ISSN 2076-1546

УДК 004.4:003.26:681.326.3 DOI: 10.46972/2076-1546.2022.22.01

А. О. Левченко, С. Г. Трутнєв, Н. П. Ісмаілова, І. В. Шарипова

ПРОГРАМНА РЕАЛІЗАЦІЯ ПІДСИСТЕМ ОБМІНУ ДАНИМИ ЕКСПЕРТІВ У РОЗПОДІЛЕНИХ КОМПЛЕКСАХ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ БОЙОВИХ ДІЙ

Інтенсивний розвиток інформаційних систем створює умови для розробки і впровадження сучасних інформаційних засобів, що дозволяють автоматизувати і тим самим більш ефективно реалізовувати процеси управління. Разом зі зростаючою складністю інформаційних систем і використовуваних у них інформаційних технологій збільшується обсяг вимог, що до них висуваються.

Одним із напрямків реалізації інформаційних систем у сучасних зразках бойової техніки є блоки управління інформаційних систем, які забезпечують не тільки управління зразком бойової техніки, але й оперативний обмін даними з екіпажем. Сучасні комплекси імітаційного моделювання бойових дій (типу PEO STRI американської компанії Alion Science & Technology) дозволяють проводити імітацію бою підрозділу з обміном даними між екіпажем (експертами).

Основну роль у забезпеченні безпеки в підсистемах обліку сучасних комплексів моделювання бойових дій повинні відігравати напрацьовані й перевірені методи сучасної криптографії. Використання того чи іншого криптографічного протоколу або алгоритму має бути продиктовано необхідністю та обґрунтованістю.

Оскільки безпечний обмін даними є критичним питанням у сучасних умовах розвитку Збройних Сил України в цілому та в підсистемах обліку сучасних комплексів моделювання бойових дій зокрема, а під час обміну даними повинні вживатися такі заходи, за яких передача даних з кожного робочого місця системи недоступна третім стороннім особам, запропоновано використання технології блокчейн у сфері електронного обміну даними. У такому процесі підвищується ймовірність недопущення витоку даних. Однак під час захищеного обміну даними неможливо визнати цю процедуру повністю адекватною, тому що такий спосіб інформаційного обміну не можна верифікувати, якщо буде велика кількість операторів (тобто на оперативно-тактичному рівні).

Ключові слова: *обмін даними; захист даних робочого місця; моделювання; блокчейн; інформаційні системи; бойові дії.*

Постановка проблеми в загальному вигляді. Обмін даними між інформаційно-керувальними системами є основною проблемою особливо на тактичному рівні. З розвитком комп’ютерних технологій та автоматизованих систем необхідність удосконалення автоматизації процесів обміну даними на сьогоднішній день є найбільш актуальною. Не менш важливим також є обмін даними, які містять у собі закриту інформацію від третіх осіб.

Наявні системи обміну даними застарілі та не в повному обсязі забезпечують автоматизовану передачу інформації в комп’ютерних системах, крім того, вони складні

у використанні. Одним із таких процесів, які необхідно автоматизувати, є робота на комплексах імітаційного моделювання бойових дій, наприклад, відпрацювання тактичних заходів з різними силами на різноманітних ділянках місцевості, порядок організації взаємодії зі своїми підрозділами, а також із підпорядкованими, що мають розподілену структуру, зокрема в навчальних закладах під час проведення занять. Крім того, великий інтерес викликає можливість автоматизувати обмін даними на різних рівнях. Саме тому більшість розробок на даний момент здійснюється в цьому напрямку.

Аналіз останніх досліджень і публікацій. У [4, 16] досліджено питання розвитку технології розподіленого реєстру (блокчейну) і можливостей його застосування в різних сферах людської діяльності. У згаданих роботах додатково проаналізовано принципи, згідно з якими працює технологія блокчейн. Визначено її найсильніші сторони захисту від хакерських атак або змін складових ланцюгів та блоків.

