаті були виміряні певні характеристики і аспекти реалізації БД. Міра оцінки створюється з використанням багатьох елементів і якостей відповідних БД.

Більшість публікацій є вузько направленими чи орієнтованими на конкретний тип або вид систем керування базами даних (СКБД) і в них пропонуються впровадження класичних методів захисту БД по відношенню саме до них. Отже, вони більш орієнтовані на захист від конкретних кіберзагроз, а не захист БД у цілому.

Таким чином, аналіз публікацій та останніх подій першої в світі кібервійни, дозволяє зробити висновок про те, що проблема захисту БД є важливою в умовах ведення активних бойових дій у кіберпросторі. Тому тема дослідження є актуальною.

Метою статті є аналіз існуючих кіберзагроз, вразливостей БД і кібератак на них, методів кіберзахисту, а також програмних рішень щодо захисту БД, з виділенням їхніх основних недоліків та формулюванням шляхів їхнього усунення.

Виклад основного матеріалу дослідження. Для забезпечення необхідного рівня захисту БД ІСВП, спочатку потрібно зрозуміти саму природу виникнення кіберзагроз. При розгляді безпеки БД, завжди потрібно враховувати три основні аспекти кіберзахисту: конфіденційність, цілісність та доступність (рис. 1). Вони представляють собою певну модель, яка є базовою для розробки систем кіберзахисту, які використовуються при виявлені потенційних загроз і відповідних рішеннях для забезпечення кіберзахисту БД. Будь-яке рішення відносно безпеки БД є повним, якщо воно забезпечує всі ці три аспекти.

Рисунок 1 – Основні аспекти безпеки бази даних

Конфіденційність даних у БД – передбачає захист збережених у БД даних від будь-якого неправомірного та несанкціонованого доступу. Вона досягається за рахунок використання механізмів контролю доступу, застосуванням різних рівнів методів доступу та шифрування даних у БД.

Цілісність БД – передбачає підтримку точності, послідовності та достовірності даних, які можуть бути забезпечені комплексними рішеннями, які включають контроль доступу і обмеження цілісності даних у БД.

Доступність – означає, що дані у БД повинні бути оперативно доступними, у реальному масштабі часу. Це є можливим, лише у випадку постійної підтримки БД в працездатному стані. Доступність даних у БД, також, включає швидке відновлення БД після збоїв (програмно або апаратного забезпечення) [8].

У теперішній час важливість безпеки БД зростає, оскільки більшість критичних функцій суспільства та військових підрозділів стали диджиталізованими. БД є невід'ємною частиною будь-якої ІСВП і вона переважно містить конфіденційні дані. ІСВП має певне середовище функціонування, відповідно до цього безпека БД залежить від різних рівнів, а саме: фізичної безпеки; безпеки мережі функціонування; безпеки операційної системи; безпеки системи керування БД (рис. 2).

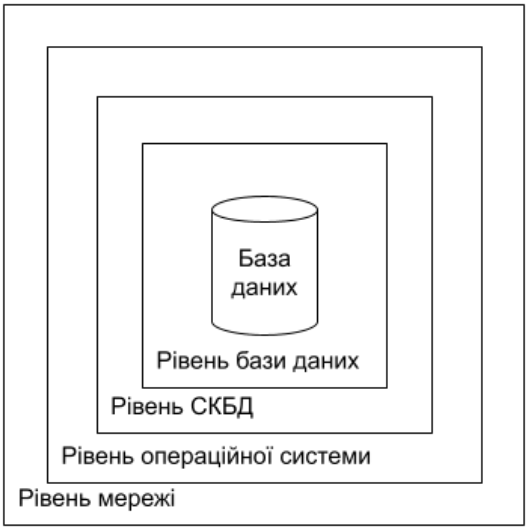

Рисунок 2 – Рівні безпеки бази даних

Кожен рівень безпеки відіграє важливе значення для коректного і безперебійного функціонуванні БД.

Рівень безпеки БД включає захист об'єктів конкретної БД та її суб'єктів (користувачів, ролей), які мають відповідні права та привілеї доступу до них.

Рівень СКБД включає процеси та потоки, які потрібні для її функціонування, а також вбудовані системи аудиту та моніторингу.

Рівень операційної системи (ОС) включає захист від несанкціонованого доступу користувачів ОС до процесів та служб, які відносяться до функціонування СКБД та файлової системи, де зберігаються файли БД та резервні копії БД, журнали транзакцій. Даний рівень, також, передбачає кіберзахист від шкідливого програмного забезпечення (ШПЗ), яке може бути імплементованим в роботу ОС.

Рівень мережі передбачає захист інтерфейсів доступу до БД, протоколів передачі даних, мережевих пристрої та серверного обладнання, функціонування яких впливає на коректну роботу БД.

Виходячи з цього можна визначити основні задачі, які повинна вирішувати система кіберзахисту БД:

– резервне копіювання/відновлення БД. СКБД повинна надавати засоби резервного копіювання БД з можливістю її відновлення після збоїв. Резервні копії потрібно зберігати в окремо захищених місцях;
– уникнення несанкціонованого використання об’єктів БД, шляхом багатофакторного доступу, включаючи засоби керування даними;
– балансування навантаження і тестування серверного обладнання;
– фізичну безпеку системи, враховуючи сервер БД;
– моніторинг та оцінку стану системи на наявність вразливостей щодо кібератак.

Для забезпечення належного рівня безпеки БД ІСВП, необхідним є чітке розуміння та знання кіберзагроз та природи їхнього виникнення.

Під загрозою БД будемо розуміти будь-яку ситуацію, подію або особу, які можуть негативно впливати на безпеку БД і безперебійне функціонування ІСВП у цілому. Загрози БД можуть бути навмисними або випадковими, внутрішніми та зовнішніми.

Аналіз звіту компанії Verizon Data Breach Investigations Report за 2021, який був сформований на основі аналізу 79635 інцидентів в різних галузях і регіонах людської діяльності, показує що саме внутрішні загрози є однією з найпоширеніших причин порушення безпеки БД.

Внутрішні загрози БД – це загроза безпеці з одного з трьох джерел, кожне з яких має привілейований доступ до БД:

– зловмисний інсайдер із злими намірами;
– недбала особа в організації, яка піддає БД кібератаці через необережні дії;
– стороння особа, яка отримує облікові дані за допомогою соціальної інженерії чи іншими методами або отримує доступ до облікових даних БД.

Зовнішні загрози БД – це загрози поза організацією або підрозділом в якому функціонує БД. Хакери, організовані групи кіберзлочинців, спеціалізовані урядові організації, військові підрозділи є прикладами зовнішніх джерел загроз БД. Зовнішні користувачі можуть отримувати доступ до БД, наприклад, за допомогою вебзастосунків або комп’ютерних мереж.

Аналіз публікацій [8] - [11] дозволяє визначити наступні загрози безпеки БД (табл. 1).

