КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.780
УДК 004.51

Твердохліб Арсеній Олександрович
аспірант кафедри комп'ютерної інженерії
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0002-6591-2866
a.tverdokhlib@stud.duikt.edu.ua

МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У ВИСОКОНАВАНТАЖЕНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ ЗА ДОПОМОГОЮ СМАРТ-КОНТРАКТІВ

Анотація. Розвиток високонавантажених комп'ютерних систем у сучасних інформаційних середовищах є критично важливим аспектом технологічного прогресу, який зумовлює необхідність розробки новітніх підходів до забезпечення їхньої кібербезпеки. Висока інтенсивність обміну даними, складність обчислювальних процесів та велика кількість взаємодіючих вузлів формують серйозні виклики для традиційних методів захисту інформації. Класичні централізовані моделі безпеки поступово втрачають свою ефективність через високий ризик компрометації центрів обробки даних, можливість здійснення атак типу «відмова в обслуговуванні» (DDoS), несанкціонованого доступу та експлуатації вразливостей систем. У даній статті запропоновано концептуальний підхід до підвищення рівня кібербезпеки високонавантажених комп'ютерних систем шляхом інтеграції технологій блокчейну та смарт-контрактів. Проведено ґрунтовний аналіз актуальних загроз і ризиків, що притаманні таким системам, а також досліджено ефективність використання смарт-контрактів у контексті аутентифікації користувачів, контролю доступу, верифікації даних та захисту від атак. Особливу увагу приділено перевагам децентралізованих рішень для забезпечення кібербезпеки, включаючи усунення єдиної точки відмови, підвищення прозорості безпекових процесів та автоматизацію механізмів контролю. Запропонована архітектурна модель ґрунтується на використанні смарт-контрактів для управління доступом до обчислювальних ресурсів, перевірки цілісності транзакцій та мінімізації впливу зовнішніх загроз. Аналіз останніх досліджень у сфері блокчейн-технологій та їхнього застосування у високонавантажених середовищах дозволив оцінити перспективність впровадження такого підходу. Результати дослідження демонструють, що інтеграція смарт-контрактів у високонавантажені комп'ютерні системи сприяє підвищенню рівня безпеки завдяки автоматизації процесів перевірки даних, виключенню посередників у транзакціях та посиленню стійкості до атак. Окреслено перспективні напрями подальших наукових досліджень, зокрема оптимізацію механізмів виконання смарт-контрактів для зниження обчислювального навантаження, а також інтеграцію блокчейн-рішень у гібридні моделі безпеки, що поєднують децентралізовані та централізовані підходи.

Ключові слова: кібербезпека; високонавантажені комп'ютерні системи; блокчейн; смарт-контракти; контроль доступу; криптографія; захист даних; розподілені обчислення.

ВСТУП

Сучасні високонавантажені комп'ютерні системи відіграють ключову роль у функціонуванні численних критично важливих галузей, зокрема фінансового сектору, хмарних обчислень, інтернету речей, штучного інтелекту, обробки великих даних та розподілених інформаційних систем [1]. Високий рівень інтенсивності обробки інформації, зростання кількості підключених пристроїв та необхідність забезпечення безперервності функціонування цих систем створюють нові виклики для розробників щодо розробки та впровадження ефективних механізмів захисту від кіберзагроз [2], [3].

Зі збільшенням масштабів використання високонавантажених систем відбувається пропорційне зростання рівня кіберзагроз. Централізовані методи управління безпекою демонструють низку обмежень, що негативно впливають на їхню ефективність. Зокрема, компрометація централізованих серверів може спричинити втрату контролю над усією системою [4]. Крім того, атаки типу «відмова в обслуговуванні» можуть значно знизити продуктивність та доступність обчислювальних ресурсів [5], тоді як можливість несанкціонованої модифікації даних становить серйозний ризик для їхньої цілісності та достовірності [6]. Відсутність прозорості в управлінні безпекою створює додаткові труднощі у формуванні довіри між сторонами та потребує залучення посередників для гарантування відповідності стандартам захисту.

Одним із перспективних підходів до вирішення зазначених проблем є використання технологій блокчейну та смарт-контрактів [7]. Блокчейн забезпечує децентралізовану архітектуру, що мінімізує ризики централізованого контролю та компрометації даних. Смарт-контракти, у свою чергу, дозволяють автоматизувати критично важливі процеси, включаючи контроль доступу, перевірку автентичності транзакцій та моніторинг активності в системі [8, с. 12]. Висока прозорість і незмінність записів у блокчейні гарантують збереження та захист інформації від несанкціонованих змін [9, с. 42].

Інтеграція смарт-контрактів у високонавантажені комп’ютерні системи сприяє створенню децентралізованих механізмів автентифікації та авторизації. Смарт-контракти забезпечують автоматизоване управління доступом до обчислювальних ресурсів, перевірку цілісності даних і запобігання кібератакам. Крім того, усунення необхідності залучення посередників у процесах безпеки сприяє підвищенню ефективності захисту та зменшенню ризиків внутрішніх загроз.

Дослідження можливостей інтеграції смарт-контрактів у високонавантажені комп’ютерні системи є актуальним напрямом сучасної науки. У цій статті здійснено комплексний аналіз механізмів забезпечення кібербезпеки на основі блокчейну. Проведено всебічний аналіз сучасних загроз, ідентифіковано основні недоліки традиційних підходів до безпеки та запропоновано концептуальну модель використання смарт-контрактів для підвищення рівня захищеності таких систем.