Автор роботи [11], який є засновником Інституту блокчейн-дослідженнь (Institute for Blockchain Studies), більш детально розглянув можливості використання та провадження технології блокчейн у різних сферах діяльності. Логічним продовженням його дослідження є [12, 15], де проаналізовано захищені системи електронного голосування на основі криптографічних алгоритмів.

Варто зазначити, що багато популярних інтернет-джерел та таблоїдів звертають увагу на велику переспективу розвитку цієї технології, зокрема й у військовій сфері. Деякі з них зазначають, що технологія блокчейн має великі перспективи в захисті інформаційних систем (ІС) із закритим доступом.

Формулювання завдання дослідження. Основною метою роботи з визначення доцільних шляхів створення підсистем обміну даними є підвищення безпеки криптографічного захисту даних в інформаційно-керувальних системах та комплексах імітаційного моделювання шляхом модифікації протоколу передачі даних із використанням технології блокчейн. Головну роль у забезпеченні безпеки в проєктованій підсистемі обміну даними програмної реалізації підсистем обміну даними експертів у розподілених комплексах імітаційного моделювання бойових дій повинні відігравати напрацьовані та перевірені методи сучасної криптографії, використання того чи іншого криптографічного протоколу або алгоритму. Отже, логічним є продовжити вивчення використання технології блокчейн для підвищення криптографічного захисту в розподілених системах.

Завданням роботи є вивчення можливостей створення програмної реалізації підсистем обміну даними в розподілених системах імітаційного моделювання бойових дій. Розробка відповідного програмного забезпечення надасть можливість у подальшому проводити порівняльний аналіз технології криптографічного захисту в реальних умовах.

Виклад основного матеріалу. Створення систем обміну даними із застосуванням технології блокчейн тільки починає впроваджуватися у військову сферу, тоді як, наприклад, переваги проведення виборів через мережу загального користування є очевидними. Серед них можна виділити корисні і для підсистем обміну даними в системах моделювання бази даних (БД):

можливість дистанційної роботи;

конфіденційність оператора;

можливість перегляду переданих даних;

економія часу;

відповідність рекомендаціям кодексу корпоративного управління;

здійснення підрахунку голосів (обмін даними) за менший проміжок часу;

простота використання сервісу.

Для досягнення мети дослідження необхідно вирішити такі завдання:

1) вивчення протоколів електронного обміну даними;

2) огляд систем електронного обміну даними та сфери застосування;

3) дослідження криптографічних методів, що використовуються в комплексах імітаційного моделювання;

4) модифікація протоколу обміну даними з використанням технології блокчейн.

Безпосередньо обмін даними може бути відкритим чи закритими. Відкритий забезпечує обмін даними, що не містять інформації з обмеженим доступом. Закритий обмін даними призначений для обмеженого кола посадових осіб [13], що не обов'язково передбачає обмін між елементами розподіленої системи даних, які містять інформацію з обмеженим доступом.

Отже, під час закритого обміну даними вживаються заходи, щоб інформація, передана оператором, була недоступною третім особам. У такому разі підвищується ймовірність уникнення витоку даних для сторонніх. Електронний обмін даними – термін, який використовують для різних типів передачі інформації, охоплюючи ним як процес здійснення обміну даними за допомогою електронних засобів, так і процес автоматичної передачі інформації за допомогою електронних пристроїв та спеціального програмного забезпечення. Якщо система забезпечення кібергігієни в державних органах дозволяє вирішити питання безпосереднього переносу даних, то ймовірність їх втрати або підміни під час передачі телекомунікаційним обладнанням залишається високою. Системи електронного обміну даними можна поділити на два типи: ті, які потребують безпосереднього втручання оператора, й ті, що дозволяють обмін даними дистанційно.

Сучасна система обміну даними для програмної реалізації підсистем обміну даними експертів у розподілених комплексах імітаційного моделювання бойових дій має відповідати таким вимогам:

1) авторизованість (тільки авторизовані користувачі можуть здійснювати обмін даними);

2) унікальність (кожен користувач має право доступу до визначеного адміністратором об'єму даних);

3) точність (система передавання даних без коригування, тобто інші користувачі не можуть вносити зміни до них);

4) верифікованість (можливість перевірити, чи точні дані передані користувачем);

5) таємність (забезпечення прихованості інформації; ніхто не може визначити, звідки та кому вона була передана);

6) автоматизованість (користувач, передаючи дані, не повинен визначати адресатів, а система самостійно здійснює передачу даних необхідним абонентам).

