DOI: 10.58254/viti.4.2023.07.82

УДК 004.056(53+57)

д-р техн. наук Субач І. Ю. ORCID: 0000-0002-9344-713X (ІСЗЗІ «КПІ ім. Ігоря Сікорського»)
Власенко О. В. ORCID: 0000-0001-6671-870X (ВІТІ ім. Героїв Крут)

АРХІТЕКТУРА ІНТЕЛЕКТУАЛЬНОЇ SIEM-СИСТЕМИ ДЛЯ ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ У БАЗАХ ДАНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

У статті розглянуто актуальні завдання кіберзахисту баз даних інформаційно-комунікаційних систем. Проаналізовано ефективність поточних заходів щодо захисту баз даних і зроблено висновок, що існуючі системи не враховують багаторівневість захисту, що є критичним аспектом у сфері кібербезпеки. Запропоновано забезпечення кіберзахисту баз даних із використанням інтелектуальних можливостей SIEM-системи. Пропонується новий підхід до архітектури SIEM-системи, який враховує різні рівні контуру захисту інформаційно-комунікаційної системи. Розроблена архітектура надає можливість ефективно виявляти та реагувати на кібератаки на всіх рівнях захисту: від операційної системи до баз даних. Основним аспектом цієї архітектури є багаторівневий захист бази даних, що дозволяє ефективно виявляти та реагувати на кібератаки. Запропонований підхід включає додавання джерел даних із застосунків різних рівнів контуру захисту інформаційно-комунікаційної системи, модуля аналізу даних про події в базі даних, який функціонує на основі застосування методів теорії нечітких множин та нечіткого логічного виводу та модуля кореляції правил для покращення виявлення кіберінцидентів. А також інтеграцію OLAP-технологій для отримання глибокого і аналітичного погляду на стан безпеки бази даних. Запропонована архітектура для виявлення кіберінцидентів дозволяє підвищити ефективність за показником точності виявлення кіберінцидентів, пов'язаних із функціонуванням бази даних інформаційно-комунікаційної системи. Результатом дослідження є покращення можливостей SIEM-системи у виявленні та реагуванні на кіберінциденти у сфері бази даних інформаційної системи військового призначення. Подальшим напрямком досліджень є побудова моделі функціонування системи кіберзахисту бази даних інформаційно-комунікаційної системи.

Ключові слова: *база даних, інформаційно-комунікаційна система, кіберзахист, кіберінцидент, SIEM-система, теорія нечітких множин, нечіткі правила, архітектура SIEM.*

I. Subach, O. Vlasenko Architecture of intelligent SIEM for detecting cyber incidents in databases of military information and communication systems.

The article looks at the current supply of cyber defense to the databases of information and communication systems. The effectiveness of continuous visits to databases is analyzed. The analysis indicates that existing systems are not immune to security, which is a critical aspect in the field of cybersecurity. A new approach to the architecture of the SIEM system is being introduced, which is aimed at different parts of the protection circuit of the information and communication system. The fragmented architecture makes it possible to effectively detect and respond to cyber attacks at all levels of protection, from the operating system to databases. A new approach is being introduced to ensure cyber security of databases with the benefit of the intelligent capabilities of the SIEM system. The main aspect of this architecture is rich database protection, which allows you to effectively detect and respond to cyber attacks. The registration approach includes the addition of data from different levels to the security circuit of the information and communication system, the module for analyzing data about categories in the database, which operates on the basis of The use of fuzzy multiplicity theory methods, fuzzy logic inference and rule correlation module to improve the detection of cyber incidents. And also the integration of OLAP technologies to provide a deep and analytical view of the database security system. The architecture for identifying cyber incidents has been designed to improve the efficiency of identifying cyber incidents related to the functioning of the database of information and communication systems and. The result of the investigation is a reduction in the capabilities of the SIEM system in identifying and responding to cyber identities in the database of the military information system. Further, we directly monitor the operational model of the cybersecurity system of the information and communication system database.

Keywords: *database, information and communication system, cyber protection, cyber incident, SIEM system, fuzzy set theory, fuzzy rules, SIEM architecture.*

Постановка завдання. Існуючі умови ведення кібервійни заставляють державні інститути все більше і більше приділяти увагу кіберзахисту своїх інформаційно-комунікаційних систем (далі – ІКС). Дотримання безпечного функціонування ІКС є однією з головних задач будь-якого підрозділу кіберзахисту. Переважна більшість конфіденційної та

цінної інформації, яка функціонує в ІКС, зберігається в базах даних (далі – БД), тому ядром будь-якої ІКС можна сміливо вважати БД. У БД переважно зберігається службова чи конфіденційна інформація, що робить їх основною ціллю для зловмисників. Кіберзахист БД постійно викликає занепокоєння через витоки даних з ІКС різного походження, які в подальшому набувають широко розголошення. Вторгнення (кібератаки) в БД стали більш складними та перетворилися у форму внутрішніх і зовнішніх вторгнень в комбінованому вигляді, що ускладнює їх виявлення. Зловмисники постійно змінюють тактику кібератак на БД, тому захист даних в ІКС є одним із пріоритетних напрямів кіберзахисту ІКС у цілому.

Отже, вирішення задачі кіберзахисту баз даних стає пріоритетом для будь-якого підрозділу, який оперує значущим обсягом конфіденційної інформації та є актуальною науковою задачею.

Аналіз наукових публікацій. Більшість публікацій розглядають кіберзахист БД виключно додаванням механізмів усунення ризиків безпеки БД до стандартних функцій захисту систем керування базами даних (далі – СКБД), таких як: покращена автентифікація; підзвітність та аудит; контроль доступу; шифрування даних та використання політики висновків [1; 2]. Але в деяких випадках тільки цих механізмів усунення ризиків не достатньо для надійного захисту БД ІКС.