Таблиця 1 – Класифікація загроз безпеці БД відповідно до рівнів безпеки

Найменування загрози	**Рівень безпеки**	**Вид загрози**	**Опис загрози**
Надмірні привілеї	Рівень БД та СКБД	Внутрішня	Користувачі БД можуть мати різні права доступу до даних, в деяких випадках вони можуть бути надмірними. Надмірні права часто призводять до непотрібних небезпек. Надання надто великої кількості привілеїв або невчасне скасування цих привілеїв може призвести до зловживанню ними.

Продовження таблиці 1

Відмова в обслуговуванні (DOS)	Рівень мережі	Зовнішня	Категорія кібератак, при якій зловмисник атакує цільовий сервер БД великою кількістю запитів. При цьому сервер БД більше не може відповідати на запити від фактичних користувачів. Умови відмови в обслуговуванні (DOS) можуть бути створені за допомогою багатьох різних методів. Наприклад, перевантаження ресурсів сервера (пам'яті, центрального процесору) шляхом надсилання до СКБД спеціальних SQL-запитів. Перевантаження ресурсів особливо поширене серед БД.
Шкідливе програмне забезпечення	Рівень ОС	Зовнішня	ШПЗ різними способами може проникнути до середовища функціонування БД або комп'ютерів користувачів (наприклад, за допомогою фішингової атаки) і змушувати законних користувачів БД дозволяти доступ до даних, оскільки шкідливий код, встановлений на їх комп'ютерах, використовує їх можливості доступу для проникнення до даних.
Підвищення привілеїв	Рівень БД та СКБД	Внутрішня	Зловмисники можуть скористатися вразливістю програмного забезпечення платформи БД, щоб змінити права доступу звичайного користувача на права адміністратора БД. Вразливості можуть бути виявлені у вбудованих функціях, процедурах, що зберігаються, реалізаціях протоколів і навіть в операторах SQL. Маючи права адміністратора БД, розробник-шахрай може відключати механізми аудиту, створювати підроблені облікові записи.
Вразливості ОС	Рівень ОС	Зовнішня	Можуть призвести до несанкціонованого доступу до БД, пошкодженню даних або відмові в обслуговуванні. Наприклад, комп'ютерний хробак Blaster Worm скористався вразливістю ОС Windows 2000, щоб створити умови для відмови в обслуговуванні.
SQL-ін'єкції	Рівень БД	Зовнішня	При атаці з використанням SQL-ін'єкцій зловмисник, зазвичай додає неавторизовані оператори БД у вразливий канал даних SQL. Цільові канали даних включають процедури, що зберігаються, і вхідні параметри вебзастосунків. Введені оператори передаються до БД, де вони виконуються. Використовуючи SQL-ін'єкцію, зловмисники можуть отримати необмежений доступ до всієї БД.
Уразливості та неправильна конфігурація БД	Рівень БД та СКБД	Зовнішня	Зазвичай можна знайти вразливі та оновленні СКБД або виявити БД, які все ще мають облікові записи та параметри конфігурації за замовчуванням. Зловмисники знають, як використовувати ці вразливості для атак на БД.
Слабка автентифікація	Рівень СКБД	Зовнішня	Слабкі схеми аутентифікації дозволяють зловмисникам видавати себе за звичайних користувачів БД отриманням облікових даних для входу. Зловмисник може використати будь-яку кількість стратегій отримання облікових даних.
Слабкий аудит	Рівень СКБД	Зовнішня	Автоматичний запис будь-яких транзакцій БД, що включають конфіденційні дані, має бути частиною кожного розгортання БД. Відсутність контролю транзакцій та збору даних аудиту операцій з БД становить ризик організації на багатьох рівнях.

Кінець таблиці 1

Слабозахищені резервні копії	Рівень СКБД	Зовнішня	Носії та файли резервних копій часто не захищені від атак. У результаті численні вразливості безпеки виникають унаслідок втрат резервних копій БД.
Вразливість протоколів зв'язку з БД	Рівень мережі	Зовнішня	Пропрієтарні протоколи застосовуються адміністратором БД для зв'язку між клієнтом БД та іншими серверами за допомогою відповідних команд. Вразливість у цих протоколах може призвести до різних шахрайських дій, таких як несанкціонований доступ до даних, відмова в обслуговуванні, пошкодження даних. На додаток до цих загроз, їх посилює той факт, що у журналі аудиту не буде записів про ці шахрайські дії, оскільки ці протоколи охоплюються власним аудитом БД.

Також, загрози БД можливо класифікувати на фізичні та логічні. Фізичні загрози полягають у знищенні пристроїв зберігання даних, викраденням файлів БД. Логічні загрози – це несанкціонований доступ безпосередньо до даних, які зберігаються в БД.

Зловмисники можуть скомпрометувати захист БД від імені різних категорій її суб'єктів, включаючи адміністратора БД, адміністратора сервера, розробників і користувачів. Виходячи з цього можна виділити три основні типи зловмисників (рис. 3) [8]:

– зловмисник (англ. Intruder) – це сторонній неавторизований користувач, який завдає спроби отримати доступ до персональних даних з метою заволодіння корисною інформацією з БД через низку спеціальних маніпуляцій;

– інсайдер (англ. Insider) – є переважно одним із законних довірених користувачів, які зловживають своїми правами або перевищують їх з метою отримання інформації;

– адміністратор (англ. Admin) – користувач з привілеями керування системою, який порушуючи політику безпеки зловживає своїми правами, слідкуючи за діями користувачів та безпосередньо СКБД і отримує конфіденційну інформацію.

Рисунок 3 – Типи зловмисників БД

Атаки на базу даних можуть здійснюватися в будь-якій формі: активні атаки, пасивні атаки, прямі або опосередковані. Проникаючи до системи зловмисник може провести атаки двох типів [9]:

– прямі атаки (англ. Direct Attacks) – ці атаки концентруються на цільові дані. Вони можливі і ефективні, якщо є порушення чи перебої у механізмах безпеки;

– опосередковані атаки (англ. Indirect Attacks) – під час цієї атаки зловмисник явно не атакує ціль. Атака здійснюється на інші дані та проміжні елементи для доступу до цільових даних.

Атаки на БД можуть бути різного характеру і їх, також, можна розділити на два типи: пасивні та активні. При пасивній атаці зловмисник тільки перевіряє дані, які є в БД, і не

виконує жодних змін. При активній атаці фактичні значення БД змінюються [7]. Вони є більш проблематичними, ніж пасивні атаки, тому що можуть ввести користувача в оману і надавати йому недостовірну інформацію. Існують різні способи виконання пасивних і активних атак, класифікація яких наводиться у табл. 2 [9].

