ISSN 2071-1077(print)
ISSN 2663-2411(online

**doi: 10.32620/oikit.2026.107.10**

УДК 004.89
О. І. Феоктистова, А. Д. Єрьоменко

# Підхід до забезпечення конфіденційності у корпоративних системах софтверних фірм на основі технології блокчейн

*Національний аерокосмічний університет «Харківський авіаційний інститут»*

У статті розглянуто проблематику забезпечення конфіденційності даних у корпоративних інформаційних системах софтверних компаній та обґрунтовано доцільність використання технології блокчейн як основи для побудови децентралізованих моделей контролю доступу. Проведено огляд класичних підходів (на основі моделей Белла–ЛаПадули, Брюера–Наша, Кларка–Вілсона) та показано їхні обмеження у багатокористувацьких середовищах із високою динамікою зміни прав і ролей. Запропоновано узагальнену архітектуру системи забезпечення конфіденційності та децентралізованого управління доступом у корпоративних інформаційних системах, що поєднує три ключові компоненти: permissioned-блокчейн для гарантованого аудиту й незмінності записів, токенізацію доступу для гнучкого й контекстного управління повноваженнями користувачів, а також розподілене зберігання криптографічних ключів (multi-signature, Shamir's Secret Sharing) для мінімізації внутрішніх загроз і зловживань. Показано, що застосування смарт-контрактів для формалізації та автоматичного виконання політик доступу забезпечують формалізацію політик доступу, автоматичне надання/відкликання прав і прозорий журнал транзакцій у реальному часі. Окреслено практичні напрями впровадження технологій: електронний документообіг, фінансові операції, комплаєнс й аудит, управління авторськими правами на програмні продукти, а також захист ідентичностей і персональних даних із урахуванням вимог GDPR. Проаналізовано технологічні та правові виклики (масштабованість і затримки, енергоспоживання окремих алгоритмів консенсусу, колізії з «правом на забуття», інтеграція з ERP/CRM). У підсумку доведено, що інтеграція блокчейну з сучасними засобами криптографії створює цілісну екосистему довіри, яка підвищує рівень конфіденційності та стійкості корпоративних систем до кібератак, а також формує підґрунтя для подальших досліджень у напрямі розвитку гібридних моделей із застосуванням штучного інтелекту та хмарних обчислень.
***Ключові слова*:** конфіденційність, корпоративні системи, блокчейн, криптографія, софтверні фірми, інформаційна безпека.

## Вступ

У сучасних умовах розвитку цифрової економіки та активної цифровізації бізнес-процесів, забезпечення інформаційної безпеки у корпоративних системах набуває стратегічного значення. Софтверні компанії акумулюють значні обсяги комерційно важливої інформації, що охоплює вихідний програмний код, технічну документацію, бази знань, а також персональні дані клієнтів і партнерів. Будь-який витік чи несанкціоноване використання таких даних здатен спричинити істотні фінансові збитки, репутаційні втрати та зростання конкурентних ризиків.

Традиційні засоби захисту інформації, що ґрунтуються на централізованих моделях контролю доступу, використанні VPN або антивірусних систем, не завжди забезпечують належний рівень конфіденційності у багатокористувацькому середовищі. Це обумовлено як технічними обмеженнями, так і людським фактором, адже значна частка інцидентів у галузі інформаційної безпеки виникає внаслідок необачності або помилкових дій персоналу.

У цьому контексті актуальним завданням постає пошук інноваційних інструментів захисту корпоративних даних. Одним із перспективних рішень є застосування технології блокчейн, що забезпечує децентралізованість, незмінність і прозорість процесів зберігання та обміну інформацією. Особливого значення проблема конфіденційності набуває у глобалізованому інформаційному середовищі, де захист даних стає предметом не лише внутрішньо корпоративних стратегій, а й міжнародних ініціатив. Це вимагає консолідації зусиль законодавців, розробників програмного забезпечення, керівників організацій і пересічних співробітників з метою створення комплексних механізмів запобігання витоку даних і втручанню у функціонування корпоративних інформаційних систем.

## Аналіз останніх публікацій та досліджень

Проблематика забезпечення конфіденційності даних активно досліджується як у зарубіжній, так і у вітчизняній науковій літературі. У працях зарубіжних дослідників акцентовано увагу на нормативно-правових засадах, ролі прав суб’єктів даних і практиках «privacy/data protection by design» [1-3]. У європейському контексті ключовим орієнтиром виступає General Data Protection Regulation (GDPR), а також аналітичні дослідження його застосування, зокрема у взаємодії з технологією блокчейн [4].

Для українського правопорядку релевантні порівняльно-правові аналізи зближення із правом ЄС та огляди сучасних трендів імплементації вимог GDPR [5-7]. На рівні організаційної практики окрема увага приділяється людському фактору та формуванню культури кібербезпеки як передумові сталого дотримання конфіденційності [8-9].

Питання інтеграції новітніх технічних засобів у корпоративні середовища – зокрема застосування блокчейн-технологій для підвищення цілісності та довіри до інформаційних систем – відображені як у працях українських авторів, так і в європейських оглядах [10-12]. Загалом, попри значний масив досліджень, зберігається потреба в перенесенні теоретичних напрацювань у практику корпоративного управління; особливо актуальним є впровадження технології блокчейн разом із підходами «by design» для забезпечення належного рівня конфіденційності та цілісності даних у корпоративних системах [3-4, 12].

Загалом науковий дискурс демонструє, що, попри наявність значного масиву результатів досліджень, існує нагальна потреба у вирішенні завдання інтеграції теоретичних напрацювань у практику корпоративного управління. Особливо актуальним є застосування новітніх інструментів, зокрема технології блокчейн, для забезпечення належного рівню конфіденційності та цілісності даних у корпоративних системах.

## Виклад основного матеріалу

У сучасних умовах розвитку цифрової економіки конфіденційність інформації є ключовим елементом забезпечення інформаційної безпеки корпоративних систем. Під конфіденційністю розуміють обмеження доступу до відомостей лише для уповноважених користувачів, що передбачає запобігання несанкціонованому розголошенню або використанню даних. Для софтверних компаній, які оперують вихідним кодом, базами клієнтів, внутрішньою технічною документацією та іншими стратегічними активами, дотримання конфіденційності

є критичним чинником конкурентоспроможності та стабільності функціонування.

