МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

УДК 004.056.5
DOI: https://doi.org/10.37734/2409-6873-2021-2-18

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ БАЗАХ ДАНИХ

Н. В. АНТОНЕНКО
кандидат економічних наук, доцент,
Національний транспортний університет
М. С. ГРАБОЛЮК
студентка факультету менеджменту, логістики та туризму,
Національний транспортний університет
Н. О. Семенченко
студентка факультету менеджменту, логістики та туризму,
Національний транспортний університет

Анотація. Мета *статті полягає у дослідженні наявних проблем у забезпеченні захисту баз даних в інформаційних системах.* ***Методика дослідження.*** *Для досягнення поставленої мети були використані методи логічного узагальнення та наукової абстракції.* ***Результати.*** *У процесі аналізу проблем безпеки розглянуто моделі захисту баз даних. Проаналізовано процедури ідентифікації осіб, їх аутентифікації та авторизації в базах даних. Доведено, що рольова модель захисту баз даних є найбільш прийнятною для застосування в сучасних СУБД. Сформульовано заходи щодо побудови доступних систем захисту серверів, що спеціалізуються на обробці великих масивів даних.* ***Практична значущість результатів дослідження.*** *Відзначено, що використання на практиці запропонованих моделей безпеки дасть змогу підвищити результативність заходів щодо забезпечення захисту баз даних в інформаційних системах.*

Ключові слова: *захист інформації, база даних, інформаційна безпека, безпека даних, захист даних, несанкціонований доступ.*

Постановка проблеми в загальному вигляді та зв'язок із найважливішими науковими чи практичними завданнями. Завдання гарантування захисту інформації позиціонується як одне з найважливіших під час побудови вивіреної інформаційної структури на базі програмно-керованого пристрою для обробки інформації. Розглянута проблема включає в себе як фізичний захист встановлених на комп'ютері програм і створених баз даних, так і програмний захист, що передбачає відмову у несанкціонованому доступі до інформації, переданої лініями зв'язку і розташованої на запам'ятовуючому пристрої. Таким чином, розроблення заходів захисту інформації в сучасних базах даних необхідне для виключення будь-якого втручання сторонніх осіб, вірусів і зловмисних програм у роботу комп'ютерних комплексів.

Аналіз останніх досліджень і публікацій. Теоретичні аспекти проблем захисту даних у сучасних інформаційних системах були розглянуті у роботах таких учених, як Н.В. Чернухіна [1], В.М. Матвіюк [1], В.В. Єрохін [2], Д.О. Погонишева [2], І.Г. Степченко [2], С.М. Смірнов [3], С.Д. Кузнєцов [4], М.А. Полтавцева [5], О.М. Горбачевська [6], К.О. Турхановська [7], С.В. Філько [8; 9], І.В. Філько [8; 9]. Незважаючи на значну кількість наукових праць, присвячених питанням захисту інформації в сучасних базах даних, загалом спостерігається дефіцит методичних розробок, теоретичних та методологічних напрацювань, які стосуються забезпечення фізичного і програмного захисту корпоративних систем від несанкціонованого доступу.

Формування цілей статті (постановка завдання). Основною метою написання статті є висвітлення проблем гарантування безпеки баз даних та визначення дієвих шляхів розвитку систем захисту інформації від розголошення, витоку і несанкціонованого доступу.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Згідно з даними аналітичного центру InfoWatch, за минулі 13 років у всьому світі з комерційних компаній і державного сектору витекло приблизно 44 млрд записів персональних даних, з них близько 14 млрд записів тільки за останній рік [10]. Відомо, що більше 60% таких атак влаштовані безпосередньо співробітниками організацій, а із залученням зовнішніх порушників – понад 30% [8; 9]. Зрозуміло, що саме атаки на бази даних та сховища – одна з найголовніших небезпек для будь-якої організації або підприємства. Також потрібно відзначити, що сім з восьми витоків, що становлять понад десять мільйонів записів, спричинені зовнішніми атаками [8].

Відомості, які знаходяться на збереженні в базах даних різного обсягу або в корпоративних сховищах, стають найчастішими об'єктами уваги зловмисників. Вони цікавляться персональними даними співробітників, наявною інформацією про клієнтів, замовників,

конкурентів. Також під прицілом у них знаходиться вся внутрішня операційна інформація, інтелектуальна власність, платіжна та фінансова інформація.