Постановка проблеми. Високонавантажені комп’ютерні системи є фундаментальною складовою цифрової економіки, телекомунікаційної інфраструктури, фінансових операцій, державного управління та хмарних обчислень [10]. Їхня безперервна взаємодія з користувачами та іншими системами створює значні виклики щодо забезпечення кібербезпеки. Постійне зростання обсягу цифрових даних, які передаються та обробляються у таких системах, підвищує ймовірність зловмисного втручання [11, с. 27].

Динамічний розвиток кіберзагроз, що спрямовані на високонавантажені комп’ютерні системи, вимагає адаптації існуючих підходів до захисту інформації. Несанкціонований доступ до конфіденційних даних може спричинити порушення безперервності функціонування системи [12]. Зловмисні дії, спрямовані на модифікацію або знищення критично важливої інформації, становлять серйозну загрозу цілісності інформаційних процесів [13]. Масові розподілені атаки на відмову в обслуговуванні можуть призвести до суттєвого зниження продуктивності та недоступності цифрових ресурсів для легітимних користувачів [14, с. 55].

Традиційні методи забезпечення кібербезпеки зазвичай ґрунтуються на централізованих системах автентифікації та контролю доступу. Однак концентрація ідентифікаційних даних у централізованих вузлах створює критичну вразливість:

компрометація такого вузла може спричинити загрозу безпеці всього цифрового середовища. Крім того, багаторівневі механізми контролю доступу часто не встигають адаптуватися до швидко змінюваних кіберзагроз, що зумовлює виникнення додаткових вразливостей.

Методи виявлення загроз, засновані на аналізі поведінки користувачів і мережевого трафіку, працюють із затримкою, що дозволяє зловмисникам реалізовувати атаки до активації захисних механізмів. Централізовані підходи до автентифікації, такі як паролі або двофакторна аутентифікація, не гарантують належного рівня безпеки, оскільки можуть бути обійдені шляхом соціальної інженерії або мережевих атак.

Блокчейн-технологія пропонує новітню парадигму забезпечення кібербезпеки високонавантажених комп'ютерних систем, усуваючи необхідність централізованого управління і забезпечуючи прозорість та незмінність даних. Децентралізований контроль доступу, реалізований через смарт-контракти, дозволяє автоматизувати перевірку прав користувачів без залучення посередників, що значно підвищує рівень безпеки. Смарт-контракти можуть виконувати функції управління цифровими ідентифікаціями, автентифікації користувачів та перевірки їхніх дій, що мінімізує ризики шахрайства та витоку конфіденційних даних.

Автоматизовані системи реагування на загрози, засновані на смарт-контрактах, здатні блокувати потенційно небезпечні дії в режимі реального часу, що значно зменшує ймовірність компрометації системи. Крім того, смарт-контракти можуть бути інтегровані з механізмами виявлення аномальної активності та моніторингу транзакцій без необхідності безпосереднього втручання адміністраторів.

Інтеграція блокчейн-технологій у високонавантажені комп'ютерні системи сприяє формуванню децентралізованої моделі кібербезпеки, яка усуває єдині точки відмови, мінімізує внутрішні загрози та забезпечує автоматизований контроль безпеки. Використання смарт-контрактів у системах захисту інформації є перспективним напрямом досліджень, що потребує подальшого аналізу ефективності та можливих обмежень даної технології у масштабованих інформаційних середовищах.

У цій статті проведено дослідження можливостей застосування блокчейн-технологій для забезпечення кібербезпеки високонавантажених систем. Крім того, було проаналізовано архітектурні особливості інтеграції смарт-контрактів та пропонується модель їхнього використання для захисту даних і контролю доступу.

Аналіз останніх досліджень і публікацій. Кібербезпека високонавантажених комп'ютерних систем є одним із ключових напрямів сучасних досліджень у сфері інформаційних технологій [1]. В умовах стрімкого зростання цифрових трансакцій, збільшення кількості підключених пристроїв та обсягів оброблюваних даних загрози кібербезпеці набувають дедалі складнішого характеру [2], [3]. У численних наукових дослідженнях акцентується увага на методах протидії несанкціонованому доступу, атакам типу DDoS, витоку даних та іншим формам загроз інформаційної безпеки.

Актуальні дослідження демонструють наявність значних вразливостей централізованих систем автентифікації та контролю доступу. Автори роботи [4, с. 19] аналізують механізми підвищення безпеки, засновані на багатофакторній автентифікації та криптографічних алгоритмах. Водночас централізовані підходи залишаються схильними до атак на сервери автентифікації, що може призвести до компрометації ключових елементів безпеки.

Методи запобігання атакам типу DDoS розглядаються у роботах [5], [6], де пропонується застосування алгоритмів машинного навчання для ідентифікації аномальної активності у мережі. Ці підходи дозволяють підвищити ефективність

виявлення загроз, проте централізовані механізми безпеки не завжди здатні оперативно реагувати на кібератаки без безпосереднього втручання адміністраторів.

Перспективним напрямом розвитку кібербезпеки є використання блокчейн-технологій. У дослідженні [7, с. 33] підтверджено ефективність блокчейну для управління цифровими ідентифікаціями та безпечного зберігання конфіденційної інформації. Основною перевагою цієї технології є відсутність єдиної точки відмови, що суттєво знижує ризики атак на централізовані сервери.

