DOI 10.31891/2307-5732-2023-327-5-98-102
УДК 004.41

ПІРОГ ОЛЕКСАНДР
Державний університет Житомирська політехніка
https://orcid.org/0009-0001-6111-9676
e-mail: pirogov@ztu.edu.ua
ГОЛОВНЯ ОЛЕНА
Державний університет Житомирська політехніка
https://orcid.org/0000-0003-0095-7585
e-mail: olenaholovnia@gmail.com
КОЛОЩУК МАРИНА
Державний університет Житомирська політехніка
https://orcid.org/0009-0001-5825-2054
e-mail: kkik_kms@ztu.edu.ua

РОЗРОБКА ТА ТЕСТУВАННЯ ВЕБ-ОРІЄНТОВАНОЇ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ З ВИКОРИСТАННЯМ ЕЛЕМЕНТІВ БЛОКЧЕЙН ТЕХНОЛОГІЙ

У статті розглянуто можливі шляхи вирішення бюрократичних та корупційних проблем у держорганах за допомогою блокчейн-технологій, проаналізовано веб-сервіси, що в даний час використовуються для управління документами, та виявлено, що існує багато пропозицій он-лайн систем управління документами в корпоративному верхньому ціновому сегменті навіть з використанням технологій блокчейну. В нижньому ціновому сегменті пропозиції захисту документів можливі або за додаткову ціну, або з використанням сторонніх інструментів, підключених або розроблених самостійно.

Аналіз моделі загроз показав, що основними порушниками є інсайдер, що має доступ до адміністрування додатку реєстрації документів або до адміністрування бази даних додатку, що несе в собі загрозу зміни ним цих даних, та зовнішній порушник, що може використовувати основні вразливості веб-додатків, такі як SQL-ін'єкції, CSRF, XSS атаки, атаки повного перебору реєстраційних даних, задля розвідки, отримання адміністративних прав доступу та внесення змін в реєстраційні дані.

Розроблено та протестовано додаток, що реалізує визначені механізми захисту: Використання технології блокчейн для неможливості непомітної зміни реєстраційних даних зареєстрованих документів; Збереження хеш-суми зареєстрованих документів та верифікація зареєстрованих документів; Налаштування розмежування доступу для збереження конфіденційної та комерційної таємниці в установі; Захист від інших вразливостей веб-додатків.

Встановлено, що інтерес до блокчейн технологій продовжує зростати з реформуванням та розвитком всіх сфер української держави, а саме медичної реформи, судової та правоохоронної реформи, розвитком електронної держави та так званої «діджиталізації» держави та в умовах триваючої кібервійни з державою-агресором. Використання блокчейн технологій може вирішити багато проблем, пов'язаних з бюрократією, корупцією, крадіжками та шахрайствами.

Отже, застосування блокчейн логіки в системах електронного документообігу надійно запобігає спробам зловмисників змінити зареєстровані документи.

Ключові слова: блокчейн; система електронного документообігу; СЕД.

PIROH OLEKSANDR
Zhytomyr Polytechnic State University
HOLOVNIA OLENA
Zhytomyr Polytechnic State University
KOLOSHCHUK MARIIA
Zhytomyr Polytechnic State University

DEVELOPMENT AND TESTING OF A WEB-ORIENTED ELECTRONIC DOCUMENT MANAGEMENT SYSTEM USING BLOCKCHAIN TECHNOLOGIES ELEMENTS

The article examines possible ways to solve bureaucratic and corruption problems in state organizations with the help of blockchain technologies, analyzes the web services currently used for document management and reveals that there are many offers of online document management systems in the corporate upper price segment, even using blockchain technologies. In the lower price segment, document protection offers are possible either for an additional price or with the use of third-party tools, connected or developed independently.

Threat model analysis showed that the main offenders are an insider who has access to the administration of the document registration application or to the administration of the application database, which carries the threat of changing this data, and an external offender who can use the main web applications vulnerabilities, such as SQL injection, CSRF, XSS attacks, brute force attacks, for reconnaissance, obtaining administrative access and making changes to registration data.

