УДК 004.9

МУЛЬТИШАРОВА КІБЕРБЕЗПЕКА БАЗ ДАНИХ У CRM-СИСТЕМАХ

В. О. Чорняк, О. В. Тимченко

Національний Університет «Львівська Політехніка»,
вул. Степана Бандери, 12, Львів, 79013, Україна,

У статті представлено методичний підхід до розробки та використання критеріїв оцінювання продуктивності CRM-систем, що ґрунтується на поєднанні стратегічних та операційних індикаторів. Проблема, на розв'язання якої спрямовано дослідження, полягає у відсутності уніфікованого набору показників та інтегрованої оцінної моделі, здатної врахувати як кількісні, так і якісні аспекти функціонування CRM. Тому метою роботи є формування системи критеріальних ознак для вимірювання продуктивності, що забезпечує об'єктивну та адаптивну оцінку ефективності використання CRM-технологій у різних бізнес-контекстах.

Методологічною основою дослідження слугує контент-аналіз літературних джерел, опитування експертів та застосування багатокритеріальних методів оцінювання. Запропоновано процедуру вагового нормування критеріїв, що дає змогу синтезувати інтегральний показник продуктивності. Це уможливлює порівняння різних CRM-систем, а також оперативне виявлення слабких місць та резервів для подальшого вдосконалення.

Результати експериментальної апробації свідчать про практичну релевантність та універсальність розробленого підходу. Застосування методики дає змогу оптимізувати ресурси, підвищити точність прийняття управлінських рішень та стимулювати розвиток клієнтоорієнтованої стратегії підприємств. Подальші дослідження можуть бути спрямовані на автоматизацію процесу оцінювання, інтеграцію з інтелектуальними системами та розширення методологічної бази.

Ключові слова: *CRM-система, захист баз даних, RBAC/ABAC, Transparent Data Encryption, row-level security, Zero Trust, STRIDE, MITRE ATT&CK, SIEM, CVSS-оцінка ризику.*

Постановка проблеми. У протягом останнього десятиліття CRM-системи еволюціонували з суто клієнтських реєстрів у високонавантажені корпоративні платформи, що інтегрують модулі продажів, маркетингу, служб технічної підтримки — сервіс-деску (Service desk) та аналітики, оперуючи петабайтними масивами персоніфікованих даних. Згідно з галузевими опитуваннями компаній Gartner та IDC, середній обсяг транзакцій у хмарній CRM-інстанції середнього підприємства перевищує 10^6 CRUD-операцій на добу, а частка операцій, чутливих до конфіденційності (PII, PCI, PHI), перевищує 60 %. Така концентрація критичних даних перетворює сховище CRM на «єдину точку катастрофи», де порушення принципів конфіденційності (Confidentiality), цілісності (Integrity) та доступності

(Availability) бази даних призводить до каскадних наслідків — від втрати репутації до багатомільйонних штрафів за GDPR та PCI DSS 4.0 [1-3].

Аналіз публічних інцидентів 2020–2024 рр. показує, що понад 48 % компрометацій CRM-даних ініційовані зсередини мережевого периметру, тоді як зовнішні загрози часто використовують ланцюги експлойтів, де першим кроком є захоплення облікових даних до БД. Наявні підходи — точкове шифрування (Transparent Data Encryption, колонкові алгоритми), статичні політики RBAC чи DAC та периметрові WAF/IDS — демонструють обмежену ефективність, коли проти організації застосовується комбінована техніка MITRE ATT&CK (T1078 + T1505 + T1562). Проблема ускладнюється переходом від монолітної до мікросервісної архітектури CRM, де зростає кількість міжсервісних API-викликів, а класичні засоби сегментації мережі втрачають релевантність [4-6].

Таким чином, актуальність дослідження зумовлена потребою в універсальній мультишаровій моделі безпеки, здатній забезпечити Zero-Trust-контроль доступу (безпека без периметра) без істотної деградації продуктивності транзакційних операцій. В Zero Trust моделі безпеки вимагається дотримання суворого контролю доступу та недовіри до довільного користувача, навіть того, хто вже перебуває в периметрі мережі.