Таблиця 2 – Класифікація способів здійснення пасивних та активних атак на БД

Тип атаки	**Способи здійснення**	**Опис атаки**
Пасивна атака	Статичний витік	При цій атаці дані з БД можуть бути отримані шляхом виконання моментального знімку БД у певний час.
	Витік інформації	У цій атаці дані можливо отримати, зв'язавши значення БД з позицією цих значень в індексі.
	Динамічний витік	Можна спостерігати та аналізувати зміни, що відбуваються в БД протягом певного періоду часу та отримувати відповідні дані.
Активна атака	Спуфінг	У цій атаці зашифроване текстове значення замінюється згенерованим шкідливим значенням.
	Зрощування	При цій атаці значення зашифрованого тексту замінюється на інше значення зашифрованого тексту.
	Відтворення	Це різновид атаки, коли значення зашифрованого тексту замінюється старою версією, раніше оновленою або віддаленою.

Щоб усунути загрози безпеці БД, кожний підрозділ повинен мати систему захисту БД, яка обов'язково має бути реалізованою на основі ефективних методів кіберзахисту. Існує багато методів захисту БД, але їх можна структурувати на два типи. Перший – полягає в усуненні ризиків безпеки. Будь-яка організація повинна мати політику безпеки, якої необхідно дотримуватися. Другий тип – включає використання програмного інструменту, який буде значно впливати на покращення безпеки БД (табл. 3) [5] - [10].

Таблиця 3 – Класифікація методів захисту БД

Тип методу	**Метод**	**Опис методу**
Усунення ризиків	Контроль доступу	У системі захисту БД перевірка справжності відіграє життєво важливу роль. Якщо перевірка є коректною, ймовірність загроз зменшується. Різні користувачі мають різні права на доступ до різних об'єктів БД. Механізми контролю доступу мають справу з управлінням правами доступу. Це основний метод захисту об'єктів даних у БД, що підтримується більшістю СКБД. Методи контролю доступу спрямовані на забезпечення конфіденційності даних. Якщо будь-який користувач хоче отримати доступ до будь- Для автентифікації легітимних користувачів БД потрібен надійний метод аутентифікації. Контроль доступу гарантує, що всі зв'язки між БД та іншими об'єктами системи відповідають визначеним політикам і елементам керування. Жодний зловмисник не доступиться до даних ні всередині, ні ззовні, що захищає БД від потенційних помилок. Помилки можуть бути настільки серйозними, що можуть створити проблеми в роботі організації. Завдяки контролю над правами доступу, також, можна зменшити ризики, які можуть вплинути на безпеку БД на основних серверах. Наприклад, якщо будь-яку таблицю видалено або доступ змінено випадково, результати можна відкотити для певних файлів, але шляхом застосування контролю доступу їх видалення можна обмежити.

Кінець таблиці 3

	Політика висновків	Це важливо для захисту даних на певному рівні. Це відбувається, коли потрібно запобігти аналізу конкретних даних у формі фактів на певному вищому рівні безпеки. Політика висновків також допомагає визначити, як захистити інформацію від розголошення.
	Ідентифікація та автентифікація користувача	Це основне зобов'язання щодо забезпечення безпеки, оскільки процес ідентифікації визначає групу людей, яким дозволено доступ до даних. Щоб забезпечити безпеку, ідентифікатор проходить автентифікацію, і це зберігає конфіденційні дані в безпеці та від їх зміни неавторизованим користувачем.
	Підзвітність і аудит	Підзвітність і аудиторські перевірки необхідні для забезпечення фізичної цілісності даних, які потребують певного доступу до БД і які обробляються шляхом аудиту та для зберігання записів. Дані, розміщені на серверах для аутентифікації, обліку та доступу користувача, можна аналізувати за допомогою аудиту та підзвітності.
	Шифрування	Шифрування – це процес перетворення інформації до зашифрованого виду або коду, щоб її не могли прочитати всі інші люди, крім тих, хто володіє ключем до зашифрованого тексту.
Програмний інструмент	Брандмауер БД	Це своєрідні брандмауери вебзастосунків, які контролюють також БД для захисту від атак на них, а також дозволяють відслідковувати і перевіряти доступ до БД за допомогою журналів, які вони ведуть.
	Моніторинг даних у реальному часі	Адміністратор може перевіряти, аналізувати, контролювати і робити зміни під час виконання операцій вставки, видалення, оновлення даних. Збираючи дані з різних середовищ існування БД, можливо своєчасно реагувати на нестандартні (не шаблонні) дії користувачів системи в режимі реального часу і приймати рішення щодо усунення загрози.
	Багатофакторна автентифікація	Метод і технологія для підтвердження ідентифікації користувача вимагаючи наявність двох чи більше облікових даних, щоб користувач зміг увійти в систему чи виконати транзакцію.

Механізми усунення ризиків безпеки БД, такі як автентифікація, авторизація, контроль доступу та шифрування даних допомагають захистити СКБД від інсайдерів та зловмисників. Проте, для більш надійного захисту БД ІСВП потрібна комплексна система захисту, яка буде постійно відслідковувати всі дії, які відбуваються в БД і в середовищі, у якому вона функціонує.

Слід зауважити, що традиційні СКБД призначають права користувачам для контролю доступу до ресурсів БД. У них вбудовано свої системи моніторингу подій, які відслідковують дії користувачів. Проте, вони обмежені в своєму функціоналі, а також не можуть обробляти несанкціоновані запити користувачів, які можна визначити як кібератаку, під час якої шкідливий код додається до рядків, що передаються на SQL-сервер для виконання. Імплементація коду безпосередньо в змінні введення користувача, які можуть бути об'єднані з командами SQL, можна вважати ключовою формою впровадження SQL-ін'єкцій.

Кібератаки типу SQL-ін'єкція є ключовою проблемою у захисті систем БД, оскільки їх важко розділити із законними запитами користувачів. Крім того, СКБД не може гарантувати конфіденційність даних та їх захист від цих загроз. Таким чином, традиційна архітектура СКБД повинна бути адаптованою до нових кіберзагроз і забезпечення високої конфіденційності та безпеки даних. Дослідження показують, що для підвищення безпеки та кращого захисту БД від загроз різного типу, необхідно до СКБД додавати систему моніторингу активності, яка базується на сучасних інформаційних технологіях.

Дані інформаційні технології повинні бути призначені для захисту не тільки даних у БД, але й самої СКБД і кожного застосунку, який звертається до неї, від неправомірного використання, пошкодження і вторгнення.

