of people, groups of people, society as a whole and the military and political leadership of the state.
Information warfare is the spread of certain ideas, views or ideology, and is a means of certain politics. The global tool for its implementation is mass media and various communications.
The article also discusses the theory of information warfare in the political sphere, it should be considered that it takes place at the strategic, operational and tactical levels.
Mainly, the highest political elite of the state operates at the strategic level, and the information units of the political path operate at the operational and tactical levels.
Key words: information war, information weapon, information struggle, information and psychological influences, information struggle.

Хорошко Володимир Олексійович, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Khoroshko Volodymyr, doctor of technical sciences, professor, professor of the department of security of information technologies of the National Aviation University.
E-mail: professor_va@ukr.net..
Orcid ID: 0000-0001-6213-7086.

Хохлачова Юлія Євгеніївна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Khokhlachova Yuliia, candidate of technical sciences, associate professor, associate professor of the department of security of information technologies of the National Aviation University.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

Пірцхалава Тіна Павлівна, студентка Навчально наукового інституту Міжнародних відносин Київського національного університету ім. Тараса Шевченка.

Pirtskhalava Tina, student of the Educational Scientific Institute of International Relations of Kyiv National University named after Taras Shevchenko.
E-mail: kesane1827@gmail.com.
Orcid ID: 0000-0002-4320-3073.

Іванченко Ігор Сергійович, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Ivanchenko Ihor, candidate of technical sciences, associate professor, associate professor of the Department of Information Technology Security of the National Aviation University.
E-mail: igor-p-l@ukr.net.
Orcid ID: 0000-0003-3415-9039.

DOI: 10.18372/2410-7840.24.16931
УДК 654.071

РОЗРОБКА БЕЗПЕКИ СИСТЕМ ЕЛЕКТРОННОГО УРЯДУВАННЯ НА ОСНОВІ БЛОКЧЕЙНУ

Святослав Василишин, Іван Опірський

В реаліях захисту інформації у кіберпросторі існує багато засобів та підходів до безпеки урядового, бізнес та приватних секторів, одним з яких цілком ймовірно можуть стати системи побудовані на основі блокчейну. З кожним роком кількість інформації яка проходить через всесвітню павутину та кількість користувачів зростає у геометричній прогресії, разом з цими факторами росте й кількість технологій, які забезпечують безпеку та конфіденційність даних користувачів в мережі. З теперішніми темпами технології здатні старіти швидше ніж встигають зайняти свою нішу на ринку, а відтак їхня підтримка перестає бути актуально, що дозволяє зловмисникам прориватися крізь захист або знаходити нові вразливості у вже існуючих системах. Блокчейн одна з технологій яка поки не так часто використовується саме в урядових та бізнес системах, як технологія навколо якої можна побудувати захист своєї мережі. Дужче часто це зумовлено тим, що такі інституції потребують індивідуальних підходів для рішення своїх проблем та потреб, а розробка свого підходу на основі блокчейну потребує дуже багато грошових інвестицій та спеціалістів, яких на ринку в даний момент ще не так багато. Однак в майбутньому, коли блокчейн стане доступнішим не тільки для оперування крипто валютами й для використання їх у внутрішніх системах він буде

здатний запропонувати новий стандарт у захисті інформаційних систем і стати одним з найпотужніших на ринку в силу своєї міцної системи захисту. В даній статті пропонується система безпеки урядових, приватних та бізнес секторів побудованих з використанням даної технології.
Ключові слова: *блокчейн, захист інформації, конфіденційність, вузли зв'язку, передача даних.*

ВСТУП

Широка доступність Інтернету спонукала країни по всьому світу використовувати технології як засіб спілкування та обміну послугами між громадянами та іншими філіями. Користувачі електронного уряду насолоджуються онлайн-послугами, не виходячи зі своїх комфортних домівок, уникаючи довгих черг у державних установах, заощаджуючи час і транспортні витрати, і в той же час постачальники послуг можуть надавати послуги ефективніше та ефективніше. Загалом урядові мережі можуть спілкуватися одна з одною краще, ніж бізнес-мережі, оскільки більшість із них підключено для передачі інформації громадськості без конкуренції. У майбутньому кількість пристроїв, які використовують послуги електронного уряду, різко зросте через швидку еволюцію розумних будинків, Інтернету речей (IoT), розумних міст та інших взаємопов'язаних мереж. Згідно з опитуванням ООН щодо електронного урядування, 2014 р., майже всі уряди в усьому світі зараз надають своїм громадянам та іншим зацікавленим сторонам електронні послуги через вебсайти та мобільні додатки.

Системи електронного уряду збирають, зберігають і обробляють значну кількість конфіденційної інформації про громадян, співробітників, клієнтів, продукти, дослідження та фінансовий стан серед іншого за допомогою електронних комп'ютерів. Компрометація такої інформації зазвичай призводить до втрати довіри та впевненості користувачів, можливостей, фінансових переваг тощо. Було виявлено, що понад 80% веб-сайтів електронного уряду по всьому світу були вразливі до міжсайтових сценаріїв (XSS) і впровадження запитів (SQL) через відсутність належних механізмів автентифікації, застосованих до вхідних даних від користувачів. Останнім часом багато країн світу зіткнулися з великою загрозою атак на відмову в обслуговуванні (DoS) і шкідливих програм, націлених на їхні мережі. Наприклад, уряд США зазнав однієї з найбільших атак на електронний уряд у 2015 році, що призвело до витоку конфіденційної інформації понад 4 мільйонів державних службовців, включаючи інформацію про перевірку безпеки, номери соціального страхування, особи та паролі. Відповідно до звіту в 2016 році уряд Танзанії постраждав від кібертерористів, технологічних шпигунів, хакерів і цифрових шахраїв, що призвело до збитків у розмірі близько 85 мільйонів доларів США. Крім того, у 2014 році було зламано понад 1500 облікових записів користувачів у Сінгапурі на урядовій платформі, де хакери отримали доступ для створення нових підприємств і подання заявок на отримання дозволів на роботу.

Тому дуже важливо забезпечити безпеку, приватність, конфіденційність, цілісність і доступність систем електронного урядування. Існуючі системи електронного урядування, такі як веб-сайти електронного урядування та системи керування електронними ідентифікаторами, є централізованими, де один або дубльовані центральні сервери та бази даних зберігають та надають інформацію користувачам. Централізоване управління та система перевірки, ймовірно, страждатиме від єдиної точки збою, що робить систему мішенню для кібератак, таких як DDoS, DoS та іншого шкідливого програмного забезпечення. Будь-яка система електронного урядування залишатиметься вразливою до порушень конфіденційності та безпеки, якщо не буде розроблено та не буде доступно для боротьби з цими загрозами в майбутньому кращі технології безпеки та контрзаходи.