У науковій літературі та практиці інформаційної безпеки сформовано низку класичних моделей забезпечення конфіденційності. Серед них вагоме місце займає модель Белла-ЛаПадули (Bell-LaPadula), яка ґрунтується на контролі доступу до даних на основі багаторівневої системи безпеки та принципу «читати вниз, записувати вгору». Вона широко застосовується у військових і державних структурах, однак має обмежене використання у корпоративному середовищі через надмірну жорсткість. Інша модель – модель Брюера-Наша (Brewer-Nash) – спрямована на усунення конфлікту інтересів, коли доступ до комерційної інформації залежить від контексту і попередніх дій користувача. У свою чергу, модель Кларка–Вілсона (Clark–Wilson) фокусується на забезпеченні цілісності транзакцій та правильності обробки даних, використовуючи концепції сертифікації та примусу, що особливо актуально для банківських та фінансових систем [12].

Водночас традиційні моделі та методи не позбавлені обмежень. Передусім ці обмеження мають місце внаслідок того, що поширені на даний час методичні засоби ґрунтуються на централізованих підходах, що робить корпоративні системи вразливими до внутрішніх загроз та помилок адміністраторів. Значною проблемою є також складність у відстеженні несанкціонованих змін, адже класичні механізми логування не завжди забезпечують повну прозорість та незмінність даних. Це створює ризики як для збереження конфіденційної інформації, так і для довіри між підрозділами компанії та зовнішніми партнерами.

Таким чином, теоретичні засади конфіденційності у корпоративних системах, попри наявність усталених моделей, потребують подальшого розвитку та вдосконалення. Сучасні виклики цифрової трансформації, глобалізації бізнесу й ускладнення кіберзагроз зумовлюють необхідність пошуку нових рішень, серед яких важливу роль може відігравати технологія блокчейн, що здатна забезпечити децентралізований, прозорий і водночас гнучкий підхід до управління конфіденційною інформацією.

*Модель децентралізованого управління доступом*. Упродовж останнього десятиліття технологія блокчейн еволюціонувала від вузькоспеціалізованого інструмента у сфері фінансових транзакцій до універсальної технологічної платформи, здатної забезпечувати безпечну обробку та збереження даних у різних галузях корпоративної діяльності. Її архітектура, заснована на децентралізованому зберіганні даних у вигляді ланцюга блоків, кожен з яких містить набір транзакцій і криптографічний хеш попереднього, надає системі унікальні властивості: незмінність даних, прозорість та стійкість до маніпуляцій. Для корпоративних структур, що оперують значними масивами конфіденційної та комерційно чутливої інформації, це відкриває нові горизонти у сфері управління доступом та формування більш захищених цифрових інфраструктур [21, с. 72].

Сутність моделі децентралізованого управління доступом полягає у використанні смарт-контрактів, які автоматизують надання, перевірку та відкликання доступу до ресурсів корпоративної системи. На відміну від традиційних, централізованих підходів, де адміністратор виступає єдиною точкою контролю, у блокчейн-системі права доступу визначаються прозорими правилами, що зберігаються у розподіленому реєстрі та є обов’язковими для всіх учасників мережі. Така модель унеможливлює несанкціоноване втручання адміністратора, знижує ризик зловживань і мінімізує ймовірність технічних помилок при налаштуванні прав доступу.

Фундаментальні принципи функціонування блокчейну, які лежать в основі

моделі децентралізованого управління доступом, охоплюють:

– децентралізацію, що усуває залежність від центрального сервера та знижує вразливість системи до цілеспрямованих атак;

– криптографічний захист, реалізований через хешування, цифрові підписи та асиметричне шифрування, що гарантує автентичність і цілісність транзакцій;

– консенсусні алгоритми (Proof of Work, Proof of Stake, Practical Byzantine Fault Tolerance та ін.), які забезпечують достовірність операцій навіть у разі часткової недобросовісності учасників мережі;

– незмінність записів, що принципово унеможливлює коригування або видалення вже підтверджених транзакцій, створюючи додатковий рівень довіри до системи [22].

Перевагою цієї моделі для корпоративних структур є те, що вона дозволяє персоналізувати доступ до інформаційних ресурсів відповідно до ролі користувача, забезпечуючи при цьому прозорий аудит усіх дій. Завдяки блокчейн-технології з’являється можливість формування детального журналу операцій у реальному часі, що не лише спрощує аудит, а й створює основу для системи превентивного моніторингу загроз. У разі спроби порушення політик безпеки відповідні події фіксуються у реєстрі й можуть бути автоматично передані у систему оповіщення.

Таким чином, модель децентралізованого управління доступом демонструє високий потенціал у забезпеченні конфіденційності, цілісності та доступності даних у корпоративних інформаційних системах. Вона не лише усуває класичні проблеми централізованих підходів (вразливість до зловживань, помилки адміністрування, концентрація влади), але й формує нову парадигму управління цифровими ресурсами, що ґрунтується на принципах довіри, прозорості та автономності.

Важливою складовою конфіденційності у блокчейн-системах виступають криптографічні механізми захисту, котрі унеможливлюють несанкціонований доступ до даних. Хеш-функції використовуються для перевірки цілісності блоків, цифровий підпис забезпечує юридично значущу ідентифікацію учасників транзакції, а алгоритми асиметричного шифрування гарантують безпеку каналів обміну інформацією. Для корпоративних структур особливу значущість мають смарт-контракти, які автоматизують контроль доступу та формалізують регламент взаємодії між внутрішніми підрозділами та зовнішніми контрагентами. Поряд із цим усе більшої популярності набувають permissioned blockchain-системи (наприклад, Hyperledger Fabric, Quorum), які поєднують переваги розподіленого реєстру з можливістю налаштування приватних мереж, доступ до яких мають лише уповноважені учасники [16, с. 54].