Опис рішень для програмної реалізації системи обміну даними. Під час досліджень спроєктовано та розроблено варіанти реалізації сервісу для обміну даними на

основі технології блокчейн з використанням розподіленої та традиційної БД, які дозволяють домогтися максимальної продуктивності, зберігаючи при цьому всі переваги використання цієї технології.

Для розробки програмної реалізації використовувалася мова JavaScript для створення користувацького інтерфейсу та сервера. За БД обрано MongoDB, яка зберігає дані у форматі JSON, що дозволяє застосовувати універсальний формат серіалізації даних, які використовуються для клієнта та на сервері. Це сприяє легкості читання, зрозумілості та цілісності додатка.

Для створення моделей даних, які мають зберігатися в централізованій документоорієнтованій MondoDB, використовують бібліотеку Mongoose [3], що надає можливість створювати чітку схему для роботи з БД. Прикладом створення схеми даних може правити модель User – користувач системи:

```
const userSchema = mongoose.Schema({
  _id: mongoose.Schema.Types.ObjectId,
  email: { type: String, required: true, unique: true,
    match: /[a-z0-9!#$%&'*+/=?^_`{|}~-]+(?:\.[a-z0-9!#$%&'*+/=?^_`{|}~-]+)*@(?:[a-z0-9](?:[a-z0-9-]*[a-z0-9])?\.)+[a-z0-9](?:[a-z0-9-]*[a-z0-9])?/
  },
  socialNumber: { type: String, required: true, unique: true, match: /[0-9]{10}/},
  password: { type: String, required: true },
  isAdmin: Boolean
});
module.exports = mongoose.model('User', userSchema).
```

Також ця бібліотека дозволяє описати тип валідації моделі даних.

Для входу в систему був створений клас UserController, що є контролером, який дозволяє зареєструватися та виконати автентифікацію в системі. Для реєстрації користувачеві необхідно ввести свою електронну пошту, ідентифікаційний номер, а також пароль, що мають бути унікальними. Після успішної авторизації користувач може розпочинати роботу з виділеними йому обов’язками в системі.

Клас Candidate Controller призначений для обліку користувачів у системі. Лише її адміністратор може створювати чи видаляти дані користувачів. Переглядати інформацію, надану користувачами, може будь-який авторизований користувач системи.

Клас Vote Controller призначений для обміну даними із заданими датою, часом початку та закінчення обробки даних.

Клієнтський додаток містить логіку роботи з блокчейн, де реалізовані класи роботи з ним.

Клас Block відображає сутність блока в розподіленій базі блокчейн. Він містить хеш, хеш попереднього блоку, дату створення, список транзакцій, а також число, яке було знайдено під час майнінгу. У даному класі реалізовані методи пошуку хеш-образу даного блоку, майнінг блоку, а також перевірка валідності транзакцій.

Клас Transaction є моделлю підтвердження користувача в розподіленій системі блокчейн. Він містить адреси відправника й одержувача, тобто адреси пристроїв та дату створення. У даному класі реалізовано методи обчислювання хеш-образу транзакції, створення та перевірки підпису.

Клас Blockchain відображає сутність розподіленої БД у запропонованому протоколі системи. Він містить ланцюг блоків, параметр складності знаходження хеш-образу для майнінгу, а також список транзакцій, що очікують майнінгу. Реалізовано метод створення первинного блоку, оскільки його розглядають як окремий випадок. Первинний блок не має блоків нащадків. Також описано методи додання транзакцій у список очікуваних, визначення достовірності користувача та перевірки валідності БД блокчейн.

