

ІТ-ПРОЕКТ СИСТЕМИ ПЕРЕВІРКИ АВТЕНТИЧНОСТІ ДАНИХ НА ОСНОВІ BLOCKCHAIN ТЕХНОЛОГІЇ

О. Прокіпчук¹, В. Висоцька¹, М. Назаркевич², В. Данилик¹

¹Національний університет «Львівська політехніка»,
вул. Степана Бандери 12, 79013 Львів, Україна

²Львівський національний університет імені Івана Франка,
вул. Тарнавського 107, 79017 Львів, Україна
mariia.nazarkevych@lnu.edu.ua

Розроблювана інформаційна система покликана допомагати покупцям товарів ідентифікувати оригінальний продукт, шляхом розміщення на товарі двох ідентифікаційних скановуваних кодів, що ведуть до інформації, яка знаходиться у захищеній структурі даних блокчейну. Дана система є економічно доцільна для компаній виробників товарів, адже вона може суттєво знизити матеріальну шкоду, що завдається виробниками контрафактних товарів. Також очікується позитивне сприйняття даного програмного продукту потенційними споживачами товарів, оскільки система дозволить користувачам мати, саме те, що вони хочуть – не натрапити на підробку та зберегти гроші. Реалізація ІТ-проекту ґрунтується на трьох напрямках як опрацювання проблематики, проектування взаємозв'язків та реалізації демо-версії проекту. Опрацювання проблематики є теоретичним та методологічним фундаментом, на якому будуть триматись наступні аспекти. Аспект є сукупністю аналізу проблем, можливих рішень та обхідних шляхів на різних рівнях реалізації системи. Критеріями успішності аспекту є переконливість та конкурентоспроможність. Переконливість показує те, наскільки реалізація системи викликає довіру у кінцевого покупця товарів. Конкурентоспроможність показує коефіцієнт захищеності системи відносно методів підробки товарів та шляхів обходження захисту від підробок. Сукупність критеріїв визначають рівень успішності проекту при умові виконання критеріїв наступних аспектів. Другим аспектом є проектування взаємозв'язків. Даний аспект передбачає визначення архітектури системи та зв'язків між ними на різних рівнях реалізації. Встановлює поведінку продукту у його застосуванні. Критеріями цього аспекту є гнучкість та стабільність. Гнучкість забезпечує можливість системи до розширення з докладанням якомога менших зусиль, а також тонкої конфігурації окремих компонентів без глобального втручання у реалізацію. Стабільність визначає те, наскільки система може працювати без відхилення від очікувань при збільшенні навантаження або масштабності реалізації. Останнім аспектом є реалізація системи. Аспект відповідає за усі етапи втілення попередньо підготовлених планів в реальність. Реалізація є найдовшою та найвибагливішою. Потрібно починати цей етап після повного виконання попередніх. Критеріями останнього аспекту є точність та захищеність. Точність показує відношення кількості успішно виявлених оригінальних товарів до усіх спроб виявлення товарів за допомогою розробленої системи. Захищеність показує ступінь захисту системи від можливих атак та способів компрометації даних.

Ключові слова: мережевий зв'язок, інформаційна система, контрафактний товар, технологія блокчейн, життєвий цикл продукту, інтелектуальна система пошуку інформації, ключ продукту.

Вступ та аналіз останніх досліджень та публікацій.

Закупівля товарів уже давно стала невід'ємною частиною буденного життя кожного з нас. Складно уявити себе без цих результатів виробництва як великих компаній, так і дрібних приватних підприємств [1]. В минулому основою подібних відносин було натуральне виробництво [2]. Це такий тип виробництва, в якому окремі соціальні групи виробляли усі необхідні товари для підтримки життя та потреб цього угруповання. Інакше кажучи кожна група була ізольована від інших та виробляла товари для себе. З часом такий тип виробництва почав витісняти ефективніше товарне виробництво [1-3]. Тут уже товари виробляються з ціллю їхнього обміну або продажу. Відповідно кожен товар має свою споживчу цінність та корисність, за допомогою яких можна укласти угоду на збут цього товару [3-6]. Такий вид виробництва виявився більш ефективним ніж натуральне виробництво адже кожен виробник забезпечує ринок тими товарами, на яких спеціалізується, відповідно кожен покупець отримує можливість отримувати товари вищої якості [7-9]. На сьогоднішній день таке виробництво дуже сильно розвинулось. На ринок вийшло багато компаній-гігантів, що конкурують між собою за кінцевого покупця. Через неможливість конкуренції або просто з метою легкої наживи деякі виробники заробляють тим, що поставляють контрафактні або фальсифіковані товари [10-15]. Контрафактними є ті товари, виробництво яких порушує авторське право виробника. Для прикладу, якщо хтось створить ноутбук використовуючи логотип компанії Asus або ж певні технології запатентовані цією компанією, то цей товар буде порушувати авторське право компанії Asus [2]. Більш загальним поняттям для контрафакту є фальсифікат. Тут вироблений товар може не порушувати чиесь авторське право, але фактичний продукт і його позиціонування будуть відрізнятися. Наприклад, якщо ви купили молоко, де на етикетці написано «10% жирності», хоча насправді там лише 5 відсотків жирності, тоді це фальсифікат [16-20]. З цього можна зробити висновок, що контрафакт завжди є й фальсифікатом, а фальсифікат не обов'язково буде контрафактом. Вважати, що контрафактна продукція є непоширеною і швидко карається законом, є помилковим. Ця проблема уже тривалий час шкодить багатьом країнам та компаніям наносячи при цьому мільярдні збитки, а також забираючи сотні життів. Для прикладу за 2017 рік контрафактна продукція нанесла світових збитків у 323 мільярди доларів, що є гігантською сумою. Найбільшими країнами-постачальниками контрафактної продукції є Китай (~ 54%), Гонконг (~ 27%), Туреччина (~ 4%), Сінгапур (~ 2%), Німеччина (~ 1%), Індія (~ 1%), Македонія (~ 0.9%), Тайланд (~ 0.8%) та Малайзія (~ 0.7%). Китай є лідером по виробництву контрафактної продукції у світі, та по виробництву оригінальної продукції Китай також не лідером [3-5]. Таким чином країни з низькою вартістю праці створюють підробки та продають їх в країнах першого світу, заробляючи при цьому колосальні гроші. Країнами, що найбільше страждають від такої продукції є наступні: США (24%), Франція (17%), Італія (15%), Швейцарія (11%), Німеччина (9%), Японія (6%), Південна Корея (3%) Британія (2%) та інші країни (13%). Дані зібрані за 2014-2016 роки Організацією економічного співробітництва та розвитку (далі OECD). Оскільки найбільше підробок створюється на продукції компаній, розташованих у США, остання несе від цього найбільші збитки [4-5].

