DOI: 10.25140/2411-5363-2022-3(29)-102-113
УДК 004.65

Марина Ларченко
кандидат юридичних наук, доцент, студентка ІІ курсу магістратури ОП Кібербезпека
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: urlinka2006@gmail.com. **ORCID:** https://orcid.org/0000-0002-2643-980X
ResearcherID: X-9681-2018

СУЧАСНІ ПРОБЛЕМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ БАЗ ДАНИХ

Україна перебуває на етапі впровадження європейських стандартів захисту інформації, однак подальшого вдосконалення потребує програмна складова її захисту. Криптографічний захист баз даних може використовувати шифрування даних, які вже потім (після шифрування) зберігаються у файлі, а також шифрування безпосередньо каталогів і файлів. Підхід до захисту баз даних має бути комплексним. Так, шифрування не можна використовувати для вирішення проблем контролю доступу. Водночас застосування добре налаштованої програми криптографічного захисту, яка використовує надійний алгоритм, здатне суттєво підвищити цілісність, конфіденційність та доступність інформації бази даних.

Ключові слова: *безпека баз даних; захист персональних даних; криптографічний захист; ключ; алгоритм шифрування.*
Табл.: 1. Бібл.: 22.

Актуальність теми дослідження. Бази даних сьогодні використовуються всюди. Вони вміщують різноманітну інформацію, що підлягає захисту. За змістом інформація поділяється на: інформацію про фізичну особу; інформацію довідково-енциклопедичного характеру; інформацію про стан довкілля (екологічна інформація); інформацію про товар (роботу, послугу); науково-технічну інформацію; податкову інформацію; правову інформацію; статистичну інформацію; соціологічну інформацію та інші види (Закон України «Про інформацію» ст. 10). За порядком доступу інформація поділяється на відкриту та з обмеженим доступом (ч. 1 ст. 20). Інформацією з обмеженим доступом, у свою чергу, є конфіденційна, таємна та службова інформація. Зокрема, конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом (ст. 21) [1].

Постановка проблеми. Захист інформації є необхідним для підтримки таких її властивостей, як цілісність (неможливість модифікації інформації неавторизованим користувачем), конфіденційність (інформація не може бути отримана неавторизованим користувачем) та доступність (авторизований користувач може використовувати інформацію відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу).

Загрозами безпеці інформації є: знищення, модифікація, блокування, несанкціонований доступ, витік, розголошення. Зокрема, криптографічний захист баз даних дозволяє попередити доступ до інформації, яку вони містять, за допомогою математичних перетворень повідомлення. Йдеться передусім про запобігання несанкціонованій модифікації та несанкціонованого розголошення інформації.

Очевидно, що постійно зростає складність самих даних та функцій створюваних баз даних, відповідно змінюються і методи атак зловмисників, удосконалюються самі технології, а традиційні методи не завжди відповідають вимогам часу. У сучасному інформаційному світі бази даних щоденно зазнають серйозних загроз їхній безпеці, що стало можливим через розвиток комп'ютерних мереж, наявності технічних прорахунків та з інших причин. Інциденти безпеки завдають значних збитків власникам баз даних в усьому світі, тому дослідження їх безпеки, зокрема криптографічного захисту, є актуальними.

Аналіз останніх досліджень та публікацій. Питанням криптографічного захисту баз даних приділяли чимало уваги вітчизняні та закордонні науковці. Так, Є. Б. Лопін провів ґрунтовне дослідження часових показників шифрування/дешифрування файлів

баз даних медичних інформаційних систем [10]. Ю. В. Борсуковський та В. Ю. Борсуковська досліджували конкретні прикладні аспекти захисту аутентифікаційних даних клієнтів у базах [7]. О. Войтович та І. Микитюк описали метод захисту баз даних шляхом багатошарового користувацького доступу [11]. С. А. Антоненко досліджував криптографічні основи застосування електронного цифрового підпису в Україні [14].

Виділення недосліджених частин загальної проблеми. Проведений аналіз останніх досліджень і публікацій показав, що ці та інші роботи стосуються окремих аспектів криптографічного захисту інформації. Також багато досліджень українських науковців зосереджені переважно у сфері правового регулювання захисту баз даних в Україні. Закордонні ж дослідження здебільшого мають порівняльний або ознайомлювальний характер щодо застосовуваних у світі криптографічних алгоритмів. Натомість в умовах зростаючої цифровізації економіки бази даних зазнають дедалі більших ризиків порушення конфіденційності, цілісності та доступності, бо завжди є той, хто бажає реалізувати вторгнення заради досягнення якоїсь своєї мети. Тому необхідною є розробка сучасних способів боротьби із загрозами безпеці баз даних.

Метою статті є виокремлення актуальних проблем криптографічного захисту баз даних та окреслення деяких шляхів їх вирішення.

Виклад основного матеріалу. Основними джерелами загроз для баз даних є наступні: неефективний захист інформації, аномальні користувачі (незаконна поведінка, несанкціонований доступ), ненадійна технічна система захисту та зовнішні атаки. Загрози базам даних можна також поділити на кілька категорій: фальшування (підміна) даних, розкриття даних, відстежування (збір) даних [2].

Одним з найбільш проблемних правових питань в умовах розвитку цифрового суспільства та економіки є захист персональних даних. Глобалізація та цифровізація призвели до того, що дані користувача однієї країни можуть використовувати треті особи з іншої країни (у тому числі незаконно). Вітчизняні дослідники наголошують, що цифрова інформація, яка вміщена в базах даних, стала активом з високою доданою вартістю: зловмисне використання персональних даних та дезінформаційні кампанії мають високий потенціал для дестабілізації суспільства [3].