Аналіз останніх досліджень та публікацій. Безпека баз даних у CRM визначається перетином нормативних вимог (GDPR, PCI DSS 4.0, ISO/IEC 27001:2022) і технічних практик [5]. Усі документи вимагають шифрування даних, контрольованого доступу, журналювання та періодичної оцінки ризиків. На технічному рівні це означає використання TDE (Transparent Data Encryption), мікросегментації прав через RBAC/ABAC і централізованого логування з передачею подій в управління безпекою, інформацією та подіями – SIEM, яке поєднує функції SIM (управління інформацією безпеки) та SEM (управління подіями безпеки).

Сучасні дослідження підтримують концепцію гібридного контролю доступу: базова роль плюс атрибути сеансу (час, локація, тип пристрою) та дозволяють створити гнучку, контекстну політику доступу. У системи управління базами даних PostgreSQL це реалізується через Безпеку на рівні рядка (RLS - row-level security) і дає змогу використовувати членство в групі або контекст виконання для керування доступом до рядків у таблиці бази даних. Для каналів передачі використовуються TLS 1.3 з розширенням ESNI (Encrypted Server Name Indication), а також Взаємна безпека транспортного рівня (mTLS), що дає змогу двом сторонам автентифікувати одна одну під час початкового підключення - рукостискання SSL/TLS для внутрішніх сервісів.

Останні публікації підкреслюють роль поведінкової аналітики — SIEM із машинним навчанням скорочує час реакції на інциденти до хвилин. Таким чином, нормативні вимоги стимулюють побудову багаторівневої, адаптивної системи захисту, здатної до автоматичної реакції та масштабування в умовах мікросервісної архітектури CRM.

Метою роботи є розроблення й експериментальна валідація інтегрального підходу до захисту баз даних CRM-систем, який синергійно поєднує криптографічні, ізоляційні та поведінкові механізми.

Виклад основного матеріалу дослідження. ***Архітектура сучасної CRM-системи*** зазвичай побудована за принципами мікросервісного дизайну із чіткою декомпозицією функціональних блоків на окремі контейнери або сервіси. Це забезпечує гнучкість масштабування та незалежність розробки, але одночасно ускладнює реалізацію централізованих механізмів безпеки, зокрема для рівня бази даних. Центральним елементом у цій конфігурації виступає кластер баз даних — як правило, SQL або NewSQL-типу (наприклад, PostgreSQL, CockroachDB або TiDB), який підтримує транзакційність і сильну узгодженість (strong consistency), тобто всі вузли бачать однакові дані незалежно від часу, що є критично важливим для цілісності клієнтських записів [7, 8].

У типовому сценарії взаємодія починається з клієнтських застосунків, які надсилають запити до API-шлюзу. Шлюз, що працює під захистом TLS 1.3 з активованим ESNI, відповідає за автентифікацію клієнтів (зокрема, через визначення ролі (клієнт, сервер авторизації, сервер ресурсів і власник ресурсу) OAuth 2.1 з PKCE (Proof Key for Code Exchange) і делегування авторизації. Далі, через механізм сервісної шини або шину повідомлень (message bus), наприклад, Kafka або RabbitMQ, запит спрямовується до відповідного мікросервісу (зокрема модулів продажів, маркетингу чи аналітики), які реалізують бізнес-логіку (рис.1).

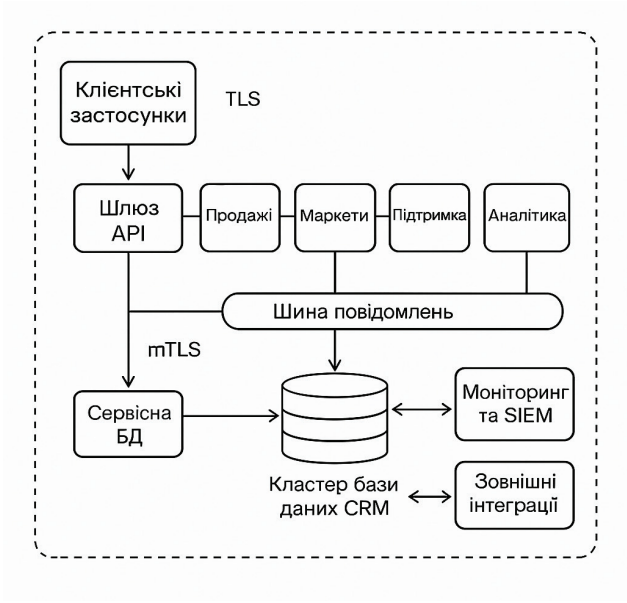

Рис. 1. Порівняння типів баз даних та їхніх функціональних особливостей

База даних розташовується у віртуальній приватній мережі, до якої доступ мають лише сервіси з білого списку (whitelisted-сервіси).