Об'єкт дослідження: перевірка автентичності товарів з використанням blockchain технології. Предмет дослідження: засоби створення об'єднаної децентралізованої системи блокчейну, що забезпечує можливість перевірки товару на автентичність для усіх виробників-учасників цієї мережі. Розроблена система подана у вигляді виконуваних файлів, що готові до застосування. Головним загальним модулем є модуль блокчейну, що

може бути використаний виробниками товарів. Інші ж розроблені модулі є непрактичними і розроблені лише для демонстрації роботи основного модулю. Система надає загальний шаблон, що може бути реалізований виробниками товарів для доступу до захищеної мережі блокчейну. Існує 2 основних шляхи боротьби з контрафактом: спосіб пошуку та блокування виробників контрафакту та спосіб визначення справжніх товарів покупцями. Кожен виробник продукції є окремим вузлом мережі P2P. Виробники створюють одиниці товарів у вигляді окремих гаманців і дають їм певний баланс. Потім вони розміщують відкритий і закритий ключі товарів у форматі URL і розміщують QR-коди з цією URL-адресою на упаковці товарів, таким чином передаючи право власності на товари покупцеві. Коли покупець сканує приватний код, залишок товару повертається виробнику. При скануванні публічного коду система визначає статус товару на основі балансу товарного гаманця: якщо баланс нульовий, то товар уже спожитий, якщо ні – то товар не спожитий. Таким чином покупець може визначити, чи використовувався цей товар коли-небудь до нього чи розпаковувався. Якщо покупець отримує вживаний товар, він може повернути його назад в магазин. Для реалізації блокчейну використовувалися засоби мови програмування Java. В якості криптографічного алгоритму обрано RSA, а для хешування – алгоритм SHA256. Для оптимізації процесу розробки програмного забезпечення використовувався фреймворк Spring Boot.

Формулювання мети та постановка задачі.

Згідно з системним підходом [21] побудовано дерево цілей (рис. 1). Принципи системного підходу розглядають ІС з точки зору їхньої конкретизації у застосуванні даної системи, зокрема, згідно з принципом:

- остаточної мети – усі компоненти системи функціонують задля забезпечення функціоналу перевірки автентичності товарів;
- єдності, зв'язаності і модульності система ззовні розглядається як єдине ціле та містить внутрішню структуру, що на загальному рівні представляється у вигляді входів (ключ товару, посилання на виробника) та виходів (висновок про товар, додаткова інформація про товар);
- ієрархії система є ієрархічною структурою, на вершині якої розташовуються модулі програмного застосування виробника та клієнтського застосування покупця, що конкретизуються підпрограмами та компонентами на нижчих рівнях;
- функціональності структура системи побудована навколо функціоналу ведення захищеного обліку товару та знаходження конкретних одиниць і при додаванні нового функціоналу, попередня структура буде змінена;
- розвитку система є гнучкою та готова до розширення свого функціоналу, також блокчейн прекрасно забезпечує захищене безупинне накопичення інформації;
- децентралізації система прямує до мінімальної централізації, використовуючи сервер лише для встановлення комунікації між вузлами мережі;
- невизначеності система розробляється з урахуванням непередбачуваних ситуацій та забезпечує обробку таких у процесах створення, керування та визначення товарів.

Опрацювання проблематики є теоретичним та методологічним фундаментом, на якому будуть триматись наступні аспекти. Аспект є сукупністю аналізу проблем, можливих рішень та обхідних шляхів на різних рівнях реалізації системи. Критеріями

успішності аспекту є переконливість та конкурентоспроможність. Переконливість показує те, наскільки реалізація системи викликає довіру у кінцевого покупця товарів. Конкурентоспроможність показує коефіцієнт захищеності системи відносно методів підробки товарів та шляхів обходження захисту від підробок.

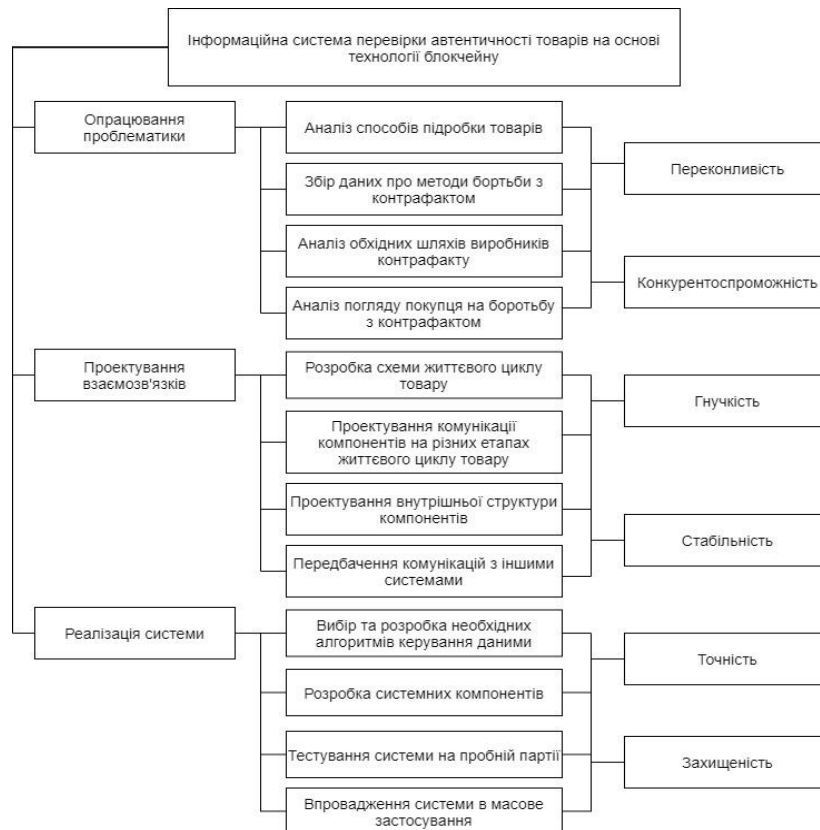


Рис. 1. Дерево цілей

Fig. 1. Goal tree

Сукупність критеріїв визначають рівень успішності проекту при умові виконання критеріїв наступних аспектів. Другим аспектом є проектування взаємозв'язків. Даний аспект передбачає визначення архітектури системи та зв'язків між ними на різних рівнях реалізації. Встановлює поведінку продукту у його застосуванні. Критеріями цього аспекту є гнучкість та стабільність. Гнучкість забезпечує можливість системи до розширення з докладанням якомога менших зусиль, а також тонкої конфігурації окремих компонентів без глобального втручання у реалізацію. Стабільність визначає те, наскільки система може працювати без відхилення від очікувань при збільшенні навантаження або масштабності реалізації. Останнім аспектом є реалізація системи. Аспект відповідає за усі етапи втілення попередньо підготовлених планів в реальність. Реалізація є найдовшою та найвибагливішою. Потрібно починати цей етап після повного виконання попередніх. Критеріями останнього аспекту є точність та захищеність. Точність показує відношення