Здебільшого в наших реаліях поширені дослідження у сфері забезпечення безпеки баз даних, що орієнтовані на опрацювання вже відомих нам вразливих частин, за високої потребі захищеності не лише конкретних комунікацій, а й операційних систем та компонентів інфраструктури, які разом створюють додаткові перешкоди при спробах злому. Проте нині потрібна реалізація основних моделей доступу, а також аналіз специфіки конкретних систем управління базами даних, оскільки розробники часто розглядають не все програмне забезпечення підприємства чи організації, а лише конкретний програмний продукт.

У сфері безпеки СУБД нині існує досить мало досліджень щодо конкретних методів захисту, які задовольняють сучасні вимоги до інформаційної безпеки програмних рішень і дають змогу цілісно поглянути на проблему захисту від несанкціонованого доступу до бази даних (БД).

Усі методи захисту інформації в системах управління базами даних можна об'єднати у дві великі групи. До першої групи методів – основних методів захисту – відносять: захист записів і полів таблиць баз даних; захист паролем; шифрування; розділення прав доступу до об'єктів БД [3]. Як додаткові засоби захисту БД використовують методи забезпечення цілісності зв'язків таблиць; вбудовані засоби контролю даних; методи організації спільного використання об'єктів баз даних у мережі [5].

Найбільш популярним і простим способом захисту баз даних від будь-якого *доступу* до *інформації* з порушенням посадових повноважень є захист інформаційного середовища паролем. Паролі створюються безпосередньо користувачами, а доступ до необхідної інформації надається адміністраторами. Паролі зберігаються у спеціальних зашифрованих файлах СУБД. Перевагою захисту інформації СУБД паролем є те, що це найпростіший метод захисту інформації в системах управління базами даних, який не вимагає спеціальних знань у користувачів і адміністраторів і не потребує ніяких витрат на своє впровадження. Проте захист баз даних паролем має низку недоліків, до яких можна віднести його вразливість під час зберігання в СУБД у незашифрованому вигляді і неможливість використання, якщо користувач з якихось причин не записав або не запам'ятав його.

До більш ефективного, ніж пароль, методу захисту баз даних від несанкціонованого доступу відноситься процес шифрування, який передбачає перетворення інформації в непридатний для використання вигляд шляхом застосування певного алгоритму шифрування. При цьому обов'язковим є застосування одного або двох ключів залежно від того, який спосіб шифрування використовується – симетричний чи асиметричний. У симетричному кодуванні для шифрування і для дешифрування використовується один і той самий ключ. При асиметричному способі шифрування застосовуються два ключі, один із яких – секретний, а другий – несекретний. Несекретний ключ призначений для шифрування і разом з адресою користувача публікується у відкритому доступі, тоді як другий ключ, секретний, відомий тільки одержувачу і бере участь у процесі дешифрування. За допомогою шифрування досягається повна безпека баз даних, яка передбачає дотримання конфіденційності, цілісності і доступності СУБД.

Досить дієвим методом захисту баз даних від несанкціонованого доступу до інформаційного середовища є розділення між користувачами прав доступу до об'єктів БД, що дає змогу різним спеціалістам здійснювати певні дії над об'єктами СУБД. Якщо власник об'єкта, а також адміністратор баз даних наділені усіма правами, то решта користувачів мають тільки ті права доступу до об'єктів, які їм надані системними адміністраторами.

Доцільно зазначити, що прогрес у створенні систем безпеки БД залежить від появи нових типів і видів загроз, оскільки зміни інформаційного середовища відбуваються постійно відповідно до етапів створення моделей БД – від розроблення основної комплектації програмно-керованого пристрою для обробки інформації до залучення хмарних сховищ. Оцінюючи конструкцію захисту, потрібно звернути увагу на заходи, що підвищують рівень безпеки, серед яких:

– обмеження доступу до серверів БД, які обслуговують користувачів;

– поділ засобами системи управління БД усіх користувачів на довірених і частково довірених;

– автоматизація та контроль аудиторської перевірки лог-файлів, що містять дані про дії користувачів у БД;

– маскування даних за допомогою шифрування;

зміна засобів аутентифікації, які були використані в СУБД, для забезпечення багаторівневості в операційні системи і проміжному програмному забезпеченні;

– відмова від послуг адміністратора даних, який має повну довіреність.