The application has been developed and tested that implements certain protection mechanisms: Use of blockchain technology for the impossibility of imperceptibly changing the registration data of registered documents; of Registered documents hash sum storage and registered documents verification; Setting up delimitation of access to preserve confidential and commercial secrets in the institution; Protection against other web application vulnerabilities.

It has been established that interest in blockchain technologies continues to grow with the reform and development of all spheres of the Ukrainian state, namely medical reform, judicial and law enforcement reform, the development of the electronic state and the so-called "digitalization" of the state, and in the context of the ongoing cyber war with the aggressor state. The use of blockchain technology can solve many problems related to bureaucracy, corruption, theft and fraud.

Therefore, the application of blockchain logic in electronic document management systems reliably prevents attempts by criminals to change registered documents.

Keywords: blockchain; electronic document management systems; EDMS.

Постановка проблеми

Система електронного документообігу (СЕД) – дуже важлива частина інформаційного ландшафту сучасної організації. Електронний документообіг у сьогоднішній день широко впроваджується у таких захищених законом сферах як: медицина, судова діяльність, освіта, фінанси, державні послуги (Дія). СЕД також призначена для вирішення критично важливих бізнес-завдань, пов'язаних з управлінням, зберіганням та інтеграцією документів, різних файлів та іншої важливої інформації, що міститься в інформаційних системах та бізнес-додатках. Для нормальної роботи електронного документообігу необхідний безпечний та надійний процес обробки та зберігання інформації. Захищений електронний документообіг – одне з найважливіших завдань забезпечення спільної безпеки в організації, якій необхідно приділяти дуже велике значення та пильну увагу. Для забезпечення інформаційної безпеки використовуються сучасні криптографічні засоби захисту та шифрування інформації для однозначного розмежування доступу до неї, а одним з новітніх методів є застосування технології блокчейн для збереження даних і виключення їх фальсифікації, що особливо актуально в період переходу людства до використання INDUSTRY 4.0.

Аналіз останніх джерел

Консалтингова компанія Booz Allen Hamilton представила огляд [1] можливих шляхів вирішення бюрократичних проблем у держорганах за допомогою блокчейн-технологій. Завдяки прозорій та децентралізованій системі, перевірка даних може здійснюватись будь-яким учасником, що дозволить зміцнити довіру громадян до держорганів. Перевагами використання блокчейн-технологій є захист конфіденційних даних, зниження витрат та підвищення ефективності, спрощення процесів, зменшення навантаження на аудит, підвищення безпеки та забезпечення цілісності даних. Крім бюрократії, поширеною урядовою проблемою є корупція. Використання блокчейну може бути використано для обмеження корупції, шахрайства, крадіжок та нецільового використання державних ресурсів. Forbes зазначив про основні тренди використання блокчейну [2] наступне: блокчейн для відстеження та розповсюдження вакцин, зростання корпоративного блокчейну, зростання застосування NFT, блокчейн як послуга (Blockchain-as-a-Service, BaaS). Аналітики Gartner опублікували список рекомендацій про те, в яких сферах урядовим органам потрібно впроваджувати блокчейн [3]. За прогнозами дослідників, до 2025 блокчейн-технології стануть основою для глобальної децентралізованої системи ідентифікації. Перед урядовими чиновниками стоїть низка варіантів використання цієї технології: вибори, гуманітарні та соціальні послуги, ринки цифрових активів, підвищення ефективності, діловодство.

Розроблено багато веб-сервісів, що в даний час використовуються для управління документами [4]. Найбільш відомими та вживаними є Google Drive [5], Dropbox [6] та OneDrive [7]. Також широко використовуються додатки, які мають експертний висновок щодо відповідності вимогам технічного захисту інформації в Україні [8]: MODX [9], Tresorit [10], FileCloud [11], SmartVault [12], iDOC [6], CleverForms [13], Megapolis.DocNet [14]. Різні приватні платформи (наприклад, IBM Hyperledger Fabric, Corda [15], Waves Enterprise [16]) дозволяють забезпечити конфіденційний обмін даними всередині блокчейн-мережі різними способами, в основному за рахунок взаємодії приватних баз даних поза блокчейн-мережею, зі зберіганням хеш-сум цих даних у блокчейні.

