відповідальності. У 2023 році розслідування програми «Схеми» виявило факти зловживань у сфері державних закупівель, що призвело до відкриття кримінальних проваджень та звільнення посадовців. Також, завдяки розслідуванням Bihus.Info було викрито незаконні дії у сфері будівництва, що сприяло припиненню корупційних практик. Електронні петиції стали ефективним інструментом впливу громадян на прийняття рішень. У 2023 році петиція щодо прозорості у використанні бюджетних коштів набрала необхідну кількість голосів, що зобов'язало органи влади розглянути питання та вжити відповідних заходів.

Виявлені у дослідженні кейси доводять, що найефективнішими є ті інструменти, які забезпечують не лише контроль, а й попередження – прозорі процедури, публічність, автоматизовані системи обліку і звітності. Такі приклади, як електронні платформи «Прозоро» і «Є-дата», практика поліграфічних перевірок, створення громадських рад, інтеграція даних через систему «Трембіта» – усе це зменшує простір для ручного втручання та формує нову культуру публічного управління. У подальшому доцільно зосередити зусилля на розширенні практики запровадження комплаєнс-систем у всіх центральних органах виконавчої влади.

Ковальова Тетяна,
кандидат юридичних наук, доцент,
Київський інститут Національної гвардії України

ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ЦІЛІСНОСТІ ОБМІНУ ІНФОРМАЦІЄЮ МІЖ СУБ'ЄКТАМИ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

В умовах складної геополітичної ситуації та гібридних загроз, ефективна міжвідомча взаємодія між суб'єктами сектору безпеки і оборони України є критично важливим фактором забезпечення національної безпеки. Ефективна та безпечна міжвідомча взаємодія є критично важливим елементом забезпечення національної безпеки та обороноздатності України, особливо в умовах триваючої російської агресії та зростання кіберзагроз. Суб'єкти сектору безпеки і оборони України, включаючи Збройні Сили України, Службу безпеки України, Національну гвардію України, Державну прикордонну службу України, розвідувальні органи та інші відомства, здійснюють інтенсивний обмін різноманітною інформацією, необхідною для координації дій, прийняття стратегічних рішень та реагування на загрози. Проте, традиційні методи обміну інформацією часто є вразливими до кібератак, несанкціонованого доступу, витоку та фальсифікації даних. У цьому контексті, технологія блокчейн, завдяки своїм фундаментальним принципам децентралізації, криптографічного захисту та незмінності даних, відкриває нові перспективи для забезпечення безпечного та цілісного обміну інформацією між суб'єктами сектору безпеки і оборони України. Одним з таких інноваційних підходів є використання блокчейн-технологій, які завдяки своїй децентралізованій природі можуть

забезпечити високий рівень захисту даних. Блокчейн, побудований на основі криптографії та розподілених обчислень, дає можливість створювати системи, у яких інформація зберігається та передається без ризику маніпуляцій та несанкціонованого доступу.

На сьогоднішній день інформаційна взаємодія між суб'єктами сектору безпеки і оборони України часто базується на централізованих системах, що створює потенційні точки вразливості. Попри важливість традиційних засобів кіберзахисту, таких як антивіруси, міжмережеві екрани, системи виявлення та запобігання вторгненням (IDS/IPS), шифрування та парольна аутентифікація, їх ефективність не є абсолютною. Антивіруси дієві проти відомих загроз, але вразливі до нових. Фаєрволи контролюють трафік, проте складні атаки можуть їх обходити. IDS/IPS часто генерують хибні тривоги, а безпека шифрування може бути поставлена під сумнів розвитком квантових технологій.

Технологія блокчейн, як розподілений та криптографічно захищений реєстр, пропонує принципово інший підхід до забезпечення безпеки та цілісності даних. Її ключові характеристики, такі як децентралізація, прозорість (у дозволених мережах), незмінність та криптографічний захист, створюють значні переваги для безпечного обміну інформацією між суб'єктами сектору безпеки і оборони України:

Децентралізована архітектура блокчейн ускладнює успішну атаку, оскільки зловмиснику необхідно одночасно скомпрометувати значну кількість незалежних вузлів мережі. Кожен блок інформації криптографічно пов'язаний з попереднім, що унеможливлює непомітну зміну або фальсифікацію даних. Будь-яка спроба модифікації призведе до порушення ланцюжка та буде миттєво виявлена. Створення єдиної, захищеної платформи для обміну інформацією може значно прискорити процеси узгодження даних та підвищити оперативність прийняття рішень.