Клас Node відображає сутність вузла розподіленої системи. У ньому реалізовано доступ до P2P-мережі. Кожен вузол системи зберігає в собі БД блокчейн, підключення до P2P, список підключень в одноранговій мережі. Клас має методи отримання всіх поточних підключень у мережі, відправки заявки на отримання актуальної БД блокчейн та метод розповсюдження повідомлення мережею.

Після успішної авторизації в системі користувач автоматично підключається до однорангової мережі та оповіщає всіх, відсилаючи свій ідентифікатор у P2P-мережі. Після цього, знаючи підключення один одного, кожен вузол має можливість відправляти повідомлення за протоколом WebRTC, у такий спосіб реалізовано мережу спілкування без підтримки сервера.

Опис роботи системи електронного обміну даними. Після вдалої реєстрації та входу в систему користувач отримує можливість згенерувати приватний ключ, який має зберегти на своєму носії.

Після авторизації в системі користувач потрапляє на головну сторінку, на якій є короткий пояснювальний курс системи обміну даними. Далі користувач може перейти на сторінку перегляду інших користувачів системи імітаційного моделювання, на якій є основна інформація про кожного експерта (рис. 1).

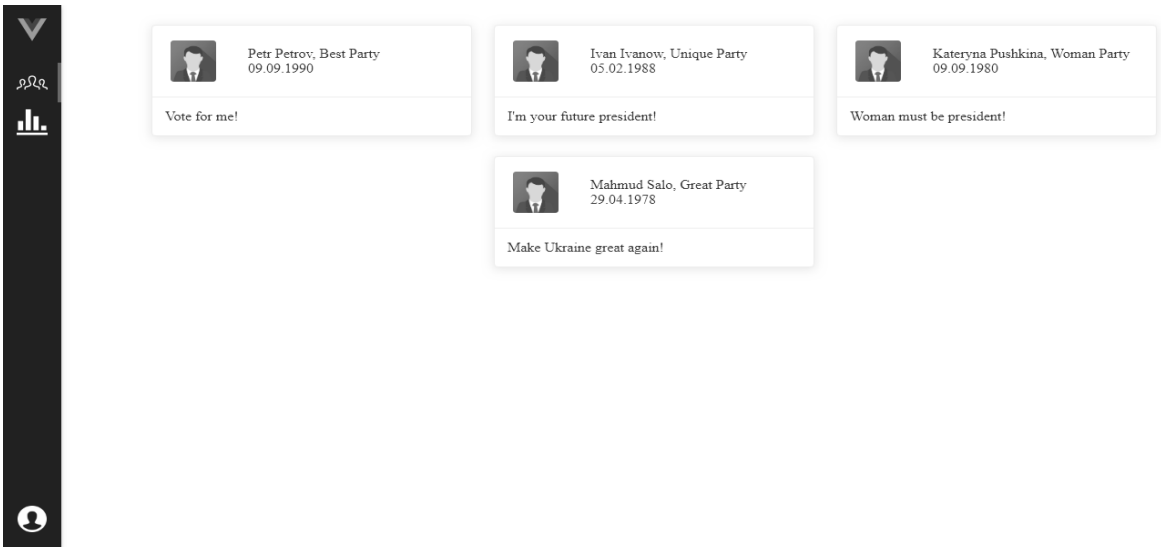

Рис. 1. Сторінка перегляду користувачів

Користувач в реальному часі може переходити на сторінку обміну даними, де створені умови, щоб передати інформацію та переглянути наявні дані на сервері в об’ємі відповідно до доступу (рис. 2).

Після того, як користувач сформував дані для передачі, з’являється вікно для введення особистого ключа.