На сьогоднішній день розроблено багато технологій і рішень для усунення вразливостей БД і забезпечення кращого моніторингу активності та виявлення кіберзагроз. Аналізуючи ринок програмного забезпечення кіберзахисту БД можемо зробити висновок, що у теперішній час існує два лідера в даній області – це компанії IBM та Oracle. Решта постачальників послуг дещо відстають від лідерів, але теж пропонують зрілі, конкурентноздатні рішення. Це компанії – Axiomatics, Imperva та Thales [11]. Основним рішенням компанії Axiomatics для захисту даних є продукт Dynamic Authorization Suite, створений на базі Axiomatics Policy Server та універсального застосунку керування доступом на основі атрибутів (англ. Attribute-Based Access Control). У набір входять Axiomatics Data Access Filter MD для керування доступом до конфіденційної інформації в реляційних БД разом із SmartGuard для фреймворків Big Data і хмарних сховищ даних. Реалізований у вигляді слабозв'язаних надбудов або проксі-серверів, пакет забезпечує контроль доступу на основі політик, визначених мовою XACML (англ. eXtensible Access Control Markup Language), а також динамічного маскування даних, фільтрації та прозорого моніторингу активності для багатьох джерел даних. Ключові особливості рішення включають динамічну контекстно-залежну авторизацію, реалізовану незалежно від постачальника, гнучкий контроль доступу до конфіденційних даних на основі динамічної фільтрації даних у реальному часі.

Компанія Impreva замість кількох продуктів SecureSphere для виявлення та оцінки, моніторингу активності, брандмауера БД, а також CounterBreach для захисту від загроз і камуфляжу для маскування, додала лише один план ліцензування FlexProtect для даних, щоб забезпечити повний захист своїх конфіденційних даних. Цей пакет захисту даних пропонує всі необхідні можливості, такі як уніфікований захист реляційних БД, сховищ даних, платформ великих даних і мейнфреймів; комплексний моніторинг діяльності, аудит і судове розслідування, доповнені розширеною аналітикою безпеки на основі профілювання поведінки; попередньо визначені політики, робочі процеси виправлення та сотні звітів про відповідність.

Широта портфоліо безпеки БД компанії Oracle вражає: завдяки низці продуктів захисту та виявлення кібератак, що охоплюють усі аспекти оцінки, захисту, моніторингу та відповідності БД, Oracle Database Security може задовольнити найскладніші вимоги клієнтів, як локально, так і в хмарі. Oracle Autonomous Database повністю автоматизує процеси надання, керування, налаштування та оновлення екземплярів БД без будь-яких простоїв, та не лише суттєво підвищує безпеку та відповідність конфіденційних даних, що зберігаються в БД Oracle, але й є переконливим аргументом для переміщення цих даних до хмари Oracle. Варто зазначити, що значна частина можливостей безпеки компанії все ще спеціально розроблена лише для БД Oracle, що робить рішення захисту даних Oracle менш придатними для підрозділів, які використовують інші типи БД.

Thales є провідним постачальником рішень для захисту даних. Її рішення реалізовано у вигляді платформи безпеки даних Vormetric – уніфікованої платформи захисту даних, яка забезпечує клієнтам гнучкість, масштабованість і ефективність для задоволення різних вимог безпеки, таких як прозоре шифрування всього середовища БД, привілейований контроль доступу користувачів, детальні дані на рівні поля, захист за допомогою шифрування, токенізація та маскування даних, а також єдиний менеджер безпеки. Відомі особливості платформи включають централізоване керування ключами шифрування та політиками в усіх середовищах і продуктах, API шифрування застосунків для вбудовування прозорого шифрування в існуючі застосунки та динамічне маскування за допомогою токенізації зі збереженням формату.

Корпорація IBM є багатонаціональною технологічною та консалтинговою компанією. IBM Security, один із стратегічних підрозділів компанії, який надає комплексне портфоліо, включаючи рішення для керування ідентифікацією та доступом, розвідки безпеки та захисту

інформації. IBM Security Guardium – комплексна платформа безпеки даних, що забезпечує повний набір функцій, включаючи виявлення та класифікацію, звітування про права, захист даних, моніторинг активності та розширену аналітику безпеки даних у різних середовищах: від файлових систем до БД і платформ великих даних, а також до гібридних хмарних інфраструктур.

Серед ключових функцій платформи Guardium – виявлення, класифікація, оцінка вразливості та звітування про права в неоднорідних середовищах даних; шифрування, редагування даних і динамічне маскування в поєднанні зі сповіщеннями в реальному часі та автоматичним блокуванням зловмисного доступу; а також моніторинг активності та розширена аналітика безпеки на основі машинного навчання.

Переваги та недоліки існуючих програмних рішень наведено в табл. 4 [11].

Таблиця 4 – Порівняльний аналіз існуючих програмних рішень захисту БД

Виробник	**Програмне рішення**	**Переваги**	**Недоліки**
IBM	IBM Security Guardium	– повний спектр можливостей безпеки для структурованих і неструктурованих даних; – підтримка гібридних багатохмарних середовищ; – розширені великі дані та когнітивна аналітика; – майже необмежена масштабованість.	– налаштування та операції можуть бути складними та ресурсо-затратними.
Oracle	Oracle Database Security Suite	– автономна хмарна платформа БД, що виключає адміністративний доступ людини; – автоматичне надання, оновлення, резервне копіювання та відновлення, без простоїв; – комплексне портфоліо продуктів для всіх сфер безпеки БД; – глибока інтеграція з іншими технологіями надання даних, тестування та хмарних технологій Oracle.	– деякі продукти доступні лише для баз даних Oracle; – продукти Big Data і NoSQL ще не інтегровані з рішеннями безпеки RDBMS.
Axiomatics	Axiomatics Dynamic Authorization Suite	– підхід, що не залежить від БД, забезпечує застосування єдиної політики для різних БД і сховищ великих даних; – 100% відповідність стандарту XACML; – спільна модель авторизації з іншими продуктами Axiomatics для програм, API.	– досить вузька функціональна спрямованість в порівнянні зі іншими програмними продуктами захисту БД; – покладається на сторонні компоненти для забезпечення дотримання правил.
Impreva	Imperva Data Security Suite	– зручні плани ліцензування для комплексного захисту даних; – кілька методів збору даних забезпечують мінімальну продуктивність; – розширена аналітика безпеки та аналітика поведінки; – велика кількість готових робочих процесів і звітів про відповідність.	– немає підтримки шифрування даних або динамічного маскування

Кінець таблиці 4

Thales	Thales Vormetric Data Security Platform	– комплексні можливості прозорого шифрування, токенізації та маскування; – висока продуктивність завдяки підтримці апаратного шифрування; – централізоване керування всіма середовищами, навіть продуктами сторонніх розробників; – стандартні API для додавання підтримки шифрування до існуючих програм.	– основна увага приділяється лише захисту даних, без охоплення інших функціональних областей.

Виходячи з проведеного аналізу, основними недоліками існуючих сучасних програмних рішень є:

– робота тільки з певними типами СКБД або лише структурованими даними;

– обмежена функціональність в певних аспектах захисту, щодо захисту БД на всіх рівнях;

– не завжди ефективні алгоритми (методи) аналізу вразливостей та захисту БД, які використовуються у них.