Типова БД може мати 15–20 тисяч підключень на секунду й їх потрібно відслідковувати. Тому для надійної системи кіберзахисту потрібний додатковий елемент, який зможе відслідковувати всі дії, які відбуваються з БД у режимі реального часу, чи наближеного до нього і реагувати на них.

У [3; 4] для покращення кіберзахисту БД запропоновано додавати систему виявлення вторгнень (далі – СВВ) до звичайних механізмів усунення ризиків. СВВ можна вважати однією з найважливіших частин будь-якої добре захищеної системи, оскільки вона має можливість виявляти кібератаки в режимі наближеного до реального часу.

СВВ до БД (далі – СВВБД) – це спеціалізовані програмні або програмно-апаратні рішення, які автоматизують процес моніторингу та аналізу дій, які відбуваються під час роботи з БД за допомогою різних методів інтелектуального аналізу даних. Нині існують два основні підходи до побудови СВВ, а саме: побудова СВВ на основі застосування сигнатурних методів та побудова СВВ на основі методів виявлення аномалій. Відповідно, у проєктуванні архітектури СВВБД дослідники віддають перевагу системам на основі аномалій тому, що вони дозволяють виявляти раніше невідомі види вторгнень (кібератак). Їхня робота, в основному, полягає у створенні на основі шаблонів поведінкового профілю суб'єктів БД, так званих моделей вторгнення. СВВБД визначають, чи є набір певних дій вторгненням шляхом застосування однієї або кількох моделей вторгнень. Модель класифікує послідовність дій як «позитивні» (немає вторгнення) або «негативні» (можливі вторгнення). Даний спосіб захисту БД, у деяких випадках, є більш ефективним ніж застосування сигнатурних методів виявлення вторгнень (кібератак), особливо під час виявлення атак нульового дня, але не завжди дозволяє захистити БД повністю.

Кібератаки, що відбуваються на прикладному рівні, набагато складніше виявляти, оскільки вони дуже часто виглядають як законні запити до БД. Наприклад, виконання складного або складеного запиту. Зловмисники знаходять доступний найбільш ресурсоємний процес і відправляють кілька десятків запитів. Кібератака даного типу спрямована на виснаження ресурсів БД, націлена на надмірне споживання оперативної пам'яті, обчислювальної потужності системи або в деяких випадках – потоку вводу-виводу. СВВБД буде розцінювати дані запити як коректні, тому що вони нічого неправомірного у своїй структурі не містять, і, як наслідок, не зможе виявити кібератаку.

Унаслідок цього, діапазон кібератак на БД є дуже великим і різнобічним. Наприклад, якщо обмежити невдалі спроби аутентифікації, зловмисники можуть заблокувати облікові

записи введенням великої кількості неправильних паролів. В іншому випадку, якщо впроваджувати сервіси автоматичного масштабування для обробки пакетів запитів, зловмисники можуть генерувати фіктивні запити для збільшення масштабу БД, доки вона не зруйнується під "власною вагою", або в хмарному середовищі із вимірюванням досягне порогової суми і, як наслідок цього, відповідна служба буде закрита. Отже, не існує єдиного стандартного вектора кібератаки на БД, а в розпорядженні зловмисників знаходиться цілий арсенал різних технік, тактик і практик порушення штатного функціонування ІКС під час роботи з БД.

Зловмисники можуть використовувати дефекти, націлюючись на певну слабкість систем кіберзахисту ІКС або помилки в конфігуруванні БД (людський фактор). Аналіз літератури та досвід експлуатації ІКС дозволяє зробити висновок про те, що за останні двадцять років спостерігається постійна ретроспективна циклічність виникнення помилок, які дозволяють зловмисникам часто дистанційно та без доступу до облікових даних проводити кібератаки на БД [5; 6].

Відповідно до аналізу щомісячного рейтингу DB-Engines [7] одними з передових СКБД є:

- багатомодельна СКБД Oracle Database, розроблена компанією Oracle[8], яка доступна для локальної роботи, а також роботи у звичайній або гібридній хмарі;
- СКБД Microsoft SQL Server – реляційна СКБД, розроблена компанією Microsoft [9], яка призначена для забезпечення інформаційних потреб різних категорій користувачів (для робочих навантажень, починаючи від невеликих застосунків до великих Інтернет-платформ із багатьма одночасними підключеннями);
- IBM DB2 – це хмарна СКБД, створена для забезпечення транзакцій із низькою затримкою та масштабною аналітикою в реальному часі від компанії IBM[10].

Проведений аналіз показує, що переповнення буфера протягом тривалого часу було основною вразливістю всіх наведених СКБД. Так, десятки атак на переповнення буфера в СКБД Oracle Database виводили БД з ладу, іноді навіть без облікових записів користувача, використовуючи привілеї PUBLIC. СКБД MS SQL Server має власну історію подібних проблем, включаючи вразливість іменованих каналів. Свого часу була зламана СКБД DB2 внаслідок відправки пакетів протоколу UDP.

Якщо розглядати рішення, побудоване на базі багаторівневого підходу до кіберзахисту БД ІКС у рамках СВВБД, то дана система повинна працювати з усіма рівнями захисту БД та відслідковувати всі дії, які відбуваються в екосистемі БД, і збирати дані для аналізу з різних джерел. Але більшість робіт, які присвячені розробці СВВБД [3; 4], зосереджені тільки на аналізі SQL-запитів чи прав доступу користувачів. Самі архітектури запропонованих раніше СВВБД не передбачають роботу з різними різнорідними даними і не розглядають проблему кіберзахисту БД ІКС комплексно. Аналіз літератури [11; 12] показує, що для обробки різнорідних даних, які отримують з багатьох джерел для кіберзахисту будь-якої системи ІКС, краще використовувати технологію, яка ґрунтується на застосуванні SIEM-систем (Security Information and Event Management).