Технологія блокчейн виявилася одним з хороших рішень для забезпечення безпечного децентралізованого середовища для обміну інформацією. Хоча спочатку він був запроваджений для обміну цифрової валюти як базова технологія, він знайшов застосування безпеки та конфіденційності в багатьох інших сферах, таких як Інтернет речей (IoT), розумні будинки, розумні міста системи освіти та охорони здоров'я. Хоча уряди в усьому світі не повністю запровадили технологію блокчейн у державному секторі, багато країн ініціювали проекти блокчейну, щоб дослідити потенціал технології блокчейн у пропонуванні державних послуг окремим особам. Кожен із цих проектів зазвичай зосереджується на конкретній послузі, наприклад, електронне

проживання, електронна охорона здоров'я, земельний реєстр тощо; вони все ще перебувають на ранніх стадіях, і не було запропоновано жодної спільної основи для інтеграції технології блокчейн у системи електронного урядування. Крім того, кожна з цих країн розробляє власну структуру блокчейну. Різні системи блокчейнів у різних країнах призводять до труднощів у спілкуванні за межами їхньої мережі для міжнародного обміну інформацією. У цьому документі представлено структуру та прототип безпечної та конфіденційної системи електронного урядування на основі блокчейну, яку може прийняти будь-який уряд з метою забезпечення як безпеки, так і конфіденційності, одночасно збільшуючи довіру до державного сектору. Система складається з одноранговоі мережі пристроїв (вузлів) електронного урядування та пристроїв користувачів. Коротко кажучи, будь-який новий пристрій електронного уряду або окремий пристрій, що приєднується до системи, буде перевірено існуючими одноранговими мережами, і один із однорангових пристроїв буде обрано для встановлення мережевого вузла та блокчейн-адреси нового пристрою. Коли новий користувач намагається зареєструватися в системі через пристрій або один із державних відомств, користувачеві призначається ідентифікатор користувача та гаманець блокчейну для збору та зберігання його/її транзакцій. Завдяки цьому, користувачі електронного уряду можуть подавати та отримувати доступ до своїх записів з будь-якого місця та з будь-якого місця, використовуючи свої ідентифікатори та адреси блокчейну. У цьому документі також проаналізовано та оцінено наслідки запропонованої системи для безпеки та конфіденційності в державних секторах за допомогою теоретичного та якісного аналізу.

Технологія блокчейн

Blockchain — це однорангова (p2p) розподілена база даних, яка підтримує список постійно зростаючих записів, які називаються блоками, вони між собою пов'язані та захищені, як правило, за допомогою криптографії з відкритим ключем. Завдяки технології блокчейн нова інформація додається до блоку та стає доступною для всіх вузлів у розподіленій мережі замість додавання до централізованої бази даних у традиційній централізованій системі. Кожен блок у блокчейні ідентифікується хеш-значенням, яке зазвичай генерується за допомогою безпечного хеш-криптографічного алгоритму 256 біт (SHA256). Хеш-значення поточного заголовка блоку (батьківського) зв'язується та зберігається в наступному блоці (дочірньому), як показано на рис. 1; отже, якщо буде зміна вмісту будь-якого блоку, його хеш також буде відповідно змінено, і ця зміна буде поширена по всій мережі, щоб зробити цей блок недійсним [1]. Завдяки цьому механізму технологія блокчейн не потребує посередника чи довіреної третьої сторони, оскільки вона є децентралізованою та розподіленою. Учасники блокчейну мають закриті ключі, призначені їм для цифрового підпису та підтвердження транзакцій, які вони здійснюють. Як показано на рис. 1, блок складається із заголовка, що містить метадані, і довгого списку транзакцій, виконаних у цьому блоці. Заголовок блоку зазвичай містить мітку часу, одноразовий номер, версію та доказ складності. Мітка часу вказує на час створення блоку; nonce - це випадкове число, згенероване консенсусним алгоритмом для обчислення хеш-значення блоку; версія вказує на номер версії блокчейну, а доказом складності є згенероване хеш-значення, яке має бути меншим за поточне цільове хеш-значення.

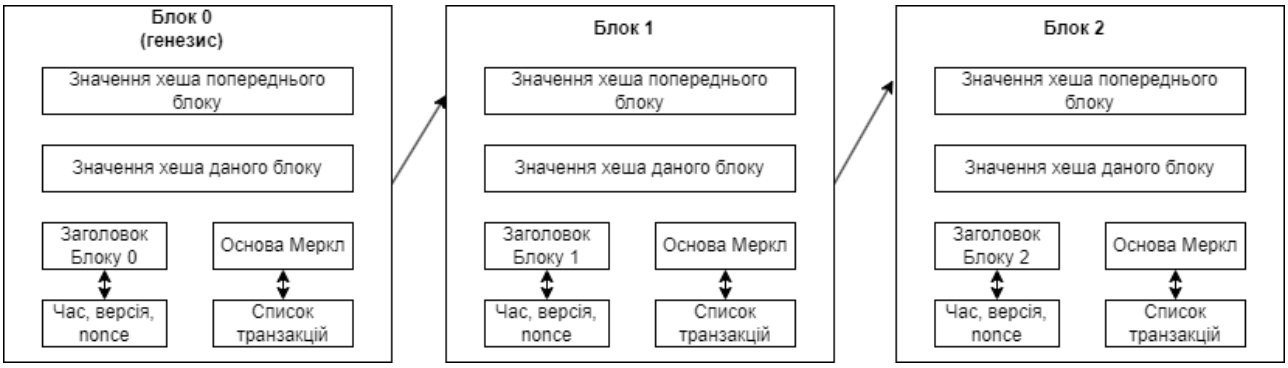

Рис. 1 Приклад блоків та їх зв'язок

Перший блок, відомий як блок генезису, жорстко закодований шляхом вбудовування деяких випадкових даних у програму блокчейну.

Незважаючи на те, що кожен блок має лише одного батьківського й одного дочірнього, дійсний блок може мати двох або більше дочірніх елементів, тимчасово створених, коли до блоку одночасно додаються два або більше вузлів (мережевих однорангових вузлів), що призводить до двох або кількох гілок від одного батьківського блоку.

Цю ситуацію зазвичай називають «розгалуженням» і усувають, приймаючи ланцюжок, який стає довшим за інші, як дійсний блокчейн, і роблячи всі інші, коротші, недійсними, із ситуацією з двома розгалуженнями, продемонстрованою на рис. 2. Сформовані гілки мають однакову довжину; у цій ситуації процес додавання нових блоків продовжується для всіх ланцюжків, які підлягають перевірці, доки одна гілка не стане довшою за інші, таким чином, дійсними. У блоці всі транзакції пов'язані між собою за допомогою дерева Меркла. Дерево Merkle - це перевернуте бінарне дерево, яке використовується технологією блокчейн для узагальнення всіх транзакцій у блоці [2].