Проте будь-яке нововведення, яке протистоїть конкретним загрозам, не може вирішити проблему загалом. Різнорідність рішень породжує конкуренцію, в результаті чого суттєво відрізняється комплекс заходів безпеки у кожного розробника у цій сфері. Компанії намагаються вкладати великі суми коштів у забезпечення безпеки власних баз даних, проте відсутність комплексного підходу до розроблення дієвої системи підтримки безпеки інформаційного простору зменшує їхні можливості попередити загрози втручання кіберзлочинців, які постійно розробляють нові способи атак. Відсутність єдиного та загальноприйнятого підходу ускладнює перспективу розроблення захисних механізмів від майбутніх кібератак. Потребує актуалізації також уся система підготовки спеціалістів із безпеки, бо постає питання щодо компетентності персоналу, який розуміється лише на давно відомих способах порушення захисту баз даних.

На думку авторів статті, найбільшої уваги все ж потребують роботи, в яких наведені ідеї випередження атак та розроблення програмних засобів, орієнтованих на перспективу застосування захисних можливостей системи бази даних.

Проаналізувавши дані за п'ять останніх років, що описують відомі прецеденти з порушення безпеки, а також ті, що містять інформацію про способи забезпечення безпеки СУБД, а також характеризують сучасні інтерфейси та архітектуру баз даних, можна говорити про наявність однакових найбільш вразливих місць у

захисті сховищ в різних системах захисту баз даних. Нині причинами вищезазначеного явища є загальновизнані факти, а саме:

– лише досить великі виробники на професійному рівні задаються проблемами безпеки в кінцевих продуктах систем для зберігання даних;

– спеціалісти, що мають доступ до БД (прикладні програмісти, адміністратори тощо), не ставлять питання безпеки інформаційного середовища на перше місце серед завдань, які вони виконують;

– під час використання систем захисту існує потреба в отриманні інформації щодо відповідності масштабів витрат на захист даних та цінності збережених даних;

– навіть базуючись на одній й тій самій моделі безпеки даних, різноманітні СУБД користуються різними мовними діалектами для забезпечення доступу до даних;

– існує потреба в постійній актуалізації інформації про нові моделі і способи зберігання даних [3; 5].

Щоб отримати конкретні результати, необхідно детальніше розглянути вищезгадані положення, взявши до уваги, наприклад, лінійки продуктів від американської корпорації Oracle. Оскільки зазначена компанія – найбільший розробник програмного забезпечення у світі, СУБД Oracle Database Server включає в себе добре розвинену систему безпеки [6]. Вона містить як основні, так і додаткові модулі, а також включає в себе засоби маскування даних, що ставить її продукцію на більш високий рівень порівняно з розробками інших компаній.

Розглянемо три моделі безпеки баз даних, що використовуються для організації доступу до таблиць та її полів: дискреційну, мандатну і рольову моделі. Дискретний доступ представлений матрицею доступу або списками управління доступом, які щодо кожного об'єкта БД містять переліки користувачів і дозволених операцій.

Відомо, що під час побудови дискреційного управління доступом до бази даних застосовується одна з трьох моделей безпеки – децентралізована, централізована або змішана, причому саме змішана модель найчастіше застосовується в СУБД. Мандатна модель безпеки баз даних призначена для запобігання будь-якому небажаному впливу суб’єктів на комп’ютерні процеси та системні пристрої. За допомогою мандатного керування доступом (англ. Mandatory access control, MAC) адміністратор мережі централізовано контролює користувачів, щоб унеможливити перевизначення ними політики доступу до файлів. Для надання прав доступу суб’єктам адміністратор мережі використовує низку категорій конфіденційності, які передбачають приписування міток стовпцям таблиці БД і подальшу передачу їх користувачам. Мандатна модель може ефективно використовуватися тільки разом із дискреційною.