Постановою Кабінету Міністрів України № 1109 від 9 жовтня 2020 року [4] затверджено перелік секторів (підсекторів), основних послуг критичної інфраструктури України, де серед інших зазначений інформаційний сектор з типами основних послуг, серед яких: 1) надання хмарних послуг, у тому числі зберігання та обробки даних у центрах обробки даних та/або хмарних сховищах, здійснення хмарних обчислень; 2) забезпечення функціонування систем електронного урядування; 3) надання електронних довірчих послуг; 4) забезпечення функціонування систем електронної ідентифікації; 5) електронні комунікації.

Державна служба спеціального зв'язку та захисту інформації рекомендує, крім іншого, для захисту баз даних: відключити віддалений доступ до інформаційних систем або переглянути коло співробітників, яким надано право віддаленого доступу до інформаційних систем, впроваджувати максимальні обмеження (фільтрація за IP, протоколами, часом доступу, користувачами тощо; застосовувати тільки надійно захищені методи віддаленого доступу та протоколи для адміністрування інформаційних систем та ресурсів, що мають належний рівень шифрування; використовувати стійкі паролі, налаштувати багатофакторну автентифікацію та забезпечити надійне збереження автентифікаційних даних [5].

У такий спосіб увага держави більше концентрується на запобіганні (що включає як недопущення та профілактику порушень конфіденційності, так і припинення дій, що вже мають місце в кіберпросторі) кіберінцидентам та кібератакам на бази даних, які включені до об'єктів критичної інфраструктури країни та усіх інших, від яких напряму залежить функціонування важливих секторів економіки.

Зокрема, Постановою Кабінету Міністрів України від 23 грудня 2020 р. № 1295 затверджено Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки [6] визначає засади функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, які здійснюються щодо об'єктів кіберзахисту, визначені частиною другою статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» [7]. Втім, дія цього Порядку не поширюється на об'єкти критичної інформаційної інфраструктури Міноборони та Збройних Сил в умовах надзвичайного і воєнного стану.

Об'єктами кіберзахисту відповідно до згаданого Закону є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів і військових формувань, утворених відповідно до закону;

2) об'єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

06.07.2010 р. Україна ратифікувала Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додатковий протокол до неї [8]. Цим самим Україна взяла на себе зобов'язання забезпечити дотримання прав і свобод людини, зокрема, право на недоторканність приватного життя, передбаченого ст. 8 Конвенції про захист прав людини і основоположних свобод та гарантованого ст. 32 Конституції України.

Також в Україні питання захисту персональних даних регулюється Законом України «Про захист персональних даних», який набрав чинності у 2011 р. та встановлює вичерпний перелік підстав обробки персональних даних (ст. 11) [9].

Також принципи обробки персональних даних (відкритість і прозорість, відповідальність, адекватність, не надмірність їх складу та змісту стосовно визначеної мети обробки), а також підстави для обробки персональних даних (згода суб'єкта персональних даних) сформувала Велика Палата Верховного Суду. Судді звернули увагу на те, що законодавством не врегульоване питання щодо наслідків відмови особи від обробки її персональних даних, тобто фактично відсутня будь-яка альтернатива такого вибору, що обумовлює низьку якість закону та порушення конституційних прав особи.

Заслуговує на увагу розгляд основних положень Директиви 2016/680 Європейського Парламенту та Ради ЄС від 27.04.2016 р. про захист фізичних осіб стосовно обробки персональних даних компетентними органами для цілей запобігання, розслідування, виявлення або переслідування кримінальних злочинів або виконання кримінальних покарань та про вільне переміщення таких даних, а також Загального Регламенту ЄС щодо захисту персональних даних (General Data Protection Regulation – GDPR) (Регламенту (ЄС) 2016/679 Європейського парламенту та Ради від 27.04.2016 р. про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних) [10]. Цей Регламент був прийнятий з метою приведення законодавства Європейського Союзу у сфері захисту персональних даних у відповідність до вимог «цифрової епохи» та на виконання Стратегії Єдиного Цифрового Ринку Європи (Digital Single Market Strategy).

Цими документами внесені такі новації в законодавство країн-членів ЄС:

- «право бути забутим» - право вимагати знищення усіх персональних даних після того, як закінчився термін їх обробки;
- право особи знати про злами баз персональних даних та їх наслідки;
- право на перенесення персональних даних: фізичні особи можуть переносити свої персональні дані при зміні провайдерів послуг;

- право притягнення до жорсткої відповідальності за порушення вимог до захисту персональних даних.

GDPR встановлює більш суворі правила до згоди на опрацювання персональних даних: обов'язок довести її наявність прямо покладається на того, хто їх збирає. Також посилено критерії до поінформованості суб'єктів персональних даних, встановлено, що інформація про те, як дані збираються та використовуються, має надаватись у стислій, прозорій, доступній формі. Обов'язок доводити факт дотримання ключових вимог щодо опрацювання персональних даних покладається на суб'єкта, який їх збирає (презумпція вини організації-порушника). Варто зауважити, що саме впровадження європейських стандартів з регулювання захисту персональних даних наблизить Україну до повної інтеграції та до Єдиного Цифрового Ринку ЄС [3].

Крім правових проблем захисту баз даних, у всьому світі існує гостра проблема їх програмного захисту.