Окремий напрям досліджень присвячений впровадженню смарт-контрактів у забезпечення кібербезпеки. У роботі [8, с. 45] аналізується потенціал смарт-контрактів для автоматизації процесів управління доступом, що усуває необхідність у довірених посередниках та мінімізує ризики шахрайства, несанкціонованого доступу й компрометації облікових записів.

Аналіз провідних наукових праць свідчить, що більшість досліджень зосереджені на окремих аспектах кібербезпеки високонавантажених комп'ютерних систем. Водночас комплексні рішення, які б інтегрували блокчейн, смарт-контракти та автоматизовані механізми реагування на загрози, залишаються недостатньо дослідженими. Подальші наукові розвідки необхідні для розробки ефективної інтеграційної архітектури, здатної забезпечити високий рівень захисту інформаційних ресурсів і стійкість до сучасних атак [9].

У цій статті здійснено комплексний аналіз сучасних методів забезпечення кібербезпеки, визначено їхні обмеження та запропоновано інноваційний підхід на основі блокчейн-технологій і смарт-контрактів для захисту високонавантажених комп'ютерних систем.

Тематика кібербезпеки високонавантажених комп'ютерних систем набуває дедалі більшої актуальності у науковому середовищі, оскільки цифрова трансформація суспільства вимагає розробки ефективних стратегій захисту інформаційних ресурсів. Багато сучасних досліджень зосереджено на аспектах автентифікації, контролю доступу, моніторингу мережевого трафіку та запобігання атакам типу «відмова в обслуговуванні» (DDoS).

Традиційні підходи до забезпечення кібербезпеки базуються на централізованих моделях управління ідентифікацією та контролем доступу. У дослідженні [13] проаналізовано класичні методи автентифікації, зокрема багатофакторну аутентифікацію та криптографічні механізми захисту даних. Автори зазначають, що централізовані системи автентифікації мають низку критичних вразливостей, зокрема ризик компрометації серверів та викрадення облікових даних користувачів.

Мета статті. Метою даного дослідження є ґрунтовний аналіз методів підвищення рівня кібербезпеки високонавантажених комп'ютерних систем шляхом застосування технології блокчейн та смарт-контрактів. У роботі розглядається потенціал децентралізованих моделей управління доступом, механізмів автоматизованої автентифікації користувачів, а також підходів до забезпечення цілісності даних у розподілених інформаційних середовищах.

У статті здійснено комплексний аналіз можливостей блокчейн-орієнтованих рішень для подолання вразливостей, притаманних традиційним централізованим системам кібербезпеки. Особливу увагу приділено дослідженню ефективності використання смарт-контрактів у процесах управління доступом до ресурсів, безперервного моніторингу безпеки та оперативного реагування на кібератаки. Запропонована концептуальна модель інтеграції блокчейн-технологій спрямована на підвищення рівня стійкості високонавантажених систем до актуальних кіберзагроз, з урахуванням вимог до масштабованості, продуктивності та стійкості до зовнішніх атак.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Технологія блокчейн у кібербезпеці високонавантажених систем. Блокчейн є однією з ключових розподілених технологій, що забезпечує стійкість до несанкціонованих модифікацій, маніпуляцій та кібератак [1, с. 17]. Фундаментальний принцип його функціонування полягає у збереженні даних у послідовному ланцюжку блоків, де кожен наступний блок містить хеш попереднього. Така архітектура гарантує незмінність інформації та унеможливлює її фальсифікацію або видалення без колективного схвалення всіх учасників розподіленої мережі [2, с. 22].

Однією з найвагоміших переваг блокчейн-технології є її децентралізований характер. На відміну від традиційних централізованих систем управління даними, що містять єдину точку відмови, блокчейн розподіляє інформацію між усіма вузлами мережі, що істотно ускладнює можливість компрометації системи шляхом атак на окремий сервер [3]. Це робить блокчейн перспективним механізмом для забезпечення кіберстійкості високонавантажених комп'ютерних систем, що вимагають надійного збереження, доступності та захисту інформаційних ресурсів [4, с. 39].

Таблиця 1

Порівняльна таблиця методів безпеки

Аспект безпеки	Традиційні методи	Блокчейн-рішення
Централізація	Централізований сервер	Децентралізована мережа
Захист даних	Може бути змінений адміністратором	Неможливо змінити запис без консенсусу
Аутентифікація	Логін/пароль, двофакторна аутентифікація	Криптографічні ключі, смарт-контракти
Контроль доступу	ACL, рольові моделі	Автоматизовані смарт-контракти
Стійкість до атак	Слабка стійкість до DDoS-атак	Висока стійкість до DDoS-атак
Прозорість та аудит	Закриті журнали подій	Публічний, незмінний реєстр
Автоматизація безпеки	Потребує людського втручання	Автоматичне виконання правил безпеки

Застосування блокчейну в сфері кібербезпеки дозволяє вирішити низку критично важливих завдань. По-перше, він ефективно протидіє несанкціонованим змінам даних, оскільки внесення змін хоча б до одного запису потребує коригування всіх наступних блоків, що потребує значних обчислювальних ресурсів [5]. По-друге, він забезпечує високий рівень прозорості процесів аутентифікації та контролю доступу, оскільки всі дії в системі фіксуються у розподіленому реєстрі, що дозволяє їхню незалежну верифікацію без можливості підробки [6, с. 48].