кількості успішно виявлених оригінальних товарів до усіх спроб виявлення товарів за допомогою розробленої системи. Захищеність показує ступінь захисту системи від можливих атак та способів компрометації даних. Наступним етапом є вибір типу інформаційної системи для реалізації мети. Вибір типу інформаційної системи буде здійснений за допомогою методу аналізу ієрархій. Для цього було обрано 4 найбільш подібні типи: система підтримки прийняття рішень (A1), інтелектуальна інформаційно-пошукова система (A2), розрахунково логічна система (A3), інформаційно-довідкова система (A4). Вибір системи буде здійснюватися на основі наступних критеріїв: переконливість (K1), конкурентоспроможність (K2), гнучкість (K3), стабільність (K4), точність (K5), захищеність (K6). Метод передбачає побудову серії матриць на основі експертних оцінок, що виражаються за допомогою шкали значущості. В результаті будуть визначені підсумкові оцінки для кожного з чотирьох типів. Шкала наведена в таблиці 2. Для кожної із матриць визначаються два підсумкові параметри: власні числа та власні вектори. Першим кроком стане створення матриці порівнянь критеріїв. Кожен з обраних критеріїв якості системи буде зіставлений між собою попарно.

Таблиця 1. Шкала відносної значущості альтернатив
Table 1. Scale of relative importance of alternatives

Рівень	Характеристика	K1	K2	K3	K4	K5	K6	BЧ	ВВ
1	Відсутність значущості	1,00	0,50	1,00	0,25	0,14	0,20	0,39	0,05
2	Слабка значущість	2,00	1,00	3,00	0,33	0,20	0,50	0,76	0,10
3	Посередня значущість	1,00	0,33	1,00	0,50	0,33	0,50	0,55	0,07
4	Істотна значущість	4,00	3,00	2,00	1,00	0,33	0,50	1,26	0,17
5	Сильна значущість	7,00	5,00	3,00	3,00	1,00	2,00	2,93	0,39
6	Дуже сильна значущість	5,00	2,00	2,00	2,00	0,50	1,00	1,65	0,22
7	Очевидна значущість								
8	Шалена значущість								
9	Абсолютна значущість								

Після побудови матриці порівнянь критеріїв необхідно побудувати матриці порівнянь альтернатив відносно критеріїв за аналогічним принципом.

K1	A1	A2	A3	A4	BЧ	ВВ	K3	A1	A2	A3	A4	BЧ	ВВ
A1	1,00	0,50	0,33	0,50	0,54	0,12	A1	1,00	4,00	3,00	2,00	2,21	0,45
A2	2,00	1,00	0,50	1,00	1,00	0,23	A2	0,25	1,00	2,00	0,33	0,64	0,13
A3	3,00	2,00	1,00	2,00	1,86	0,42	A3	0,33	0,50	1,00	0,25	0,45	0,09
A4	2,00	1,00	0,50	1,00	1,00	0,23	A4	0,50	3,00	4,00	1,00	1,57	0,32
K2	A1	A2	A3	A4	BЧ	ВВ	K5	A1	A2	A3	A4	BЧ	ВВ
A1	1,00	3,00	3,00	0,50	1,46	0,30	A1	1,00	0,50	0,25	0,25	0,42	0,08
A2	0,33	1,00	0,50	0,25	0,45	0,09	A2	2,00	1,00	0,25	0,25	0,59	0,12
A3	0,33	2,00	1,00	0,25	0,64	0,13	A3	4,00	4,00	1,00	1,00	2,00	0,40
A4	2,00	4,00	4,00	1,00	2,38	0,48	A4	4,00	4,00	1,00	1,00	2,00	0,40
K4	A1	A2	A3	A4	BЧ	ВВ	K6	A1	A2	A3	A4	BЧ	ВВ
A1	1,00	0,25	0,50	0,33	0,45	0,09	A1	1,00	2,00	0,33	0,17	0,58	0,10
A2	4,00	1,00	0,50	0,20	0,80	0,17	A2	0,50	1,00	0,25	0,14	0,37	0,07
A3	2,00	2,00	1,00	0,50	1,19	0,25	A3	3,00	4,00	1,00	0,50	1,57	0,28
A4	3,00	5,00	2,00	1,00	2,34	0,49	A4	6,00	7,00	2,00	1,00	3,03	0,55
Мета	A1	A2	A3	A4	BЧ	ВВ							
A1	1,00	1,00	0,50	0,50	0,71	0,17							
A2	1,00	1,00	1,00	0,50	0,84	0,20							
A3	2,00	1,00	1,00	1,00	1,19	0,29							
A4	2,00	2,00	1,00	1,00	1,41	0,34							

Такі матриці будуть побудовані відносно кожного критерію, а також відносно головної цілі.

На даному етапі отримано усі необхідні дані для формування фінальної таблиці.

Таблиця 2. Формування фінальної таблиці
Table 2. Formation of the final table

Альтернативи	K1	K2	K3	K4	K5	K6	Коефіцієнт значущості	Система
	0,05	0,10	0,07	0,17	0,39	0,22		
A1	0,12	0,30	0,45	0,09	0,08	0,10	0,14	підтримки прийняття рішень
A2	0,23	0,09	0,13	0,17	0,12	0,07	0,12	Інтелектуальна інформаційно-пошукова
A3	0,42	0,13	0,09	0,25	0,40	0,28	0,30	Розрахунково-логічна
A4	0,23	0,48	0,32	0,49	0,40	0,55	0,44	Інформаційно-довідкова

Останній етап полягає у створенні матриці порівняння типів інформаційних систем. За результатами порівняння найкраще обрати інформаційно-довідкову систему.

Виклад основного матеріалу.

Побудуємо контекстну діаграму з метою деталізації структури системи. Серед альтернатив обрана функціональна діаграма IDEF0 (рис. 2).