Yong Wang, Jinsong Xi, Tong Cheng у 2021 році опублікували глобальне дослідження загроз базам даних, що існують у сучасному цифровому просторі, а також проаналізували 76 опублікованих матеріалів досліджень, що містять різноманітні практичні рішення більш-менш ефективного усунення цих загроз. Класифікація цих загроз та рішень може бути наведена в табличному вигляді [2]:

Таблиця – Класифікація загроз базам даних та відповідних їм рішень

Загрози першого рівня	**Загрози другого рівня**	**Ушкодження**	**Рішення**
1	2	3	4
Дані не захищені ефективно	Фальшування даних	Дані викривлені або недійсні	Виявлення несанкціонованого доступу, аутентифікація користувача, шифрування даних
	Розкриття даних	Незаконне використання даних користувача	Аутентифікація користувача, аудит, побудова моделі машинного навчання
	Дані відстежуються або збираються	Порушення конфіденційності, розкриття	Створення спеціальної системи шифрування даних
Виключення користувача	Незаконний акт	Порушення рольового кодексу поведінки	Виявлення вторгнень, створення спеціальної системи аналізу поведінки користувачів
	Несанкціонований доступ	Незаконна обробка даних	Контроль доступу
	Слабка обізнаність про безпеку	Створюються шпарини для зловмисників	Проведення емпіричних досліджень та навчання персоналу
Вразливість системи захисту	Помилка ідентифікації	Використовується для знищення бази даних	Проведення оцінки рівня безпеки, застосовується емпірична основа
	Неточна ідентифікація	Відхиляються звичайні користувачі, але приймаються нелегальні	Аутентифікація користувача
Зовнішня атака	Спам	Займає багато місця, вчиняються шахрайські дії	Контроль доступу
	Шкідливий трафік	Сервер працює ненормально	Аудит, виявлення вторгнень
	SQL-ін'єкція	Впровадження троянського коня, незаконне привласнення прав	Контроль доступу, аналіз поведінки користувачів, прогнозування системних ризиків

Закінчення табл.

1	2	3	4
	Незаконний доступ	Зламування механізму аутентифікації системи та отримання даних	Аутентифікація користувачів, створення спеціальної системи виявлення вторгнень
	Шкідливе ПО	Незаконний доступ до секретних даних користувачів	Шифрування даних, виявлення шкідливого ПО, виявлення вторгнень
	DDoS-атака	Недоступність системних функцій	Виявлення вторгнень, контроль доступу
	Обхід та фізична атака	Пошкодження обладнання та інше	Виявлення вторгнень, перепони для захисту від несанкціонованого вторгнення

Державні установи та приватні компанії з кожним роком витрачають дедалі більше коштів на захист баз даних. Це відбувається з таких причин. Перша з них – це кіберзлочини. Так, постійно удосконалюються інструменти зловмисників, усе більш витонченими стають методи соціальної інженерії, з'являються безфайлові способи проникнення. Зокрема, згідно з оприлюдненими дослідженнями у світі лише у 2019 році було розкрито понад 9 млрд облікових записів, що містять персональну інформацію [11]. В Україні згідно зі Звітом роботи системи виявлення вразливостей Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації у 2021 році зафіксовано більше 300 000 випадків несанкціонованого доступу до інформації та більше 250 000 випадків несанкціонованої її модифікації [5]. Ця тенденція закріпилась також і у 2022 році [12].

З іншого боку, дедалі більше загострюється так звана проблема відповідності. Міжнародне законодавство щодо захисту персональної інформації ставить більше вимог до України, яка готується стати повноправним членом ЄС. Відповідальність за збереження даних покладається на організації та установи, які займаються їх збором. Це також необхідно з метою збереження конкурентоспроможності на міжнародному ринку.

Очевидно, що для ефективного захисту баз даних мають застосовуватись такі (мінімальні) вимоги з інформаційної безпеки.

1. Повинен бути забезпечений захист аутентифікаційних даних від використання сторонніми особами і зменшена ймовірність їх компрометації.

2. Ресурс повинен бути захищеним від стороннього доступу.

3. Повинен бути зручний і оперативний доступ до паролів.

4. Усі аутентифікаційні дані (логіни, паролі, URL і т.д.) повинні зберігатися в одній захищеній базі даних.

5. Логіни і паролі повинні зберігатися в зашифрованому вигляді, база даних повинна повністю шифруватися.

6. Для доступу до бази даних повинен використовуватися майстер-пароль і додаткові засоби захисту.

7. База даних повинна зберігатися на захищеному носії.

8. Відносно невисокою має бути загальна вартість рішення.

9. Процеси використання аутентифікаційних даних повинні бути, по можливості, максимально автоматизовані.

10. Повинна бути забезпечена можливість перевірки аутентифікаційних даних на витік до хакерських баз даних [13].

Крім цього, бажаним для суб'єктів використання баз даних є функції: 1) апаратного шифрування; 2) відновлення паролю без ризику для даних; 3) створення зашифрованої і захищеної паролем резервної копії даних на комп'ютері, NAS або хмарі; 4) портативне

рішення безпеки для обміну даними, яке дозволяє легко зашифрувати файли, щоб ділитися ними з колегами і партнерами; 5) можливість встановити час і дату, по спливанні яких дані на пристрої будуть автоматично знищені; 6) швидкість переміщення даних; 7) захист від брутфорс-атаки; 8) антивірусний захист; 9) здатність до оновлення [13].