Для покращення і вдосконалення кіберзахисту БД, як важливого елементу ІКС, у роботі [12] запропоновано розглядати систему кіберзахисту БД у контексті багаторівневої архітектури захисту ІКС із вбудованими до неї додатковими структурно-функціональними елементами. Вона повинна базуватись на різних рівнях безпеки, запропонованих у [12]: рівні СКБД та БД, рівні операційної системи та рівні мережі. Консолідація інформації, отриманої з цих рівнів, робить захист БД більш досконалим і ефективним. Цей підхід дозволяє створити багаторівневу систему кіберзахисту БД, де кожен рівень відповідає за конкретні аспекти безпеки БД.

Отже, інформаційна технологія для кіберзахисту БД ІКС, основою якої має бути інтелектуальна SIEM-система, дозволяє збирати дані від різних джерел, аналізувати їх

в реальному часі, виявляти аномальні дії та надавати офіцерам безпеки інформацію, необхідну для здійснення відповідних заходів із кіберзахисту.

Слід зауважити, що системам керування інформацією та подіями безпеки (SIEM-системам) нині приділяється дуже велика увага. У багатьох наукових публікаціях пропонуються покращені механізми роботи SIEM-систем. Дана технологія є дуже актуальною в сучасних наукових дослідженнях.

У [11–15] представлено систематичний огляд поточного стану технології SIEM, а також майбутніх етапів їхнього розвитку. Зроблено висновок, що парадигма технології повільно змінюється від покращення моніторингу/попередження до переведення на міжнародні стандарти, яким мають відповідати всі інструменти безпеки під час кожного внутрішнього чи зовнішнього аудиту, схиляючись до безпеки як послуги, а не до локальних рішень і вдосконаленням механізмів виявлення. Автори пропонують нову структуру, сумісну із загальним регламентом про захист даних (General Data Protection Regulation), використовуючи кілька технологій: блокчейн, шифрування, контейнери та ін.

У [16] наведено виклики та напрямки щодо застосування SIEM-системи у контексті критично важливої системи від компанії в області контролю повітряного руху. Дана система для аналізу видає величезні обсяги неструктурованих текстових журналів. Представлено проблеми, пов'язані з обробкою таких журналів, поточну роботу над інтеграцією SIEM-системи з відкритим кодом і напрямки моделювання базових сценаріїв поведінки системи для визначення індикаторів компромісу.

У [17] зроблено висновок про те, що використання, встановлення та обслуговування SIEM-систем є дуже витратними процесами. Як наслідок, такі системи досі не використовуються на малих і середніх підприємствах (МСП). Запропоновано систему в проєкті SIMU, яка базується на сценаріях застосування для кіберзахисту МСП і націлена на простішу стратегію впровадження. Використання протоколу IF-MAP дозволяє інтегрувати різну інформацію з багатьох компонентів безпеки в одному форматі даних. Вже реалізовані клієнти та відкрита архітектура полегшують включення типових мережевих пристроїв і служб, зменшуючи витрати на управління та інвестиції. Це додатково підтверджується загальною орієнтацією на рішеннях із відкритим кодом.

Використовувати СВВ, інтегровану з SIEM-системою, для створення методів аналізу подій за допомогою машинного навчання пропонують у [18]. У дослідженні для аналізу, виявлення та моніторингу кібератак запропоновано створити систему з використанням найпоширеніших програмних рішень з відкритим кодом. Для створення системи використовується комбінація програмних застосунків Elastic (ELK) Stack, Slips і Zeek IDS. Для підтвердження, що вибрані компоненти правильні та надійні, проведено дослідження, яке зосереджено на вимірюванні продуктивності споживання ресурсів (центрального процесора й оперативної пам'яті).

Так, аналіз публікацій і готових рішень показав, що вектор досліджень в сфері розробки та застосування технології SIEM-систем спрямований на покращення системи в цілому. Моніторинг подій в БД перекладається на відповідні СВВ та інтерфейсні модулі для отримання інформації з них. Висновок про неефективність використання тільки СВВ для захисту БД було зроблено в [12]. Для ефективного опрацьовування подій безпеки потрібна покращена архітектури SIEM-системи з урахування багаторівневої системи захисту БД.

Метою статті є розробка архітектури інтелектуальної системи управління інформацією та подіями безпеки для виявлення кіберінцидентів в БД інформаційної системи військового призначення.

Виклад основного матеріалу дослідження. Внаслідок аналізу бойових дій у кіберпросторі під час першої в світі кібервійни та враховуючи існування різноманітних кіберзагроз, кількість яких постійно збільшується, виникає гостра потреба побудови

ефективної системи кіберзахисту ІКС шляхом розробки та вдосконалення існуючої архітектури SIEM-системи, яка стає важливим фактором захисту ІКС. У цілому, SIEM-система являє собою широкий спектр послуг для одночасного керування інформацією про події безпеки. SIEM-система також забезпечує своєчасний аналіз сповіщень безпеки. Сучасна архітектура системи повинна забезпечувати можливості представлення, аналізу та збору інформації з різнорідних джерел даних [11].

Архітектуру перспективної проактивної SIEM-системи представлено у [11]. Вона є багаторівневою та містить наступні рівні: рівень збору даних (COL), рівень управління даними (CON) та рівень аналізу даних (ANL), а також четвертий рівень (DEC) – рівень прийняття та реалізації рішень.