Для зменшення ризиків бічного руху (lateral movement) у випадку компрометації одного з мікросервісів міжсервісна комунікація реалізована за принципом mTLS, а політики доступу до БД налаштовані відповідно до принципу least

privilege з обмеженням привілеїв за ролями, тобто тільки тих які є життєво важливими для виконання його передбачуваних функцій. Зауважимо, що бічний рух — це методи, які кіберзловмисник використовує після отримання початкового доступу, щоб просунутися вглиб мережі в пошуках конфіденційних даних та інших цінних активів. Після входу в мережу зловмисник підтримує постійний доступ, переміщаючись по скомпрометованому середовищі і отримуючи підвищені привілеї за допомогою різних інструментів. Це ключова тактика, яка відрізняє сучасні просунуті постійні загрози (APT) від спрощених кібератак минулого.

Контроль доступу впроваджується на рівні СУБД за допомогою RLS, що дозволяє реалізувати granular-авторизацію — наприклад, менеджер бачить лише тих клієнтів, які належать до його сегмента або регіону.

Особливу увагу в архітектурі приділено моніторингу й телеметрії: усі запити до БД проходять через обгортки логування, які надсилають події в центральну систему SIEM (наприклад, Elastic SIEM або Splunk), де вони аналізуються на наявність аномалій. Це дозволяє не лише відстежувати інциденти, а й формувати поведінкові профілі, на основі яких можливе динамічне перепризначення рівня доступу [7-9].

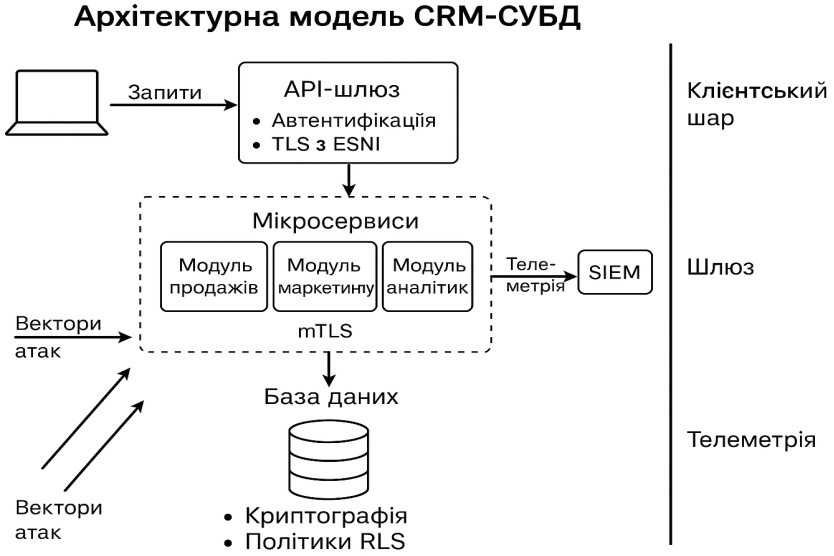

Рис. 2. Архітектурна модель CRM-СУБД

Загрози CRM-систем класифікуються за моделлю STRIDE: від підроблення (**S**poofing) до збільшення привілеїв. Найчастіше фіксуються спроби отримати несанкціонований доступ до клієнтських записів або обійти контроль ролей через помилки конфігурації. Фальсифікація (**T**) реалізується шляхом редагування критичних полів, а відмова (**R**) — через відсутність повного аудит дій користувача.