Таким чином, існує багато пропозицій он-лайн систем управління документами в корпоративному верхньому ціновому сегменті навіть з використанням технологій блокчейну. В нижньому ціновому сегменті пропозиції захисту документів можливі або за додаткову ціну, або з використанням сторонніх інструментів, підключених або розроблених самостійно.

Виклад основного матеріалу.

Метою роботи є розробка та тестування веб-орієнтованої системи електронного документообігу з використанням елементів блокчейн технологій.

Виділяють 3 типи блокчейну: публічні блокчейни з відкритим доступом (Public blockchains), приватні блокчейни з відкритим доступом (Consortium blockchains), приватні блокчейни із закритим доступом (Fully private blockchains). Приватні блокчейни із закритим доступом мають ті ж властивості, що й інші, але за умови, що прості користувачі не можуть бути учасниками мережі без підтвердження валідатора, вони не завжди мають доступ до читання файлів ланцюга. В такому разі, система повністю перестає бути відкритою та незалежною від третіх осіб. Властивості даної системи: повна закритість мережі від неавторизованих користувачів; закритість даних від непривілейованих користувачів мережі; повна залежність від кола привілейованих користувачів; неможливість проведення атаки 51%; висока стійкість та надійність мережі за умови довіри до валідаторів. Цей блокчейн більше схожий на класичні централізовані мережі, проте, володіючи властивістю ведення ланцюга взаємопов'язаних блоків, може вдало застосовуватися для внутрішніх закритих приватних мереж та систем захищеного документообігу на підприємствах або державних структурах, де необхідне зберігання службової інформації. На підставі проведеного аналізу було сформульовано такі вимоги до розробки: кожен авторизований користувач системи повинен мати доступ до документів; несанкціонований доступ до документів має бути неможливим; змінювати, підробляти чи видаляти документи з реєстру повинно бути неможливо; кожен документ повинен мати автора та бути підписаний. Виходячи з вимог, що пред'являються до системи, було визнано доцільним використання

приватного типу блокчейну із закритим доступом.

Аналіз моделі загроз (Див. Модель загроз, рис.1) вказує, що основними порушниками є:

1. Інсайдер. Він має доступ до адміністрування додатку реєстрації документів або до адміністрування бази даних додатку, що несе в собі загрозу зміни ним цих даних.

2. Зовнішній порушник (Хакер), що може використовувати основні вразливості веб-додатків, такі як SQL-ін'єкції, CSRF, XSS атаки, атаки повного перебору реєстраційних даних, задля розвідки, отримання адміністративних прав доступу та внесення змін в реєстраційні дані.

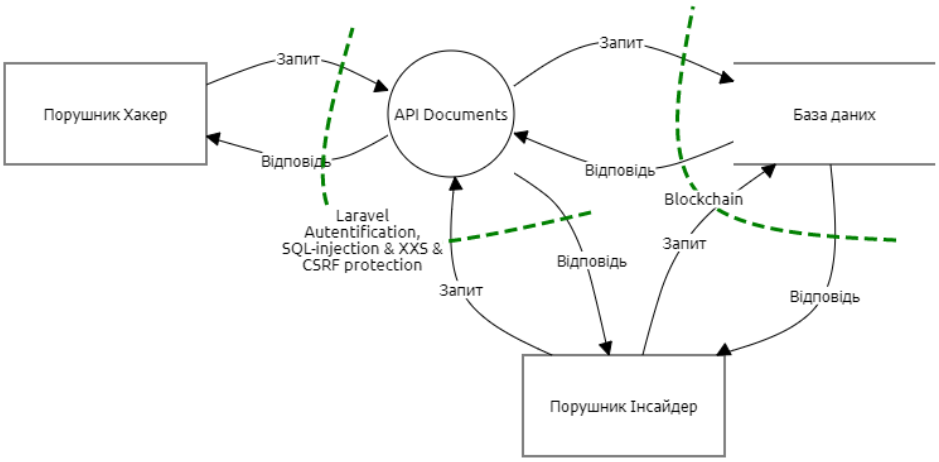

Рис. 1. Модель загроз

Використання технології Blockchain при побудові додатку виключає можливість зміни даних реєстрації Інсайдером без загрози бути викритим, а також перешкоджає можливості непомітної зміни реєстраційних даних зовнішнім порушником. Також використання при цьому хешування та зберігання цих перевірочних кодів дозволяє підтверджувати цілісність та незмінність зареєстрованих електронних документів.