На відповідних рівнях архітектури важливо мати належні засоби, алгоритми та механізми, які допомагають ефективно виконувати завдання кожного рівня. Аналізуючи основні складові елементи запропонованої архітектури, можна зробити висновок про те, що кіберзахист у цій системі відносно БД не забезпечений повністю, а точніше, вона не відповідає концепції багаторівневого захисту БД відповідно до рівнів та середовища її функціонування [9]. Тому основні структурні рівні даної архітектури потребують вдосконалення.

Основними шляхами удосконалення можуть бути:

- інтеграція SIEM-системи з конкретними зразками СКБД. Дана інтеграція дозволить отримувати дані з журналів роботи СКБД, забезпечуючи при цьому більш глибокий рівень моніторингу подій безпеки;
- розширення можливостей SIEM-системи завдяки імплементації в її архітектуру модулів контекстного аналізу SQL-запитів, що виконуються СКБД та їхнє співставлення з шаблонами злочинної поведінки та відомими вразливостями;
- розробка поведінкових моделей БД для виявлення шаблонів штатної та позаштатної активності. Застосовуючи при цьому технології машинного навчання, можна виявляти аномальну поведінку в БД, наприклад, аномальні або непередбачені запити до неї;
- інтеграція з технологіями інтелектуального аналізу подій, наприклад, UEBA – User and Entity Behavior Analytics, для виявлення аномальної поведінки користувачів, що мають доступ до БД. Це дозволить оперативно виявляти підозрілі дії користувачів, такі як спроби несанкціонованого доступу або несанкціоноване отримання привілеїв;
- інтеграція з технологіями оперативного аналізу даних (OLAP – Online Analytical Processing), що дозволить розширити аналітичні можливості SIEM-системи щодо виявлення та запобігання кіберінцидентам, пов'язаним з БД, що дозволить:

1. Здійснювати розширений аналіз даних. OLAP-технології надають можливість аналізувати великі обсяги даних, накопичених SIEM-системою з різних джерел. У свою чергу, це дозволить здійснювати більш глибокий аналіз подій безпеки, пов'язаних із БД ІКС і виявляти приховані патерни та зв'язки між різними подіями. Це може допомогти у виявленні складних загроз та аномальної поведінки користувачів та програмних застосунків, які не можна отримати іншими методами аналізу.

2. Покращити візуалізацію та звітність. OLAP-технології надають потужні можливості для візуалізації даних та генерації нерегламентованих звітів. Інтеграція даних технологій з SIEM-системами дозволить створювати візуальні панелі, графіки та звіти, адаптовані для аналізу подій у БД, щоб аналітики з безпеки мали можливість наочно надавати інформацію про події та загрози, пов'язані з БД. Це дозволить спростити моніторинг та аналіз стану БД для оперативного та обґрунтованого прийняття рішень щодо виявлення та запобігання кіберінцидентів в них.

3. Розширити можливості запитів для аналітики. OLAP-технології надають великий набір функцій для виконання складних запитів та аналітичних операцій над ними. Їхня інтеграція з SIEM-системою дозволить створювати більш гнучкі й потужні запити для аналізу

подій у БД. Це, відповідно, дозволить виявляти аномальну поведінку користувачів та виявляти аномальні запити до БД або підозрілі зміни в її структурі.

4. Покращити процес виявлення та запобігання кіберінцидентам. За допомогою OLAP-технологій SIEM-системи можуть більш ефективно аналізувати та класифікувати події БД, виявляти аномалії, незвичну поведінку користувачів, а також зв'язок між різними подіями.

5. Підвищити проактивність та прогнозованість. OLAP-технології дозволяють аналізувати великі обсяги історичних даних, що дозволить аналітикам із безпеки виявляти кібератаки, які повторюються або еволюціонують. Крім того, аналітики з безпеки можуть використовувати ці дані для створення моделей та прогнозування майбутніх потенційних кібератак або кіберінцидентів, що дозволить приймати превентивні заходи заздалегідь.

6. Централізувати управління даними. Застосування OLAP-технологій в SIEM-системах дозволить об'єднати дані про події безпеки з різнорідних різнорівневих джерел даних та систем безпеки в єдиному централізованому сховищі даних. Це значно спростить процес аналізу даних та виявлення кібератак і кіберінцидентів, так як аналітики з безпеки будуть мати доступ до повного набору даних про події, що відбуваються під час роботи з БД, який є необхідним для виявлення аномалій та проведення детального розслідування кіберінцидентів.

Отже, інтеграція OLAP-технологій із SIEM-системами для захисту БД може значно покращити процеси виявлення, аналізу та запобігання кіберінцидентів. Вона дозволить здійснювати більш глибокий та комплексний аналіз даних, підвищить оперативність реагування на кіберінциденти, а також сприятиме здійсненню проактивних заходів із захисту БД ІКС.

На рисунку 1 запропоновано удосконалену архітектуру SIEM-системи для виявлення кіберінцидентів у БД ІКС.

Рівень збору даних в архітектурі SIEM-системи дозволяє за допомогою агентів збирати з різнорідних джерел первинні дані про події в системі та здійснювати їхню первинну обробку й фільтрацію [11]. Отримані дані на цьому рівні підлягають процесу нормалізації, який перетворює різноманітні формати даних на стандартизований формат, що використовується в системі. Дані також повинні бути фільтровані для видалення зайвої або несуттєвої інформації.

Отже, для підвищення ефективності захисту БД ІКС в рамках концепції багаторівневого захисту БД виникає необхідність введення до існуючої архітектури SIEM-системи додаткових джерел даних. Перелік типових джерел, які потрібно враховувати при багаторівневому кіберзахисті БД, наведено в таблиці 1.