До основних переваг блокчейн-технологій у корпоративному секторі відносять, по-перше, неможливість несанкціонованої модифікації даних, оскільки всі транзакції підтверджуються мережею та фіксуються у розподіленому реєстрі. По-друге, блокчейн забезпечує прозорий аудит усіх транзакцій, що значно спрощує процеси внутрішнього контролю, ревізій та незалежних перевірок. По-третє, використання блокчейну сприяє підвищенню рівня довіри між учасниками системи, адже кожен із них має доступ до достовірної й незмінної версії даних. Це особливо важливо для компаній, які взаємодіють з великою кількістю контрагентів і здійснюють операції у транснаціональному середовищі[16, с. 100].

Таким чином, блокчейн постає не лише технологією зберігання інформації, а й системо утворюючим інструментом для розбудови нових моделей

корпоративної взаємодії. Його впровадження створює інноваційне інформаційне середовище, у якому конфіденційність, цілісність і прозорість даних забезпечуються комплексно та на якісно новому рівні. Перспективи подальшого розвитку полягають в інтеграції блокчейн-рішень із технологіями штучного інтелекту, великих даних та хмарних обчислень, що сприятиме формуванню стійкої цифрової інфраструктури майбутнього.

Сучасні виклики у сфері інформаційної безпеки вимагають від корпоративних структур переходу від класичних централізованих методів захисту до інноваційних рішень, здатних гарантувати вищий рівень надійності та прозорості. Особливого значення набуває інтеграція блокчейн-технологій, що поєднують криптографічні механізми, децентралізацію та консенсусні алгоритми. На відміну від традиційних підходів, блокчейн забезпечує одночасно і цілісність, і контроль доступу, і довготривале збереження даних у незмінному вигляді. Це створює передумови для формування якісно нових моделей корпоративної взаємодії, орієнтованих на мінімізацію ризиків витоку та зловживань інформацією [17, с. 15].

Однією з таких моделей є децентралізоване управління доступом, яке передбачає використання смарт-контрактів для регламентації прав і обов’язків користувачів. У цьому випадку правила доступу формалізуються у програмному коді, що виключає можливість ручного втручання з боку адміністраторів і зменшує ризики людського фактора. Будь-яка спроба змінити рівень доступу чи виконати транзакцію автоматично фіксується у блокчейні, що підвищує прозорість і відповідальність усіх учасників корпоративної системи. Важливим напрямом є метод розподіленого зберігання ключів, який передбачає застосування мультипідпису (multi-signature) та криптографічних протоколів розподілу секрету. Такий підхід дає змогу унеможливити зосередження контрольних повноважень у руках одного користувача та значно знижує ризики компрометації ключів. Для доступу до конфіденційних даних необхідна участь кількох сторін, що гарантує додатковий рівень безпеки у корпоративному середовищі [18].

Особливої уваги заслуговує модель корпоративного permissioned blockchain, яка функціонує у закритому режимі та доступна лише уповноваженим користувачам. Ця модель дозволяє інтегрувати блокчейн у внутрішні бізнес-процеси компаній без надмірної відкритості, властивої публічним мережам. Permissioned-рішення (наприклад, Hyperledger Fabric або Quorum) поєднують переваги розподіленого реєстру з вимогами корпоративної безпеки, забезпечуючи аудит усіх транзакцій і контрольований доступ до даних.

Інноваційним підходом є також метод токенізації доступу, коли права користувача на роботу з інформаційними ресурсами компанії реалізуються у вигляді цифрових токенів. Такі токени можуть мати обмежений термін дії, визначений набір прав або прив’язку до конкретного пристрою. Це створює гнучкий інструмент управління доступом, який дозволяє оперативно регулювати права користувачів, відстежувати всі їхні дії та швидко анулювати доступ у випадку виявлення загроз [17, с. 22].

Таким чином, застосування блокчейн у корпоративних системах не обмежується лише криптографічним захистом даних, а передбачає формування комплексної інфраструктури управління доступом та контролю інформаційних потоків. Моделі децентралізованого управління, permissioned blockchain, токенізація та розподілене зберігання ключів, у сукупності надають змогу створити надійну систему, яка поєднує високий рівень безпеки з прозорістю та ефективністю управління корпоративними ресурсами.

*Метод розподіленого зберігання ключів.* Забезпечення конфіденційності корпоративних даних безпосередньо залежить від ефективного управління криптографічними ключами, адже саме вони є основним механізмом автентифікації, авторизації та шифрування інформації. У традиційних системах централізоване зберігання ключів становить одну з найбільш уразливих ланок, оскільки компрометація одного адміністратора або сервера може призвести до масштабного витоку даних. У відповідь на ці виклики, дедалі більшого поширення набуває метод розподіленого зберігання ключів, який дозволяє мінімізувати ризики зловживань та забезпечити стійкість корпоративних систем до внутрішніх і зовнішніх загроз [19].

Сутність даного підходу полягає у застосуванні механізмів мультипідпису (multi-signature) та протоколів розподілу секрету, серед яких найбільш відомим є алгоритм Shamir's Secret Sharing (SSS). Використання мультипідпису передбачає, що транзакція чи доступ до конфіденційних даних вважається дійсним лише за умови підтвердження кількома сторонами одночасно. Це виключає можливість одноосібного доступу до ключів та створює багаторівневий захисний бар'єр. Протоколи розподілу секрету, своєю чергою, дозволяють поділити один криптографічний ключ на кілька частин (shares), які розподіляються між незалежними учасниками системи. Для відновлення оригінального ключа потрібне об'єднання визначеної кількості частин, що значно ускладнює несанкціонований доступ.

Застосування цього методу у корпоративних системах забезпечує низку переваг. По-перше, він мінімізує ризики, пов'язані з людським фактором, оскільки жоден окремий співробітник не може одноосібно скомпрометувати ключ. По-друге, даний метод підвищує стійкість системи до атак: навіть у разі витоку або втрати частини ключа зловмисник не зможе отримати доступ до даних без необхідної кількості інших частин. По-третє, розподілене зберігання сприяє підвищенню довіри між підрозділами та партнерами, оскільки контроль над доступом розподіляється між кількома незалежними сторонами [20].