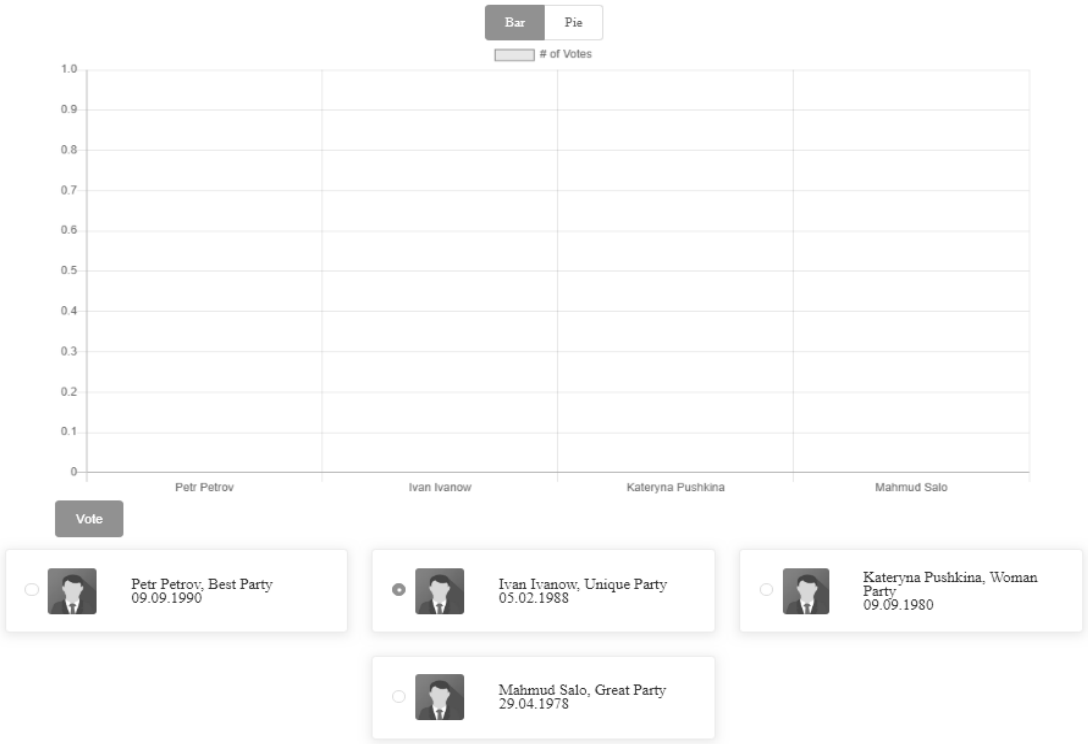

Рис. 2. Сторінка обміну даними

У той час, коли користувач підтвердив введення особистого ключа, починається процес генерації публічного ключа, після цього створюється транзакція з адресою відправника (публічного ключа), адресою отримувача. Далі генерується підпис транзакції з використанням приватного ключа. Користувач майнить блок, у який додається транзакція. Одразу, як блок було замайнено, він відсилається в мережу, де всі користувачі можуть додати його до своєї БД блокчейн. У такий спосіб було здійснено передачу даних.

Якщо користувач намагається ще раз передати ту ж саму інформацію, то він отримає повідомлення, що він вже її передав, оскільки його адреса вже присутня в БД.

Проаналізовані можливі кібератаки на SEG із застосуванням технології блокчейн, тобто на розподілену систему. Найпоширенішими є атака подвійної трати, DoS/DDoS-атаки та атака Сивілли.

Атака подвійної трати полягає в тому, що зловмиснику необхідно:

виконати транзакцію, що атакує попередню оплату;

таємно майнити, використовуючи той блок, що включає в себе останню транзакцію;

продовжувати майнити таємну альтернативну гілку блокчейну, доки вона не стане більшою, ніж публічна, після чого вона транслюється в мережу. Оскільки нова гілка довша, ніж усі відомі, вона буде дійсною і переказ транзакції отримувачу буде замінено на переказ зловмиснику.

Атака подвійної трати має ймовірність успіху, якщо зловмисник має більш, ніж 50% обчислювальної потужності. Якщо підконтрольна обчислювальна потужність становить менше ніж 50%, то ймовірність успіху експоненціально знижується. Навіть наявність більше ніж 50% ресурсів не гарантує створення альтернативної гілки [6].