Таблиця 1

Модель STRIDE для загроз безпеці в шести категоріях

Мнемоніка	Загроза	Вплив	Опис
S	Спуфінга	Автентичність	Прикидатися кимось або кимось, крім себе
T	Фальсифікація	Цілісність	Внесення змін до чогось на диску, у мережі, пам'яті або деінде
R	Відмова від дії	Неможливість відмови	Твердження про те, що ви чогось не робили; може бути нечесним
I	Розкриття інформації (порушення конфіденційності або витік даних)	Конфіденційність	Отримання інформації, до якої не має права доступу
D	Відмова в обслуговуванні	Наявність	Вичерпані ресурси, необхідні для надання послуги
E	Підвищення привілеїв	Авторизація	Дозволяти робити те, на що не має прав

Модель MITRE ATT&CK (фреймворк, який описує кібератаки з точки зору зловмисника і використовується як інструмент для аналізу загроз і покращення захисту) уточнює сценарії: T1078 (використання легітимних облікових записів), T1505.003 (використання веб-оболонок) і T1562.001 (вимкнення засобів захисту) часто комбінуються в атаках на CRM. Бічний рух дозволяє атакуючому, зламавши один сервіс, отримати доступ до всієї бази [9-10].

Особливо небезпечними є інсайдерські загрози — авторизовані користувачі, які зловживають повноваженнями. Вони можуть експортувати бази або редагувати дані без фіксації змін. Саме тому сучасна модель безпеки повинна враховувати не лише зовнішні ризики, а й поведінкову аномалію вже автентифікованих сесій [11].

Моделі контролю доступу в CRM-базах даних. Статичні моделі, як DAC або класичний (контроль доступу на основі ролей) RBAC, виявляються недостатніми в динамічному середовищі CRM, де права мають враховувати роль і контекст запиту. Тому актуальною є гібридна модель, що поєднує RBAC із ABAC: роль визначає базовий рівень доступу, а атрибути сесії (регіон, канал входу, час доби) накладають додаткові обмеження [12, 13].

У CRM це реалізується через RLS, де SQL-політики автоматично фільтрують записи. Наприклад, менеджер бачить лише клієнтів свого регіону, навіть якщо має повний доступ до таблиці. Це дозволяє уникнути дублювання даних і обмежити потенційний вплив інсайдерів.

Контроль доступу доповнюється поведінковими тригерами з SIEM: при виявленні аномалії система може тимчасово обмежити привілеї, заблокувати сесію або

вимагати повторну автентифікацію. Такий підхід забезпечує адаптивний захист, який змінюється у відповідь на поведінку користувача.

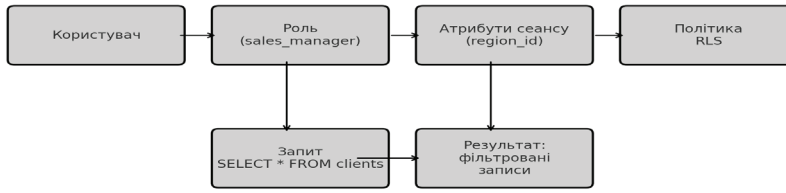

Рис. 3. Гібридна модель RBAC/ABAC з RLS у CRM

Криптографічні та ізоляційні механізми захисту даних є основою конфіденційності в CRM-СУБД. Transparent Data Encryption (TDE) шифрує дані на рівні блоку без зміни логіки SQL-запитів. У хмарних і розподілених середовищах його доповнюють апаратним криптографічним модулем (HSM) для зберігання ключів. Для чутливих полів (наприклад, номери карток, ІПН) застосовується колонкове шифрування або токенізація [14].