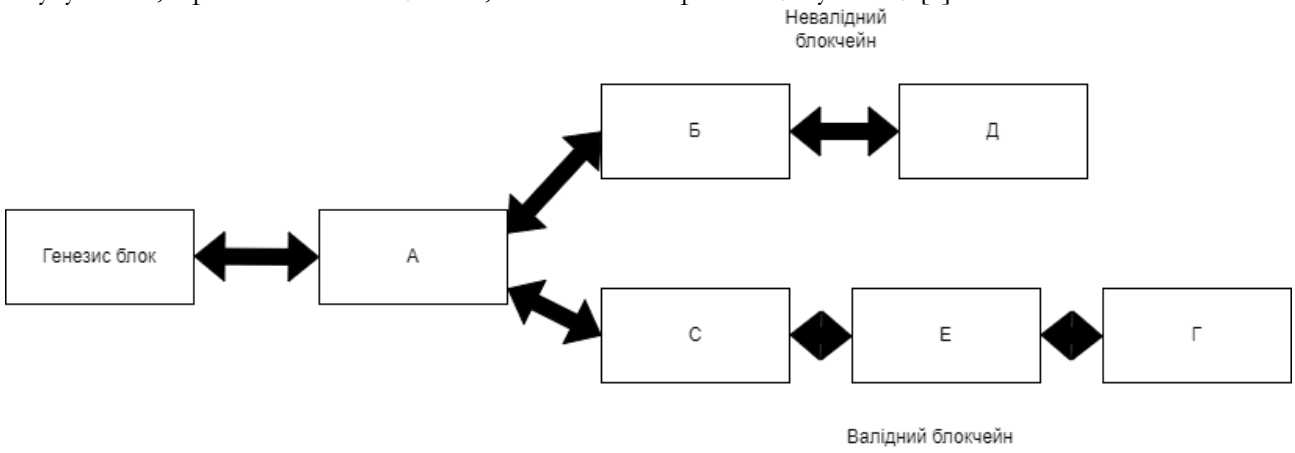

Рис. 2 Перевірка блокчейну для розгалуження

Щоб побудувати дерево Меркла, пару транзакцій рекурсивно хешують, поки вони не сформують лише один кореневий вузол у верхній частині дерева, який називається коренем Меркла , як показано на рис. 3. Точніше, корінь Меркла - це хеш усіх транзакцій, які складають блок у мережі блокчейн. Будь-яка незначна зміна даних змінить кореневий хеш Меркла, що призведе до недійсного запису [3]. Найпоширенішим криптографічним хеш-алгоритмом, який використовується для побудови дерева Меркла, є безпечний 256-бітовий хеш-алгоритм (SHA256). Якщо є непарна кількість транзакцій, хеш останньої транзакції дублюється, щоб створити парну кількість транзакцій, таким чином утворюючи збалансоване дерево. Вузли в мережі блокчейн запускають консенсусний алгоритм для перевірки транзакцій. Існує кілька консенсусних алгоритмів (протоколів), доступних для технології блокчейн. У PoW вузли-майнери, які хочуть додати (видобути) новий блок до мережі блокчейну, повинні спочатку вирішити складну математичну головоломку, яка потребує великої обчислювальної потужності. Майнер, який вирішив головоломку, додає новий блок і отримує винагороду в біткойнах [4]. На відміну від PoW, у PoS вузол, який створює новий блок, вибирається детерміновано залежно від його частки (багатства). PoS економить енергію, необхідну в PoW для вирішення математичної головоломки, а для перевірки нових транзакцій і блоків потрібна лише потужність вузла (валідатора). DPoS намагається вирішити проблему консенсусу за допомогою делегатів. DPoS використовує систему голосування та репутації в реальному часі для створення групи обмежених довірених делегатів, які будуть спостерігати та перевіряти блокування. Свідки мають право створювати блоки та додавати їх до мережі блокчейн, а також забороняти шкідливим вузлам брати участь у додаванні блоків. Загалом, у PoS та DPoS від зацікавлених сторін мережі не очікується, що вони навмисно прийматимуть неправильні рішення для мережі. Блокчейн-мережі можуть бути дозволеними або без дозволів.

Мережа без дозволу або загальнодоступний блокчейн дозволяє будь-якому користувачеві

створити особисту адресу, приєднатися до мережі та брати участь у консенсусі, тоді як дозволена або приватна мережа дозволяє приєднатися лише кільком обмеженим вузлам [5].

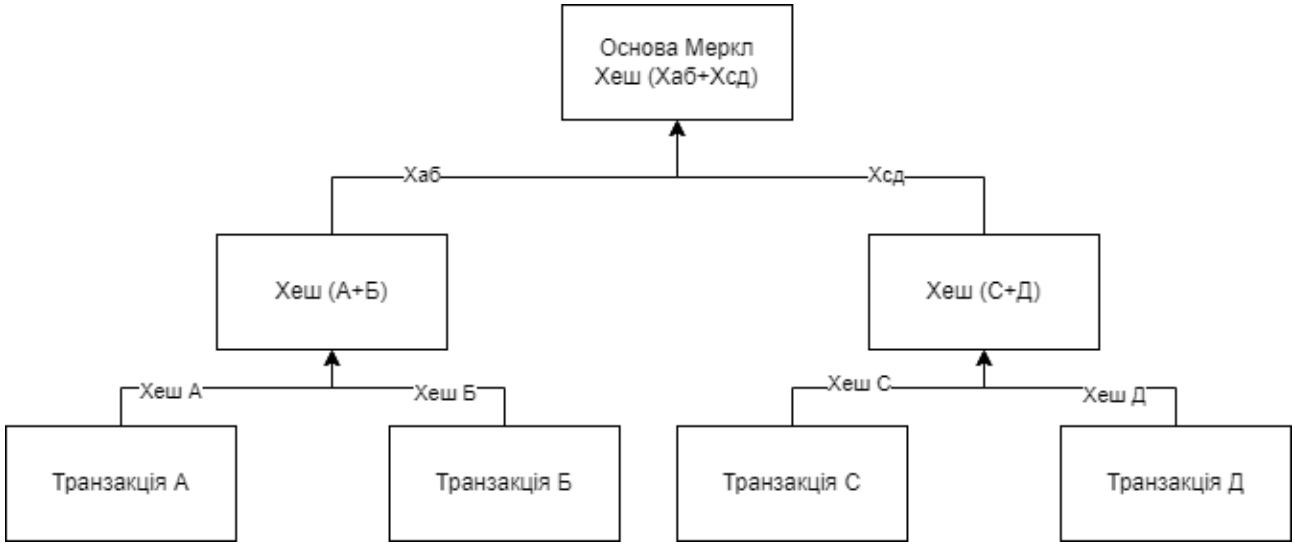

Рис. 3 Ілюстрація дерева Меркла

Системи електронного урядування

Послуги електронного уряду зазвичай можна класифікувати на 3 групи: уряд для уряду (УДУ), уряд для громадян (УДГ) і уряд для бізнесу (УДБ). УДУ пропонує онлайн-взаємодію між державними департаментами, органами влади, організаціями та іншими урядами для поширення інформації між собою за допомогою Інтернету. УДГ і УДБ дозволяють громадянам і підприємствам взаємодіяти з урядом, щоб отримати такі онлайн-послуги, як подання декларації про податок на майно, податок на прибуток, продовження/поновлення віз, паспортів і ліцензій, онлайн-голосування, подання заявок на електронні закупівлі тощо [6].