Окреслені проблеми так чи інакше вирішуються шляхом застосування різних технологій, окремі з яких заслуговують на підвищену на увагу. Їхня ефективність прямо залежить від конфігурації бази даних і сервера, на якому вона функціонує, від того, наскільки правильно спроєктована і реалізована IT-інфраструктура і топологія мережі в цілому, від людського фактору і лояльності персоналу. Атаки на вебсервери і на сервери баз даних часто переслідують ті ж самі цілі, запускаються тими самими особами і мають схожий характер. Тому і захист інформації в базах даних будується на використанні рішень, що мають схожі принципи роботи й архітектуру. Серед безлічі засобів захисту баз даних можна виділити основні й додаткові.

До основних засобів захисту інформації в базах даних відносять наступні:

- парольний захист;
- захист полів і записів таблиць бази даних;
- встановлення прав доступу до об’єктів бази даних;
- шифрування даних і програм.

До додаткових засобів захисту бази даних можна віднести такі, які, по суті, ними не є, але безпосередньо впливають на безпеку даних. Це:

- вбудовані засоби контролю значень даних відповідно до їх типів;
- підвищення достовірності даних, що вводяться;
- забезпечення цілісності зв’язків таблиць;
- організація спільного використання об’єктів баз даних у мережі.

Зокрема, аналіз прийнятих у світі підходів до розробки комплексних систем захисту баз даних показує, що окрім технічних (апаратних) пристроїв (приладів) та відповідних організаційних заходів ефективним є використання програмно-технічних засобів захисту інформації, у тому числі засобів криптографічного захисту інформації або, говорячи простою мовою, програмного забезпечення, призначеного для шифрування даних [14]. При цьому може використовуватись як шифрування даних, які вже потім (після шифрування) зберігаються в файлі, так і шифрування безпосередньо каталогів та файлів.

Загалом шифрування – це кодування даних із використанням спеціального алгоритму, внаслідок чого дані стають недоступними для читання будь-якою програмою, що не має ключа дешифрування. Якщо в системі разом з базою даних міститься важлива конфіденційна інформація, то має сенс закодувати її з метою попередження можливостей несанкціонованого доступу із зовні (по відношенню до СУБД). Тому деякі СУБД містять засоби шифрування, призначені для таких цілей, а відповідні підпрограми забезпечують санкціонований доступ до даних (після їх декодування). Шифрування також може використовуватися для захисту даних при їх передачі по лініях зв'язку.

На думку Є. Б. Лопіна, з якою варто погодитись, зберігання в базах даних зашифрованої числової, символьної (текстової) та іншої інформації значно обмежуватиме можливості її автоматизованої обробки та використання з пошуковою метою SQL-запитів, внаслідок чого більш доцільним у деяких випадках може бути використання саме шифрування файлів баз даних. Дослідник, розглядаючи часові показники шифрування/дешифрування файлів баз даних медичних інформаційних систем, пропонує використання симетричного криптографічного алгоритму Blowfish [15].

Зокрема, автором пропонується три послідовності дій, які відрізняються часовими затратами. Для зчитування-запису файлів в усіх трьох послідовностях використовувались стандартні функції Delphi FileRead та FileWrite, виділення пам'яті здійснюється функцією AllocMem, копіювання - CopyMemory, безпосередньо шифрування здійснюється під час виконання (роботи) процедури EncryptBlowFish l.

Під час роботи першої послідовності дій здійснюється зчитування з вихідного файлу (з дескриптором FileHandle_1) блоків по 8 байт до області пам'яті Buffer (перемінна-покажчик типу PChar), після шифрування дані блоки записуються до результуючого (зашифрованого) файлу (з дескриптором FileHandle_2).

При другій послідовності до області пам'яті (буферу) BufferAll (покажчик типу PChar) зчитується одразу увесь вихідний файл (FileHandle_1), після чого з нього до буферу Buffer функцією CopyMemory копіюються блоки по 8 байт, які після шифрування копіюються до результуючого буферу Buffer All Result (також покажчик типу PChar), а з нього вже записуються до результуючого файлу (FileHandle_2).

Третя послідовність є найбільш простою серед усіх – до буферу Buffer АП зчитується одразу увесь вихідний файл (FileHandle_1), після шифрування даних безпосередньо в комірках пам'яті цього буферу зашифрована інформація записується до результуючого файлу [16].

О. Войтович та І. Микитюк, досліджуючи методи захисту баз даних, пропонують виділити два шляхи відповідно до рівнів та застосування криптографічних функцій: використання криптографічних функцій для захисту користувацької аутентифікаційної інформації; використання криптографічних функцій для безпосереднього захисту інформації в базах даних.

Алгоритм гешування користувацької інформації передбачає збереження будь-яких аутентифікаційних даних у загешованому вигляді, що захищає їх від зламу таким чином, що зловмисник, отримавши до них доступ, не може їх використати у своїх цілях при подальшому зламі СУБД. Кожен користувач на етапі аутентифікації на одному з рівнів вводить аутентифікаційні дані, після чого вони гешуються, і, в загешованому вигляді порівнюються з даними, які відповідають цьому користувачеві на даному рівні захисту [17].

Для забезпечення цілісності інформації, яка зберігається у базі даних, застосовується технологія blockchain, яка є аналогом ланцюга, дані в якому накопичуються і формують постійно зростаючу базу даних [18]. Однією з головних особливостей даної технології є те, що дані, які зберігаються в ланцюгу неможливо видалити чи здійснити заміну/заміщення блока. Нові блоки завжди додаються виключно в кінець ланцюга і кожен наступний блок залежить від попереднього [17].