DDoS-атака проводиться одночасно на велику кількість комп'ютерів з метою спричинити відмову в обслуговуванні сервера чи мережі. Для запобігання цього типу атак

слугує обчислення задачі майнінгу (Proof-of-Work). Неможливо створити блок так часто, щоб організувати спам-розсилання в мережі. З підвищенням складності знаходження хеш-образу та його криптографічної стійкості витрачається більше часу, що є також ускладненням для зловмисників, яким під час спроби змінити дані в блоці буде необхідно перерахувати усю подальшу послідовність блоків, а також переконати всіх користувачів системи, що це валідна БД блокчейн, що є майже неможливим.

У табл. 1 наведено результати тестування майнінгу одного блока за підвищення складності.

Таблиця 1

Результати тестування майнінгу одного блоку

№	Складність (кількість «0» на початку хеш)	Середній затрачений час
1	00	0,02 с
2	000	0,2 с
3	0000	3 с
4	00000	45 с
5	000000	500 с (8,3 хв)
6	0000000	~ 2 год.

Отже, у разі великої складності обчислень стає майже неможливим перерахувати на одному комп'ютері достатньо великий ланцюг блоків, тобто неможливо змінити дані в розподіленій БД блокчейн. Якщо навіть зловмиснику вдалося перерахувати ланцюг блоків, йому необхідно змінити блокчейн на кожному вузлі розподіленої системи, що є неможливим.

Завдяки тому, що розподілена система організована за допомогою однорангової мережі, якщо сервер комплексу імітаційного моделювання БД буде виведено з ладу в результаті DDOS атаки, то система функціонуватиме далі, а дані не будуть втрачені чи пошкоджені.

Атака Сивілли – атака, під час якої зловмисник заповнює мережу підконтрольними йому вузлами і намагається оточити вузол жертви, заволодіти сусідніми вузлами мережі. Отримавши доступ до вузлів, зловмисник:

контролює всі вхідні та вихідні дані;

може передавати жертві некоректну інформацію;

може блокувати передачу даних.

Реалізація даної атаки стає неможливою, оскільки підключення до будь-якого вузла відбувається випадково, неможливо заздалегідь знати сусідні підключення будь-якого вузла.

Результати проведеного аналізу технології блокчейн і можливості її використання у сфері електронного обміну даними дозволяють стверджувати, що усі вимоги, розроблені щодо виконання та роботи системи імітаційного моделювання, були виконані.

Висновки. Сектор імітаційного моделювання у збройних силах провідних країн світу займає визначне місце в системі підготовки військ (сил). Навчання із застосуванням засобів імітаційного моделювання батальйонного, бригадного та вищого рівня включені в загальну систему бойової підготовки. На даний час цей досвід також успішно впроваджується й у Збройних Силах України.

Розвиток спеціального програмного та математичного забезпечення імітаційного моделювання йде в напрямку найбільш повної імітації всіх функцій застосування озброєння, бойової техніки та військових формувань.

Оскільки безпечний обмін даними є критичним питанням у сучасних умовах розвитку Збройних Сил України в цілому та в підсистемах обліку сучасних комплексів моделювання БД зокрема, а під час обміну даними повинні вживатися такі заходи, у ході яких передача даних кожного робочого місця системи недоступна третім особам, запропоновано використання технології блокчейн у сфері електронного обміну даними.