Кожен відділ електронного урядування гарантує, що лише авторизовані користувачі можуть отримати доступ до індивідуальної конфіденційної інформації. Окрім безпеки та конфіденційності, ще одним важливим фактором, який слід враховувати під час впровадження електронного уряду, є створення надійної системи, на яку користувачі можуть покластися. Гарантія безпеки та конфіденційності в системах електронного урядування відіграє вирішальну роль у збільшенні довіри між різними департаментами в уряді, оскільки це гарантує конфіденційність, цілісність і привілейований доступ до конфіденційної інформації [7]. Типові атаки, з якими стикається система електронного урядування, включають сніфери пакетів, зонди, шкідливі програми, DDoS, фішинг тощо. Завдяки кібервійні з'явилися інші нові мотиви для атак, такі як політичні розбіжності, здирництво, кібертероризм і навіть змагання за перевагу, які можуть відбуватися всередині нації або між різними націями.

Були запропоновані різні нетехнічні моделі зрілості безпеки електронного уряду для керівництва та порівняльного аналізу впровадження безпеки системи електронного уряду. Наприклад, про комплексну модель зрілості інформаційної безпеки електронного урядування для керівництва включенням безпеки в системи електронного урядування повідомляється в роботі. Ця модель зосереджена лише на налаштуванні механізмів безпеки організації, оцінці безпеки, налаштування політики безпеки та обізнаності користувачів про інформаційну безпеку, але в ній відсутні вказівки щодо вбудованої безпеки, яка може забезпечити безпеку та конфіденційність електронних послуг [8].

Як правило, безпека та конфіденційність систем електронного урядування забезпечуються за допомогою брандмауерів, систем виявлення вторгнень (IDS), інфраструктури відкритих ключів (PKI) та антивірусних механізмів. Різні методи штучного інтелекту були використані для реалізації IDS, які також можуть використовуватися системами електронного урядування.

На додаток до цих звичайних рішень, одним із апаратних рішень проблем безпеки електронного

уряду є використання системи eID для ідентифікації, автентифікації, конфіденційності та цілісності інформації користувачів. Система eID використовує смарт-картку, яка містить чіп, для зберігання персональних даних власників карток, включаючи дату народження, цивільний стан, батьківство, поточну та минулу адреси тощо, на додаток до сертифіката для автентифікації та цифрового підпису. Система eID надає засоби для унікального розрізнення між різними громадянами та підприємствами для доступу до електронних послуг.

У більшості країн міграційні служби та національні реєстри ідентифікаційних номерів пропонують eID-картки. Той самий eID можна використовувати в багатьох секторах (наприклад, оподаткування, соціальне забезпечення, освіта, послуги телефонії, банківські послуги), виконуючи різні ролі (наприклад, державного службовця чи бізнесмена) залежно від контексту. Існуючі системи управління eID не сумісні та не мають безпеки внаслідок наявності єдиної централізованої системи для ведення записів [9].

Іншим технічним рішенням для питань безпеки та конфіденційності в електронному уряді є структура автентифікації, запропонована в. У цій структурі використовуються різні процедури реєстрації та автентифікації на основі єдиного центрального порталу для громадян, пов'язаного з міністерськими департаментами. Структура складається з двох частин, а саме: постачальник ідентифікаційної інформації і постачальник послуг. Користувачі повинні зареєструватися в IdP на центральному порталі системи електронного уряду, щоб отримати унікальні ідентифікатори, які використовуватимуться для доступу до послуг від постачальників послуг. Кожного разу, коли користувач хоче отримати доступ до служби, SP повинен підтвердити свою особу за допомогою IdP на центральному порталі, щоб отримати пароль єдиного входу (SSO), який можна використовувати для доступу до різних SP.

Система електронного урядування на основі блокчейну

Запропонована структура електронного урядування на основі блокчейну проілюстрована на рис. 4. На цьому малюнку двонаправлена стрілка УДУ показує взаємодію, що відбувається між державними департаментами та організаціями, що дозволяє здійснювати одноранговий (p2p) обмін (широкомовлення) та перевірку даних, які надаються особами.

Подвійна стрілка УДГ позначає обмін інформацією між громадянами та урядом, як-от заповнення податкових форм, свідоцтв про шлюб, дозволів на ведення бізнесу, свідоцтв про народження, віз або паспортів. Подвійна стрілка УДБ вказує на обмін інформацією, як-от електронні закупівлі, податкові та страхові форми, а також електронні аукціони між державними та діловими організаціями (підприємствами) як головне джерело економічного зростання [10].

Приєднання будь-якого нового вузла електронного уряду (У) або вузла користувача (Г або Б) до мережі блокчейн перевіряється одноранговими користувачами в мережі, і токени електронного уряду призначаються для налаштування його мережевого вузла, що призводить до отримання дозволу (приватний) блокчейн. Кількість токенів електронного уряду еквівалентна загальній кількості записів, які зберігаються вузлом у мережі блокчейн. Кожен користувач має спеціальний гаманець електронного уряду для збору своїх жетонів. Після того, як запис буде подано, запис буде передано з точки зору частки на його/її адресу в блокчейні. Використовуючи протокол DPoS, будь-який вузол зможе зареєструватися в мережі як делегат. Щоб додати новий блок до блокчейну, департаменти, які спільно утворюють систему електронного уряду, голосують за делегата, який перевірить транзакції та запечатає блок.

Цей підхід відповідає вимогам безпеки, оскільки випадкові вузли не можуть приєднуватися до мережі, генерувати нові маркери та налаштовувати мережевий вузол, якщо це не схвалять інші вузли електронного уряду. Дозволена система блокчейну гарантує, що збережені записи є надійними, доступними для аудиту та прозорими [11].