Дослідники Iqra Basharat та Farooque Azam відзначили вже три рівні шифрування баз даних: шифрування на рівні зберігання, шифрування на рівні бази даних і шифрування на рівні програми. Так, шифрування на рівні сховища шифрує дані в підсистемі сховища. Воно прозоре, що дозволяє уникнути ризику будь-яких змін в існуючій програмі. При шифруванні на рівні сховища має бути гарантовано, що жодна копія не залишиться незашифрованою. Саме тому, на думку дослідників, є ризикованим вибірково шифрувати дані, наприклад, у тимчасових файлах, журналах тощо. Коли дані зберігаються або відновлюються з бази даних, то виконується шифрування рівня. Тут шифрування можна виконувати з вибірковою деталізацією, з огляду на рядок, стовпець або таблицю. Як для рівня зберігання, так і для рівня бази даних, в стратегії шифрування, ключі шифрування повинні бути доступні стороні сервера для розшифровки даних. Третій рівень шифрування, тобто на рівні програми, виконується в межах додатку.

Крім цього, алгоритм шифрування, розмір ключа та захист ключів – це параметри, що забезпечують безпеку. Чим кращій алгоритм шифрування використовується, тим кращим буде захист.

Авторами зроблено висновок, що шифрування забезпечує конфіденційність, але не дає гарантії цілісності, якщо не використовується якийсь цифровий підпис або функція гешування. Втім відомо, що використання надійних алгоритмів шифрування знижує продуктивність роботи з базою даних [19].

Загалом, на даний час у світі розроблено та використовується багато криптографічних алгоритмів, серед яких: IDEA, Twofish, AES, DES, Triple DES, RC6, SEED, Camellia, CAST-128, XTEA, "ГОСТ 28147-89" та ін. Ці та інші алгоритми використовують різні методи, які мають спільні корені.

Так, симетричне шифрування (або закритий ключ), метод шифрування, при якому один і той самий ключ використовується як для шифрування, так і для дешифрування даних. Відправник використовує ключ і алгоритм для шифрування, а одержувач використовує обидва для розшифрування. І відправник, і одержувач повинні мати ключ, який повинен залишатися приватним.

Асиметричне шифрування (або криптографія з відкритим ключем (РКС)) – метод шифрування, у якому використовуються два різні ключі: один для шифрування, а другий для розшифровки даних (відкритий та закритий ключ). Закритий ключ повинен зберігатися в секреті. Відкритий ключ не становить ризику, якщо він стає відомим.

Ключ – параметр, що визначає функціональний вихід криптографічного алгоритму. Без ключа алгоритм не мав би результату. У шифруванні ключ визначає конкретне перетворення відкритого тексту в зашифрований, або навпаки – під час дешифрування.

Шифр - алгоритм, що використовується для шифрування та дешифрування тексту, а також представлення одиниць відкритого тексту, включаючи: блочний і потоковий шифри. Block Cipher – метод, який шифрує один блок даних за раз. Потоковий шифр – метод, який шифрує один біт, байт або комп’ютерне слово за раз.

Шифрування – це перетворення відкритого тексту в зашифрований за допомогою параметра, який і називається «ключем», і обробка цих елементів за фіксованим алгоритмом для створення зашифрованого тексту, який приховує початкове значення даних. Розшифровка перетворює зашифрований текст у відкритий текст за допомогою криптографічної системи.

Тривалий час в криптографії використовувалися лише алгоритми симетричного шифрування, в яких відправник повинен був передати отримувачу разом із зашифрованим повідомленням і свій секретний ключ, яким було зашифроване це повідомлення, що створювало необхідність наявності закритого каналу для передачі секретного ключа та збільшувало ризики розкриття інформації.

Асиметричні алгоритми шифрування (на відміну від симетричних) використовують пару споріднених ключів – відкритий та секретний. При цьому, незважаючи на пов’язаність ключів у парі, обчислення секретного ключа на основі відкритого вважається технічно неможливим. В асиметричних криптосистемах відкритий ключ може вільно розповсюджуватись, у той час як закритий (приватний) ключ має зберігатись у таємниці [20].

Загалом, алгоритмом шифрування називається формула, яка використовується для перетворення інформації в нечитабельний формат. Сила алгоритму пов'язана з його здатністю максимізувати ентропію замість його секретності. Прикладами деяких алгоритмів є: DES, 3DES, AES, Blowfish і RSA [21].

Так, DES (Стандарт шифрування даних) передбачає розмір ключа 64 біт з розміром блоку 64 біт. 3DES або Triple DES (Потрійний стандарт шифрування даних) є покращенням DES; це 64-бітовий розмір блоку з розміром ключа 192 біта. RC2 — це блочний шифр із 64-бітним блочним алгоритмом зі змінним розміром ключа від 8 до 128 біт. AES (Advanced Encryption Security) — це блочний шифр. Він має змінну довжину ключа 128, 192 або 256 біт; за замовчуванням 256. Він шифрує блоки даних по 128 біт у 10, 12 і 14 раундах залежно від розміру ключа. RC6 - також блочний шифр. Має розмір блоку 128 біт і підтримує розміри ключів 128, 192 і 256 біт. Blowfish — це 64-розрядний блок блочного шифру. Blowfish приймає ключ змінної довжини, починаючи з 32 біт до 448 біт; за замовчуванням 128 біт. Blowfish не запатентований і доступний безкоштовно для будь-

якого використання. Blowfish має варіанти від 14 турів або менше. Twofish – це 128-розрядний блок блочного шифру з ключем змінної довжини (128, 192 або 256 біт). Twofish пов'язаний з більш раннім блочним шифром Blowfish і є незапатентованим безкоштовним програмним забезпеченням [21].