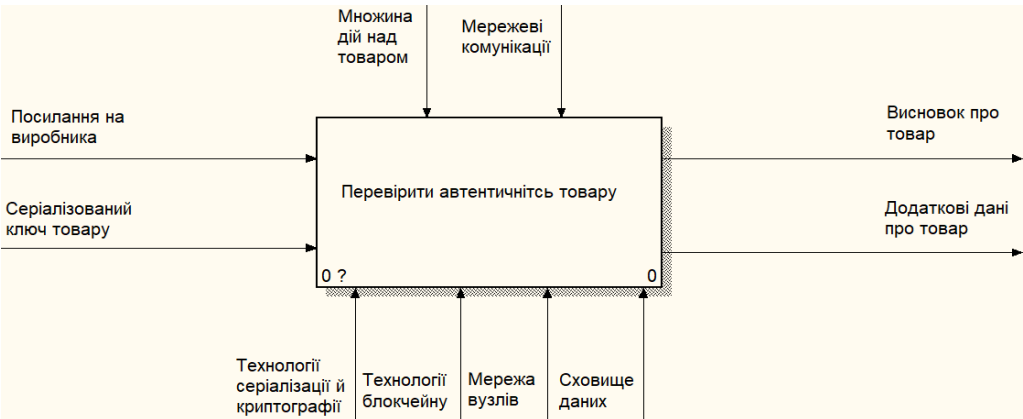


Рис. 2. IDEF0 діаграма
Fig. 2. IDEF0 diagram

Головним процесом на даній діаграмі є «Перевірити товар на автентичність». Цей процес узагальнює собою усі структури нижчих рівнів ієрархії та визначає: входи системи (стрілки зліва), виходи системи (стрілки справа), фактори впливу (стрілки вгору), ресурси (стрілки вниз). Розглянемо кожен з типів детальніше. Входи системи визначають дані або об’єкти, що необхідні системі для початку функціонування й що використовуються системою для отримання унікального результату. Виходи системи представляють результат функціонування системи. Вихід може бути як один, так і декілька. При тому виходи можуть поділятися на основні та додаткові. Додаткові виходи є необов’язковими, тож не варто покладатись на їхню присутність. Виходами розроблюваної ІС є:

- Висновок про товар. Основний вихід, що показує покупцю стан товару, а саме те, чи цей товар уже був використаний чи ні. На основі цих даних покупець робить висновок про автентичність товару.
- Додаткові дані про товар. Додатковий параметр надає покупцю загальні дані про товар або приватні дані покупця стосовно конкретної одиниці товару. Вихід залежить від програмної реалізації виробника.

Факторами впливу на систему є такі елементи, відповідно яких система виконує свою основну функцію й що здійснюють прямий або непрямий вплив на результат функціонування системи. Факторами впливу розроблюваної системи є:

- Множина дій над товаром. Даний фактор є історією усіх транзакцій, що були виконані над товаром. Здійснює вплив на процеси обробки товарів згідно вхідних даних
- Мережеві комунікації. Є множиною стандартів та реалізацій мереж, якими комунікують між собою вузли системи. Впливає на шляхи та алгоритми передачі даних в P2P мережі.

Ресурси системи - це список елементів, що беруть участь у функціонуванні процесів системи. Можуть бути як фізичними, так й інтелектуальними. Ресурсами розроблюваної системи є:

- Технології серіалізації й криптографії. Дані технології можуть відрізнятися для кожного виробника. Беруть участь у формуванні та керуванні ключами та цифровими підписами. Також використовуються для шифрування\дешифрування даних.
- Технології блокчейну. Забезпечують основні методики безпечного зберігання, передавання та доповнення даних про товари на рівні комунікації вузлів в P2P мережі.
- Мережа вузлів. Об'єднання усіх доступних виробників в одну P2P мережу, що використовуються для обміну, оновлення та забезпечення надійності даних.
- Сховище даних. На відміну від спільного блокчейну, сховище даних є особистим для кожного виробника. Використовується для зберігання тієї інформації, що не записується у блокчейн, або яку необхідно змінити.

Після цього здійснена деталізація контекстної діаграми до першого рівня. Діаграма декомпозиції зображена на рисунку 3. В результаті цього отримана модель, що складається з 4 процесів: під'єднатись до виробника, перевірити ключ на валідність, оновити стан блокчейну та перевірити стан товару. Загалом навіть такий високий рівень ієрархії процесів дозволяє досить детально передати структуру та спосіб функціонування та використання системи. Оскільки діаграма на рисунку 7 містила лише один процес, то її конкретизація містить однакові входи, виходи, фактори впливу та ресурси. Кожен з процесів керує своїми елементами, що можуть відрізнятися для кожного процесу. Між процесами містяться проміжні виходи, що дозволяють розпочати новий процес та зв'язати їх між собою в один ланцюг або ж організувати розгалуження процесів.

Діаграма декомпозиції також містить розгалуження елементів. При необхідності будь-який елемент може відноситись одночасно до всіх процесів діаграми за допомогою розгалуження. Процес «Під'єднатись до виробника» є найпершим процесом у декомпозиції головного процесу та виконує роль вхідної точки в систему (рис. 4).

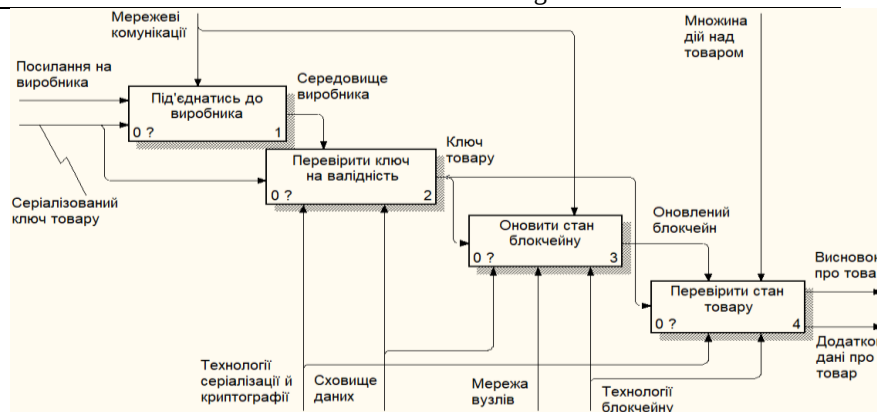


Рис. 3. Декомпозиція головного процесу
 Fig. 3. Decomposition of the main process