У практичному аспекті метод розподіленого зберігання ключів доцільно застосовувати у таких критично важливих сферах, як управління фінансовими транзакціями, захист інтелектуальної власності та збереження персональних даних. Для великих софтверних компаній це може стати ефективним інструментом контролю за доступом до вихідного коду, клієнтських баз та внутрішньої документації. Таким чином, розподілене зберігання ключів постає не лише технічним рішенням, а й концептуальною зміною підходів до управління корпоративною безпекою, де провідну роль відіграє колективна відповідальність і багаторівнева перевірка дій користувачів.

Модель корпоративного permissioned blockchain**.** Для внутрішніх потреб корпоративних структур найбільш доцільним є використання моделі permissioned blockchain, яка на відміну від публічних блокчейнів передбачає обмежений доступ до мережі виключно для уповноважених користувачів. Такий підхід дає можливість поєднати переваги розподіленого реєстру – незмінність, прозорість і відстежуваність транзакцій – із необхідністю збереження комерційної таємниці та конфіденційної інформації. У контексті діяльності софтверних компаній це означає, що транзакції між підрозділами фіксуються у захищеному середовищі, але не стають доступними для сторонніх осіб [21].

Ключовою перевагою permissioned blockchain є гнучкість у налаштуванні механізмів контролю доступу. На відміну від публічних мереж, де всі користувачі

мають рівні права щодо перегляду даних, корпоративний блокчейн дозволяє визначати рівні доступу відповідно до посадових обов'язків, функціональних ролей чи політики інформаційної безпеки підприємства. Це забезпечує високий рівень захисту критично важливої інформації, одночасно підтримуючи прозорість і підзвітність дій користувачів.

Особливе значення має інтеграція permissioned-рішень з існуючими корпоративними інформаційними системами, зокрема ERP- та CRM-платформами. Така інтеграція дозволяє автоматизувати ключові бізнес-процеси – від управління ланцюгами постачання до взаємодії з клієнтами – при цьому гарантується збереження достовірності даних. Наприклад, кожна транзакція або зміна у клієнтській базі автоматично фіксується у блокчейні, що унеможливлює їх приховане редагування чи несанкціоновану модифікацію [22].

Модель Permissioned blockchain також надає розширені можливості у сфері аудиту та комплаєнсу. Оскільки всі дії користувачів фіксуються у розподіленому реєстрі, компанія отримує інструмент для оперативного відстеження підозрілих транзакцій, перевірки коректності виконання бізнес-процесів та підтвердження відповідності нормативним вимогам. При цьому відбувається оптимізація обсягів відкритої інформації: зовнішнім учасникам демонструються лише ті дані, що визначені політикою доступу, без розкриття надмірних відомостей.

Практичні приклади реалізації permissioned blockchain включають такі платформи, як Hyperledger Fabric та Quorum, які вже продемонстрували ефективність у корпоративному секторі. Вони дозволяють не лише захистити конфіденційну інформацію, а й створити нові бізнес-моделі, що базуються на довірі та автоматизації взаємодії. Таким чином, корпоративний permissioned blockchain є перспективним рішенням для компаній, які прагнуть досягти балансу між прозорістю операцій та захистом стратегічно важливих даних.

*Метод токенізації доступу.* Серед інноваційних рішень у сфері корпоративної інформаційної безпеки особливе місце займає метод токенізації доступу, який передбачає заміну класичних механізмів автентифікації та авторизації (паролі, сертифікати, багаторівневі логіни) на систему цифрових токенів. У такій парадигмі токен виступає маркером або «ключем доступу», що надає користувачеві певні права на виконання конкретних дій у корпоративному інформаційному середовищі. Його головною відмінністю від традиційних засобів є гнучкість, багатофункціональність та можливість інтеграції з іншими технологіями кіберзахисту. Токени можуть бути обмежені в часі, прив'язані до конкретного користувача, пристрою або навіть геолокації, а також містити чітко визначений набір повноважень. Це дозволяє зменшити ризик несанкціонованого доступу та зловживань, які часто виникають у централізованих системах [23].

Використання токенів створює передумови для функціонування динамічних систем контролю доступу, що відповідають сучасним вимогам масштабованості та адаптивності корпоративних середовищ. Наприклад, співробітник компанії може отримати токен з обмеженим строком дії для виконання завдань у межах конкретного проєкту. Після завершення роботи доступ автоматично анулюється, що унеможливлює накопичення надлишкових прав і суттєво зменшує ризик зловживань. Такий підхід є особливо важливим для великих компаній із розгалуженою структурою підрозділів та різним рівнем доступу співробітників до критично важливих ресурсів.

Додатковою перевагою токенізації доступу є можливість детального моніторингу та аудиту взаємодії користувачів із корпоративними ресурсами.

Кожен токен може містити інформацію про ідентифікатор користувача, час доступу, характер виконаних операцій та рівень авторизації. Це дозволяє створювати прозору систему відстеження дій у режимі реального часу, що значно полегшує виявлення порушень і розслідування інцидентів у сфері інформаційної безпеки. Крім того, зібрані дані можуть використовуватися для аналітики та оптимізації політик доступу, що робить систему більш адаптивною та ефективною у довгостроковій перспективі [24].

Інтеграція токенізації з блокчейн-технологією забезпечує підвищений рівень захисту та прозорості порівняно з традиційними підходами до токенізації, що не передбачають використання блокчейну. Завдяки розподіленому реєстру кожна операція з видачі, передачі чи відкликання токена фіксується у блокчейні та стає незмінною. Це створює надійний механізм перевірки історії доступів, унеможливлює їх фальсифікацію та сприяє підвищенню довіри з боку як внутрішніх користувачів, так і зовнішніх партнерів. Таке поєднання є надзвичайно актуальним для компаній, що працюють у сферах із підвищеними вимогами до безпеки, зокрема у фінансовому секторі, охороні здоров’я, телекомунікаціях чи розробці програмного забезпечення, де навіть незначний витік інформації може мати серйозні наслідки.

Отже, метод токенізації доступу можна розглядати як невід’ємну складову нової парадигми управління корпоративною інформаційною безпекою. Його ключовими перевагами є поєднання децентралізації, криптографічного захисту та прозорості з гнучкістю та адаптивністю сучасних корпоративних середовищ. Такий підхід формує основу для побудови стійкої, безпечної та масштабованої цифрової інфраструктури, яка забезпечує конфіденційність, контроль і довіру на якісно новому рівні, сприяючи зростанню конкурентоспроможності компаній у глобалізованій економіці.