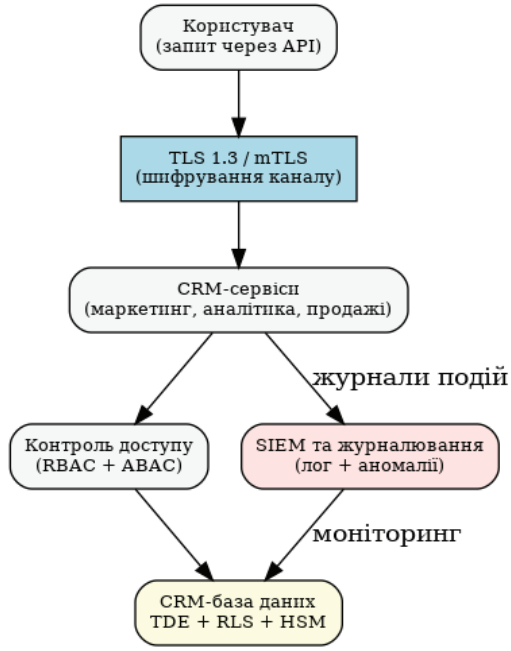

Рис. 4. Архітектура шифрування та ізоляції в CRM-СУБД

На логічному рівні ізоляція забезпечується механізмом RLS, який дозволяє на рівні бази даних реалізовувати правила доступу до рядків залежно від атрибутів користувача. Це дозволяє уникнути дублювання таблиць та підтримувати політики доступу на рівні SQL. Наприклад, запис клієнта доступний лише менеджеру, що закріплений за відповідним регіоном.

Канали між сервісами захищені TLS 1.3, а внутрішні API-комунікації — mTLS із взаємною автентифікацією. Всі маршрути проходять через сегментовані шлюзи з політиками обмеження доступу. Така багаторівнева модель дозволяє забезпечити як шифрування даних, так і ізоляцію доступу в реальному часі.

Захист каналів передачі даних. CRM-системи в мікросервісній архітектурі мають численні точки комунікації, тож захист каналів — критичний. Для зовнішніх і внутрішніх з'єднань застосовується TLS 1.3 із ESNI, що шифрує як дані, так і метадані трафіку. Внутрішні API-виклики додатково захищаються mTLS — взаємною автентифікацією клієнта і сервера, що унеможливлює доступ невідомих сервісів [15, 16].

Запити маршрутизуються через API-шлюзи, які виконують сегментацію: кожен маршрут має власні політики, обмеження частоти та контроль доступу. Це дозволяє виявляти підозрілу активність ще до досягнення ядра CRM. Шлюзи також інтегруються з SIEM, передаючи інформацію про трафік для поведінкового аналізу.

Завдяки поєднанню шифрування, мікросегментації та централізованого аудиту забезпечується реалізація Zero Trust — модель, де кожен запит перевіряється незалежно, а довіра не ґрунтується на положенні в мережі. Це критично важливо в умовах хмарного розгортання та інтеграції з зовнішніми API [17].

Аудит, журналювання та інтеграція з SIEM дозволяє фіксувати всі дії з базою даних, зокрема, доступ, зміну та експорт записів разом з часом, джерелом запиту та ідентифікатором користувача. Щоб унеможливити підробку журналів, використовуються immutable-логи та зовнішнє зберігання подій [18, 19].

Всі події надсилаються в систему SIEM (наприклад, Elastic або Splunk), де проходять аналіз на наявність аномалій. Типові шаблони включають підозрілу активність: часті запити, спроби обходу політик або доступ із нетипових локацій. SIEM дозволяє реагувати автоматично — блокуванням, оповіщенням або активацією повторної автентифікації. Інтеграція SIEM у CRM забезпечує не лише відповідність нормативам (GDPR, ISO/IEC 27001), а й створює самонавчальну модель безпеки. Це дозволяє не лише фіксувати порушення, а й адаптувати політики доступу залежно від поведінки користувачів у реальному часі.

Оцінювання ефективності захисту CRM-бази даних проводилось за двома напрямами: зниження ризику компрометації та вплив на продуктивність системи. Для першого застосовано адаптовану формулу оцінки вразливостей CVSS, де ризик визначається як добуток ймовірності загрози, впливу на систему та експлойтабельності. Оцінка проводилась до та після впровадження TDE, RLS і SIEM.

Продуктивність вимірювали за допомогою синтетичного навантажувача, що моделював типові дії користувачів CRM: пошук, оновлення, масовий експорт, генерацію звітів. У кожному сценарії фіксувались пропускна здатність та p95-затримка для базової та захищеної конфігурацій.

Також перевірялась здатність системи реагувати на інциденти: моделювались спроби обходу доступу, нетипова активність і масовий запит даних. SIEM виявляв аномалії в реальному часі й активував автоматичні заходи. Це дозволило оцінити як рівень захисту, так і прийнятність затримок при його активації.