У сфері високонавантажених комп'ютерних систем блокчейн широко застосовується для управління цифровими ідентифікаціями, реєстрації подій доступу та контролю цілісності транзакцій. Це сприяє створенню надійніших механізмів автентифікації, що не залежать від централізованих серверів та мінімізують ризик викрадення даних унаслідок їхньої компрометації.

Ще однією важливою особливістю блокчейну є його здатність до ефективного запобігання атакам типу «відмова в обслуговуванні» (DDoS). Оскільки інформація розподілена між великою кількістю вузлів, атакуючий суб'єкт не має змоги вивести систему з ладу шляхом перевантаження єдиного серверного компонента [7, с. 32]. Це особливо критично для високонавантажених систем, що працюють у режимі безперервної обробки та передачі великих обсягів даних [8].

Крім того, впровадження блокчейн-технологій сприяє підвищенню рівня довіри між учасниками цифрового середовища. У контексті розподілених обчислювальних систем, де взаємодія відбувається між численними суб'єктами, блокчейн забезпечує незалежну перевірку всіх транзакцій без потреби залучення довірених посередників. Це знижує ризики шахрайства, а також мінімізує ймовірність несанкціонованих маніпуляцій з даними.

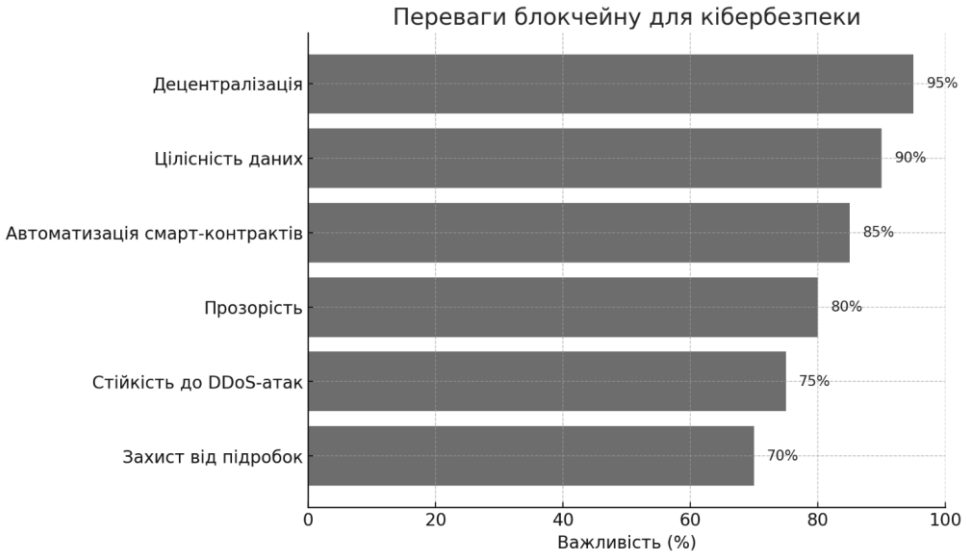

Рис. 1. Переваги блокчейну для кібербезпеки

Так, блокчейн постає як ефективна технологія для підвищення рівня кібербезпеки високонавантажених комп'ютерних систем. Його децентралізована архітектура, висока стійкість до атак та прозорість обробки даних створюють надійне середовище для захисту інформаційних систем нового покоління [15].

Смарт-контракти як інструмент кібербезпеки. У сучасних інформаційних системах, що характеризуються високим рівнем навантаження та потребою у підвищеній безпеці, дедалі більше застосовуються технології автоматизованого контролю доступу та аутентифікації. Одним із перспективних підходів до їх реалізації є використання смарт-контрактів — автономних програмних алгоритмів, що функціонують у середовищі блокчейн-мережі та виконують наперед визначені умови без залучення довірених посередників [9]. Основною перевагою цього підходу є його здатність гарантувати високий рівень надійності та прозорості процесів, що є критичним фактором у забезпеченні кіберстійкості високонавантажених комп'ютерних систем [10, с. 29]. Завдяки незмінності коду та механізму автоматизованого виконання, смарт-контракти значно знижують імовірність несанкціонованого втручання в роботу інформаційної інфраструктури [11, с. 53].

Одним із ключових аспектів використання смарт-контрактів є їхня здатність до автоматизації механізмів контролю доступу. Традиційні системи автентифікації та управління доступом часто спираються на централізовані сервери, що створює потенційні точки відмови та підвищує ризик атак на цілісність даних [12]. Використання смарт-контрактів дозволяє реалізувати децентралізовані моделі контролю доступу, де права користувачів та регламенти взаємодії фіксуються безпосередньо у блокчейні та не можуть бути змінені без відповідної авторизації [13, с. 45].

Крім того, смарт-контракти демонструють високу ефективність у процесах перевірки автентичності користувачів. У традиційних системах цей процес найчастіше

базується на використанні паролів або багатофакторної автентифікації, що, попри поширеність, не гарантує абсолютного рівня безпеки. Натомість смарт-контракти можуть виконувати автоматизовану верифікацію особи за допомогою цифрових підписів або унікальних криптографічних ідентифікаторів. Це суттєво ускладнює можливість компрометації облікових даних та підвищує загальний рівень захисту системи від несанкціонованого доступу.