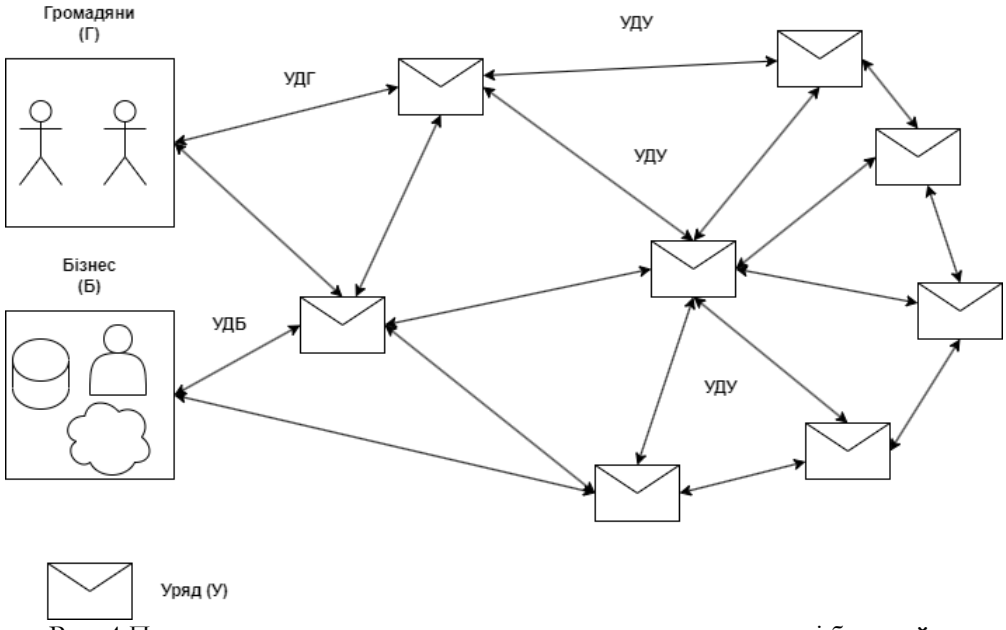

Рис. 4 Пропонована мережа електронного урядування на основі блокчейну

Вузли мережі

У термінології блокчейн існує два типи вузлів, які є повними вузлами та полегшеними вузлами. Повний вузол завантажує повну копію блокчейну, коли він приєднується до мережі блокчейну, що дозволяє йому повністю перевіряти транзакції та блоки.

Полегшений вузол не завантажує повну копію блокчейну, коли він приєднується до мережі, а завантажує лише заголовки блоків для перевірки автентичності транзакцій. Щоб мати можливість передавати свої транзакції в мережу та отримувати сповіщення, коли транзакції впливають на їхні гаманці блокчейну, полегшені вузли зазвичай посилаються на копію довіреного повного вузла блокчейну.

У запропонованій системі вузли відділу електронного урядування служать повними вузлами, тоді як пристрої користувача (У і Б) служать легкими вузлами, хоча будь-якому бізнес-вузлу дозволено завантажувати повну копію блокчейну. Підключення до мережі p2p у запропонованій мережі може бути забезпечено за допомогою бездротового широкосмугового зв'язку, завдяки тому факту, що багато країн у всьому світі намагаються об'єднати загальноміську бездротову широкосмугову мережу по всьому місту за допомогою технології Wi-Fi.

Голосування делегатів і свідків

Піри повинні узгодити стан транзакцій блоку та процес запечатування блоків у блокчейн, щоб мережа залишалася функціональною. DPoS прийнято тут як консенсусний алгоритм через його обчислювальну ефективність у додаванні транзакцій і запечатуванні блоку. Коротко, DPoS можна розглядати як представницьку демократію, де вузли електронного уряду використовують свою частку (записи), щоб обрати делегатів (інші вузли) для приєднання до мережі. Делегати відповідають за безпеку мережі та голосування за свідків серед них, які підтверджуватимуть транзакції та запечатуватимуть блоки.

Щоб обрати свідків, голоси зважуються відповідно до розміру жетонів кожного делегата або вузла голосування. Делегату не потрібно мати великий жетон, щоб бути обраним свідком, але голоси від делегатів із великими жетонами можуть призвести до того, що делегати з відносно маленькими жетонами будуть обрані свідками.

Вузли електронного уряду зберігатимуть свої індивідуальні записи, що дозволить їм мати вищі маркери для участі та голосування за свідків, що підвищує безпеку запропонованої системи. У DPoS вузлам дозволено делегувати свої права голосу іншим вузлам, яким вони довіряють голосувати за свідків від їхнього імені. Будь-який делегат, який, здається, поведе себе неправильно, буде вилучено з набору делегатів-учасників, а його голоси призначатимуться новому вузлу, який приєднується до мережі, або будь-якому існуючому вузлу, щоб забезпечити безпеку та довіру в мережі [12].

Вибір базової технології блокчейну для реалізації прототипу в основному залежить від доступності та ефективності реалізації DPoS. Тим часом обчислювальна енергія, необхідна для перевірки транзакцій, має бути доступною, а безпека створеної мережі має бути гарантована. Наприклад, платформа Ethereum реалізує DPoS і протокол смарт-контрактів для імітації реальних контрактів, таких як податкові та страхові контракти, трудові контракти та земельні реєстри. Він забезпечує важливу альтернативу в електронному урядуванні для зберігання конфіденційних записів громадян завдяки своїй здатності полегшувати переговори щодо контракту, спрощувати умови контракту, здійснювати виконання контракту та перевіряти стан виконання контракту.

Створення нового вузла

Процес реєстрації нового вузла в запропонованій мережі електронного уряду підсумовано в «Алгоритмі 1». Будь-який відділ електронного урядування може приєднатися до мережі блокчейн, налаштувавши повний мережевий вузол, тоді як інші користувачі можуть налаштувати лише легкі вузли. Як тільки новий вузол приєднається до мережі, функціональний вузол згенерує свій гаманець блокчейну та адресу, що містить відкритий і закритий ключі, як показано в рядках 7 і 8 «Алгоритму 1». Закритий ключ використовується кожним вузлом для підписання та підтвердження транзакцій, тому його потрібно зберігати безпечно (рядок 9). Після генерації адреси вузол зв'яжеться з делегатами в мережі блокчейн, щоб надіслати свій запит на реєстрацію, і один із делегатів перевірить свою реєстрацію та передасть деякі токени електронного уряду (реєстраційний запис) на свою адресу блокчейну [13].

Після цього новий вузол додається до мережі, а його реєстрація транслюється одноранговим вузлам мережі призначеним делегатом (рядки 12-14), що дозволяє іншим одноранговим вузлам мережі отримувати інформацію про його гаманець для надсилання транзакцій у наступному циклі. Крім того, новий вузол отримує інструкції щодо налаштування мережевого вузла, щоб його можна було обрати делегатом для перевірки транзакцій у наступному циклі. Згодом новий вузол налаштовує вузол мережі відповідно до наданої інструкції. Зокрема, інструкція складається з розміру початкового токена, адреси блокчейну вузла, а також відкритого та закритого ключів для підписання та перевірки транзакцій перед додаванням блоку.

Процес додавання нового вузла завершується, коли мережевий вузол успішно налаштовано та передано в мережу делегатом. Інформаційна безпека підвищується завдяки використанню зашифрованих даних, які розповсюджуються по мережі. Таким чином, навіть якщо зловмисний вузол зареєстровано як вузол відділу, він не може змінити дані, оскільки кожен учасник мережі може виявити зміну та анулювати зміни.