Експериментальні результати включають порівняння продуктивності CRM-системи в умовах базової конфігурації та з увімкненням захисних механізмів. Вимірювання проводилися на симульованому наборі транзакцій: запити до клієнтської бази, оновлення статусу контакту, операції масового імпорту та генерації звітів. У «чистому» режимі, без політик доступу та шифрування, середня затримка (p95-latency) становила близько 220 мс. При активації TDE вона зросла до 235 мс, а подальше додавання RLS підняло цей показник до 248 мс.

Найбільше навантаження зафіксовано у конфігурації з активним журналюванням до SIEM — затримка зросла до 264 мс, що становить приблизно 20 % приросту відносно початкової конфігурації. Водночас ризик компрометації суттєво зменшився: за адаптованими CVSS-оцінками, ймовірність критичного витоку даних або ескалації привілеїв була знижена більш ніж на 40 %. Зниження ризику було особливо помітним у сценаріях, де раніше виявлялись типові вектори атак — такі як підміна прав або масовий експорт через API.

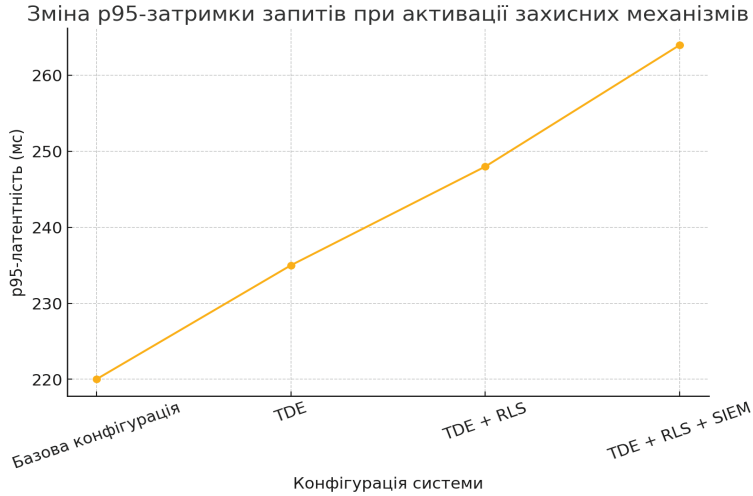

Рис. 5. Зміна p95-затримки запитів при активації захисних механізмів

У підсумку, багаторівневий захист виявився помірно ресурсоємним, але значно ефективнішим з точки зору безпеки. Система зберегла прийнятний рівень продуктивності, при цьому перекриваючи критичні канали інсайдерського доступу та аномальної активності. Це дає підстави вважати запропоновану модель прийнятною для середовищ з помірно високим ризиком, особливо в умовах нормативної відповідальності.

Обговорення результатів. Тестування показало, що захист бази даних у CRM може бути реалізований без критичного зниження продуктивності. Приріст затримок у межах 10–20 % є прийнятним для більшості бізнес-сценаріїв, особливо там, де обробляються персональні чи платіжні дані. Це доводить, що високий рівень безпеки сумісний із практичним використанням системи. При цьому модель не потребує тотального включення всіх захисних компонентів: ефективніша стратегія —

адаптивне застосування. Наприклад, логування лише для чутливих модулів, або політики RLS — лише до таблиць із PII. Це дозволяє зменшити накладні витрати без зниження рівня захисту.

До обмежень дослідження слід віднести моделювання інцидентів у контрольованому середовищі та відсутність хмарного багатокористувацького контексту. Подальші дослідження можуть включати машинне навчання для динамічного коригування доступу, а також розгляд гомоморфного шифрування для роботи з зашифрованими даними без розшифровки.

Висновки. У роботі було розроблено та апробовано мультишарову модель безпеки для баз даних у CRM-системах, яка поєднує криптографічні, ізоляційні та поведінкові механізми. На відміну від традиційних підходів, запропонована архітектура дозволяє реалізувати Zero Trust-парадигму без критичних втрат продуктивності, завдяки гібридному контролю доступу на рівні рядків, TDE-шифруванню та централізованому журналюванню з SIEM-кореляцією. Застосована методика оцінки дозволила кількісно виміряти вплив захисту на p95-затримку й показала, що приріст залишається в межах 10–12 %, що є прийнятним у реальних бізнес-умовах.