*Практичні аспекти впровадження.* Інтеграція блокчейн-технологій у корпоративні інформаційні системи має фундаментальне практичне значення, оскільки дозволяє не лише підвищити надійність захисту даних, але й сформувати нову модель взаємодії між учасниками корпоративного середовища. Завдяки властивостям децентралізації, криптографічного захисту та незмінності записів, блокчейн виступає дієвим інструментом, що сприяє підвищенню довіри між внутрішніми підрозділами компанії, а також у відносинах із клієнтами й зовнішніми партнерами. У сучасних умовах інтенсивної цифровізації саме ця технологія розглядається як одна з найбільш перспективних для забезпечення відповідності корпоративних систем міжнародним стандартам інформаційної безпеки та вимогам регуляторних органів [25].

Одним із ключових напрямів практичного застосування блокчейну є системи електронного документообігу. У корпоративних структурах значна частина даних зосереджена у вигляді контрактів, технічної документації, внутрішніх регламентів та управлінських рішень. Використання розподілених реєстрів дозволяє забезпечити їх незмінність, цілісність і достовірність. Кожна зміна чи доповнення автоматично фіксується у вигляді транзакції, яка зберігається у блокчейні та не може бути видалена чи змінена без відома учасників мережі. Це створює прозору історію використання документів, зменшує ризики шахрайських дій або навмисного викривлення даних та гарантує високий рівень правової захищеності корпоративної інформації. У результаті зростає ефективність управлінських процесів і знижується ймовірність конфліктних ситуацій між підрозділами компанії.

Не менш важливим практичним вектором є впровадження блокчейн-рішень у сфері фінансових операцій. Для софтверних компаній, що мають складну організаційну структуру і здійснюють транскордонну співпрацю, критично важливим є захищений обмін фінансовими даними та прозоре здійснення транзакцій. Використання блокчейну у цьому контексті забезпечує достовірність і автентичність операцій, унеможливлює подвійні витрати або підробку транзакцій, а також надає можливість у реальному часі відслідковувати рух коштів. Крім того, за рахунок децентралізованої природи блокчейну відбувається скорочення витрат на міжкорпоративні розрахунки, оскільки знижується потреба у фінансових посередниках, а отже, зменшується комісійне навантаження на компанії. У результаті блокчейн-технологія постає не лише як засіб підвищення безпеки, але й як інструмент економічної оптимізації бізнес-процесів [7, с. 432].

У практичній площині, впровадження блокчейну також сприяє підвищенню рівня комплаєнсу та аудиту у корпоративних системах. Всі транзакції та дії користувачів фіксуються у розподіленому реєстрі, що дозволяє створювати докладні й достовірні звіти для внутрішніх і зовнішніх перевірок. Це особливо важливо для компаній, які функціонують у середовищі жорстких регуляторних вимог (фінансовий сектор, фармацевтика, телекомунікації). Таким чином, блок-чейн-технології забезпечують не лише інформаційну, але й правову прозорість, що підвищує довіру з боку державних інституцій і міжнародних партнерів.

Отже, практичне впровадження блокчейн-технологій у корпоративні інформаційні системи виходить далеко за межі класичної парадигми кіберзахисту. Воно формує підґрунтя для розвитку комплексної цифрової інфраструктури, у якій ключові бізнес-процеси – від електронного документообігу до фінансових транзакцій і комплаєнсу – стають прозорими, надійними та ефективними. Це створює передумови для зміцнення конкурентоспроможності компаній у глобалізованій економіці, одночасно забезпечуючи відповідність стандартам кібербезпеки та сучасним моделям корпоративного управління [26].

Особливої уваги потребує застосування блокчейн-технологій у сфері управління авторським правом на програмні продукти, оскільки в умовах глобалізації та інтенсивної цифровізації проблема захисту інтелектуальної власності набуває стратегічного значення. Розробка програмного забезпечення є одним із ключових активів сучасних софтверних компаній, а будь-яке порушення авторських прав чи незаконне копіювання коду може спричинити суттєві фінансові збитки, втрату конкурентних переваг і репутаційні ризики. Традиційні механізми реєстрації прав часто характеризуються тривалими бюрократичними процедурами, обмеженою прозорістю та недостатньою здатністю протидіяти неправомірному використанню результатів інтелектуальної праці.

У цьому контексті блокчейн виступає ефективним інструментом підтвердження та захисту авторських прав. Його впровадження дозволяє створювати розподілені реєстри, у яких кожен запис щодо права власності на програмний продукт або ліцензію є незмінним, хронологічно впорядкованим і підтвердженим учасниками мережі. Така система унеможливлює фальсифікацію чи підміну інформації, забезпечує прозору й достовірну верифікацію прав на програмні продукти. Крім того, блокчейн-технології створюють передумови для розвитку нових механізмів монетизації інтелектуальної власності, зокрема за допомогою смарт-контрактів, які автоматизують процеси ліцензування, розподілу роялті та контролю за використанням програмних продуктів у реальному часі. Це

значно знижує адміністративні витрати та гарантує авторам своєчасне отримання винагороди. [17, с. 32].

Окремим важливим напрямом використання блокчейну є захист персональних даних співробітників і клієнтів. З огляду на вимоги європейського законодавства, зокрема General Data Protection Regulation (GDPR) [1], та поступову гармонізацію української правової бази з європейськими нормами, компанії повинні забезпечувати високий рівень захищеності при зберіганні, обробці й передачі персональної інформації. Використання блокчейну у цій сфері дає змогу формувати нову парадигму управління цифровою ідентичністю: кожен факт доступу до персональних даних, їх обробки або передачі фіксується у розподіленому реєстрі, що гарантує прозорість і контрольованість процесу [27].