Алгоритм 1: Додавання нової гілки в мережу електронного уряду

If (the request is from government) then
Create a node n;
else
Create a lightweight node n;
end if
$(K_{pub}, K_{pr}) \leftarrow$ generateKeys( );
Addr ← createBlockchainAdress() + (K_{pub}, K_{pr});
Walt ← createBlockchainWallet() + (K_{pub}, K_{pr});
safetyStorePrivateKey( );
Addr ← Addr + tokens;
$\alpha \leftarrow$ selectDelegate (S);
for each m $\in \{S - \alpha\}$ do
distrReg (m, n);
end for
n ← verNewNODE( );

Реєстрація користувача

Користувачі здійснюють реєстрацію за допомогою своїх мережевих пристроїв або фізично відвідуючи один із державних відомств, причому процес підсумовано в «Алгоритмі 2». Як описано в рядках 2 і 3 цього алгоритму, для користувача видається ідентифікатор, а для користувача генерується нова адреса блокчейну, що містить відкритий і закритий ключі, що дозволяє ідентифікувати власника. Гаманець блокчейну для цього нового користувача створюється та транслюється (рядки 5–8), щоб кожен вузол міг зберігати його у своїй адресі блокчейну. Потім створений гаманець блокчейну використовується для надсилання та отримання транзакцій, пов'язаних з обліковим записом користувача. Ідентифікатори користувачів і приватні ключі безпечно зберігатимуться у файлі гаманця або базі даних пристрою користувача. Користувачі можуть зручно

переглядати свої записи та нові транзакції, доступні в їхніх блокчейн-адресах, через інтерфейс гаманця.

Алгоритм 2: реєстрація нового користувача

$(K_{pub}, K_{pr}) \leftarrow$ generateKeys( );
uID $\leftarrow$ createUserID( );
Addr $\leftarrow$ createBlockchainAdress() + (K_{pub}, K_{pr});
$(uID\ , K_{pr}) \leftarrow$ safetyStore$(uID\ , K_{pr})$;
Walt $\leftarrow$ createBlockchainWallet() + (K_{pub}, K_{pr});
for each m $\in$ S do
distrWal (m, Wlt);
end for
a $\leftarrow$ verNewUSER( );

Коли користувач надсилає запис делегату, транзакція автентифікується та ініціалізується. Після цього блок оновлюється до нової версії, яка транслюється по всій мережі для перевірки, а потім передається на його/її адресу блокчейну в усіх однорангових мережах. Переданий запис зберігається в блокчейн-адресі користувача з таким вмістом даних: (1) ідентифікатор користувача, (2) значення запису, наприклад реєстрація власності, і (3) ідентифікація запису, наприклад номер податкової реєстрації . Кожен екземпляр даних у блокчейні представляє актив. Коли стороння організація (наприклад, бізнес) запитує доступ до інформації користувача з будь-яких офіційних питань, користувач повинен надати свою адресу блокчейну для перевірки. Потім організація може використовувати веб-API блокчейну для доступу до даних блокчейну, що зберігаються в адресі користувача. Усі користувачі електронного уряду зобов'язані створювати резервні копії своїх особистих ключів і зберігати їх у безпеці. Якщо будь-який користувач втратив свій особистий ключ, він повинен буде створити нову адресу блокчейну та попросити один із вузлів відділу електронного урядування перенести його/її інформацію зі старої адреси блокчейну на новостворену адресу блокчейну.

Коли зареєстрований користувач захоче отримати доступ до мережі, пристрій і ідентифікаційні дані користувача будуть перевірені та автентифіковані. Це допомагає звести до мінімуму людські помилки, які завжди вважалися основним внеском у збій і слабкою ланкою доступу до інформації, що зберігається в інформаційних системах.

У результаті державна інформація буде безпечно надходити до потрібних осіб у потрібний час і в потрібному місці. Типові людські помилки в кібербезпеці включають надсилання конфіденційних даних не тому одержувачу та ненавмисне розкриття облікових даних для входу, таких як імена користувачів і паролі. Людська помилка залишається однією з основних причин порушення кібербезпеки в державних і приватних організаціях.

Генерація нового блока

Кожен блок створюється одним активним свідком, який вибирається випадковим чином більшістю однорангових користувачів зі списку активних делегатів. Якщо свідок пропускає блок, інший свідок отримує завдання створити та перевірити блок, щоб приєднатися до мережі блокчейн. У DPoS для створення блоку встановлюється фіксований період часу, часто п'ять секунд. «Алгоритм 3» висвітлює фундаментальні кроки, які беруть участь у процесі генерації та додавання блоку до блокчейну за допомогою алгоритму консенсусу DPoS.

Алгоритм 3: створення та додавання нового блоку в блокчейн

initialize an empty set of transaction G = { };
$\alpha \leftarrow$ WitnesElect(S);
while treansaction$_t$ < T_c do
for each m $\in$ {S $-$ α} do
G $\leftarrow$ G + GetTransactionfromNode(m);
end for
end while
$b_{m+1} \leftarrow$ createBlock(b_m, G);
for each m $\in$ {S $-$ α} do
signBlock(b_{m+1}, m);
end for
B′ $\leftarrow$ B + b_{m+1};
for each m $\in$ S do
distributeBlockchain (B′, m);
end for

Блок додається через регулярний проміжок часу, Tc. У межах цього інтервалу блок проходить наступні фази діяльності. Спочатку ініціалізується порожній набір транзакцій R; і один свідок із групи делегатів обирається для створення та перевірки транзакцій для блокчейну. По-друге, всі транзакції надсилаються обраному свідку. Цей процес триває, доки свідок не припинить приймати будь-які нові транзакції для блоку. По-третє, свідок збирає новий блок і розповсюджує його представникам мережі для перегляду та перевірки. Це дозволяє тим вузлам,

які обрали свідка, цифровим підписом блоку підтвердити його правильність. Підписаний блок повертається свідку та додається до його локального блокчейну, одночасно розповсюджуючи новий блок у мережі. Свідок не може видобувати власну транзакцію, тому в рядках 4 і 9 b (свідок) виключається з набору вузлів N. Наприкінці алгоритму блокчейн поширюється на всі урядові вузли в мережі.

Аналіз безпеки та конфіденційності

Кожна система електронного урядування має гарантувати конфіденційність, цілісність і доступність послуг. Конфіденційність досягається, коли інформація не розкривається неавторизованим користувачам; Цілісність досягається шляхом захисту інформації від будь-якої форми модифікації, тоді як доступність означає, що інформація доступна в разі потреби та вільна від DoS або DDoS чи інших подібних порушень служби. У цьому розділі представлено теоретичний якісний аналіз ефективності безпеки та конфіденційності системи електронного урядування на основі блокчейну.