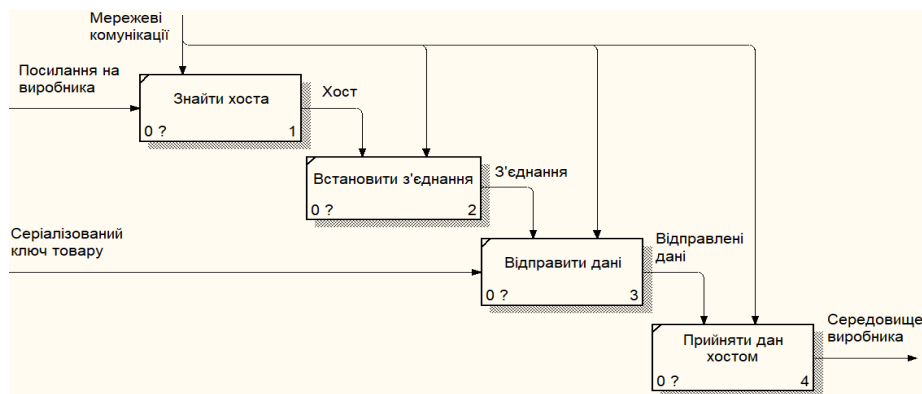


Рис. 4. Декомпозиція процесу «Під'єднатись до виробника»
 Fig. 4. Decomposition of the “Connect to Manufacturer” process

Оскільки система складається з множини вузлів виробників, що об'єднані в P2P мережу, першим кроком в застосунку буде під'єднання до конкретного виробника. Головну роль в процесі відіграє посилання на виробника, за допомогою якого здійснюється пошук та ідентифікація. Окрім цього процес приймає серіалізований ключ, як вхід та на виході видає середовище виробника, фактор впливу, від якого залежить подальша поведінка. Дана діаграма декомпозиції містить 4 процеси:

- Знайти хоста. Процес пошуку хоста за посиланням. Залежить від організації мережевих комунікацій. Виходом є конкретний знайдений в мережі хост.
- Встановити з'єднання. В даному процесі здійснюється встановлення з'єднання між клієнтом та хостом. Тип з'єднання залежить від клієнту, отриманого хоста та мережевих комунікацій. Результатом процесу є встановлене з'єднання, що можна використовувати для обміну даними.
- Відправити дані. Процес обміну даними між клієнтом та хостом. Дані для відправлення це серіалізований ключ товару, що є входом процесу. З'єднання та мережеві комунікації впливають на те, як проходить передача даних. Виходом є

відправлені дані.

- Прийняти дані хостом. Отримання даних від клієнту на основі мережевий комунікацій. Виходом процесу є середовище виробника, що в подальшому використовується визначення реалізацій подальших процесів.

Процес «Перевірити ключ на валідність» є своєрідним фільтром, що приймає, перетворює та відсіює дані. Є другим процесом, оскільки потребує середовища виробника. Основна мета полягає в тому, щоб отримати ключ, перетворити його в формат, зручний для сприймання подальшими алгоритмами та передати його далі. Усі дані, що не відповідають вимогам на будь-якому з етапів процесу безповоротно відсіюються. Ключ товару, що є виходом процесу необхідний для функціонування двох наступних процесів. Декомпозиція процесу зображена на рисунку 5.

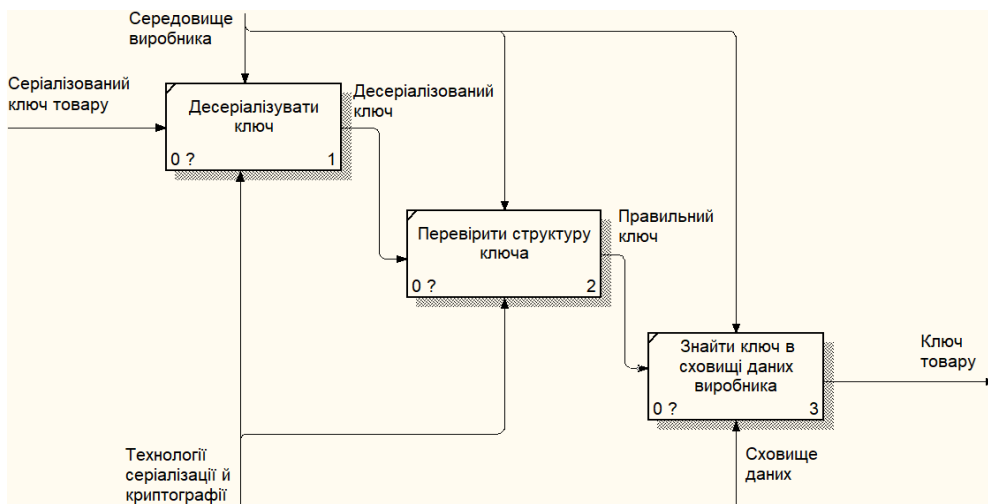


Рис. 5. Декомпозиція процесу «Під'єднатись до виробника». Продовження
Fig. 5. Decomposition of the Connect to Manufacturer process. Continued

Отримана діаграма містить наступні процеси:

- Десеріалізувати ключ. Процес отримує серіалізований ключ та перетворює його з формату зручного для передачі у зручний для сприймання алгоритмами формат. Реалізація процесу залежить від середовища виробника та використовує технології серіалізації. На виході отримуємо десеріалізований ключ товару.
- Перевірити структуру ключа. Процес використовує отриманий десеріалізований ключ та перевіряє чи це дійсно валідний криптографічний ключ, побудований за необхідними алгоритмами. Середовище виробника впливає на цей процес. Виходом є правильний ключ. Усі неправильні ключі відсіюються.
- Знайти ключ в сховищі даних виробника. Здійснює пошук у базі даних виробника за ключем, отриманим в результаті виконання попереднього процесу. Середовище виробника впливає на організацію даних та поведінку у випадках знаходження та не знаходження товару. Виходом є ключ знайденого товару.

Процес «Оновити стан блокчейну» є третім процесом серед процесів декомпозиції діаграми IDEF0. Може виконуватись одночасно з попереднім, проте виконується

синхронно для запобігання виконання зайвих дій. Мета процесу знайти вузли виробників, що мають найбільш актуальний блокчейн, запросити в них оновлення, та оновити свій блокчейн коректним оновленням. Результатом є оновлений блокчейн, з яким можуть працювати наступні процеси.

Діаграма декомпозиції процесу зображена на рис. 6.