Виходячи з цього, більшість науковців зосередили свої зусилля на розробці систем виявлення/запобігання вторгнень – IDS/IPS (англ. Intrusion Detection System/Intrusion Prevention System), які здатні підсилити кіберзахист БД та які можна вважати однією з найважливіших частин будь-якої добре захищеної системи. Проте, більшість існуючих IDS/IPS-систем розроблено для виявлення кібератак на рівні комп'ютерних мереж та операційних систем і, таким чином, не завжди здатні виявити вторгнення у БД. Вони можуть бути використані для захисту мережевих ресурсів і розрізнення зловмисних і законних транзакцій. З іншого боку, наявність різного типу загроз зробило системи виявлення/ запобігання вторгнень однією з основних стратегій безпеки для захисту БД.

В основному існує два підходи до розробки систем виявлення/запобігання вторгнень, які, у тому числі, виконують функції кіберзахисту БД [20]:

– сигнатурні IDS/IPS. Системи цього різновиду працюють за схожим з антивірусним програмним забезпеченням принципом. Вони аналізують сигнатури та зіставляють їх із базою, яка має постійно оновлюватися для забезпечення коректної роботи. Якщо атака нова та її сигнатура невідома, є ризик того, що загроза не буде виявлена;

– IDS/IPS, що засновані на аномаліях. Системи, що базуються на аномаліях, використовують, як правило, методи машинного навчання. Для ефективної роботи таких систем виявлення загроз, потрібний пробний період навчання.

На відмінну від сигнатурних, IDS/IPS засновані на аномаліях, виявляють відхилення від штатної поведінки суб'єктів БД. Однак, на практиці дуже складно точно змоделювати штатну поведінку. У свою чергу, методи, на основі яких побудовані системи виявлення вторгнень на основі аномалій для виявлення зловмисного доступу до БД, можуть бути розділені в залежності від функцій, які вони беруть із журналів аудиту. Моделювання поведінки у більшості систем формалізується у вигляді поведінкового профілю. Ці всі функції, в основному, можуть бути орієнтованими на синтаксис, контекст.

Система виявлення вторгнень у БД, що описана у [12], використовує систему штучного нейронечіткого висновку (англ. Artificial NeuroFuzzy Inference System) для фіксації профілів поведінки користувачів. Автори використали метод нечіткого висновку Sugeno та штучну нейронну мережу (англ. Artificial NeuralNetwork) для створення деяких правил "якщо – то". Вхідні транзакції, які не відповідають цим нечітким правилам, позначаються як шкідливі. У [13] описується важливість правил асоціації та кластерного аналізу для виявлення неправомірних дій на основі шаблонів використання БД. Спочатку звичайні профілі

генеруються відповідно до ролей користувачів за допомогою розгортання алгоритму кластеризації. Якщо нова транзакція не відповідає існуючим правилам, вона позначається як шахрайська. У [14] запропоновано систему виявлення вторгнень в БД на основі аномалій для виявлення шкідливих SQL-запитів, надісланих до реляційної БД на основі ролей. Спочатку для побудови профілів поведінки використовується метод аналізу основних компонентів (англ. Principal Component Analysis) для транзакцій, які виконують користувачі. Пізніше класифікатор випадкового лісу зі зваженим голосуванням (англ. Random Forest with Weighted voting) застосовується до цих профілів для виявлення нав'язливих дій. Інша гібридна система запропонована у [15]. Вона використовує згорткову нейронну мережу (англ. Convolutional Neural Network) і систему класифікатора навчання (англ. Learning Classifier System) у тандемі. Learning Classifier System розробляє нові правила для транзакцій, щоб ідентифікувати будь-які аномальні події з журналів аудиту БД, тоді як Convolutional Neural Network використовується для цілей класифікації. Отже, у теперішній час, всі розглянуті системи виявлення вторгнень на своїй меті мають виявлення вторгнень у БД за показником точності.

Методи виявлення вторгнень на основі аномалій для розпізнавання зловмисного доступу до БД можна додатково розрізняти на основі того, які функції вони отримують з журналу аудиту СКБД та SQL-запитів для моделювання поведінки суб'єктів БД. Змодельована поведінка представляється у вигляд поведінкового профілю [16]. Ці функції можуть бути орієнтованими на синтаксис, контекст і дані, що іноді в літературі називають, орієнтованими на результат [16] - [18] (рис. 4).

Методи, що використовують орієнтовані на синтаксис функції, створюють профілі поведінки за допомогою синтаксичних особливостей вбудованого SQL-запиту, але не обмежуються атрибутами в реченні проекції, запитуваних відносинах, атрибутах у пункті вибору та/або типом команди SQL [16].

Техніки, що використовують функції, орієнтовані на дані або результати, створюють профілі поведінки, використовуючи дані, що повернуті у відповідь, а SQL-запит або будь-які інші статистичні вимірювання повернутих даних, наприклад, мінімальне та максимальне значення у випадку числових даних, кількість інформації (відсоток повернутих даних), що повертається у відповідь на запит або повернуті значення атрибутів, використовуються для моделювання поведінки користувача [18].

Методи, орієнтовані на контекст, створюють профілі поведінки з використанням контекстних особливостей. Контекстуальні ознаки пов'язані з контекстом запиту, наприклад, час, коли було зроблено запит, ідентифікатор користувача особи, яка робить запит, чи кількість запитів, зроблених за певний період часу [19].

Під час моделювання нормативної поведінки можна використовувати поєднання контексту, синтаксису та функцій, орієнтованих на дані. Один із таких методів виявлення аномалій, який використовує синтаксис і орієнтований на дані особливості запропоновано в [17].

Система виявлення аномалій, яка створює профілі поведінки, закриті від людини, відома як система виявлення аномалій Black-Box. З іншого боку, система виявлення аномалій, що створює профілі поведінки, відкриті для людини, відома як система виявлення аномалій White-Box. Відкритість означає, що справжню першопричину аномалії можуть визначити адміністратори (офіцер служби безпеки, адміністратор БД), коли вони перевіряють аномалію. Інтуїтивно зрозумілі підходи White-Box можуть допомогти пояснити аномалії [20].

Аналіз існуючих досліджень в сфері систем виявлення вторгнень у БД і методів, які покладено в основу їхнього функціонування показав, що у більшості робіт розглядаються дані системи виключно в контексті запитів до БД та SQL-синтаксису, на основі чого і будують поведінковий шаблон. Проте останні витоки даних і кібератаки на БД вказують, що зловмисники в більшості випадків атакують БД не на пряму, а спочатку – рівні еко-системи в якій вона знаходиться. Наприклад, у компаніях Yahoo! у 2014 році та CAN Financial у 2019, витік даних трапився після того, як зловмисники скористались вразливостями мережі і системи.