Ще одним важливим напрямом застосування смарт-контрактів є їхня здатність запобігати несанкціонованим змінам у системі. Усі модифікації конфігурацій безпеки або параметрів доступу можуть здійснюватися виключно через алгоритми смарт-контрактів, що забезпечує прозорість процесу та його відповідність заданим політикам безпеки. У разі спроби несанкціонованого доступу або зміни критично важливих параметрів система автоматично блокує ці дії, що мінімізує ризики кібератак та внутрішніх загроз.

Оскільки високонавантажені комп'ютерні системи працюють у середовищі, де важливими є не лише безпека, а й швидкість обробки інформації та безперервність функціонування, інтеграція смарт-контрактів дозволяє реалізувати автоматизований моніторинг транзакцій та подій у реальному часі. Це забезпечує прискорене виявлення потенційних загроз та оперативне реагування на інциденти. Завдяки можливості інтеграції з системами кібербезпеки смарт-контракти можуть активувати захисні механізми у разі виявлення підозрілих дій або спроб модифікації даних.

Додатково, використання смарт-контрактів дозволяє значно знизити вплив людського фактора на рівень кібербезпеки. Автоматизація процесів аутентифікації, управління доступом та контролю за подіями унеможливлює виникнення помилок адміністраторів та виключає можливість зловмисних дій з боку внутрішніх користувачів. Це особливо важливо для секторів, що оперують конфіденційною інформацією, зокрема фінансових установ, державних інформаційних систем та корпоративних мереж, де людський фактор залишається однією з найвразливіших ланок безпеки.

Запропонована модель передбачає використання блокчейн-технології як основи для реалізації децентралізованого управління доступом, моніторингу загроз та автоматизованого реагування на кіберінциденти. На схемі (рис. 2) представлено основні структурні компоненти системи та принципи їхньої взаємодії.

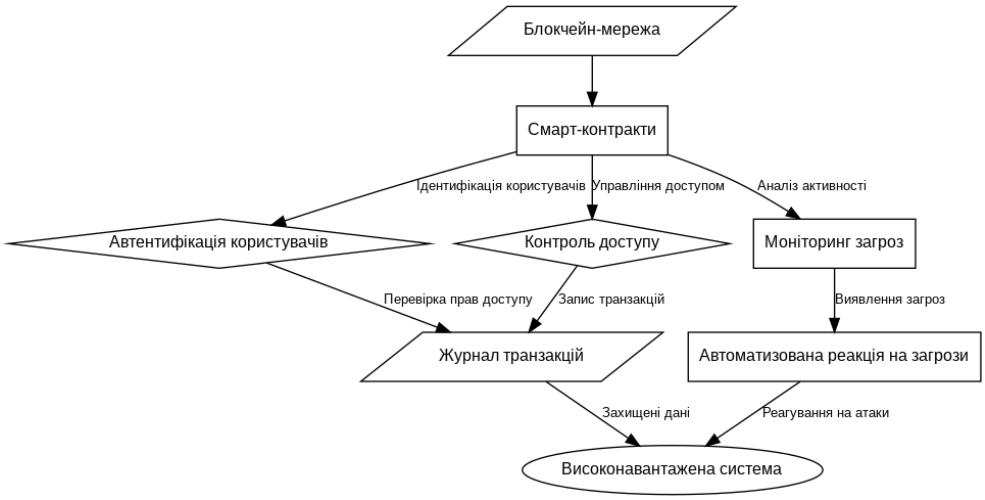

Рис. 2. Інтеграція смарт-контрактів у високонавантажені комп'ютерні системи

Таким чином, смарт-контракти є перспективним технологічним рішенням у сфері забезпечення кібербезпеки високонавантажених комп'ютерних систем. Їхнє використання дозволяє досягти високого рівня автоматизації процесів контролю доступу, автентифікації користувачів та протидії несанкціонованим діям, що сприяє мінімізації ризиків кібератак та покращенню загальної стійкості інформаційних середовищ.

Запропонована модель інтеграції смарт-контрактів у високонавантажені системи. Сучасні високонавантажені комп'ютерні системи функціонують у складному кіберсередовищі, що вимагає розробки та впровадження ефективних механізмів забезпечення безпеки. Особливу увагу варто приділяти методам контролю доступу, захисту даних та запобігання кіберзагрозам, які забезпечують безперебійну роботу інформаційної інфраструктури [1]. У цьому контексті інтеграція смарт-контрактів виступає перспективним напрямом, оскільки їх застосування сприяє автоматизації процесів автентифікації, моніторингу активності користувачів та контролю доступу, що безпосередньо підвищує рівень кібербезпеки [2, с. 15].

Одним із ключових аспектів впровадження смарт-контрактів є їхня здатність здійснювати автентифікацію користувачів на основі цифрових ідентифікаторів без залучення централізованих серверів [3, с. 24]. Завдяки використанню передових криптографічних алгоритмів ці механізми гарантують високий рівень безпеки, унеможливлюючи підробку або компрометацію автентифікаційних даних [4]. Крім того, усі транзакції та дії користувачів реєструються у розподіленій мережі блокчейну, що забезпечує прозорий аудит доступу та виключає ймовірність несанкціонованих змін або видалення записів [5, с. 38].