Отже, програмна реалізація підсистем обміну даними експертів у розподілених комплексах імітаційного моделювання бойових дій за допомогою технології блокчейн є достатньо простим у впровадженні, захищеним, однозначним і досить потужним рішенням для застосування в сучасних комплексах імітаційного моделювання БД.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Don Tapscott, Alex Tapscott. Blockchain revolution. How the technology underlying bitcoin and other cryptocurrencies is changing the world. London : Publisher Penguin, 2018. 488 p. https://doi.org/10.1177/2319714518814603
2. Javascript-фреймворки: тенденции 2019 года. URL: https://habr.com/ru/company/plarium/blog/433926/ (дата обращения: 20.01.2022).
3. Mongoose. URL: https://mongoosejs.com/ (last accessed: 20.12.2021).
4. Overview of the Blockchain Industry in Ukraine. URL: https://www.slideshare.net/Blockchainukraine/overview-of-the-blockchain-industry-in-ukraine-145456836?fbclid=IwAR2oawBP1GeGagq4gU6e35sLWGI (last accessed: 02.01.2022).
5. Peer-to-peer. URL: https://bitcoin.org/ bitcoin.pdf (last accessed: 10.01.2022).
6. SQL или NoSQL – вот в чем вопрос. URL: https://habr.com/ru/company/ruvds/blog/324936/ (дата обращения: 10.01.2022).
7. Введення. Що таке Vue.js? URL: https://ru.vuejs.org/v2/guide/ – 03.01.2018 (дата звернення: 10.01.2022).
8. Еліптична криптографія. URL: https://habr.com/ru/post/191240/ (дата звернення: 14.01.2022).
9. Належне хешування паролів. URL: https://www.securitylab.ru/analytics/427930.php (дата звернення: 14.01.2022).
10. Пірингові мережі. URL: http://dwl.kiev.ua/art//p2p/p2p-end.pdf (дата звернення: 20.01.2022).
11. Свон М. Блокчейн: схема новой экономики. Москва : Изд-во «Олимп-Бизнес», 2017. 240 с.
12. Тарасов А. І., Шпінарева І. М. Система електронного голосування із застосуванням технології блокчейн // Захист інформації в інформаційно-комунікаційних системах : зб. тез доповідей III Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів «Захист інформації в інформаційно-комунікаційних системах». Львів, 2019. С. 121.
13. Толковый словарь Дмитриева URL: https://dic.academic.ru/dic.nsf/dmitriev/807голосование (дата обращения: 20.01.2022).
14. Хеш-функції. URL: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema9 (дата звернення: 20.01.2022).
15. Яркова О. Н., Осіпова А. А. Захищена система електронного голосування на основі криптографічних алгоритмів // Вісник УРФО. Безпека в інформаційній сфері. 2014. № 2 (12). С. 9–15.

16. Яцків Н. Г., Ятсків С. В. Перспективи використання технології блокчейн у мережі Інтернет речей // Науковий вісник НЛТУ України. 2016. Вип. 26 (8). С. 381–387. https://doi.org/10.15421/40260857

Стаття надійшла до редакції 27.01.2022.

REFERENCES

1. Don Tapscott, & Alex Tapscott. (2018). *Blockchain revolution. How the technology underlying bitcoin and other cryptocurrencies is changing the world.* London: Publisher Penguin. https://doi.org/10.1177/2319714518814603
2. *Javascript-freimvorki: tendentsii 2019 goda [Javascript frameworks: trends of 2019]*. (2019). Retrieved from https://habr.com/ru/company/plarium/blog/433926/ [in Russian].
3. *Mongoose*. (n.d.). Retrieved from https://mongoosejs.com/
4. *Overview of the Blockchain Industry in Ukraine.* (n.d.). Retrieved from https://www.slideshare.net/Blockchainukraine/overview-of-the-blockchain-industry-in-ukraine-145456836?fbclid=IwAR2oawBP1GeGagq4gU6e35sLWGI
5. *Peer-to-peer. (n.d.).* Retrieved from https://bitcoin.org/ bitcoin.pdf
6. *SQL ili NoSQL – vot v chem vopros [SQL or NoSQL, that is the question]*. (n.d.). Retrieved from https://habr.com/ru/company/ruvds/blog/324936/ [in Russian].
7. *Vvedennia. Shcho take Vue.js? [Introduction. What is Vue.js?]*. (n.d.). Retrieved from https://ru.vuejs.org/v2/guide/–03.01.2018 [in Ukrainian].
8. *Eliptychna kryptohrafiia [Elliptical cryptography]*. (n.d.). Retrieved from https://habr.com/ru/post/191240/ [in Ukrainian].
9. *Nalezhne kheshuvannia paroliv [Proper hashing of passwords]*. (n.d.). Retrieved from https://www.securitylab.ru/analytics/427930.php [in Ukrainian].
10. *Pirynhovi merezhi [Peer networks]*. (n.d.). Retrieved from http://dwl.kiev.ua/art//p2p/p2p-end.pdf [in Ukrainian].
11. Svon, M. (2017). *Blokchein: skhema novoi ekonomiki [Blockchain: New Economy Scheme]*. Moscow [in Russian].
12. Tarasov, A. I., & Shpinareva, I. M. (2019). Systema elektronnoho holosuvannia iz zastosuvanniam tekhnolohii blokchein [Electronic voting system using blockchain technology]. In *Zakhyst informatsii v informatsiino-komunikatsiinykh systemakh: zb. tez dopovidei III Vseukr. nauk.-prakt. konf. molodykh uchenykh, studentiv i kursantiv «Zakhyst informatsii v informatsiino-komunikatsiinykh systemakh» [Protection of information in information and communication systems: collection. theses of reports of the III All-Ukrainian science and practice conf. of young scientists, students and cadets "Protection of information in information and communication systems"]*. Lviv, 2019. (pp. 121–122) [in Ukrainian].
13. *Tolkovyi slovar' Dmitrieva [Dmitriev's Explanatory Dictionar]*. (n.d.). Retrieved from https://dic.academic.ru/dic.nsf/dmitriev/807golosovanie [in Russian].
14. *Khesh-funktsii [Hash functions]*. (n.d.). Retrieved from https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema9 [in Ukrainian].
15. Yarkova, O. N., & Osipova, A. A. (2014). Zakhyshchena systema elektronnoho holosuvannia na osnovi kryptohrafichnykh alhorytmiv [A secure system of electronic voting based on