Записи, що зберігаються в запропонованій системі, захищені криптографією з відкритим ключем, яка захищає від зловмисних спроб змінити та/або неавторизованого доступу, тоді як користувачам мережі призначаються закриті ключі для підтвердження та підписання транзакцій.

Шифрування та цифровий підпис використовуються в мережі для забезпечення безпеки, конфіденційності та контролю доступу до збережених записів. Крім того, більшість консенсусних алгоритмів блокчейну (у цьому випадку DPoS) вимагають від зловмисника контролю принаймні 51% одноранговых мереж, щоб змінити запис, чого, як правило, неможливо досягти. Точніше, щоб змінити будь-який блок у ланцюжку блоків, зловмисник повинен змінити кожну копію цього блоку в мережі, а потім переконати більшість вузлів, що новий блок є дійсним. Крім того, для підвищення конфіденційності даних, що зберігаються в запропонованій мережі, усі блоки користувачів хешуються, а незрозумілі хеші транзакцій зберігаються в блокчейні.

Запропонована система є децентралізованою системою p2p, де дані користувача зберігаються в різних вузлах, що гарантує доступність системи, уникаючи будь-якої єдиної точки збою. Використовуючи DPoS, будь-якому зловмиснику важко запускати DDoS або DoS атаки проти системи, оскільки потрібна реєстрація для того, щоб вузол почав обмінюватися інформацією з рештою одноранговых мереж. Будь-які транзакції, отримані від вузла мережі, перевіряються свідками, що ускладнює зловмисним вузлам ініціювання зловмисних з'єднань.

Послуги безпеки та відповідні загальні заходи, які надає запропонована структура, підсумовані в таблиці 1, що забезпечує адекватну конфіденційність і безпеку транзакцій. Для підвищення обчислювальної ефективності пристрої користувача запускатимуть полегшені клієнти для зберігання транзакцій, а не повну копію блокчейну, яка є дорогою з точки зору зберігання.

Очікується, що пристрої електронного уряду будуть обчислювальнопотужними з достатньою ємністю для зберігання та ефективної обробки записів користувачів. Мережа здатна запропонувати продуктивність, яку забезпечують технологія блокчейн і консенсусний протокол DPoS, наприклад масштабованість, швидкість, сумісність і прозорість, і вона може обробляти велику кількість транзакцій. Підхід криптографії еліптичної кривої (ECC) використовується для реалізації шифрування та цифрового підпису в запропонованій структурі, що є загальною практикою для більшості існуючих технологій блокчейну, таких як Bitcoin та Ethereum.

Таблиця 1

Служби безпеки та загальні заходи

Служба безпеки	Протидія (заходи)
Автентифікація	Блокчейн-адреса та цифровий підпис
Контроль доступу	Цифровий підпис і шифрування
Конфіденційність	Шифрування
Цілісність	Шифрування та цифровий підпис
Невідмовність	Шифрування та цифровий підпис
Доступність	Розподілений/децентралізований
Довіра	Децентралізація, шифрування та цифровий підпис

Зверніть увагу, що ECC і RSA (Rivest-Shamir-Adleman) пропонують подібний рівень безпеки, але ECC споживає набагато меншу кількість бітів. Наприклад, 256-бітний ключ у ECC пропонує такий самий рівень безпеки, як і RSA, що використовує 3072-бітний ключ. Коротший ключ зазвичай означає низьке споживання процесора, низьке використання пам'яті та швидке створення ключа.

Ці переваги також сприяють швидкому створенню транзакцій і запечатуванню блоків. Короткий виклад дослідження довжини ключа між RSA та ECC наведено в таблиці 2. 256-бітні ключі ECC широко поширені в технології блокчейн, оскільки вони можуть забезпечити необхідний рівень безпеки для більшості програм [14].

Таблиця 2

Порівняння довжин ключів RSA та ECC у бітах

Довжина ключа RSA	Довжина ключа ECC	Приблизне співвідношення (RSA:ECC)
1024	160	6:1
2048	224	9:1
3072	256	12:1
7680	348	20:1
15360	512	30:1

Окрім безпеки та збереження конфіденційності, система електронного урядування на основі блокчейну також забезпечує низку інших переваг, підсумованих у таблиці 3. Ці функції роблять технологію блокчейн перспективним напрямом у впровадженні системи електронного урядування, яка може забезпечити зручний, безпечний та відмовостійкий канал зв'язку між державним сектором та громадянами. Непрямі переваги, які приносять технології блокчейну, такі як скорочення бюрократії, виключення використання паперу, скорочення транзакційних витрат і контроль корупції, можуть змінити екосистему управління з вищим ступенем довіри з боку громадян [15].

Таблиця 3

Особливості системи електронного урядування на базі блокчейну

Особливість	Пояснення
Зменшення людських помилок	Пристрої та ідентифікаційні дані користувачів проходять автентифікацію заздалегідь перед отриманням доступу до мережі
Підвищення суспільної довіри	Люди мають прямий контроль над своєю інформацією, і всі учасники мережі автентифіковані
Більша масштабованість	Систему можна легко масштабувати, оскільки вона дозволяє автоматично додавати нові пристрої та користувачів до мережі відповідно до механізму консенсусу
Підвищена надійність	Дані зберігаються на кількох серверах/розташуваннях. Протокол консенсусу гарантує, що дані можуть бути змінені лише за згодою всіх учасників
Підвищена відмовостійкість	Уникає єдиної точки збою, а система, отже, стійка до зловмисного програмного забезпечення, атак DoS і DDoS
Покращена можливість перевірки	Легко відстежити історію всіх транзакцій, оскільки вони залишаються незмінними в мережі
Краща можливість перевірки	Усі нові транзакції перевіряються всіма учасниками мережі перед додаванням до блокчейну
Право власності на інформацію	Особи несуть відповідальність за надання доступу до їх інформації
Покращений доступ до інформації	Інформація зберігається в кількох місцях, що покращує легкий і швидкий доступ

Підвищена якість даних	Усі транзакції та записи, що зберігаються в системі, перевіряються заздалегідь, що робить збережену інформацію автентичною з необхідною якістю
Більша прозорість	Усі вузли в мережі спільно використовують ту саму копію блокчейну, а нові транзакції додаються на основі механізму консенсусу
Зниження експлуатаційних витрат	Для обробки транзакцій сторонні організації не потрібні
Покращена ефективність і швидкість	Будь-хто в мережі може отримати доступ до всіх записів, що підпадають під привілей доступності, і нові записи поширюються на всі вузли-учасники

ВИСНОВОК

У цьому документі пропонується структура електронного урядування, яка може забезпечити безпеку та конфіденційність у державному секторі за допомогою технології блокчейн. Теоретичний і якісний аналіз безпеки та конфіденційності фреймворку показує, що криптографія, незмінність і децентралізоване управління та контроль, запропоновані технологією блокчейн, можуть забезпечити необхідну безпеку та конфіденційність у системах електронного урядування. Запропонована система також має потенціал для вирішення проблем сумісності між урядовими департаментами, що є одним із обмежень існуючих систем електронного урядування. Оскільки ця робота обмежена структурою та теоретичним обговоренням, активна майбутня робота полягає у впровадженні такої структури, а потім у подальшому дослідженні її повного потенціалу в реальному середовищі. Зауважте, що технологія блокчейну, така як Ethereum, все ще перебуває на ранніх стадіях розвитку, і тому іншою частиною майбутньої роботи буде застосування відповідної версії технології блокчейну в державних секторах для задоволення та підвищення безпеки та конфіденційності індивідуальних даних.