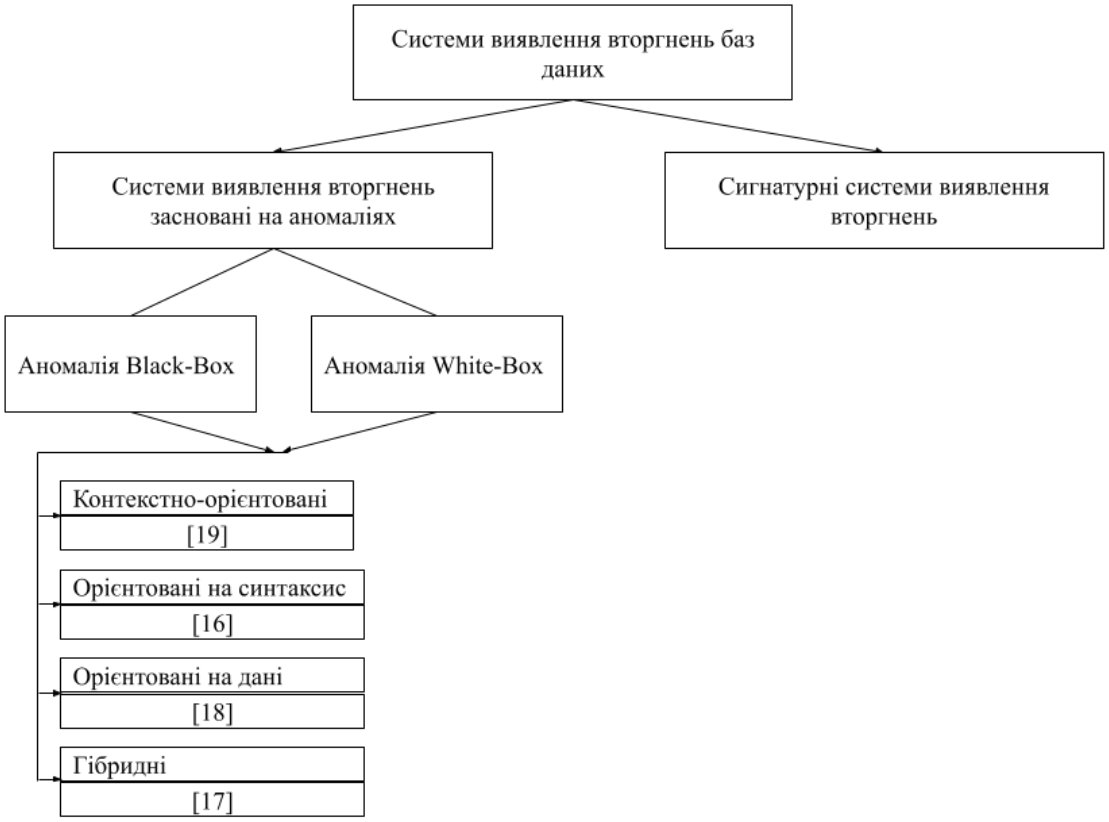

Рисунок 4 – Таксономія систем виявлення аномального доступу до СКБД

У лютому 2018 року GitHub-платформа для розробників програмного забезпечення, була вражена DDoS-атакою зі швидкістю 1,35 терабіт на секунду та тривала приблизно 20 хвилин. Незважаючи на те, що GitHub був добре підготовлений до DDoS-атаки, система захисту своєчасно не зреагувала на кібератаку. Аналіз цієї кібератаки показав, що вона відзначилася своїм масштабом і тим фактом, що була здійсненою за допомогою стандартного програмного забезпечення Memcached для прискорення роботи веб-сайтів і мереж. Дані приклади свідчать про те, що систему захисту БД потрібно розглядати в контексті комплексного рішення, відповідно до всіх рівнів захисту БД та СКБД, які відповідають за їхнє функціонування.

Більшість сучасних систем виявлення/запобігання вторгнень у БД не здатні попередити шкідливі дії до того моменту, поки вони не закінчать своє виконання. Враховуючі конфіденційність даних в ІСВП, це робить доступні в поточний момент часу рішення захисту БД на основі систем IDS/IPS не завжди ефективними.

Для усунення наведених недоліків доцільно здійснювати захист БД на всіх рівнях та всіх складових архітектури кіберзахисту ІСВП, яка побудована, наприклад, на основі інтелектуальної SIEM-системи [2], з вбудованими спеціалізованими модулями, які реалізують функції шкідливої активності саме по відношенню до БД.

При цьому, однією з головних цілей використання підсистеми захисту БД є підвищення рівня її кіберзахисту в існуючій архітектурі SIEM-системи, за рахунок забезпечення можливості опрацювання інформації про події та кіберінциденти, пов’язані безпосередньо з БД та здійснення попереджувального управління інцидентами та подіями безпеки у близькому до реального часу режимі.

Подібне рішення, в умовах неповноти та неточності інформації про події, що відбуваються в системі, може бути реалізованим шляхом застосування методів інтелектуального аналізу даних, зокрема, методів теорії нечітких множин та нечіткого логічного виводу. Переваги даних методів наведено в публікації [22]. Слід зауважити, що в якості вхідних даних для функціонування запропонованої системи, повинні залучатися не тільки дані безпосередньо про БД, а й операційну систему, комп’ютерну мережу та інші програмні застосунки, які взаємодіють з БД.

Висновки. Таким чином, аналіз сучасних кіберзагроз БД, їхніх вразливостей та методів і технологій їхнього кіберзахисту, дозволяє зробити висновок про існуюче у теперішній час протиріччя в науці і практиці, суть якого полягає у невідповідності вимог, які висуваються до методів кіберзахисту БД ІСВП та їхніми можливостями щодо його здійснення.

Усунення сформульованого протиріччя може бути здійсненим шляхом вирішення актуального наукового завдання з розробки моделей, методів і методик кіберхахисту БД ІСВП в умовах неповноти та неточності інформації на основі теорії нечітких множин та нечіткого логічного виводу.

У перспективах подальших досліджень є побудова архітектури SIEM-системи зі спеціалізованими модулями виявлення несанкціонованих вторгнень у БД ІСВП.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] E. Burtescu, "Database Security, Attacks and Control Methods", *Journal of Applied Sciences and Technology*, pp. 449-453, 2009.

[2] І. Субач, В. Кубрак, та А. Микитюк, "Архітектура та функціональна модель перспективної проактивної інтелектуальної системи SIEM-системи для кіберзахисту об'єктів критичної інфраструктури", *Information Technology and Security*, vol 7, iss. 2, pp. 208-215, 2019, doi: https://doi.org/10.20535/2411-1031.2019.7.2.190570.

[3] В. Я. Пєвнєв, "Безпека баз даних: загрози та превентивні заходи", *Сучасні інформаційні системи*, т. 2, № 1, с. 69-72, 2018, doi: https://doi.org/10.20998/2522-9052.2018.1.13.

[4] P. Paul, and P. S. Aithal, "Database Security: An Overview and Analysis of Current Trend", *International Journal of Management, Technology, and Social Sciences (IJMTS)*, vol. 4, no. 2, pp. 53-58, 2019, doi: https://dx.doi.org/10.2139/ssrn.3497728.

[5] A. Mousa, M. Karabatak, and T. Mustafa, "Database Security Threats and Challenges", *in Proc. 8th International Symposium on Digital Forensics and Security (ISDFS)*, Remote/ Online, 2020, pp. 1-5, doi: https://doi.org/10.1109/ISDFS49300.2020.9116436.