Таблиця 1

Розподілені джерела для підсистеми багаторівневого кіберзахисту БД

№ з/п	Тип джерела	Опис
1	Журнали подій операційних систем Windows або Linux	Якщо СКБД розгорнута на основі операційних систем (ОС) сімейства Windows, то всі дії, що відбуваються у програмних і апаратних компонентах, підключених до системи, реєструються. ОС Windows за замовчуванням використовує шість категорій журналів для реєстрації подій: журнал додатків, системний журнал, журнал безпеки, журнал служби каталогів, журнал DNS-сервера та журнал сервера реплікації файлів. Якщо СКБД функціонує в середовищі ОС Linux-подібній ОС, то є можливість знайти часову шкалу подій, пов'язаних з ядром, сервером і програмними застосунками. Дані записуються в журнали, враховуючи чотири основні категорії: журнали подій, журнали служб, журнали програм і системні журнали. Наприклад, у каталозі */var/log/syslog* зберігаються загальні журнали активності системи, а в */var/log/auth.log* – журнали автентифікації та авторизації
2	Журнали брандмауера	Містять деталі невдалих входів до системи, відхилені IP-адреси, вихідні маршрутизовані пакети і дії з внутрішніх серверів
3	Журнали вебсерверів	Аналіз записів журналів вебсервера надає можливість зрозуміти, які кінцеві користувачі взаємодіють із вебресурсами, що працюють з відповідними БД

№ з/п	Тип джерела	Опис
4	Журнали застосунків	Використовуються для відстеження подій, які розробники вставляють у програми
5	Журнали СВВБД	Містять дані про події в БД, які отримуються під час аналізу синтаксису запитів до СКБД та поведінкового профілю користувачів БД
6	Журнали СКБД	Містять дані з журналів подій в СКБД. Наприклад, у СКБД MySQL основних журналів чотири: Error Log (стандартний журнал помилок, які виникають під час роботи сервера); Binary Log (журнал всіх команд зміни БД, необхідний для реплікації та бекапів); General Query Log (основний журнал всіх запитів); Slow Query Log (журнал повільних запитів)
7	Журнали мережі	Містять інформацію про такі події, як зловмисний трафік, зниження пропускної здатності, скидання пакетів та інші докази підозрілої активності

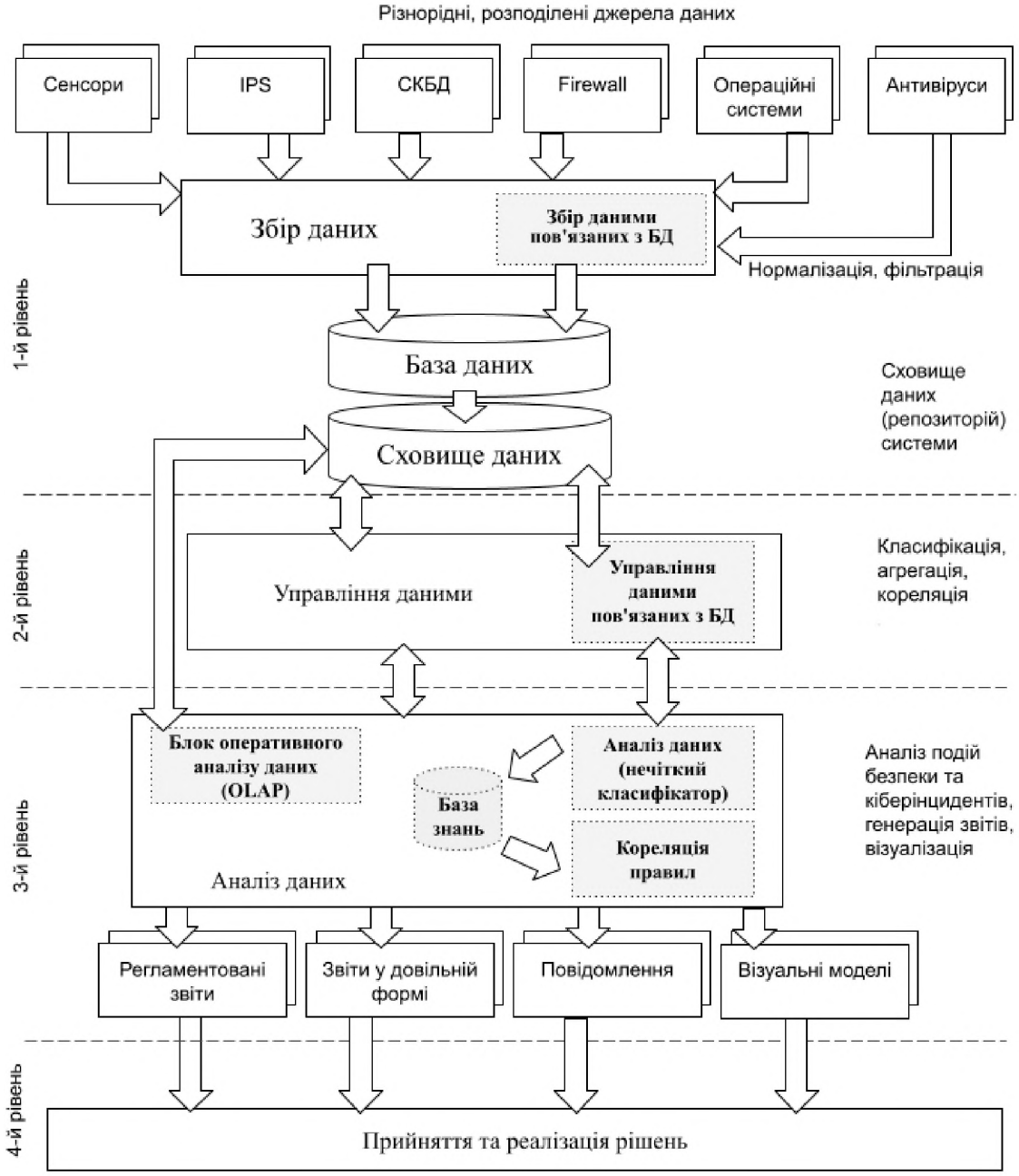

Рис. 1. Удосконалена архітектура інтелектуальної SIEM-системи для виявлення кіберінцидентів в БД ІКС