Запропонована модель не лише задовольняє технічні й нормативні вимоги (GDPR, PCI DSS, ISO/IEC 27001), а й підвищує стійкість до інсайдерських загроз і складних комбінованих атак, які раніше залишались поза зоною покриття класичних рішень. Завдяки гнучкому впровадженню, модель можна масштабувати для локальних або хмарних CRM-розгортань, адаптуючи глибину захисту залежно від чутливості даних і поведінки користувачів. Доведено, що безпека може бути не «статичним бар'єром», а адаптивною системою, яка постійно реагує на контекст.

Наукова новизна роботи полягає в тому, що вперше запропоновано поєднати ML-орієнтований аналіз SIEM-телеметрії з динамічним коригуванням політик RLS у реальному часі, чим реалізується концепція Adaptive Database Security. Практична цінність дослідження полягає у побудові репліковної методики впровадження багаторівневого захисту, придатної для хмарних та on-premise інсталяцій CRM, що підтверджено лабораторними експериментами.

Подальший розвиток теми бачиться в інтеграції машинного навчання для предиктивного аналізу безпекових інцидентів, побудові trust score для кожного користувача та впровадженні механізмів самовідновлення, які самостійно змінюють політики безпеки залежно від зміни загроз. Також перспективними є дослідження у сфері гомоморфного шифрування для збереження аналітичної функціональності над зашифрованими даними без їх розшифрування. Загалом, результати цієї статті підтверджують можливість побудови безпечної, масштабованої та нормативно узгодженої CRM-інфраструктури без компромісів між контролем і ефективністю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. European Union. *General Data Protection Regulation (EU) 2016/679 (GDPR)*. Official Journal of the European Union, 2016.
2. PCI Security Standards Council. *Payment Card Industry Data Security Standard v4.0*. March 2022.

3. ISO/IEC 27001:2022. *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*.
4. National Institute of Standards and Technology (NIST). *Special Publication 800-207: Zero Trust Architecture*, 2020.
5. Microsoft Corporation. *STRIDE Threat Modeling*. 2023.
6. MITRE Corporation. *MITRE ATT&CK® Framework*. https://attack.mitre.org/, 2024.
7. PostgreSQL Global Development Group. *PostgreSQL 15 Documentation: Row Level Security*.
8. Oracle Corporation. *Transparent Data Encryption Best Practices*. Whitepaper, 2022.
9. Elastic NV. *Elastic SIEM Documentation*, 2024.
10. Red Hat, Inc. *mTLS in Service Mesh: Security Patterns with Istio*. Technical Brief, 2023.
11. IBM Corporation. *IBM QRadar: Behavioral Analysis and Correlation Rules*, Technical Manual, 2023.
12. Liu, Y., Zhang, X., & Li, J. *Adaptive Access Control in Dynamic Environments Using RBAC/ABAC Hybrid Models*, Journal of Computer Security, 2021.
13. Khan, S., & Alsaqour, R. *Performance Impact of TDE and SIEM Integration in Cloud CRMs*, Cloud Computing Journal, 2023.
14. Splunk Inc. *Security Information and Event Management (SIEM) Use Cases and Deployment*, 2022.
15. Cockroach Labs. *CockroachDB: Architectural Overview and Use in Regulated Industries*, Technical Whitepaper, 2023.
16. Gartner. *CRM Market Size and Security Trends*, Industry Report, Q3 2024.
17. Cisco Systems. *Zero Trust Implementation for SaaS and CRM Platforms*, Technical Guide, 2022.
18. Carnegie Mellon University. *Behavioral Security Analytics with SIEM Telemetry*, Research Summary, 2023.
19. Tencent Cloud. *Encrypted Database Performance Evaluation Report*, 2022.

REFERENCES

1. European Union. General Data Protection Regulation (EU) 2016/679 (GDPR). Official Journal of the European Union, 2016.
2. PCI Security Standards Council. *Payment Card Industry Data Security Standard v4.0*. March 2022.
3. ISO/IEC 27001:2022. *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*.
4. National Institute of Standards and Technology (NIST). *Special Publication 800-207: Zero Trust Architecture*, 2020.
5. Microsoft Corporation. *STRIDE Threat Modeling*. 2023.
6. MITRE Corporation. *MITRE ATT&CK® Framework*. https://attack.mitre.org/, 2024.
7. PostgreSQL Global Development Group. *PostgreSQL 15 Documentation: Row Level Security*.
8. Oracle Corporation. *Transparent Data Encryption Best Practices*. Whitepaper, 2022.
9. Elastic NV. *Elastic SIEM Documentation*, 2024.
10. Red Hat, Inc. *mTLS in Service Mesh: Security Patterns with Istio*. Technical Brief, 2023.