[6] R. A. Teimoor, "A Review of Database Security Concepts, Risks, and Problems", *UHD Journal of Science and Technology*, vol. 5, no. 2, pp. 38-46, 2021, doi: https://doi.org/10. 21928/uhdjst.v5n2y2021.pp38-46.

[7] J. Juma, and D. Makupi, "Understanding Database Security Metrics: A Review", *Mara International Journal of Scientific & Research Publications*, vol. 1, no. 1, pp. 40-48, 2017.

[8] J. Swati, and Ch. Dimple, "A Relative Study on Different Database Security Threats and their Security Techniques", *International Journal of Innovative Science and Research Technology*, vol. 5, no. 1, pp. 794-799, 2020, doi: http://dx.doi.org/10.13140/RG.2.2.11657.60000.

[9] S. Gahlot, B. Verma, and A. Khandelwal, "Database Security: Attacks, Threats and Control Methods", *International Journal of Engineering Research & Technology*, vol. 5, no. 10, 2017.

[10] J. C. Ogbonna, F. O. Nwokoma, and A. Ejem, "Database Security Issues: A Review", *International Journal of Science and Research*, vol. 6, no. 8, pp. 1812-1816, 2017.

[11] Database and Big Data Security, 2019. [Online]. Available: https://www.kuppingercole.com/ research/lc79015/database-and-big-data-security. Accessed on: Aug. 9, 2022.

[12] A. Brahma, and S. Panigrahi, "A new approach to intrusion detection in databases by using artificial neuro fuzzy inference system", *International Journal of Reasoning-based Intelligent Systems*, vol. 7, no. 3-4, pp. 254-260, 2015, doi: https://dx.doi.org/10.1504/IJRIS.2015. 072952.

[13] I. Singh, V. Darbari, L. Kejriwal, and A. Agarwal, "Conditional adherencebased classification of transactions for database intrusion detection and prevention", in *Proc. International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 42-49, Jaipur, India, 2016, doi: https://doi.org/10.1109/ICACCI.2016.7732023.

[14] C. A. Ronao, and S.-B. Cho, "Anomalous query access detection in rbac-administered databases with random forest and PCA", *Information Sciences*, vol. 369, pp. 238-250, 2016, doi: https://doi.org/10.1016/j.ins.2016.06.038.

[15] S.-J. Bu, and S.-B. Cho, "A hybrid system of deep learning and learning classifier system for database intrusion detection", in *Proc. International Conference on Hybrid Artificial Intelligence Systems*, pp. 615-625, La Rioja, Spain, 2017, doi: https://doi.org/10.1007/978-3-319-59650-1_52.

[16] S. R. Hussain, A. M. Sallam, and E. Bertino, "Detecting anomalous database transactions by insiders", in *Proc. 5th ACM Conference on Data and Application Security and Privacy*, pp. 25-35, Charlotte , NC , USA, 2015, doi: http://dx.doi.org/10.1145/2699026.2699111.

[17] A. Sallam, D. Fadolalkarim, E. Bertino, and Q. Xiao, "Data and syntax centric anomaly detection for relational databases", *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 6, no. 6, pp. 231-239, 2016, doi: https://doi.org/10.1002/widm.1195.

[18] M. Sunu, M. Petropoulos, and H. Q. Ngo, "A datacentric approach to insider attack detection in database systems", in *Proc. 13th International Conference on Recent Advances in Intrusion Detection*, pp. 382-401, Ottawa, Ontario, Canada, 2010, doi: http://dx.doi.org/10.1007/978-3-642-15512-3_20.

[19] A. Mahdi, P. Sander, and S. Etalle, "Behavior analysis in the medical sector: Theory and practice", in *Proc. 33rd Annual ACM Symposium on Applied Computing*, pp. 1637-1646, New York, NY, USA, 2018, doi: https://doi.org/10.1145/3167132.3167307.

[20] M. I. Khan, S. N. Foley, and B. O'Sullivan, "Database Intrusion Detection Systems (DIDs): Insider Threat Detection via Behavioural-based Anomaly Detection Systems – A Brief Survey of Concepts and Approaches", in *Emerging Information Security and Applications*, W. Meng, and S. K. Katsikas, vol. 1403, Eds. Cham : Springer, 2022, pp.178-197, doi: https://doi.org/10.1007/978-3-030-93956-4_11.

[21] R. G. Santos, J. Bernardino, and M. Vieira, "Approaches and Challenges in Database Intrusion Detection", *ACM SIGMOD Record*, vol. 43, no. 3, pp. 36-47, 2014, doi: https://doi.org/10.1145/2694428.2694435.

[22] І. Субач, В. Фесьоха, та Н. Фесьоха, "Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі, відкритих на основі загальнодоступних ліцензій", *Information technology and security*, vol. 5, iss. 1, pp. 29-41, 2017, doi: https://doi.org/10.20535/2411-1031.2017.5.1.120554.

Стаття надійшла до редакції 02.09.2022.

REFERENCES

[1] E. Burtescu, "Database Security, Attacks and Control Methods", *Journal of Applied Sciences and Technology*, pp. 449-453, 2009.

[2] I. Subach, A. Mykytiuk, and V. Kubrak, "Architecture and functional model of a perspective proactive intellectual SIEM for cyber protection of objects of critical infrastructure", *Information Technology and Security*, vol 7, iss. 2, pp. 208-215, 2019, doi: https://doi.org/10.20535/2411-1031.2019.7.2.190570.

[3] V. Pevnev, and S.Kapchynskyi, "Database security: threats and preventive measures", *Advanced Inforamation Systems*, vol. 2, no. 1, pp. 69-72, 2018, doi: https://doi.org/10.20998/2522-9052.2018.1.13.

[4] P. Paul, and P. S. Aithal, "Database Security: An Overview and Analysis of Current Trend", *International Journal of Management, Technology, and Social Sciences (IJMTS)*, vol. 4, no. 2, pp. 53-58, 2019, doi: https://dx.doi.org/10.2139/ssrn.3497728.

[5] A. Mousa, M. Karabatak, and T. Mustafa, "Database Security Threats and Challenges", *in Proc. 8th International Symposium on Digital Forensics and Security (ISDFS)*, Remote/ Online, 2020, pp. 1-5, doi: https://doi.org/10.1109/ISDFS49300.2020.9116436.

[6] R. A. Teimoor, "A Review of Database Security Concepts, Risks, and Problems", *UHD Journal of Science and Technology*, vol. 5, no. 2, pp. 38-46, 2021, doi: https://doi.org/10.21928/uhdjst.v5n2y2021.pp38-46.

[7] J. Juma, and D. Makupi, "Understanding Database Security Metrics: A Review", *Mara International Journal of Scientific & Research Publications*, vol. 1, no. 1, pp. 40-48, 2017.