Для отримання даних із різнорідних, розподілених джерел необхідно мати набір агентів, які дозволяють зчитувати дані з них. Вони складаються з інтерфейсу доступу до певного джерела та самої інформації для передачі в SIEM-систему. Журнали роботи тих чи інших компонент ІКС є безпосередньо джерелами даних для отримання інформації про події безпеки.

Сховище даних повинно забезпечувати структуроване зберігання даних про події безпеки, у тому числі пов'язані з БД, та підтримувати інтеграцію з різними джерелами даних. Для ефективного аналізу подій безпеки, які відбуваються під час роботи з БД ІКС, доцільно використовувати інформацію з розподілених джерел про події, пов'язані з нею.

Рівень управління даними стосується всіх даних про події безпеки, які зберігаються у сховищі даних SIEM-системи та які надходять як початкові дані до механізмів їхнього аналізу. Він включає виконання таких функцій, як класифікація, агрегація та пріоритезація. Класифікація, агрегація та пріоритезація дозволяють системі обробити інформацію, отриману з різних джерел, і надають контекст для ефективного аналізу та прийняття рішень щодо безпеки. Ці функції також дозволяють отримати найважливішу інформацію з різноманітних подій і повідомлень для її подальшої обробки.

У модулі *управління даними, пов'язаними з БД* (CONDB), відбувається пріоритезація подій у рамках БД, а також їх класифікація та агрегація. Агрегація даних, пов'язаних з БД, дозволяє зменшити кількість подій, що відображаються шляхом зведення пов'язаних подій до одного представлення. Наприклад, події, пов'язані з одним користувачем, можуть буди агреговані в одну подію або групу. Класифікація даних дозволяє визначити типи подій або інцидентів на основі їхніх характеристик або атрибутів, а також допомагає представити події в структурованій формі для подальшого аналізу та обробки. Функція пріоритезації встановлює рівень важливості для кожної події, пов'язаної з БД, на основі потенційного впливу на безпеку БД.

Рівень аналізу даних відіграє ключову роль у забезпеченні безпеки та виявленні загроз у системі. Його основне завдання – обробка та аналіз великого обсягу подій безпеки, журналів, сповіщень та інших даних, що надходять до SIEM-системи. На ньому використовуються різні техніки аналізу даних для виявлення аномалій, кореляції подій і забезпечення ефективного моніторингу та реагування на безпекові інциденти. Для успішного виявлення кібератак на БД до рівня аналізу даних необхідно інтегрувати модуль аналізу даних (наприклад, нечіткий класифікатор) та модуль кореляції правил.

Особливого розгляду заслуговує застосування методів теорії нечітких множин та лінгвістичних змінних для виявлення та класифікації кіберінцидентів, пов'язаних з БД ІКС. Оскільки в теорії нечітких множин об'єкти можуть мати часткову приналежність до визначеної множини, на відміну від традиційної логіки, де об'єкт або належить до певної множини або – ні, то це дозволяє враховувати невизначеність (неповноту, обмеженість) та розмитість (нечіткість) даних, які можуть виникати під час аналізу кіберінцидентів. Відповідно, це дозволяє створювати нечіткі правила і моделі, які враховують різні рівні впевненості аналітиків із безпеки в процесі виявлення кіберінцидентів. Наприклад, можна застосовувати нечіткі правила, які грунтуються на лінгвістичних змінних для того, щоб визначити степінь підозрілої активності в БД або ризику виникнення кіберінциденту.

Крім того, методи теорії нечітких множин дозволяють знизити рівень хибних спрацьовувань системи та покращити точність виявлення кіберінцидентів. Вони можуть враховувати контекстні фактори, аналізувати відхилення від нормальної поведінки з врахуванням неоднозначності даних, що дозволяє покращити ефективність SIEM-системи у процесі виявлення кіберінцидентів [13].

Модуль аналізу даних (нечіткий класифікатор) (ANLDB) використовує методи теорії нечітких множин та лінгвістичних змінних для обробки та аналізу подій, що відбуваються

у БД. Функціональним призначенням цього модуля є виявлення аномалій під час роботи з БД для ідентифікації кіберінцидентів в ній.

Основні характеристики модуля аналізу даних про події в БД SIEM-системи, робота якого ґрунтується на методах теорії нечітких множин, включають:

- застосування нечітких правил. Модуль використовує нечіткі правила для опису аномалій та патернів поведінки в БД. Ці правила повинні містити лінгвістичні змінні та операції над ними для визначення рівня відповідності події або шаблону;
- використання нечіткої логіки для виявлення аномалій. За допомогою нечіткої логіки модуль може визначати, наскільки певна подія або група подій є аномальною в контексті роботи з БД. Використовуючи нечіткі операції, модуль може враховувати неоднозначності та невизначеності, що можуть виникати під час аналізу подій у БД;
- моделювання патернів поведінки. Модуль може використовувати нечітку логіку для моделювання типових патернів поведінки користувачів (програмних застосунків) під час роботи з БД. При цьому повинні враховуватися різні фактори, такі як типи запитів, часові затримки, обсяги даних та інші атрибути, для виявлення незвичайної або підозрілої активності;
- гнучкість та адаптивність. Робота модуля повинна бути гнучкою та адаптивною до змін у БД. Він повинен навчатися на основі нових даних та оновлювати нечіткі правила і моделі для забезпечення ефективної аналітики роботи інфраструктури кіберзахисту в змінному середовищі.