Крім того, блокчейн забезпечує користувачам розширені можливості контролю над власними цифровими ідентичностями. Це включає вибіркове надання доступу до певних категорій даних, а також можливість відкликання дозволу на їх використання у будь-який момент. Таким чином, реалізується принцип «self-sovereign identity» (суверенної ідентичності), за якого контроль над персональною інформацією належить безпосередньо власникові даних, а не корпоративним чи державним структурам. Такий підхід значно підвищує рівень довіри користувачів до компаній і створює конкурентні переваги на ринку, де питання захисту приватності стають дедалі більш актуальними [28, с. 96].

Практичне впровадження блокчейн-рішень у корпоративні інформаційні системи охоплює широкий спектр завдань, що варіюються від управління авторським правом і підтвердження легітимності програмних продуктів до забезпечення захищеної обробки персональних даних. Завдяки своїм базовим характеристикам – децентралізованості, прозорості, незмінності та криптографічному захисту – технологія блокчейн формує підґрунтя для створення сучасної цифрової екосистеми, у межах якої конфіденційність, безпека та довіра реалізуються комплексно. Це сприяє не лише підвищенню ефективності функціонування корпоративних структур, але й забезпечує відповідність їхньої діяльності актуальним міжнародним стандартам інформаційної безпеки.

Разом із тим, застосування блокчейн-технологій супроводжується низкою обмежень, які необхідно враховувати в корпоративному контексті. По-перше, окремі алгоритми консенсусу (зокрема, Proof of Work) характеризуються високими енергетичними витратами та низькою придатністю для масштабних корпоративних мереж. По-друге, актуальною проблемою залишається масштабованість і латентність: процес підтвердження транзакцій у розподіленому середовищі є суттєво більш тривалим порівняно з централізованими системами. По-третє, специфіка збереження персональних даних у блокчейні може суперечити положенням GDPR, зокрема праву на «забуття», що створює правові колізії. Крім того, інтеграція блокчейн-рішень із наявними ERP-, CRM- та іншими корпоративними платформами потребує значних ресурсів і високого рівня технічної експертизи.

## Висновки

Таким чином, упровадження блокчейн-технологій у корпоративні інформаційні системи становить стратегічно важливий етап розвитку цифрової інфраструктури софтверних компаній. Використання децентралізованих механізмів управління доступом, криптографічних протоколів захисту та незмінності записів істотно знижує ймовірність витоку інформації, внутрішніх

зловживань і кібератак. У корпоративному середовищі блокчейн виступає не лише технологією зберігання даних, а й фундаментом нової парадигми взаємодії, де прозорість, довіра та відповідальність стають ключовими складовими цифрової культури.

Практичне застосування блокчейн-рішень у корпоративних процесах підтверджує їхню ефективність у сфері документообігу, фінансових операцій, управління авторським правом і захисту персональних даних. Завдяки цьому формується цілісна екосистема, у якій інформація зберігається у захищеному середовищі з доступом, обмеженим для несанкціонованих користувачів. Водночас прозорість і відстежуваність усіх транзакцій сприяють підвищенню рівня довіри не лише між структурними підрозділами підприємства, але й у взаєминах із зовнішніми партнерами та клієнтами.

Разом із тим, широке впровадження блокчейн-технологій супроводжується низкою практичних викликів. Серед них – необхідність інтеграції з уже існуючими ERP-, CRM- та іншими корпоративними платформами, забезпечення масштабованості рішень і оптимізація енергоспоживання. Важливим чинником успішної реалізації є підготовка кваліфікованого персоналу та формування корпоративної культури інформаційної безпеки, що передбачає дотримання міжнародних стандартів і протоколів захисту даних на всіх рівнях управління.

Перспективними напрямами подальших досліджень є розробка гібридних моделей кібербезпеки, що поєднують блокчейн із технологіями штучного інтелекту та хмарними обчисленнями. Така інтеграція забезпечить не лише високий рівень конфіденційності, а й адаптивність систем до нових загроз, а також ефективне управління великими масивами даних. У перспективі це сприятиме формуванню комплексних платформ корпоративної безпеки, здатних підтримати стійкий розвиток підприємств в умовах глобалізованої цифрової економіки.

У межах проведеного дослідження запропоновано концептуальну модель інтеграції блокчейн-рішень у корпоративні інформаційні системи, що базується на комплексному поєднанні трьох ключових елементів: permissioned blockchain для забезпечення контролю транзакцій і аудиту; токенізація доступу як механізм гнучкого управління правами користувачів; розподілене зберігання ключів для мінімізації внутрішніх загроз. Зазначена архітектура забезпечує синергетичний ефект, поєднуючи високий рівень конфіденційності, прозорості та стійкості корпоративних систем до кібератак із відповідністю сучасним міжнародним стандартам інформаційної безпеки.

## Список літератури

1. The EU General Data Protection Regulation (GDPR): A Commentary / C. Kuner, L. A. Bygrave, C. Docksey. – Oxford : Oxford University Press, 2020. – (Updated 2021).

2. Solove, D. J. The Limitations of Privacy Rights // Notre Dame Law Review. – 2022/2023.

3. A Guide to Privacy by Design / Agencia Española de Protección de Datos (AEPD). – 2019.

4. Blockchain and the General Data Protection Regulation (GDPR): Reconciling Two Conflicting Positions? : Study / European Parliamentary Research Service. – 2019.

5. Pylypchuk, V. H. Reform and development of the personal data protection system in Ukraine / V. H. Pylypchuk, V. M. Bryzhko // Information and Law. – 2017.

6. Головацький Н. Т. Правове регулювання захисту персональних даних:

GDPR та досвід України // Вісник юридичного факультету УжНУ. – 2024.

7. Врублевська-Місюна, К. М. Міжнародно-правові стандарти захисту персональних даних та їх імплементація в Україні // Вісник юридичного факультету УжНУ. – 2022.

8. Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity / ENISA. – 2019.

9. Cyber Security Culture in Organisations / ENISA. – 2018.

10. Баранов, О. А. Інтернет речей (IoT) і блокчейн // Інформація і право. – 2018. – № 1(24).

11. Чукут, С. А. Блокчейн чи система електронного документообігу: правові аспекти впровадження // Інвестиції: практика та досвід. – 2018.