На додаток, у ґрунтовній монографії Christopher Diaz описано та продемонстровано рішення для усунення ризиків цілісності баз даних, включаючи блокування СУБД, блокування таблиць і блокування рядків. Також детально розписано блокування читання та блокування запису, а також описано та продемонстровано концепції блокування оновлень та блокування спільного використання; роз'яснено концепцію тупикового блокування, її ризики для доступності та рішення щодо запобігання [22].

Якщо база даних є зашифрованою, то вона також не застрахована від ризиків. Зокрема, це можуть бути: 1) зловживання з боку адміністратора або інша інсайдерська атака; 2) якщо ключі зберігаються на одному сервері із зашифрованими даними, вони, ймовірно, будуть розкриті одночасно, якщо база даних буде скомпрометована; 3) у випадку застосування ненадійного алгоритму шифрування, може бути підібрано ключ; 4) використання одного ключа для шифрування великої кількості даних є небезпечним з огляду на масштаби втрат у випадку його отримання зловмисниками; 5) користувачі іноді схильні забувати свої паролі, а надійне зберігання ключів – велика проблема.

Отже, шифрування не вирішує всіх проблем безпеки. Зокрема: 1) шифрування не можна використовувати для вирішення проблем контролю доступу; 2) ключі шифрування необхідно регулярно змінювати як частину належної практики безпеки, у цей час база має бути недоступною; 3) необхідно автономно зберігати копію бази даних у віддаленому місці певний проміжок часу; 4) роль адміністратора може бути розділеною на двох і більше осіб з тим, щоб кожен з них не мав повного доступу до всієї бази даних, або ця роль може бути обмеженою лише адмініструванням бази без доступу до самої інформації.

Висновки. Захист бази даних стає все більш складним завданням для організації, бо конфіденційні дані часто стають метою зловмисників. Державні установи, зокрема ті, що віднесені до об'єктів критичної інфраструктури, так само як і приватні компанії з кожним роком витрачають усе більше коштів на їх захист. Однією з обов'язкових вимог до безпеки бази даних є її криптографічне перетворення, яке здійснюється як під час переміщення інформації по мережах так і під час зберігання в сховищі в системах баз даних. Це може запобігти атакам як зовнішніх так і внутрішніх зловмисників. І хоча шифрування бази даних не може подолати всі загрози безпеці, застосування добре налаштованої програми, яка використовує надійний алгоритм, здатне суттєво підвищити цілісність, конфіденційність та доступність інформації бази даних.

Подальше удосконалення та розвиток національної системи криптографічного захисту баз даних потребуватиме узгодженого вирішення питань на законодавчому (нормативно-правовому), загальносистемному, процедурно-функціональному, функціонально-технічному та програмно-технічному рівнях.

Список використаних джерел

1. Про інформацію [Електронний ресурс] : Закон України від 2 жовтня 1992 року № 2657-XII. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

2. Yong Wang. Guangxi Key Laboratory of Cryptography and Information Security / Yong Wang, Jinsong Xi, Tong Cheng // Journal of Information Security. – January 2021. – Vol. 12, No. 1. – DOI: 10.4236/jis.2021.121002.

3. Когут Ю. І. Кібербезпека та ризики цифрової трансформації компаній : практичний посібник / Ю. І. Когут. – К. : Консалтингова компанія «СІДКОН», 2021. – 372 с.

4. Деякі питання об'єктів критичної інфраструктури [Електронний ресурс] : Постанова Кабінету Міністрів України від 09.10.2020 р. № 1109. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

5. 2021. Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Оперативний центр реагування на кіберінциденти державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації [Електронний ресурс]. – К., TLP:WHITE. – 8 с. – Режим доступу: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf.

6. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки [Електронний ресурс] : Постанова Кабінету Міністрів України від 23 грудня 2020 р. № 1295 та Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text.

7. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України від 05.10.2017 р. № 2163-VIII. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#n56.

8. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних [Електронний ресурс] : Закон України від 06.07.2010 р. № 2438-VI. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2438-17#Text.

9. Про захист персональних даних [Електронний ресурс]: Закон України від 1 червня 2010 року № 2297-VI. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

10. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

11. Intelligent IT Distribution: офіційний сайт [Електронний ресурс]. – Режим доступу: https://iitd.com.ua/shifruvannja-ta-zahist-baz-danih.

12. 2022 (Q1). Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Оперативний центр реагування на кіберінциденти державного центру кіберзахисту [Електронний ресурс]. – К.: TLP:WHITE, 2021. – 9 с. – Режим доступу: https://scpc.gov.ua/api/docs/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7.pdf.

13. Борсуковський Ю. В. Прикладні аспекти захисту аутентифікаційних даних / Ю. В. Борсуковський, В. Ю. Борсуковська // Кібербезпека: освіта, наука, техніка. – 2019. – № 3(3). – С. 42-52. – DOI 10.28925/2663-4023.2019.3.4252.

14. Антоненко С. А. Криптографічні основи застосування електронного цифрового підпису в Україні [Електронний ресурс] / С. А. Антоненко // Правова інформатика. – 2013. – № 4(40). – С. 19-28. – Режим доступу: http://ippi.org.ua/sites/default/files/ 13asatpu.pdf.