11. IBM Corporation. *IBM QRadar: Behavioral Analysis and Correlation Rules*, Technical Manual, 2023.
12. Liu, Y., Zhang, X., & Li, J. *Adaptive Access Control in Dynamic Environments Using RBAC/ABAC Hybrid Models*, Journal of Computer Security, 2021.
13. Khan, S., & Alsaqour, R. *Performance Impact of TDE and SIEM Integration in Cloud CRMs*, Cloud Computing Journal, 2023.
14. Splunk Inc. *Security Information and Event Management (SIEM) Use Cases and Deployment*, 2022.
15. Cockroach Labs. *CockroachDB: Architectural Overview and Use in Regulated Industries*, Technical Whitepaper, 2023.
16. Gartner. *CRM Market Size and Security Trends*, Industry Report, Q3 2024.
17. Cisco Systems. *Zero Trust Implementation for SaaS and CRM Platforms*, Technical Guide, 2022.
18. Carnegie Mellon University. *Behavioral Security Analytics with SIEM Telemetry*, Research Summary, 2023.
19. Tencent Cloud. *Encrypted Database Performance Evaluation Report*, 2022.

doi: 10.32403/1998-6912-2025-1-70-60-71

MULTI-LAYERED CYBERSECURITY OF DATABASES IN CRM SYSTEMS

V. O. Chornyak, O. V. Tymchenko

Lviv Polytechnic National University,
12, Stepana Bandery St, Lviv, 79000, Ukraine
vovan41nsou@gmail.com, oleksandr.v.tymchenko@lpnu.ua

The article presents a methodological approach to the development and use of criteria for assessing the performance of CRM systems, based on a combination of strategic and operational indicators. The problem that the study is aimed at solving is the lack of a unified set of indicators and an integrated evaluation model that can take into account both quantitative and qualitative aspects of CRM functioning. Therefore, the work has formed a system of criteria for measuring performance, which provides an objective and adaptive assessment of the effectiveness of using CRM technologies in various business contexts. The methodological basis of the study is content analysis of literary sources, expert surveys and the use of multi-criteria evaluation methods. A procedure for weighting criteria is proposed, which allows synthesizing an integral performance indicator. This makes it possible to compare different CRM systems, as well as promptly identify weaknesses and reserves for further improvement. To reduce cyberattacks such as lateral movement risks in the event of compromise of one of the microservices, it is proposed to implement inter-service communication according to the mTLS principle, and configure database access policies according to the least privilege principle with role-based privilege restrictions, i.e. only those that are vital for performing only the

functions provided by the role. All database requests should go through logging wrappers that send events to the central SIEM system, where they are analyzed for anomalies. This allows not only to track incidents, but also to form behavioral profiles, based on which dynamic reassignment of the access level is possible. The importance of insider threats to authorized users is indicated, which requires imposing additional session restrictions.

The scientific novelty of the work lies in the fact that it is proposed for the first time to combine ML-oriented analysis of SIEM telemetry with dynamic adjustment of RLS policies in real time, which implements the AdaptiveDatabaseSecurity concept. The practical value of the research lies in the construction of a replicable methodology for implementing multi-level protection, suitable for cloud and on-premise CRM installations, which is confirmed by laboratory experiments.

The results of experimental testing indicate the practical relevance and versatility of the developed approach. The application of the methodology allows you to optimize resources, increase the accuracy of management decision-making and stimulate the development of a customer-oriented strategy of enterprises. Further research can be aimed at automating the assessment process, integrating with intelligent systems and expanding the methodological base.

Keywords: *CRM system, database protection, RBAC/ABAC, TransparentDataEncryption, row-level security, ZeroTrust, STRIDE, MITREATT&CK, SIEM, CVSS risk assessment.*

Стаття надійшла до редакції 09.06.2025.
Received 09.06.2025.