Для ефективного впровадження блокчейн-технологій у секторі безпеки і оборони України можуть бути розглянуті такі архітектурні моделі: приватний блокчейн (доступ до мережі надається лише авторизованим суб'єктам сектору безпеки і оборони, що забезпечує високий рівень контролю над даними та учасниками), консорціумний блокчейн (мережа контролюється групою авторизованих організацій (наприклад, ключовими відомствами сектору безпеки і оборони), що забезпечує баланс між децентралізацією та контролем).

Використовувати блокчейн-технологій можна для обміну інформацією при реєстрації та обміні інформацією про оперативну обстановку, переміщення сил та засобів, результати спеціальних операцій, обміні розвідувальною інформацією, управлінні доступом до критично важливої інформації, для ідентифікації та авторизації користувачів, для захищеного документообігу, для відстеження постачання військової техніки та обладнання, тощо.

Децентралізовані системи на основі блокчейну демонструють істотні переваги при забезпеченні захисту від кіберзагроз завдяки своїй архітектурі та власним функціональним можливостям.

Водночас існують проблеми, які потребують вирішення. Однією з них є висока енергоємність деяких блокчейн-алгоритмів (наприклад, Proof of Work), що робить їх менш придатними для використання в умовах нестабільного

електропостачання, особливо під час воєнних дій. Іншою проблемою є обмежена масштабованість блокчейн-мереж, що може ускладнити їх застосування в державних структурах. Для подолання цих проблем рекомендується перехід на менш енерговитратні алгоритми (наприклад, Proof of Stake) та інтеграція блокчейн-технологій з існуючими системами кібербезпеки для забезпечення всебічного захисту даних. Також необхідно здійснювати постійний моніторинг та оновлення систем для реагування на нові загрози. Майбутні дослідження повинні зосередитися на оптимізації енергоефективності блокчейн-систем, їх адаптації до умов війни та подальшому розвитку інтеграції блокчейну з іншими інструментами кіберзахисту.

Впровадження блокчейн-технологій у секторі безпеки і оборони України стикається з низкою викликів:

- необхідність розробки, впровадження та інтеграції блокчейн-рішень з існуючими складними інформаційними системами;
- масштабованість та продуктивність: Забезпечення здатності блокчейн-мережі обробляти великі обсяги транзакцій з високою швидкістю;
- відсутність спеціалізованого законодавства, що регулює використання блокчейн-технологій у сфері державної безпеки;
- недостатня кількість фахівців з розробки, впровадження та підтримки блокчейн-систем у військовому та правоохоронному секторах;
- значні фінансові витрати на розробку, обладнання, програмне забезпечення та навчання персоналу.

Для успішного впровадження блокчейн-технологій необхідно:

- розробити державну стратегію впровадження блокчейн у секторі безпеки і оборони;
- творити міжвідомчі робочі групи для координації зусиль та обміну досвідом;
- інвестувати в науково-дослідні розробки та підготовку кваліфікованих фахівців;
- розробити необхідну нормативно-правову базу, що враховуватиме специфіку використання блокчейн у сфері державної безпеки;
- забезпечити поступове та поетапне впровадження блокчейн-рішень, починаючи з пілотних проектів у найбільш критичних сферах обміну інформацією;
- активно вивчати та адаптувати кращий міжнародний досвід використання блокчейн у військових та правоохоронних структурах країн-партнерів.

Використання блокчейн-технологій має значний потенціал для кардинального підвищення рівня безпеки та забезпечення цілісності обміну інформацією між суб'єктами сектору безпеки і оборони України. Впровадження приватних або консорціумних блокчейн-мереж може стати ключовим елементом у зміцненні інформаційної стійкості держави в умовах сучасних гібридних загроз. Успішна реалізація цього потенціалу вимагає скоординованих зусиль усіх зацікавлених відомств, державної підтримки, відповідного законодавчого забезпечення та інвестицій у розвиток кадрового потенціалу. Поетапне впровадження блокчейн-технологій може стати важливим кроком на шляху до створення більш безпечної, ефективної та довіреної системи інформаційної взаємодії у секторі безпеки і оборони України.