Застосування методів теорії нечітких множин та нечіткої логіки у модулі аналізу даних SIEM-системи допомагає покращити ефективність виявлення кіберінцидентів під час роботи з БД ІКС в умовах неповноти та неточності інформації, знижує кількість помилкових спрацювань та дозволяє більш гнучко моделювати складні сценарії аналізу даних для кіберзахисту.

База знань містить нечіткі правила для ідентифікації кіберінцидентів, у тому числі під час роботи з БД ІКС.

Модуль кореляції ознак (COLANALDB) використовується для виявлення зв'язків та взаємозв'язків між різними правилами, які були сформульовані та завантажені у БД SIEM-системи для аналізу подій під час роботи з БД ІКС.

Основна мета роботи модуля кореляції правил полягає в тому, щоб ідентифікувати складні кібератаки/кіберінциденти, які можуть бути непомітними під час аналізу окремих правил. У ньому аналізуються ознаки кіберінцидентів (враховуючи багаторівневість системи захисту БД) і виявляються зв'язки (кореляції) між різними подіями або шаблонами, що можуть вказувати на складні кіберінциденти/кібератаки.

Модуль кореляції ознак виконує наступні функції:

- виявлення зв'язків (кореляцій). Модуль аналізує різні правила аналізу даних про події в ІКС під час роботи з БД та відшукує спільні атрибути, взаємозв'язки або закономірності між ними. Наприклад, він може виявити, що певні події, які здавалися незначними при окремому аналізі, коли комбінуються з іншими подіями, можуть свідчити про спробу ознаки злому або несанкціонованого доступу;
- формування комплексних подій. На основі знайдених зв'язків модуль може створювати комплексні події, які включають декілька правил аналізу. Ці комплексні події можуть бути використані для виявлення більш складних кібератак або шаблонів поведінки, які не можуть бути виявлені окремими правилами;
- пріоритезація та реагування. Модуль кореляції може також допомогти у визначенні пріоритетності виявлених комплексних подій безпеки. На основі цього модуля можна визначити, які дії або заходи безпеки потрібно прийняти для запобігання кібератакам та запобігання або зменшення їхніх наслідків.

Загалом, модуль кореляції правил допомагає збільшити ефективність аналізу подій в БД ІКС шляхом виявлення складних кібератак/кіберінцидентів, які можуть бути непомітними при звичайному аналізі.

Отже, для ефективного кіберзахисту БД ІКС модель перспективної проактивної SIEM-системи [11] можна вдосконалити для виявлення складних кібератак/кіберінцидентів, що відбуваються під час роботи саме з БД ІКС, шляхом імплементації до неї елементів, які реалізують принцип багаторівневості кіберзахисту БД (1):

$$M_{SIEM} = \langle COL, CON, ANL, DEC \rangle, \quad (1)$$

де $COL = \langle \{LEV\}_{l=1}^{m}, \{PUR\}_{i=1}^{n}, NOR, NORBD \rangle$ – підсистема збору та обробки даних з різнорідних джерел: $\{LEV\}_l$, $l = \overline{1,m}$, – множина рівнів кіберзахисту БД ІКС; $\{PUR\}_{il}$, $i = \overline{1,n}; l = \overline{1,m}$, – множина модулів (конекторів) завантаження даних із різнорідних джерел даних із різних рівнів кіберзахисту БД ІКС; *NOR* – модуль нормалізації даних (приведення різних форматів даних до єдиного формату для зберігання); NORDB – модуль нормалізації та селекції даних, пов'язаних із подіями під час роботи з БД;

$CON = \langle FIL, CLS, AGR, COR, CONDB \rangle$ – підсистема керування даними: *FIL* – модуль фільтрації даних (видалення неважливих даних для аналізу); *CLS* – модуль класифікації подій на заздалегідь визначені класи; *AGR* – модуль агрегації подій до більш узагальненого рівня; *COR* – модуль кореляції подій (знаходження взаємозв'язків між різними подіями), *CONDB* – підсистема керування подіями, пов'язаними з БД, що включає фільтрацію, агрегацію, класифікацію та пріоритезацію;

$ANL = \langle MDL, PRI, \{GEN\}_{m=1}^{l}, \{VIZ\}_{p=1}^{q}, BOLAP, ANLDB, CORANLDB \rangle$ – підсистема аналізу даних: *MDL* – модуль моделювання кібератак і кіберінцидентів та їх прогнозування; *PRI* – модуль пріоритезації (визначення важливості подій безпеки); $\{GEN\}_m$, $m = \overline{1,l}$, – множина модулів генерації регламентованих та нерегламентованих звітів; $\{VIZ\}_p$; $p = \overline{1,q}$ – множина модулів візуалізації даних; *BOLAP* – блок оперативного аналізу даних; *ANLDB* – підсистема аналізу даних, пов'язаних із БД; *CORANLDB* – модуль кореляції нечітких правил;

DEC – підсистема прийняття на реалізації рішень.

Слід зауважити, що застосування методів теорії нечітких множин та нечіткої логіки у модулі аналізу даних про події у БД ІКС дозволяє виявляти кіберінциденти у БД, забезпечуючи при цьому більш гнучку аналітику подій безпеки. Крім того, завдяки модулю кореляції нечітких правил SIEM-система стає більш ефективнішою у виявленні складних кібератак на БД ІКС.