ЛІТЕРАТУРА

[1] Lafaille, C. What is Blockchain Technology. 2018. Available online: https://www.investinblockchain.com / what-is-blockchain-technology.

[2] CoinDesk. How Bitcoin Mining Works. 2018. Available online: https://www.coindesk.com/information/ how-bitcoin-mining-works.

[3] Tuwiner, J. What Is Bitcoin Mining and How Does It Work? 2019. Available online: https://www. buybitcoinworldwide.com/mining.

[4] Gautham. PoW Blockchain Could Be Vulnerable to Balance Attack. 2017. Available online: https: //www.newsbtc.com/2017/01/29/pow-blockchain-balance-attack.

[5] Stan Higgins. Bitcoin Mining Pools Targeted in Wave of DDOS Attacks. 2015. Available online: https:// www.coindesk.com/bitcoin-mining-pools-ddos-attacks.

[6] Proof of Stake. 2018. Available online: https:// lisk.io/academy/blockchain-basics/how-does-blockchainwork/proof-of-stake.

[7] Komodo. Komodo: Advanced Blockchain Technology, Focused on Freedom. 2018. Available online: https:// komodoplatform.com/wp-content/uploads/2018/06/ Komodo-Whitepaper-June-3.pdf.

[8] B. Gates, Enabling secure anywhere access in a connected world, 2007. Available from: https://www. metamuse.net/2007/02/bill-gates-enabling-secure-anywhere.html.

[9] A-Gentle-Introduction-To-Bitcoin-WEB.pdf.https: //bravenewcoin.com/assets/Reference-Papers/A-Gentle-Introduction/A-Gentle-Introduction-To-BitcoinWEB.pdf.

[10] Andrychowicz, M., Dziembowski, S., Malinowski, D., & Mazurek, Ł. (2015). On the malleability of bitcoin transactions. In M. Brenner, N. Christin, B. Johnson, & K. Rohloff (Eds.), Financial cryptography and data security (Vol. 8976, pp. 1-18). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-48051-9_1.

[11] Antonopoulos, A. (2015). Mastering bitcoin. Retrieved November 15, 2017. Режим доступу: http://chimera.labs.oreilly.com/books/1234000001802/ch07.html.

[12] Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking bitcoin: Routing attacks on cryptocurrencies (pp. 375–392). IEEE. https://doi.org/10.1109/ SP. 2017.29.

[13] Araoz, M. (2016, July 29). The hitchhiker's guide to smart contracts in Ethereum. Режим доступу: https://

blog.zeppelin.solutions/the-hitchhikers-guide-to-smartcontracts-in-ethereum-848f08001f05.

[14] Asia, O. (2018, January 29). Tracing back stolen cryptocurrency (XEM) from Japan's Coincheck. Режим доступу: https://www.forbes.com/sites/outofasia/2018/01/29/tracing-back-stolen-cryptocurrency-xem-from-japans-coincheck/.

[15] Ateniese, G., Faonio, A., Magri, B., & de Medeiros, B. (2014). Certified bitcoins. In I. Boureanu, P. Owesarski, & S. Vaudenay (Eds.), Applied cryptography and network security (Vol. 8479, pp. 80-96). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-07536-5_6.

SECURITY DEVELOPMENT OF ELECTRONIC GOVERNMENT SYSTEMS BASED ON BLOCKCHAIN

In the realities of protecting information in cyberspace, there are many means and approaches to the security of the government, business, and private sectors, one of which is likely to be systems built on the basis of blockchain. Every year, the amount of information that passes through the World Wide Web and the number of users grows exponentially, together with these factors, the number of technologies that ensure the security and privacy of user data in the network grows. At the current rate, technologies can age faster than they have time to occupy their niche in the market, and therefore their support ceases to be relevant, which allows attackers to break through protection or find new vulnerabilities in already existing systems. Blockchain is one of the technologies that are not so often used in government and business systems as a technology around which you can build your network protection. Very often, this is due to the fact that such institutions need individual approaches to solve their problems and needs. The development of their system on the basis of blockchain requires a lot of financial investment and specialists, which are not so many on the market at the moment. However, in the future, when the blockchain becomes more accessible not only for operating cryptocurrencies and for their use in internal systems, it will be able to offer a new standard in the protection of information systems and become one of the most powerful on the market due to its strong protection system. This article proposes a security system built using this technology for government, private, and business sectors.

Keywords: blockchain, information protection, privacy, communication nodes, data transfer.

Василишин Святослав Ігорович аспірант кафедри захисту інформації Національного університету «Львівська політехніка».

Vasylyshyn Sviatoslav, Postgraduate Student of the Department of Information Protection of the National University "Lviv Polytechnic".
Email: swat2244@gmail.com.
Orcid ID: 0000-0003-1944-2979.

Опірський Іван Романович, д.т.н., проф., професор кафедри захисту інформації Національного університету «Львівська політехніка».

Opirskyy Ivan, Doctor of Technical Sciences, Professor, Professor of the Department of Information Protection of the National University "Lviv Polytechnic"
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.

DOI: 10.18372/2410-7840.24.16932
УДК 004.681

МОДЕЛІ ОЦІНЮВАННЯ ЗАЛИШКОВОГО РИЗИКУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Володимир Хорошко, Юлія Хохлачова, Володимир Погорелов, Ахмад Аясрах

Для забезпечення базових характеристик безпеки ресурсів інформаційних систем за рахунок унеможливлення доступу неавторизованих користувачів до інформації та розкриття її змісту необхідно застосовувати засоби (апаратурні чи програмні) адміністрування доступу, управління фізичним доступом, захисту від витоків інформації технічними каналами, засоби криптографічного перетворення (для шифрування та дешифрування закритої інформації, а також засоби генерації та розповсюдження ключів), засоби охоронної сигналізації та організаційного обмеження доступом тощо. В роботі розроблено моделі процесу взаємодії засобів реалізації кібератак з засобами кіберзахисту для забезпечення базових характеристик безпеки ресурсів інформаційних систем в яких, за рахунок величини залишкового ризику та варіювання режимами функціонування або несанкціонованого