Виборне управління доступом, при якому права доступу суб'єктів системи на об’єкти групуються і утворюють ролі, називається рольовою моделлю організації доступу до таблиць та її полів. Під час застосування цієї моделі захисту баз даних використовується матриця доступу і динамічні правила розмежування доступу, які визначають роль користувача і порядок його дій під час роботи в системі БД. Рольова модель забезпечує найвищий рівень безпеки організації доступу до БД за рахунок чіткого визначення ролей адміністратора і користувача баз даних на читання, зміну, запис і видалення об’єктів. Рольова технологія управління доступом настільки потужна і гнучка, що дає змогу застосовувати як дискретне, так і мандатне управління доступом до БД.

Далі розглянемо методи забезпечення безпеки сховища інформації. Незалежними від змісту і складу даних можна назвати такі запити до безпечної системи БД:

– Діяльність у довіреному середовищі.

До довіреного інформаційного середовища відноситься комплекс захисних механізмів, які дають змогу опрацьовувати інформацію без порушення політики безпеки. У цьому разі СУБД працює у довіреній інформаційній системі з належними способами обміну даними.

– Формування фізичної безпеки джерела даних.

Це питання вимагає більш докладного дослідження, оскільки використані в деяких моделях СУБД дані можуть впливати на процес шифрування і захист інформації.

– Побудова безпечного і сучасного налаштування СУБД.

До названого аспекту мають стосунок такі питання забезпечення безпеки, як вчасне встановлення оновлень, відключення незастосовуваних модулів або використання продуктивної політики паролів.

– Організація безпечних інтерфейсів та звернень (у тому числі врахування інтерфейсу СУБД і системи доступу до інформації).

– Надійне формування даних і операцій над ними.

Перейдемо до розгляду сутності таких програмно–технічних засобів безпеки, як аутентифікація та ідентифікація. Ідентифікація й аутентифікація є головними методами захисту інформаційного простору компанії або товариства. Ідентифікація – процес розпізнавання абонента в системі, зазвичай шляхом попередньо визначеного імені (ідентифікатора) чи будь-якого іншого теоретичного повідомлення про нього, яке сприймається системою. Згадане поняття, безсумнівно, означає встановлення особи користувача. Аутентифікація – операція підтвердження приналежності користувачеві даних у системі заявленого ним ідентифікатора. Шляхом аутентифікації система пересвідчується в тому, що суб’єкт саме той, за кого себе видає. Нині є кілька методів ідентифікації й аутентифікації користувачів. У кожного з них є певні плюси і мінуси, внаслідок чого поодинокі технології можуть бути використані в різних СУБД. Проте сьогодні немає однозначного рішення щодо умови застосування тих або інших методів ідентифікації та аутентифікації користувачів. З огляду на вищезазначене, розробники програмного забезпечення і користувачі баз даних самостійно приймають рішення про визначення способу ідентифікації у своїх СУБД.

Відомо про два найчастіше уживаних типи ідентифікації [7]:

– парольна ідентифікація, за якої будь-який зареєстрований користувач системи отримує комплекс індивідуальних реквізитів;

– апаратна ідентифікація – названий тип ідентифікації базується на визначенні особи користувача за надійним предметом, ключем, який знаходиться в його винятковому користуванні.

Способи аутентифікації умовно поділяються на однофакторні і двофакторні. У свою чергу однофакторні способи об'єднують логічні методи аутентифікації (фрази, що пишуться з клавіатури); ідентифікаційні методи (представниками загального інформування є фізичні об'єкти) та біометричні методи (використовують аналіз виняткових якостей людини).

Надійність аутентифікації та ідентифікації зменшується під дією низки причин. По-перше, комп'ютерна система обробляє інформацію у тому вигляді, в якому була отримана: інакше кажучи, осередок інформації залишається анонімним. По-друге, практично всі аутентифікаційні відомості можуть бути вкрадені або підроблені. Також є неузгодженість між користувачами і системними адміністраторами з питань встановлення правил вводу інформації до бази даних.