Функціонал смарт-контрактів також охоплює контроль доступу до ресурсів, який реалізується шляхом перевірки користувацьких прав відповідно до наперед визначених правил [6]. Запити на авторизацію обробляються в автоматичному режимі, що дозволяє мінімізувати людський фактор та запобігти потенційним загрозам, пов'язаним із компрометацією адміністраторських облікових записів [7, с. 42]. У разі виявлення порушень політик безпеки смарт-контракти автоматично блокують спроби несанкціонованого доступу, тим самим знижуючи ризики зовнішніх та внутрішніх атак [8, с. 50].

Не менш важливою є функція моніторингу активності користувачів у режимі реального часу. Усі дії, пов'язані з автентифікацією та доступом до системи, фіксуються у блокчейні, що надає можливість детального аналізу та перевірки записів будь-яким учасником мережі [9, с. 61]. Такий підхід сприяє виявленню аномальної активності та дозволяє ефективно аналізувати потенційні загрози, запобігаючи шахрайським діям [10]. Додатково, використання алгоритмів машинного навчання для обробки транзакцій підвищує точність виявлення атак та сприяє адаптивному налаштуванню захисних механізмів [11, с. 74].

Однією з визначальних переваг смарт-контрактів є їхня здатність здійснювати автоматизоване реагування на кіберзагрози без безпосереднього втручання адміністратора. У разі виявлення потенційно небезпечних дій ці механізми можуть блокувати транзакції, змінювати політики доступу або тимчасово обмежувати взаємодію користувачів із системою [12]. Така модель забезпечує високий рівень стійкості інформаційної інфраструктури до атак, а також мінімізує ймовірність витоку конфіденційних даних або компрометації критичних сервісів [13, с. 83].

ISSN 2663 - 4023

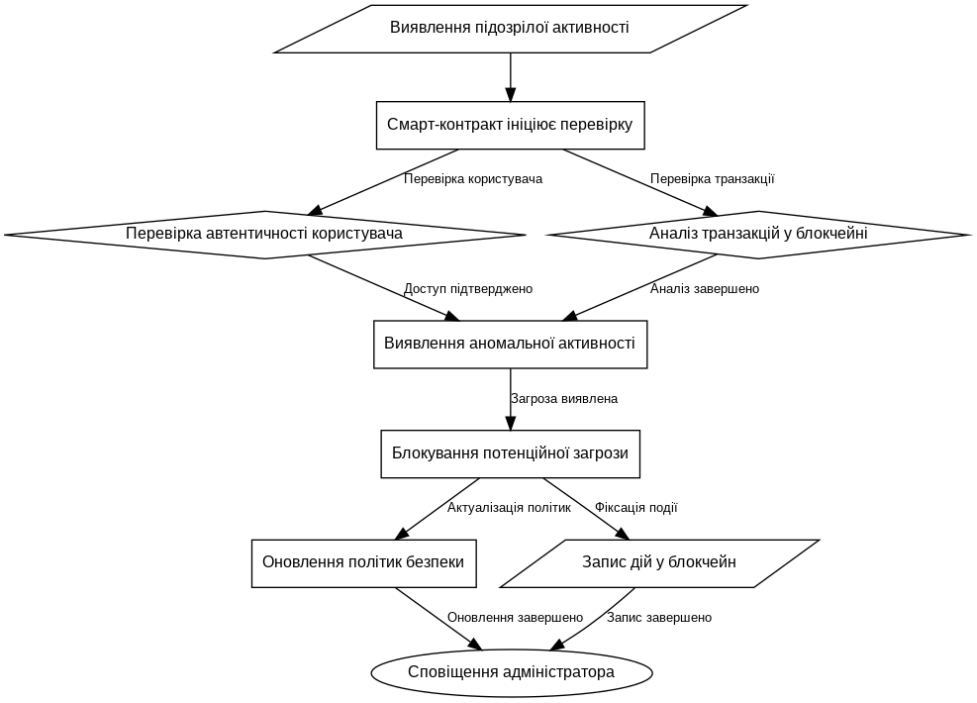

Рис. 3. Автоматизоване реагування на загрози через блокчейн

Загалом, застосування запропонованої моделі інтеграції смарт-контрактів до високонавантажених комп'ютерних систем сприяє усуненню централізованих точок відмови та автоматизації механізмів контролю доступу [14]. Відмова від посередників у процесах автентифікації та авторизації мінімізує ризики атак на сервери ідентифікації та компрометації ключових облікових записів.

Однак, слід зазначити, що висока обчислювальна складність операцій у блокчейні може негативно впливати на продуктивність системи, що вимагає розробки механізмів оптимізації виконання смарт-контрактів [6]. Використання гібридних рішень, що поєднують блокчейн із традиційними методами забезпечення безпеки, дозволяє знизити навантаження на систему та підвищити ефективність обробки даних [7, с. 48].

У підсумку, інтеграція смарт-контрактів у високонавантажені комп'ютерні системи забезпечує високий рівень безпеки, прозорості та стійкості до атак [8, с. 61]. Подальші дослідження у цій галузі мають бути спрямовані на підвищення швидкодії смарт-контрактів, їхню адаптацію до масштабованих обчислювальних середовищ, а також розширення функціональних можливостей механізмів автоматичного реагування на кіберзагрози [9].