12. Data Protection Engineering (including GDPR Pseudonymisation Guidelines) / ENISA, ISMS Forum. – 2021.

13. Trends in Network Security and Data Protection : аналіт. звіт / Gartner. – 2024. – Режим доступу: https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartneridentifies-top-cybersecurity-trends-for-2024 (дата звернення: 10.08.2025).

14. Електронне урядування та електронна демократія. Ч. 13: Захист інформації в системах електронного урядування / за заг. ред. А. І. Семенченка, В. М. Дрешпака. – Київ : ФОП Москаленко О. М., 2017. – 72 с.

15. Про доступ до публічної інформації : Закон України № 2939-VI від 13.01.2011. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 18.08.2025).

16. Посібник з європейського права у сфері захисту персональних даних / Агенція Європейського Союзу з питань основоположних прав та Рада Європи. – Київ, 2018. – 432 с. – Режим доступу: https://www.echr.coe.int/Documents/Handbook_data_protection_UKR.pdf (дата звернення: 15.08.2025).

17. Цілина, М. Зарубіжний досвід забезпечення захисту конфіденційної інформації // Український журнал з бібліотекознавства та інформаційних наук. – 2022. – № 9. – С. 22–32. – Режим доступу: https://doi.org/10.31866/2616-7654.9.2022.259142 (дата звернення: 20.08.2025).

18. Про захист персональних даних : Закон України № 2297-VI від 01.06.2010. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 20.08.2025).

19. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. – Wiley, 2021.

20. Про інформацію : Закон України № 2657-XII від 02.10.1992. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 22.09.2025).

21. Cisco Cybersecurity Reports : огляд сучасних атак та методів захисту мереж / Cisco Systems. – 2022. – Режим доступу: https://www.cisco.com/c/en/us/products/security/cybersecurity-reports.html (дата звернення: 14.08.2025).

22. Ouaknine, E. The Importance of Document Security and How to Make Sure You Are Working Safely. – 2020. – Режим доступу: https://www.upslide.net/en/the-importance-of-document-security-and-how-to-make-sure-you-are-working-safely/ (дата звернення: 14.08.2025).

23. Особливості роботи з документами з грифом «Для службового користування» // Юридична газета online. – 2019. – Режим доступу: https://yur-gazeta.com/publications/practice/sudova-praktika/osoblivosti-roboti-z-dokumentami-z-grifom-dlya-sluzhbovogo-koristuvannya.html (дата звернення: 10.08.2025).

24. Україна 2030е – країна з розвинутою цифровою економікою / Український інститут майбутнього. – 2018. – Режим доступу: https://strategy.uifuture.org/kraina-z-rozvinutoyucifrovoyuekonomikoyu.html#6-2-2

(дата звернення: 15.08.2025).

25. Криптографічні алгоритми шифрування AES, RSA, ECC : огляд сучасних технологій. – Режим доступу: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/ (дата звернення: 05.08.2025).

26. Carbo Dzh. Don’t Just Rely On Data Privacy Laws to Protect Information. – 2020. – Режим доступу: https://www.securitymagazine.com/articles/91775-dont-just-rely-on-data-privacy-laws-to-protect-information (дата звернення: 15.08.2025).

27. Інтеграція України у Єдиний цифровий ринок ЄС: потенційні економічні переваги. – Київ, 2020. – Режим доступу: https://ucep.org.ua/doslidzhennya/intehratsiia-ukrainy-u-yedynyi-tsyfrovyi-rynok-es-potentsiini-ekonomichni-perevahy.html (дата звернення: 10.08.2025).

28. Мединська, Т. В. Цифровізація органів податкового адміністрування в контексті сучасних викликів і загроз / Т. В. Мединська, Н. М. Ногінова // Наукові записки Національного університету «Острозька академія». Серія «Економіка». – 2022. – № 24(52). – С. 90–96.

## References

1. Kuner, C., Bygrave, L. A. and Docksey, C. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford: Oxford University Press (Updated 2021).

2. Solove, D. J. (2022/2023). The Limitations of Privacy Rights. Notre Dame Law Review.

3. Agencia Española de Protección de Datos (AEPD) (2019). A Guide to Privacy by Design.

4. European Parliamentary Research Service (2019). Blockchain and the General Data Protection Regulation (GDPR): Reconciling Two Conflicting Positions? Study.

5. Pylypchuk, V. H. and Bryzhko, V.M. (2017). Reform and development of the personal data protection system in Ukraine. Information and Law.

6. Holovatskyi, N. T. (2024). Pravove rehuliuvannia zakhystu personalnykh danykh: GDPR ta dosvid Ukrainy. Visnyk Yurydychnoho Fakultetu UzhNU.

7. Vrublevska-Misiuna, K. M. (2022). Mizhnarodno-pravovi standarty zakhystu personalnykh danykh ta yikh implementatsiia v Ukraini. Visnyk Yurydychnoho Fakultetu UzhNU.

8. ENISA (2019). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity.

9. ENISA (2018). Cyber Security Culture in Organisations.

10. Baranov, O. A. (2018). Internet rechei (IoT) i blokchein. Informatsiia i Pravo, 1(24).

11. Chukut, S. A. (2018). Blokchein chy systema elektronnoho dokumentoobihu: pravovi aspekty vprovadzhennia. Investytsii: Praktyka ta Dosvid.

12. ENISA and ISMS Forum (2021). Data Protection Engineering (including GDPR Pseudonymisation Guidelines).

13. Gartner (2024). Trends in Network Security and Data Protection. Available at: https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartneridentifies-top-cybersecurity-trends-for-2024 (Accessed: 10 August 2025).

14. Semenchenko, A. I. and Dreshpak, V. M. (eds.) (2017). Elektronne uriaduvannia ta elektronna demokratiia. Part 13: Zakhyst informatsii v systemakh elektronnoho uriaduvannia. Kyiv: FOP Moskalenko O.M.

15. Verkhovna Rada of Ukraine (2011). Pro dostup do publichnoi informatsii: Law No. 2939-VI of 13 January 2011. Available at:

https://zakon.rada.gov.ua/laws/show/2939-17#Text (Accessed: 18 August 2025).