15. Blowfish [Электронный ресурс] / созд. 33.102.141.21 ; Wikimedia Foundation, Inc. – Электрон, дан. – [б. м.], созд. 5 декабря 2006. – Режим доступа: http://ru.wikipedia.org/wiki/Blowfish. – Загл. с экрана.

16. Лопін Є. Б. Аналіз часових показників шифрування/дешифрування файлів баз даних медичних інформаційних систем / Є. Б. Лопін // Медична інформатика та інженерія. – 2013. – № 4. – С. 28-35.

17. Войтович О. Метод захисту баз даних шляхом багатошарового користувацького доступу / О. Войтович, І. Микитюк // Матеріали міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерне моделювання» ІТКМ – 2018. 14-19 травня 2018 р. – Івано-Франківськ – Яремче, 2018. – С. 182-186.

18. Щербань Е. Что такое блокчейн, и как он работает [Электронный ресурс]. – Режим доступа: https://revolverlab.com/how-its-worksblockchain-6d0355c43bfc.

19. Iqra Basharat. Database Security and Encryption: A Survey Study / Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar // International Journal of Computer Applications (0975 – 888). – June 2012. – Vol. 47, No. 12. – Pp. 28-34.

20. Антоненко С. А. Криптографічні основи застосування електронного цифрового підпису в Україні / С. А. Антоненко // Правова інформатика. – 2013. – № 4(40). – С. 19-28.

21. Nigm El Sayed. Cryptography and Database Security: Concepts, Compliance Risks and Technical Challenges [Electronic resource] / Nigm El Sayed, El-Rabaie El-Sayed, Faragallah Osama, Mousa, Ayman // ResearchGate. – 2010. – Режим доступу: https://www.researchgate.net/publication/263754046_Cryptography_and_Database_Security_Concepts_Compliance_Risks_and_Technical_Challenges.

22. Christopher Diaz. Database Security. Problems and Solution. Mercury Learning and Information. – Dulles, Virginia, Boston, Massachusetts, New Delhi, 2022. – 261 p.

References

1. Pro informatsiiu [On information], Law of Ukraine № 2657-XII (dated October 2, 1992). https://zakon.rada.gov.ua/laws/show/2657-12#Text.

2. Yong Wang, Jinsong Xi, Tong Cheng. (January 2021). Guangxi Key Laboratory of Cryptography and Information Security. *Journal of Information Security*, 12(1). doi: 10.4236/jis.2021.121002.

3. Kohut, Yu.I. (2021). *Kiberbezpeka ta ryzyky tsyfrovoi transformatsii kompanii [Cyber security and risks of digital transformation of companies]*. Konsaltynhova kompaniia «SIDKON».

4. Deiaki pytannia obiektiv krytychnoi infrastruktury [Some issues of critical infrastructure objects], Resolution of the Cabinet of Ministers of Ukraine № 1109 (dated October 9, 2020). https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

5. 2021. Zvit roboty sy`stemy vyiavlennia vrazlyvostei i reaguvannia na kiberintsydenty ta kiberataky: Operatyvnyi centr reahuvannia na kiberintsydenty derzhavnoho centru kiberzakhystu Derzhavnoi sluzhby specialnoho zviazku ta zakhystu informatsii [2021. Report on the work of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks: The operational center for responding to cyber incidents of the state cyber protection center of the State Service for Special Communications and Information Protection]. TLP:WHITE. https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf.

6. Deiaki pytannia zabezpechennia funktsionuvannia systemy vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky [Some issues of ensuring the functioning of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks], Decree of the Cabinet of Ministers of Ukraine dated December 23, 2020 No. 1295 and the Procedure for the functioning of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks. https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text.

7. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the main principles of ensuring cyber security of Ukraine], Law of Ukraine № 2163-VIII (dated October 5, 2017). https://zakon.rada.gov.ua/laws/show/2163-19#n56.

8. Pro ratyfikatsiiu Konventsii pro zakhyst osib u zviazku z avtomatyzovanoiu obrobkoiu personalnykh danykh ta Dodatkovoho protokolu do Konventsii pro zakhyst osib u zviazku z avtomatyzovanoiu obrobkoiu personalnykh danykh stosovno orhaniv nahliadu ta transkordonnykh potokiv danykh [On the ratification of the Convention on the Protection of Individuals in Connection with Automated Processing of Personal Data and the Additional Protocol to the Convention on the Protection of Individuals in Connection with Automated Processing of Personal Data in relation to supervisory bodies and cross-border data flows]: Law of Ukraine № 2438-VI (dated 06.07.2010). https://zakon.rada.gov.ua/laws/show/2438-17#Text.

9. Pro zakhyst personalnykh danykh [On the protection of personal data], Law of Ukraine № 2297-VI (dated June 1, 2010). https://zakon.rada.gov.ua/laws/show/2297-17#Text.

10. Rehlament Yevropeiskoho Parlamentu i Rady (IeS) 2016/679 vid 27 kvitnia 2016 roku pro zakhyst fizychnykh osib u zviazku z opratsiuvanniam personalnykh danykh i pro vilnyi rukh takykh danykh, ta pro skasuvannia Dyrektyvy 95/46/IeS (Zahalnyi rehlament pro zakhyst danykh) [Regulation of the European Parliament and Council (EU) 2016/679 of April 27, 2016 on the protection of natural persons in connection with the processing of personal data and on the free movement of such data, and on the repeal of Directive 95/46/EC (General Regulation on data protection)]. https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

11. Intelligent IT Distribution: ofitsiinyi sait [Intelligent IT Distribution: official site]. https://iitd.com.ua/shifruvannja-ta-zahist-baz-danih.