Висновки. У цій статті було розглянуто проблематику кіберзахисту БД в ІКС військового призначення.

Аналізуючи сучасні тенденції та потенційні загрози, було запропоновано підхід до багаторівневого захисту БД на рівнях СКБД і БД, операційної системи та мережі. Окрім цього, у статті була розглянута архітектура інтелектуальної SIEM-системи, яка доповнюється додатковими блоком оперативного аналізу даних (OLAP), модулями аналізу даних і кореляції ознак для ефективного виявлення та запобігання кіберінцидентам. Цей підхід дозволяє покращити рівень безпеки та надійності БД в умовах постійно зростаючих загроз кібербезпеці.

Враховуючи актуальність та постійно зростаючу складність кіберзагроз, введення запропонованого підходу та архітектури SIEM-системи в практику військових ІКС є кроком у напрямку надійного та ефективного кіберзахисту важливих даних та ресурсів.

Перспективним напрямком подальших досліджень є побудова моделі функціональної системи кіберзахисту БД ІКС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A. Mousa, M. Karabatak, and T. Mustafa Database Security Threats and Challenges, *in 2020 8th International Symposium on Digital Forensics and Security (ISDFS).* 2020: IEEE. P. 1–5. DOI: 10.1109/ISDFS49300.2020.9116436.

2. Ramyar A. Teimoor A. Review of Database Security Concepts, Risks, and Problems. *UHD Journal of Science and Technology*. 2021. Vol. 5, no. 2. P. 38–46. DOI: 10.21928/uhdjst.v5n2y2021.

3. M. I. Khan, S. N. Foley, B. O'Sullivan. Database Intrusion Detection Systems (DIDs): Insider Threat Detection via Behavioural-based Anomaly Detection Systems – A Brief Survey of Concepts and Approaches. *Emerging Information Security and Applications.* 2022. P. 178–197. DOI: 10.1007/978-3-030-93956-4.

4. R. G. Santos, J. Bernardino, M. Vieira. Approaches and Challenges in Database Intrusion Detection. *ACM SIGMOD Record*. 2014. Vol. 43, no. 3. P. 36–47. DOI: 10.1145/2694428.2694435.

5. S. Rathore, A. Sharma Database Security - Attacks, Threats and Challenges. *International Journal of Engineering Research & Technology (IJERT), ICCCS*, 2017. Vol. 5, no. 10. ISSN: 2278-0181.

6. Database Denial of Service: Attacks. *Blog.* URL: https://securosis.com/blog/database-denial-of-service-the-attacks (дата звернення: 03.06.2023).

7. DB-Engines Ranking // Knowledge Base of Relational and NoSQL Database Management Systems. URL: https://db-engines.com/en/ranking (дата звернення: 02.06.2023).

8. Oracle Database Documentation URL: https://docs.oracle.com/en/database/ (дата звернення: 05.06.2023).

9. Microsoft SQL documentation URL: https://learn.microsoft.com/uk-ua/sql/?view=sql-server-ver16 (дата звернення: 05.06.2023).

10. Db2 database product documentation URL: https://www.ibm.com/support/pages/db2-database-product-documentation (дата звернення: 05.06.2023).

11. І. Субач, В. Кубрак, А. Микитюк. Архітектура та функціональна модель перспективної проактивної інтелектуальної системи SIEM-системи для кіберзахисту об'єктів критичної інфраструктури. *Information Technology and Security.* 2019. № 7 (2). P. 208–215. DOI: https://doi.org/10.20535/2411-1031.2019.7.2.190570.

12. І. Субач, О. Власенко. Інформаційні технології захисту баз даних від кібератак в інформаційних системах військового призначення". *Information Technology and Security.* 2022. № 10 (2). P. 177–193. DOI: https://doi.org/10.20535/2411-1031.2022.10.2.270412.

13. І. Субач, В. Фесьоха. Модель виявлення аномалій в інформаційно-телекомунікаційних мережах органів військового управління на основі нечітких множин та нечіткого логічного виводу. *Зб. наук. праць ВІТІ*. 2017. № 3. С. 158–164. URL: http://nbuv.gov.ua/UJRN/Znpviti_2017_3_21.

14. І. Ю. Субач, В. В. Фесьоха, Н. О. Фесьоха. Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі, відкритих на основі загальнодоступних ліцензій. *Information technology and security*. 2017. Vol. 5, iss. 1. Pp. 29–41. DOI: https://doi.org/10.20535/2411-1031.2017.5.1.120554.

15. López Velásquez J. M., Martínez Monterrubio S. M., Sánchez Crespo L. E. et al. Systematic review of SIEM technology: SIEM-SC birth. *Int. J. Inf. Secur.* 2023. DOI: https://doi.org/10.1007/s10207-022-00657-9.

16. M. Cinque, D. Cotroneo, A. Pecchia. Challenges and Directions in Security Information and Event Management (SIEM). *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, Memphis, TN, USA, 2018. Pp. 95–99. DOI: 10.1109/ISSREW.2018.00-24.

17. K.-O. Detken, T. Rix, C. Kleiner, B. Hellmann, L. Renners. Siem approach for a higher level of it security in enterprise networks. In Proc. IDAACS, Warsaw, Poland, 2015. P. 322–327.

18. Muhammad, Adabi & Sukarno, Parman & Wardana, Aulia. Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning. *Procedia Computer Science.* 2023. Vol. 217. P. 1406–1415. DOI: 10.1016/j.procs.2022.12.339.