16. European Union Agency for Fundamental Rights and Council of Europe (2018). Posibnyk z yevropeiskoho prava u sferi zakhystu personalnykh danykh. Kyiv. Available at: https://www.echr.coe.int/Documents/Handbook_data_protection_UKR.pdf (Accessed: 15 August 2025).

17. Tsilyna, M. (2022). Zarubizhnyi dosvid zabezpechennia zakhystu konfidentsiinoi informatsii. Ukrainskyi Zhurnal z Bibliotekoznavstva ta Informatsiinykh Nauk, 9, pp. 22–32. https://doi.org/10.31866/2616-7654.9.2022.259142

18. Verkhovna Rada of Ukraine (2010). Pro zakhyst personalnykh danykh: Law No. 2297-VI of 1 June 2010. Available at: https://zakon.rada.gov.ua/laws/show/2297-17#Text (Accessed: 20 August 2025).

19. Schneier, B. (2021). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.

20. Verkhovna Rada of Ukraine (1992). Pro informatsiiu: Law No. 2657-XII of 2 October 1992. Available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text (Accessed: 22 September 2025).

21. Cisco Systems (2022). Cisco Cybersecurity Reports. Available at: https://www.cisco.com/c/en/us/products/security/cybersecurity-reports.html (Accessed: 14 August 2025).

22. Ouaknine, E. (2020). The Importance of Document Security and How to Make Sure You Are Working Safely. Available at: https://www.upslide.net/en/the-importance-of-document-security-and-how-to-make-sure-you-are-working-safely/ (Accessed: 14 August 2025).

23. Yurydychna Hazeta Online (2019). Osoblyvosti roboty z dokumentamy z hryfom “Dlia sluzhbovoho korystuvannia”. Available at: https://yur-gazeta.com/publications/practice/sudova-praktika/osoblivosti-roboti-z-dokumentami-z-grifom-dlya-sluzhbovogo-koristuvannya.html (Accessed: 10 August 2025).

24. Ukrainian Institute for the Future (2018). Ukraina 2030e – kraina z rozvynutoiu tsyfrovoiu ekonomikoiu. Available at: https://strategy.uifuture.org/kraina-z-rozvinutoyucifrovoyu-ekonomikoyu.html#6-2-2 (Accessed: 15 August 2025).

25. Hostpro (2025). Kryptohrafichni alhorytmy shyfruvannia AES, RSA, ECC: ohliad suchasnykh tekhnolohii. Available at: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/ (Accessed: 5 August 2025).

26. Carbo, Dzh. (2020). Don’t Just Rely on Data Privacy Laws to Protect Information. Available at: https://www.securitymagazine.com/articles/91775-dont-just-rely-on-data-privacy-laws-to-protect-information (Accessed: 15 August 2025).

27. UCEP (2020). Intehratsiia Ukrainy u Yedynyi tsyfrovyi rynok YeS: potentsiini ekonomichni perevahy. Available at: https://ucep.org.ua/doslidzhennya/intehratsiia-ukrainy-u-yedynyi-tsyfrovyi-rynok-es-potentsiini-ekonomichni-perevahy.html (Accessed: 10 August 2025).

28. Medynska, T. V. and Nohinova, N. M. (2022). Tsyfrovizatsiia orhaniv podatkovoho administruvannia v konteksti suchasnykh vyklykiv i zahroz. Naukovi Zapysky Natsionalnoho Universytetu “Ostrozka Akademiia”. Seriia “Ekonomika”, 24(52), pp. 90–96.

Надійшла до редакції 06.02.2026, розглянута на редколегії 10.02.2026

 ISSN 2071-1077(print)
ISSN 2663-2411(online

# Models and Methods for Ensuring Confidentiality in Corporate Systems of Software Firms Based on Blockchain Technology

This article examines the issues of ensuring data confidentiality in corporate information systems of software companies and substantiates the feasibility of using blockchain technology as a basis for building decentralized access control models. A review of classical approaches based on the Bell–LaPadula, Brewer–Nash, and Clark–Wilson models is conducted, and their limitations in multi-user environments with highly dynamic changes in rights and roles are demonstrated. A generalized architecture for ensuring confidentiality and decentralized access management in corporate information systems is proposed, integrating three key components: a permissioned blockchain for guaranteed auditing and record immutability, access tokenization for flexible and context-aware authorization management, and distributed cryptographic key storage (multi-signature and Shamir's Secret Sharing) to minimize internal threats and abuse. It is shown that the use of smart contracts for formalizing and automatically enforcing access policies enables automated granting and revocation of rights as well as transparent real-time transaction logging. Practical areas of implementation are outlined, including electronic document management, financial operations, compliance and auditing, software copyright management, and identity and personal data protection in accordance with GDPR requirements. Technological and legal challenges, such as scalability and latency, energy consumption of certain consensus algorithms, conflicts with the "right to be forgotten," and integration with ERP/CRM systems, are analyzed. The study concludes that integrating blockchain with modern cryptographic tools creates a comprehensive trust ecosystem that enhances data confidentiality and resilience of corporate systems to cyberattacks and provides a foundation for further research into hybrid models involving artificial intelligence and cloud computing.

**Keywords**: confidentiality; corporate systems; blockchain; cryptography; software companies; information security.

**Відомості про авторів:**

**Єрьоменко Артем Дмитрович** – аспірант кафедри інженерії програмного забезпечення, м. Харків, Національний аерокосмічний університет, Україна, a.yeromenko@khai.edu, +380664851101, ORCID: 0009-0009-2621-7797

**Феоктистова Олена Ігорівна** – к.т.н., доцент кафедри інженерії програмного забезпечення, м. Харків, Національний аерокосмічний університет, Україна, o.feoktystova@khai.edu, +380955194499, ORCID:0000-0001-8490-3108

**About the authors:**

**Artem YEROMENKO** – PhD student, Department of Software Engineering, Kharkiv, National Aerospace University, Ukraine, a.yeromenko@khai.edu, +380664851101, ORCID: 0009-0009-2621-7797

**Olena FEOKTYSTOVA** – PhD in Technical Sciences, Associate Professor, Department of Software Engineering, Kharkiv, National Aerospace University, Ukraine, o.feoktystova@khai.edu, +380955194499, ORCID: 0000-0001-8490-3108