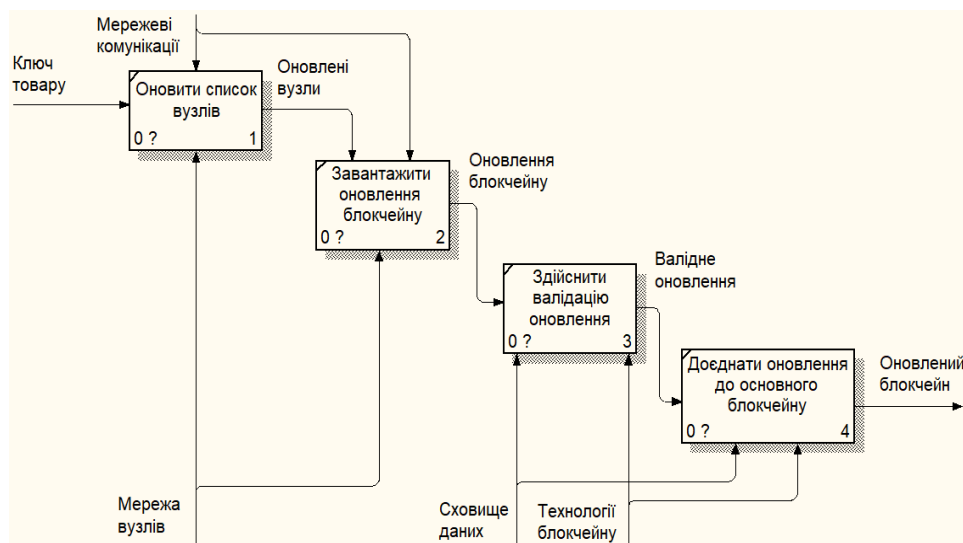


Рис. 6. Декомпозиція процесу «Оновити стан блокчейну»

Fig. 6. Decomposition of the “Update Blockchain State” process

Розроблена діаграма містить 4 процеси:

- Оновити список вузлів. Процес використовує не пустий ключ товару, як тригер для початку виконання операцій. Завантажує список вузлів P2P мережі за допомогою комунікації з сусідніми вузлами або шляхом звернення до спеціалізованого серверу. Мережеві комунікації впливають на вузли, отримані в процесі завантаження. Виходом є список оновлених вузлів.
- Завантажити оновлення блокчейну. Здійснює моніторинг завантажених вузлів P2P мережі в пошуку вузлів з найбільшою кількістю блоків у блокчейні. Отримує оновлення блокчейну у вузла з найбільшим пріоритетом. Виходом є оновлення блокчейну. Мережеві комунікації впливають на процес завантаження.
- Здійснити валідацію оновлення. Бути вузлом P2P мережі можуть різні кінцеві пристрої. Серед них можуть бути й зловмисники, що прагнуть підміняти/спотворити дані, тому кожне отримане оновлення перевіряється на валідність. Використовує сховище даних виробника та технології блокчейну для процесу перевірки. Валідне оновлення є виходом процесу.
- Додати оновлення до основного блокчейну. Після того, як отримано коректне оновлення, необхідно дописати блоки з оновлення до основного блокчейну виробника, що зберігається в його сховищі. Додання виконується з використанням технологій блокчейну. Виходом процесу є оновлений блокчейн, що відображає найбільш актуальний стан товарів.

Процес «Перевірити стан товару» є завершальним процесом, вихід якого є результатом роботи усього процесу «Перевірки товару на автентичність». Так чи інакше процес потребує даних отриманих в попередніх процесах або їхніх похідних. Процес відповідає за збір необхідних даних у блокчейні відповідно вхідних параметрів, опрацювання цих даних з метою отримання результату, а також виконання додаткових дій по можливому отриманню додаткових даних про товар, що в подальшому аналогічно будуть відправлені клієнтові. Декомпозиція процесу зображена на рисунку 7. Розроблена діаграма складається з наступних процесів:

- Знайти потрібні транзакції за ключем. Переглядає блокчейн та відбирає усі транзакції, відправником або отримувачем яких є товар з ключем, що отриманий із входу транзакції. Використовує оновлений блокчейн для пошуку, пошук здійснюється технологіями блокчейну. Виходом є знайдені транзакції.
- Дістати та дешифрувати дані про товар. Аналізує отримані транзакції на предмет зашифрованих даних та розшифровує їх використовуючи ключ товару. Використовує технології криптографії та блокчейну для маніпуляції з даними. На виході отримуємо додаткові дані про товар.
- Розрахувати баланс товару. Найбільш важливий процес, що обраховує стан товару, використовуючи отримані транзакції. За допомогою технологій блокчейну та згідно з виконаними транзакціями процес отримує баланс товару та відправляє висновок клієнтові.

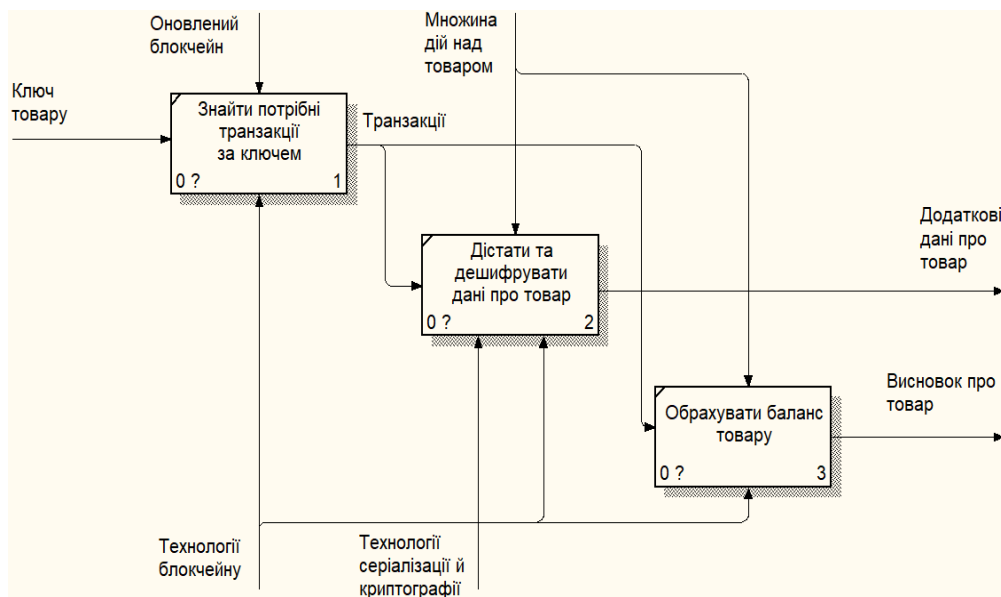


Рис. 7. Декомпозиція процесу «Перевірити стан товару»
Fig. 7. Decomposition of the process "Check the condition of the product"

Останнім етапом системного аналізу є побудова діаграми ієрархії задач, що відображає структуру системи у вигляді ієрархії. Діаграма подана на рисунку 8.