Висновки із зазначених проблем і перспективи подальших досліджень у цьому напрямі. Розглянувши всі наявні методи і засоби захисту даних у БД, можна зробити висновок про те, що застосування виключно якогось одного методу не може забезпечити повного збереження інформації. З огляду на це, для покращення рівня безпеки даних у БД пропонується застосовувати комплексні заходи, що включають як програмно–технічні засоби безпеки, так і адміністративні методи, до яких відносять захист записів і полів таблиць баз даних; захист паролем; шифрування; розділення прав доступу до об'єктів БД. Узагальнюючи вищенаведене, можна відзначити, що перспективами подальших досліджень у напрямі створення надійних систем захисту баз даних є гармонізація й удосконалення існуючих методів захисту інформаційного середовища шляхом розроблення методик уніфікації механізмів захисту, систематизації вразливостей СУБД і формалізації сучасних моделей захисту даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Чернухина Н.В., Матвиюк В.М. Основные аспекты информационной безопасности при работе в компьютерных сетях. *Новые парадигмы общественного развития: экономические, социальные, философские, политические, правовые, общенаучные тенденции и закономерности* : материалы междунар. науч.-практ. конф. (Новосибирск – Тихорецк – Саратов, 28 декабря 2015 года). Новосибирск, 2016. С. 122–123.

2. Ерохин В.В., Погонышева Д.А., Степченко И.Г. Безопасность информационных систем : учебное пособие. Москва, 2015. 184 с.

3. Смирнов С.Н. Безопасность систем баз данных. Москва, 2007. 352 с.

4. Кузнецов С.Д. Базы данных: учебник. Москва, 2012. 496 с.

5. Полтавцева М.А., Зегжда Д.П., Супрун А.Ф. Безопасность баз данных: учеб. пособие. Санкт-Петербург, 2015. 125 с.

6. Горбачевская Е.Н., Катьянов А.Ю., Краснов С.С. Информационная безопасность средствами СУБД Oracle. *Вестник ВУиТ*. Тольятти. 2015. № 2 (24). С. 72–85.

7. Турхановская К.А., Орлова Ю.А. Нечеткая модель для логического вывода при определении класса защищенности информационных систем управления предприятием. *Известия Волгоградского государственного технического университета.* Волгоград. 2016. № 7 (186). С. 110–115.

8. Филько С.В., Филько И.В. Информационная безопасность ERP-систем. *Учет, анализ, аудит: проблемы теории и практики*. Красноярск. 2016. Вып. 17. С. 115–119.

9. Филько С.В., Филько И.В. Анализ подходов к оценке рисков информационной безопасности в корпоративных информационных системах. *Учет, анализ, аудит: проблемы теории и практики.* Красноярск. 2016. Вып. 17. С. 120–124.

10. Скандал! Цифра? Дія… Юридична газета online. URL:https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/skandal-cifra-diya.html (дата звернення: 18.10.2021).

REFERENCES

1. Chernuhina N.V., Matviyuk V.M. (2016) Osnovnyie aspektyi informatsionnoy bezopasnosti pri rabote v kompyuternyih setyah [The main aspects of information security when working in computer networks]. *Novyie paradigmyi obschestvennogo razvitiya: ekonomicheskie, sotsialnyie, filosofskie, politicheskie, pravovyie, obschenauchnyie tendentsii i zakonomernosti:* materialyi mezhdunarodnoy nauchno-prakticheskoy konferentsii [New paradigms of social development: economic, social, philosophical, political, legal, general scientific trends and patterns: materials of the international. scientific-practical conf]. Novosibirsk (pp. 122–123). (in Russian)

2. Erohin V.V., Pogonyisheva D.A., Stepchenko I.G. (2015). *Bezopasnost informatsionnyih sistem* [Information Systems Security]. Moscow. (in Russian)

3. Smirnov S.N. (2007) *Bezopasnost sistem baz dannyih* [Database systems security]. Moscow. (in Russian)

4. Kuznetsov S.D. (2012) *Bazyi dannyih* [Databases]. Moscow. (in Russian)

5. Poltavtseva M.A., Zegzhda D.P., Suprun A.F. (2015) *Bezopasnost baz dannyih [Database Security].* St. Petersburg [in Russian].