12. 2022 (Q1). Zvit roboty systemy vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky: Operatyvnyi tsentr reahuvannia na kiberintsydenty derzhavnoho tsentru kiberzakhystu [2022 (Q1). Report on the work of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks: Operational center for responding to cyber incidents of the state cyber protection center]. TLP:WHITE. https://scpc.gov.ua/api/docs/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7.pdf.

13. Borsukovskyi, Yu.V., Borsukovska, V.Iu. (2019). Prykladni aspekty zakhystu autentyfikatsiinykh danykh [Applied aspects of protection of authentication data]. Kiberbezpeka: osvita, nauka, tekhnika – Cyber security: education, science, technology, (3(3)), 42-52. doi: 10.28925/2663-4023.2019.3.4252.

14. Antonenko, S.A. (2013). Kryptohrafichni osnovy zastosuvannia elektronnoho tsyfrovoho pidpysu v Ukraini [Cryptographic basics of using electronic digital signature in Ukraine]. *Pravova informatyka – Legal informatics, 4*(40), 19-28. http://ippi.org.ua/sites/default/files/13asatpu.pdf.

15. Blowfish. (2006). http://ru.wikipedia.org/wiki/Blowfish.
16. Lopin, Ye.B. (2013). Analiz chasovykh pokaznykiv shyfruvannia/deshyfruvannia failiv baz danykh medychnykh informatsiinykh system [Analysis of time indicators of encryption/decryption of files of databases of medical information systems]. *Medychna informatyka ta inzheneriia – Medical informatics and engineering*, (4), 28-35.
17. Voitovych, O., Mykytiuk, I. (2018). Metod zakhystu baz danykh shliakhom bahatosharovoho korystuvatskoho dostupu [The method of protecting databases by means of multi-layer user access]. *Materialy mizhnarodnoi naukovo-praktychnoi konferentsii «Informatsiini tekhnolohii ta kompiuterne modeliuvannia» ITKM – 2018 – Materials of the International Scientific and Practical Conference "Information Technologies and Computer Modeling" ITKM – 2018* (pp. 182-186).
18. Shcherban, E. (2017). Chto takoe blokchein, y kak on rabotaet [What is blockchain, and how does it work]. https://revolverlab.com/how-its-worksblockchain-6d0355c43bfc.
19. Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar. (2012). Database Security and Encryption: A Survey Study. *International Journal of Computer Applications (0975 – 888)*, *47*(12), 28-34.
20. Antonenko, S.A. (2013). Kryptohrafichni osnovy zastosuvannia elektronnoho tsyfrovoho pidpysu v Ukraini [Cryptographic basics of electronic digital signature application in Ukraine]. *Pravova informatyka – Legal informatics*, (4(40)), 19-28.
21. Nigm, El Sayed, El-Rabaie, El-Sayed, Faragallah, Osama, Mousa, Ayman. (2010). Cryptography and Database Security: Concepts, Compliance Risks and Technical Challenges. *ResearchGate.* https://www.researchgate.net/publication/263754046_Cryptography_and_Database_Security_Concepts_Compliance_Risks_and_Technical_Challenges.
22. Christopher Diaz. (2022). *Database Security. Problems and Solution. Mercury Learning and Information.* Dulles, Virginia, Boston, Massachusetts, New Delhi.

Отримано 30.08.2022

UDC 004.65

Maryna Larchenko
PhD in Law, Associate Professor, 2st year undergraduate student, OP Cybersecurity
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: urlinka2006@gmail.com. **ORCID:** https://orcid.org/0000-0002-2643-980X
ResearcherID: X-9681-2018

MODERN PROBLEMS OF CRYPTOGRAPHIC PROTECTION OF DATABASES

In the conditions of growing digitalization of society, the issue of database protection is extremely urgent. Currently, Ukraine is at the stage of introducing European information protection standards, but the software component of its protection also needs further improvement. Information security threats are destruction, modification, blocking, unauthorized access, leakage, disclosure. In particular, cryptographic protection of databases allows preventing access to the information they contain by means of mathematical transformations. It is primarily about prevention of unauthorized modification and unauthorized disclosure of information.

Cryptographic protection of databases can use encryption of data that is stored in a file (after encryption), as well as encryption of directories and files themselves. The approach to database protection should be comprehensive. Therefore, encryption cannot be used to solve access control problems. Encryption keys should be changed regularly as part of good security practices. The database should be unavailable during this time. A copy of the database must be stored offline at a remote location for some time. The administrator role can be split between two or more people so that each person does not have full access to the entire database, or the role can be limited to just administering the database without access to the information itself.

Protecting the database is becoming an increasingly difficult task for an organization, because sensitive data is often the target of attackers. One of the mandatory requirements for database security is its cryptographic transformation, which is carried out both during the movement of information over networks and during storage in database systems. This can prevent attacks from both external and internal attackers. Although, database encryption cannot overcome all security threats, the application of a well-configured program that uses a reliable algorithm can significantly increase the integrity, confidentiality and availability of database information.

Further improvement and development of the national system of cryptographic protection of databases will require a coordinated resolution of issues at the legislative (normative-legal), system-wide, procedural-functional, functional-technical, and software-technical levels.

Key words: *database security; personal data protection; cryptographic protection; key; encryption algorithm.*
Table: 1. References: 22.

Ларченко М. Сучасні проблеми криптографічного захисту баз даних. *Технічні науки та технології.* 2022. № 3(29). С. 102-113.