[8] J. Swati, and Ch. Dimple, "A Relative Study on Different Database Security Threats and their Security Techniques", *International Journal of Innovative Science and Research Technology*, vol. 5, no. 1, pp. 794-799, 2020, doi: http://dx.doi.org/10.13140/RG.2.2.11657.60000.

[9] S. Gahlot, B. Verma, A. Khandelwal, "Database Security: Attacks, Threats and Control Methods", *International Journal of Engineering Research & Technology*, vol. 5, no 10, 2017.

[10] J. C. Ogbonna, F. O. Nwokoma, and A. Ejem, "Database Security Issues: A Review", *International Journal of Science and Research*, vol. 6, no. 8, pp. 1812-1816, 2017.

[11] Database and Big Data Security, 2019. [Online]. Available: https://www.kuppingercole.com/research/lc79015/database-and-big-data-security. Accessed on: Aug. 9, 2022.

[12] A. Brahma, and S. Panigrahi, "A new approach to intrusion detection in databases by using artificial neuro fuzzy inference system", *International Journal of Reasoning-based Intelligent Systems*, vol. 7, no. 3-4, pp. 254-260, 2015, doi: https://dx.doi.org/10.1504/IJRIS.2015.072952.

[13] I. Singh, V. Darbari, L. Kejriwal, and A. Agarwal, "Conditional adherencebased classification of transactions for database intrusion detection and prevention", in *Proc. International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 42-49, Jaipur, India, 2016, doi: https://doi.org/10.1109/ICACCI.2016.7732023.

[14] C. A. Ronao, and S.-B. Cho, "Anomalous query access detection in rbac-administered databases with random forest and PCA", *Information Sciences*, vol. 369, pp. 238-250, 2016, doi: https://doi.org/10.1016/j.ins.2016.06.038.

[15] S.-J. Bu, and S.-B. Cho, "A hybrid system of deep learning and learning classifier system for database intrusion detection", in *Proc. International Conference on Hybrid Artificial Intelligence Systems*, pp. 615-625, La Rioja, Spain, 2017, doi: https://doi.org/10.1007/978-3-319-59650-1_52.

[16] S. R. Hussain, A. M. Sallam, and E. Bertino, "Detecting anomalous database transactions by insiders", in *Proc. 5th ACM Conference on Data and Application Security and Privacy*, pp. 25-35, Charlotte , NC , USA, 2015, doi: http://dx.doi.org/10.1145/2699026.2699111.

[17] A. Sallam, D. Fadolalkarim, E. Bertino, and Q. Xiao, "Data and syntax centric anomaly detection for relational databases", *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 6, no. 6, pp. 231-239, 2016, doi: https://doi.org/10.1002/widm.1195.

[18] M. Sunu, M. Petropoulos, and H. Q. Ngo, "A datacentric approach to insider attack detection in database systems", in *Proc. 13th International Conference on Recent Advances in Intrusion Detection*, pp. 382-401, Ottawa, Ontario, Canada, 2010, doi: http://dx.doi.org/10.1007/978-3-642-15512-3_20.

[19] A. Mahdi, P. Sander, and S. Etalle, "Behavior analysis in the medical sector: Theory and practice", in *Proc. 33rd Annual ACM Symposium on Applied Computing*, pp. 1637-1646, New York, NY, USA, 2018, doi: https://doi.org/10.1145/3167132.3167307.

[20] M. I. Khan, S. N. Foley, and B. O'Sullivan, "Database Intrusion Detection Systems (DIDs): Insider Threat Detection via Behavioural-based Anomaly Detection Systems – A Brief Survey of Concepts and Approaches", in *Emerging Information Security and Applications*, W. Meng, and S. K. Katsikas, vol. 1403, Eds. Cham : Springer, 2022, pp.178-197, doi: https://doi.org/10.1007/978-3-030-93956-4_11.

[21] R. G. Santos, J. Bernardino, and M. Vieira, "Approaches and Challenges in Database Intrusion Detection", *ACM SIGMOD Record*, vol. 43, no. 3, pp. 36-47, 2014, doi: https://doi.org/10.1145/2694428.2694435.

[22] I. Subach, V. Fesokha, and N. Fesokha, "Analysis of existing solutions for preventing invasion in information and telecommunication networks", *Information technology and security*, vol. 5, iss. 1, pp. 29-41, 2017, doi: https://doi.org/10.20535/2411-1031.2017.5.1.120554.

IHOR SUBACH,
OLEKSANDR VLASENKO

INFORMATION TECHNOLOGIES FOR DATABASE PROTECTION AGAINST CYBER ATTACKS IN MILITARY INFORMATION SYSTEMS

With the beginning of the Russian Federation's large-scale invasion of Ukraine, the number of cyberattacks on state authorities, critical infrastructure facilities, and units whose activities involve the processing of critically important information, including the information systems (IS) of the Armed Forces of Ukraine, has significantly increased. Modern information systems for military purposes (ISMP) are an integral part of any system of management of defense and security forces of the state and play an important role in the management of troops on the battlefield. The database (DB) is an integral part of any ISMP, and its cyber protection is one of the most important factors in ensuring the integrity, confidentiality and availability of data. The article presents an analysis of the current state of cyber protection of databases in ISMP. A comparative analysis of existing cyber threats and types and types of cyber-attacks on the resources of database management systems (DBMS) is given. Database security levels are defined, and database security threats are classified according to them. The existing methods and modern software solutions for database protection (DBMS) against various types of cyberattacks are considered, their advantages and disadvantages are described. A promising direction for improving existing systems for detecting cyberattacks in the aspect of implementing database protection at all levels of the DBMS ecosystem, as well as all components of the ISMP cyber protection architecture, is proposed, the essence of which is the intelligent processing of the received consolidated data. Consolidation of database data (processing of information about events and cyber incidents directly related to the database) subject to analysis provides a basis for the development of new approaches to the detection of cyber-attacks, which are based on monitoring non-typical scenarios (exploits) of their implementation. This approach provides an opportunity to resolve the identified contradiction in the field of database cyber protection in the context of the inconsistency of the requirements that are put forward for the methods of cyber protection of the ISMP database and the possibilities for their implementation. In addition, the implementation of the proposed approach in combination with the theory of fuzzy sets will allow effective cyber protection of databases in conditions of incompleteness and inaccuracy of information.

Keywords: database, cyber defense, cyber threat, cyber-attack, intrusion detection system, fuzzy set theory.

Субач Ігор Юрійович, доктор технічних наук, доцент, завідувач кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-9344-713X, igor_subach@ukr.net.

Власенко Олександр Володимирович, ад'юнкт, Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна, ORCID0000-0001-6671-870X, oleksvlas@gmail.com.

Subach Ihor, doctor of technical science, associate professor, head at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Vlasenko Oleksandr, postgraduate student, Military institute of telecommunications and information technologies named after the Heroes of Kruty, Kyiv, Ukraine.