ВИСНОВКИ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Сучасні інформаційні технології характеризуються високим рівнем навантаження на комп'ютерні системи, що вимагає інноваційних підходів до забезпечення кібербезпеки. У цьому контексті технологія блокчейну та смарт-контракти відіграють ключову роль, надаючи нові можливості для підвищення захищеності цифрових платформ. У даній статті відзначається, що децентралізована архітектура, прозорість операцій і автоматизація безпекових процесів істотно знижують ризики, пов'язані з вразливостями централізованих систем.

Однією з фундаментальних переваг блокчейну є його здатність забезпечувати цілісність даних, що унеможливлює несанкціоновані модифікації та підвищує рівень довіри до системи. Завдяки механізмам розподіленого зберігання та верифікації транзакцій блокчейн сприяє зниженню ризиків компрометації окремих вузлів мережі та підвищує її стійкість до атак. Крім того, смарт-контракти дозволяють автоматизувати процеси контролю доступу, перевірки автентичності користувачів і моніторингу активності, що мінімізує ймовірність виникнення людських помилок у питаннях безпеки. Автоматизовані механізми реагування на загрози забезпечують оперативне блокування потенційно небезпечних дій і адаптивне налаштування політик безпеки відповідно до актуальних моделей загроз.

Значний науковий інтерес викликає розробка моделей інтеграції смарт-контрактів у високонавантажені інформаційні системи. Запропоновані підходи орієнтовані на усунення обмежень централізованого управління безпекою, підвищення ефективності захисту даних і зниження ймовірності атак. Використання блокчейну як базової інфраструктури для ідентифікації користувачів і перевірки доступу створює надійні механізми кібербезпеки, здатні ефективно функціонувати в розподілених середовищах.

Водночас подальші дослідження у цій сфері є необхідними для покращення продуктивності блокчейн-систем у середовищах із високим рівнем навантаження. Оптимізація алгоритмів виконання смарт-контрактів сприятиме зниженню обчислювальних витрат і підвищенню швидкості обробки транзакцій. Крім того, інтеграція блокчейну з традиційними механізмами забезпечення безпеки дозволить створити гібридні моделі, які поєднують переваги децентралізації та ефективності сучасних інформаційних технологій.

Розширення функціональних можливостей смарт-контрактів у контексті адаптивного управління безпекою, а також впровадження алгоритмів машинного навчання для аналізу загроз, сприятиме подальшому розвитку розподілених механізмів кібербезпеки. Запропонований підхід є перспективним напрямом для застосування у високонавантажених комп'ютерних системах, оскільки він забезпечує автоматизований контроль доступу, підвищену стійкість до атак та безперервний моніторинг загроз у реальному часі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Avada Media. (2023). *Smart Contract Development for DeFi Projects.* https://avada-media.ua/services/razrabotka-smart-kontraktov-dlya-defi-proyektov/
2. Binance Academy. (2022). *What Is a Smart Contract Security Audit?* https://academy.binance.com /uk/articles/what-is-a-smart-contract-security-audit
3. Bright Sky. (2023). *Online Security.* https://us.bright-sky.org/en/online-safety-guide
4. datami. (2024). *Smartphone Security and Cybersecurity*. https://datami.ee/ua/blog/bezpeka-i-kiberbezpeka-smartfoniv/
5. H-X Technologies. (2022). *Contracts in the Digital Age - Smart Contracts.* https://www.h-x.technology/ua/ blog-ua/deals-in-the-digital-age-ua
6. H-X Technologies. (2024). *Smart Account Security.* https://h-x.technology/uk/articles/smart-account-security
7. H-X Technologies. (2025). *Best Smart Contract Analysis Tools 2025.* https://www.h-x.technology/ua/blog-ua/the-best-smart-contract-analysis-tools-2025-ua
8. López Vivar, A., Sandoval Orozco, A. L., & García Villalba, L. J. (2024). *A security framework for Ethereum smart contracts.* arXiv preprint arXiv:2402.03555. https://arxiv.org/abs/2402.03555
9. Mavridou, A., & Laszka, A. (2017). *Designing secure Ethereum smart contracts: A finite state machine based approach.* arXiv preprint arXiv:1711.09327. https://arxiv.org/abs/1711.09327
10. Smart Power. (2023). *How to Protect Your Accounts from Hacking?* https://www.smartpower.com.ua/ 2023/07/07/yak-zahystyty-svoyi-akaunty-vid-zlamu/

11. WhiteBIT. (2024). *Smart Contracts in Blockchain: What They Are and How They Work.* https://blog.whitebit.com/uk/about-smart-contracts/
12. Wikipedia. (2024). *Smart Contract.* https://en.wikipedia.org/wiki/Smart_contract
13. Vashchenok, D. O., & Galchynskyi, L. Yu. (2023). *Improving Smart Contract Security in the Ethereum Network*. Educational and Scientific Physico-Technical Institute. https://ela.kpi.ua/handle/123456789/54876
14. Nadozirnyi, O. V. (2023). *Algorithms and Systems for Protecting Smart Contracts Based on Blockchain Technologies.* West Ukrainian National University. https://dspace.wunu.edu.ua/handle/316497/46437
15. Tverdokhlib, A. O., & Korotin, D. S. (2022). Efficiency of Computer Systems Operation Using Blockchain and Database Technologies. *Tavria Scientific Bulletin. Series: Technical Sciences, (6).* https://journals.ksauniv.ks.ua/index.php/tech/article/view/308/284