Існує декілька способів представлення такої діаграми. Для виконання даної роботи була обрана деревовидна структура. Діаграма виконана на основі розробленої функціональної діаграми. Основною задачею є «Перевірити товар на автентичність». Вона складається з таких підзадач:

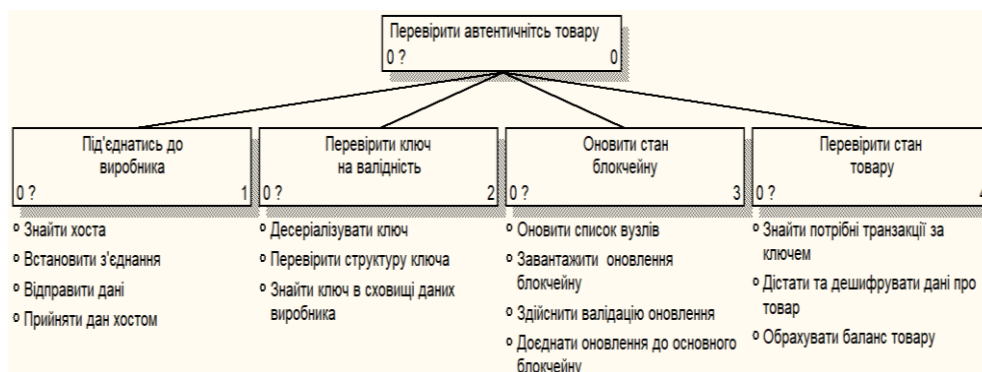


Рис. 8. Діаграма ієрархії задач
 Fig. 8. Task hierarchy diagram

- Під'єднатись до виробника. Складається з наступних підзадач: *Знайти хоста* → *Встановити з'єднання* → *Відправити дані* → *Прийняти дані хостом*.
- Перевірити ключ на валідність. Складається з наступних підзадач: *Десеріалізувати ключ* → *Перевірити структуру ключа* → *Знайти ключ в сховищі даних виробника*.
- Оновити стан блокчейну. Складається з наступних підзадач: *Оновити список вузлів* → *Завантажити оновлення блокчейну* → *Здійснити валідацію оновлення* → *Додати оновлення до основного блокчейну*.
- Перевірити стан товару. Складається з наступних підзадач: *Знайти потрібні транзакції за ключем* → *Дістати та дешифрувати дані про товар* → *Обрахувати баланс товару*.

Висновки.

Боротьба з контрафактом активно триває кожен день і уже розроблено немало способів визначення автентичних товарів. Найбільш популярними є: законодавчий, метод розроблення рекомендацій, метод ускладнення копіювання, метод моніторингу підозрілих оголошень та метод ведення обліку кожної одиниці товару. Розроблювана система належить до останньої категорії. Ринок використання методів захисту від контрафакту є досить розвинутим, адже більшість компаній уже користуються принаймні одним із цих методів. Серед аналогів системи, можна виділити продукт Microsoft Aura Ledger, що також використовує технології блокчейну. Та поставляється у вигляді програмного забезпечення для виробників товару. Перевага розроблюваного продукту в тому, що він об'єднує багатьох виробників у єдину мережу для забезпечення більшої надійності та прозорості даних, а також використання двох-ступеневої ідентифікації, що дає більшу точність. Основними споживачами є виробники товарів, що зазнають матеріальних збитків від виробників контрафакту. Такі виробники бажають мінімізувати

вплив контрафактної продукції на їхній прибуток, а також зберегти репутацію та довіру їхніх покупців. Конкурентами є інші постачальники програмного забезпечення для захисту від підробок на тому ж рівні захисту. Рівні захисту на окремому виробництві можуть комбінуватись. Згідно уже існуючих прикладів держави позитивно ставляться до методів боротьби з контрафактом та готові співпрацювати. Враховуючи загальний стан боротьби з контрафактом, а також низьку поширеність таких методів в Україні можна зробити висновок про те, що доцільно розробити метод боротьби з контрафактом для українського ринку, що є вдосконаленням схожого програмного продукту (Microsoft Aura Ledger), який уже набув певної популярності закордоном. Споживачами продукту стануть виробники товарів, що при покупці отримають набір необхідного програмного забезпечення, а також доступ до спільної мережі блокчейну.

Подяка.

Дана стаття підготована завдяки грантової підтримки Національного Фонду Досліджень України, реєстраційний номер проєкту 2023.04/0012 «Розроблення інформаційної системи автоматичного виявлення джерел дезінформації та неавтентичної поведінки користувачів чатів» за конкурсом ««Наука для зміцнення обороноздатності України»».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Li X., Wang C. The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. *Decision support systems*, 2017, 95: 49-60. DOI: [10.1016/j.dss.2016.12.001](https://doi.org/10.1016/j.dss.2016.12.001)
- [2] Чубенко А.Г., Лошицький М.В., Павлов Д.М., Бичкова С.С., Юнін О.С. Термінологічний словник з питань запобігання та протидії легалізації доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції, К.: Баїте, 2018. – 826 с.
- [3] Allison. Behind the industry of counterfeit products in China and lawsuit success cases, 2021. URL: <https://daxueconsulting.com/counterfeit-products-in-china/>.
- [4] Buttice, V., Caviggioli, F., Franzoni, C., Scellato, G., Strykowski, P., & Thumm, N. Counterfeiting in digital technologies: An empirical analysis of the economic performance and innovative activities of affected companies. *Research Policy*, 49(5) (2020) 103959. DOI: [10.1016/j.respol.2020.103959](https://doi.org/10.1016/j.respol.2020.103959)
- [5] Richter F. The Industries Most Affected by Counterfeit Products, 2019. URL: <https://www.statista.com/chart/17410/counterfeit-and-pirated-products-by-category/>.
- [6] Prokipchuk, O., Chyrun, L., Bublyk, M., Panasyuk, V., Yakimtssov, V., & Kovalchuk, R. (2021). Intelligent System for Checking the Authenticity of Goods Based on Blockchain Technology. In *MoMLeT+ D*, pp. 618-665. <https://eur-ws.org/Vol-2917/paper40.pdf>
- [7] Kumar R., Tripathi R. Traceability of counterfeit medicine supply chain through Blockchain. In: 11th international conference on communication systems & networks (COMSNETS). IEEE, 2019. p. 568-570. DOI: [10.1109/COMSNETS.2019.8711418](https://doi.org/10.1109/COMSNETS.2019.8711418)
- [8] Alipour S. Ninety-Eight Per Cent of Fake or Lookalike iPhone Chargers Put Consumers at Risk of Lethal Electric Shock and Fire, 2017. URL: <https://www.electricalsafetyfirst.org.uk/media-centre/press-releases/2017/12/ninety-eight->