6. Gorbachevskaya E.N., Katyanov A.Yu., Krasnov S.S. (2015). Informatsionnaya bezopasnost sredstvami SUBD Oracle [Information security of Oracle DBMS]. *Vestnik VUiT – VUiT Bulletin*, no. 2 (24), pp. 72–85. (in Russian)

7. Turhanovskaya K.A., Orlova Yu.A. (2016) Nechetkaya model dlya logicheskogo vyivoda pri opredelenii klassa zaschischennosti informatsionnyih sistem upravleniya predpriyatiem [Fuzzy model for logical inference when determining the security class of enterprise management information systems]. *Izvestiya Volgogradskogo gosudarstvennogo tehnicheskogo universiteta* [Bulletin of the Volgograd State Technical University], no. 7 (186), pp. 10–115. (in Russian)

8. Filko S.V., Filko I.V. (2016) Informatsionnaya bezopasnost ERP – sistem [Information security ERP]. *Uchet, analiz, audit: problemyi teorii i praktiki* [Accounting, analysis, audit: problems of theory and practice], no. 17, pp. 115–119. (in Russian)

9. Filko S.V., Filko I.V. (2016) Analiz podhodov k otsenke riskov informatsionnoy bezopasnosti v korporativnyih informatsionnyih sistemah [Analysis of approaches to assessing information security risks in corporate information systems]. *Uchet, analiz , audit: problemyi teorii i praktiki* [Accounting, analysis, audit: problems of theory and practice], no. 17, pp. 120–124. (in Russian)

10. Skandal! Tsifra? DIya… [Scandal! Digit? Action…]. *Yuridichna gazeta online* [Legal newspaper online]. Retrieved from https://yur-gazeta.com /publications /practice/ informaciyne-pravo- telekomunikaciyi/skandal-cifra-diya.html (accessed 18 October 2021). (in Ukrainian)

Н. В. Антоненко, М. С. Граболюк, Н. О. Семенченко, *Национальный транспортный университет.* ***Проблемы защиты информации в современных базах данных.***

Аннотация. Цель *статьи заключается в исследовании имеющихся проблем в обеспечении защиты баз данных в информационных системах.* ***Методика исследования.*** *Для достижения поставленной цели были использованы методы логического обобщения и научной абстракции.* ***Результаты.*** *В процессе анализа проблем безопасности рассмотрены модели защиты баз данных. Проанализированы процедуры идентификации лиц, их аутентификация и авторизация в базах данных. Доказано, что ролевая модель защиты баз данных является наиболее приемлемой для применения в современных СУБД. Сформулированы меры по построению доступных систем защиты серверов, специализирующихся на обработке больших массивов данных.* ***Практическая значимость результатов исследования.*** *Отмечено, что использование на практике предложенных моделей безопасности позволит повысить результативность мероприятий по обеспечению защиты баз данных в информационных системах.*

Ключевые слова: *защита информации, база данных, информационная безопасность, безопасность данных, защита данных, несанкционированный доступ.*

Nadiia Antonenko, Marina Grabolyuk, Natalia Semenchenko*, National Transport University.* ***Problems of information protection in modern databases.***

Annotation. The purpose *of the article is to study the existing problems in ensuring the protection of databases in information systems.* ***Methodology of research.*** *Methods of logical generalization and scientific abstraction were used to achieve this goal.* ***Results.*** *The urgency of ensuring the protection of all modern corporate systems from unauthorized access has been confirmed. In the process of analyzing security problems, database protection models are considered. It is also noted that there are two groups of methods of information protection in database management systems: the first – protection of records and fields of database tables; password protection; encryption; separation of access rights to database objects, the second – methods to ensure the integrity of table relationships; built-in data control tools; methods of organizing the sharing of database objects in the network. Both positive and negative aspects of key methods of combating unauthorized access to databases are revealed. The main security models that ensure the confidentiality of information are studied, as well as the procedures for identification of persons, their authentication and authorization in databases are considered. The stages of evolution of information protection in database management systems (DBMS) are considered. Modern complex problems of theoretical and practical character at creation of system of protection of databases are allocated. It is proved that the role model of database protection is the most acceptable for use in modern DBMS. Measures have been formulated to build affordable server security systems that specialize in processing large data sets.* ***Findings.*** *It is determined that the prospects of further research in the direction of creating reliable database protection systems are harmonization and improvement of existing methods of information environment protection by developing methods of unification of protection mechanisms, systematization of DBMS vulnerabilities and formalization of modern data protection models.* ***The practical significance of the research results.*** *The use in practice of the proposed security models will increase the effectiveness of measures to ensure the protection of databases in information systems.*

Keywords: *information protection, database, information security, data security, data protection, unauthorized access.*