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Arsenii Tverdokhlib
Postgraduate Student, Department of Computer Engineering,
State University of Information and Communication Technology, Kyiv, Ukraine
ORCID ID: 0000-0002-6591-2866
a.tverdokhlib@stud.duikt.edu.ua

METHODS OF ENSURING CYBERSECURITY IN HIGHLY LOADED COMPUTER SYSTEMS USING SMART CONTRACTS

Abstract. The development of high-load computing systems in modern information environments represents a critical aspect of technological progress, necessitating the creation of innovative approaches to cybersecurity. The increasing intensity of data exchange, the complexity of computational processes, and the growing number of interacting nodes pose significant challenges to traditional information security methods. Classical centralized security models are gradually losing their effectiveness due to the high risk of data processing center compromise, the vulnerability to denial-of-service (DDoS) attacks, unauthorized access, and system exploits. These risks emphasize the necessity of implementing decentralized security mechanisms that can withstand emerging cyber threats and ensure the reliability of high-load computing infrastructures. This article presents a conceptual approach to enhancing the cybersecurity of high-load computing systems through the integration of blockchain technology and smart contracts. A comprehensive analysis of current threats and risks inherent in such systems has been conducted, along with an investigation into the efficiency of smart contracts in user authentication, access control, data verification, and attack prevention. Particular attention is given to the advantages of decentralized security solutions, including the elimination of single points of failure, the enhancement of transparency in security processes, and the automation of control mechanisms. The study also evaluates the resilience of blockchain-based security frameworks in mitigating both internal and external cyber threats. The proposed architectural model leverages smart contracts for managing access to computing resources, verifying transaction integrity, and minimizing the impact of external threats. The analysis of recent research in blockchain technologies and their application in high-load environments provides insights into the feasibility and advantages of such an approach. By utilizing smart contracts, it becomes possible to automate security procedures, reduce reliance on centralized authentication servers, and ensure that system interactions remain tamper-proof and resistant to adversarial attacks. The research findings indicate that integrating smart contracts into high-load computing systems enhances cybersecurity by automating data verification processes, eliminating intermediaries in transactions, and strengthening resilience against attacks. Furthermore, the study outlines promising directions for future research, including the optimization of smart contract execution mechanisms to reduce computational overhead and the integration of blockchain-based solutions into hybrid security models that combine decentralized and centralized approaches. This approach offers a strategic pathway for developing robust, scalable, and resilient cybersecurity frameworks tailored to the needs of high-performance computing infrastructures.

Keywords: cybersecurity; high-load computer systems; blockchain; smart contracts; access control; cryptography; data protection; distributed computing.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Avada Media. (2023). *Smart Contract Development for DeFi Projects.* https://avada-media.ua/services/razrabotka-smart-kontraktov-dlya-defi-proyektov/
2. Binance Academy. (2022). *What Is a Smart Contract Security Audit?* https://academy.binance.com /uk/articles/what-is-a-smart-contract-security-audit
3. Bright Sky. (2023). *Online Security.* https://us.bright-sky.org/en/online-safety-guide
4. datami. (2024). *Smartphone Security and Cybersecurity*. https://datami.ee/ua/blog/bezpeka-i-kiberbezpeka-smartfoniv/
5. H-X Technologies. (2022). *Contracts in the Digital Age - Smart Contracts.* https://www.h-x.technology/ua/ blog-ua/deals-in-the-digital-age-ua

6. H-X Technologies. (2024). *Smart Account Security*. https://h-x.technology/uk/articles/smart-account-security
7. H-X Technologies. (2025). *Best Smart Contract Analysis Tools 2025.* https://www.h-x.technology/ua/blog-ua/the-best-smart-contract-analysis-tools-2025-ua
8. López Vivar, A., Sandoval Orozco, A. L., & García Villalba, L. J. (2024). *A security framework for Ethereum smart contracts.* arXiv preprint arXiv:2402.03555. https://arxiv.org/abs/2402.03555
9. Mavridou, A., & Laszka, A. (2017). *Designing secure Ethereum smart contracts: A finite state machine based approach.* arXiv preprint arXiv:1711.09327. https://arxiv.org/abs/1711.09327
10. Smart Power. (2023). *How to Protect Your Accounts from Hacking?* https://www.smartpower.com.ua/2023/07/07/yak-zahystyty-svoyi-akaunty-vid-zlamu/
11. WhiteBIT. (2024). *Smart Contracts in Blockchain: What They Are and How They Work.* https://blog.whitebit.com/uk/about-smart-contracts/
12. Wikipedia. (2024). *Smart Contract.* https://en.wikipedia.org/wiki/Smart_contract
13. Vashchenok, D. O., & Galchynskyi, L. Yu. (2023). *Improving Smart Contract Security in the Ethereum Network*. Educational and Scientific Physico-Technical Institute. https://ela.kpi.ua/handle/123456789/54876
14. Nadozirnyi, O. V. (2023). *Algorithms and Systems for Protecting Smart Contracts Based on Blockchain Technologies.* West Ukrainian National University. https://dspace.wunu.edu.ua/handle/316497/46437
15. Tverdokhlib, A. O., & Korotin, D. S. (2022). Efficiency of Computer Systems Operation Using Blockchain and Database Technologies. *Tavria Scientific Bulletin. Series: Technical Sciences, (6).* https://journals.ksauniv.ks.ua/index.php/tech/article/view/308/284