- [per-cent-of-fake-or-lookalike-iphone-chargers-put-consumers-at-risk-of-lethal-electric-shock-and-fire/](#) .
- [9] Casassus B. Health agency reveals scourge of fake drugs in developing world, 2017. URL: <https://www.nature.com/news/health-agency-reveals-scurge-of-fake-drugs-in-developing-world-1.23051> .
- [10] Hamelin N., Nwankwo S., El Hadouchi R. Faking brands': consumer responses to counterfeiting. Journal of Consumer Behaviour, 12(3), (2013) 159-170. doi.org/10.1002/cb.1406
- [11] Zhang L. Platformizing family production: The contradictions of rural digital labor in China. The Economic and Labour Relations Review, 32(3), (2021). 341-359. <https://doi.org/10.1177/103530462110370>
- [12] Nermain A. I., Thanasi-Boçe M., Ali O. Boosting Luxury Sustainability Through Blockchain Technology. Blockchain Technologies in the Textile and Fashion Industry, 17 (2022). https://doi.org/10.1007/978-981-19-6569-2_2
- [13] Doszhan R., Alimbekova G., Kalymbekova Z., Talasbek M. Risk management in the financing of ICO projects: Prospects for the use of modern technologies in Kazakhstan. In E3S Web of Conferences 159 (2020) 04017. EDP Sciences. <https://doi.org/10.1051/e3sconf/202015904017>
- [14] Asadizanjani N., Tehranipoor M., Forte, D. Counterfeit electronics detection using image processing and machine learning. In Journal of physics: conference serie, 787 (2017) 012023. [doi:10.1088/1742-6596/787/1/012023](https://doi.org/10.1088/1742-6596/787/1/012023)
- [15] Lee H., Yeon C. Blockchain-based traceability for anti-counterfeit in cross-border e-commerce transactions. Sustainability, 13(19) (2021) 11057. <https://doi.org/10.3390/su131911057>
- [16] Pal K. Internet of things and blockchain technology in apparel manufacturing supply chain data management. Procedia Computer Science, 170 (2020) 450-457. <https://doi.org/10.1016/j.procs.2020.03.088>
- [17] Mlalila N., Kadam D. M., Swai H., Hilonga A. Transformation of food packaging from passive to innovative via nanotechnology: concepts and critiques. Journal of food science and technology, 53 (2016) 3395-3407. DOI: [10.1007/s13197-016-2325-6](https://doi.org/10.1007/s13197-016-2325-6)
- [18] How holograms can stop counterfeiting, 2014. URL: <https://www.packagingdigest.com/smart-packaging/how-holograms-can-stop-counterfeiting>
- [19] Saxena N., Thomas I., Gope P., Burnap P., Kumar N. Pharmacrpt: Blockchain for critical pharmaceutical industry to counterfeit drugs. Computer, 53(7) (2020) 29-44. DOI: [10.1109/MC.2020.2989238](https://doi.org/10.1109/MC.2020.2989238)
- [20] Bulchand-Gidumal J., Melián-González S. Fighting fake reviews with blockchain-enabled consumer-generated reviews. Current Issues in Tourism, (2023) 1-15. <https://doi.org/10.1080/13683500.2023.2173054>
- [21] Масікевич Ю. Г., Шестопалов О. В., Негадайло А. А. та ін. [Теорія систем в екології](#). Суми : Сумський державний університет, 2015. – 330 с.
-

**IT PROJECT OF DATA AUTHENTICATION VERIFICATION SYSTEM BASED ON
BLOCKCHAIN TECHNOLOGY****O. Prokipchuk¹, V. Vysotska¹, M. Nazarkevych², V. Danylyk¹**¹*Lviv Polytechnic National University,
12 Bandery St., UA-79013, Lviv, Ukraine*²*Lviv Ivan Franko National University,
107 Tarnavskogo St., 79017 Lviv, Ukraine*mariia.nazarkevych@lnu.edu.ua

The developed information system is designed to help buyers of goods to identify the original product by placing two identification scan codes on the product, which lead to information located in a protected blockchain data structure. This system is economically feasible for companies producing goods, because it can significantly reduce material damage caused by manufacturers of counterfeit goods. A positive perception of this software product by potential consumers of goods is also expected, as the system will allow users to have exactly what they want - not to come across fakes and save money. The implementation of the IT project is based on three directions, such as working out problems, designing interconnections, and realizing a demo version of the project. Working out the issues is the theoretical and methodological foundation on which the following aspects will be based. An aspect is a collection of problem analysis, possible solutions and workarounds at different levels of system implementation. The success criteria of the aspect are persuasiveness and competitiveness. Persuasiveness shows the extent to which the implementation of the system inspires confidence in the final buyer of the goods. Competitiveness shows the security factor of the system in relation to methods of counterfeiting goods and ways of bypassing protection against counterfeiting. The set of criteria determines the level of success of the project, provided that the criteria of the following aspects are met. The second aspect is designing relationships. This aspect involves defining the system architecture and the connections between them at different levels of implementation. Sets the behavior of the product in its application. The criteria for this aspect are flexibility and stability. Flexibility provides the ability to expand the system with as little effort as possible, as well as the fine configuration of individual components without global intervention in the implementation. Stability determines how much the system can work without deviating from expectations when the load increases or the scale of the implementation increases. The last aspect is the implementation of the system. The aspect is responsible for all stages of the implementation of previously prepared plans into reality. Implementation is the longest and most demanding. It is necessary to start this stage after complete completion of the previous ones. The criteria of the last aspect are accuracy and security. Accuracy shows the ratio of the number of successfully detected original products to all product detection attempts by the developed system. Security shows the degree of system protection against possible attacks and methods of data compromise.

Keywords: network communication, information system, counterfeit good, blockchain technology, product life cycle, intelligent information retrieval system, manufacturer environment.

*Стаття надійшла до редакції 22.09.2024.
Прийнята до друку 04.10.2024.*