cryptographic algorithms]. *Visnyk URFO. Bezpeka v informatsiinii sferi [Bulletin of URFO. Security in the information sphere.]*, *2* (12), 9–15 [in Ukrainian].
16. Yatskiv, N. H., & Yatskiv, S. V. (2016). Perspektyvy vykorystannia tekhnolohii blokchein u merezhi internet rechei [Prospects for the use of blockchain technology in the Internet of Things]. *Naukovyi visnyk NLTU Ukrainy [Scientific Bulletin of the NLTU of Ukraine]*, *26* (8), 381–387. https://doi.org/10.15421/40260857 [in Ukrainian].

A. O. Levchenko, S. H. Trutnev, N. P. Ismailova, I. V. Sharipova

SOFTWARE IMPLEMENTATION OF EXPERTS DATA EXCHANGE SUB-SYSTEMS IN DISTRIBUTED COMPLEXES FOR SIMULATION OF COMBAT ACTIONS

The comprehensive development of information systems creates conditions for the development and implementation of modern information tools that automate, and thereby more effectively implement management processes. At the same time, due to the increasing complexity of information systems and the information technologies used in them, the volume of requirements for them is growing.

One of the directions for introducing IS into modern models of military equipment is information systems control units. Modern information systems control units not only provide control of the military equipment sample, but also provide operational data exchange with the crew. Modern database modeling complexes (such as PEO STRI, the American company "Alion Science & Technology") make it possible to simulate the combat actions of a unit with the exchange of data between the crew (experts).

The main role in ensuring the security of accounting subsystems of modern database modeling complexes should be played by well-tried and tested methods of modern cryptography. The use of one or another cryptographic protocol or algorithm should be dictated by necessity and validity.

Since in the modern conditions of the development of the Armed Forces of Ukraine in general and in the accounting subsystems of modern database modeling complexes in particular, ensuring secure data exchange is an urgent task, such measures should be taken when exchanging data in which data transmission from each workstation of the system is not available to third parties. persons, therefore it is proposed to use blockchain technology in the field of electronic data exchange.

Thus, when exchanging data, such measures are used in which the transfer of data from each workstation of the system was not available to third parties.

This process increases the likelihood of eliminating the possibility of data leakage. However, with secure data exchange, this procedure cannot be considered completely adequate, since this method of data exchange cannot be tested on a large number of operators (that is, at the operational-tactical level).

Keywords: *data exchange, workplace data protection modeling, blockchain, information systems, military operations.*