Фреймворк Laravel включає функції, необхідні для створення сучасних, підтримуваних, розподілених веб-додатків. Завдяки кешуванню, оптимізації фронтенду та правильному поділу коду на компоненти вдається забезпечувати справді швидкий доступ до даних. У фреймворку добре розроблені механізми аутентифікації. Laravel пропонує ряд вбудованих функцій безпеки: Захист від SQL-ін'єкцій, захист від підробки міжсайтових запитів (CSRF), захист від XSS атак та ін. Фреймворк захищає за замовчуванням, унеможливлює нелегітимні SQL-запити за рахунок нормалізації всіх параметрів підчас побудови, а також екранування заборонених html-тегів і виведення його як текстових даних без можливості виконання. Тому у сервісі були використані наступні технології: фреймворк Laravel, реляційна база даних MySql, сховище даних з використанням блокчейн технологій.

В системі створені наступні ролі:

- Користувач. Він буде мати права на реєстрацію документів, перегляд зареєстрованих документів, до яких він має доступ згідно з його рівнем доступу (від 1 до 4) та перевірку дійсності (автентичності та цілісності) документів.

- Адміністратор. Може все те, що й користувач, та на додачу ще має можливість додавати (видавати атрибути доступу в систему) та видаляти користувачів.

- Суперадміністратор. Може все те, що й адміністратор, та ще має права додавання та видалення Адміністраторів.

У цій схемі є Суперадміністратор, що створює локальних адміністраторів у відокремлених (територіально та/або адміністративно) підрозділах установи чи підприємства.

Створено дві основні бази даних:

1. Документи (Documents) з наступними полями: номер документа (DocumentID), ID виконавця (реєстранта) (UserID), дата та час реєстрації (Signing Date&Time), назва документа (Document's Name), рівень доступу до документу (Access level) – має значення 1, 2, 3, 4, код перевірки (Verification code) – хешоване значення на основі самого документа, та коду перевірки попереднього документа, що вираховується за формулою:

$$VC_i = SHA\ (SHA\ (DocFile) + VC_{i-1}), \quad (1)$$

де VC – код перевірки (Verification code),

DocFile – файл, що перевіряється,

SHA – функція хешування SHA 256.

2. Користувачі (Users) з наступними полями: ідентифікатор користувача (UserID), ПІБ користувача

(Fullname), рівень доступу до документу (Access level) – має значення 1, 2, 3, 4, роль (Role) – суперадміністратор, адміністратор, користувач, ключ доступу (Key) – пароль входу в систему.

Розроблено додаток, що реалізує визначені механізми захисту: Використання технології блокчейн для неможливості непомітної зміни реєстраційних даних зареєстрованих документів; Збереження хеш-суми зареєстрованих документів та верифікація зареєстрованих документів; Захист від brute force атак за рахунок обмеження кількість спроб аутентифікації та влаштування таймауту у зв'язку з перевищенням кількості спроб, а також перевірки вибору достатньо безпечного паролю; Захист від викрадення паролів за рахунок зберігання в хешованому вигляді; Налаштування розмежування доступу для збереження конфіденційної та комерційної таємниці в установі; Захист від впровадження SQL ін'єкцій за рахунок використання методів управління записами БД Eloquen; Захист від XSS та деяких інших атак за рахунок валідації вхідних даних та фільтрації виводу вихідних даних, які було отримано з ненадійних джерел; Захист від CSRF атак за рахунок використання токенів CSRF; Захист сесій за рахунок використання персональних токенів.

Під час тестування не було виявлено вразливостей додатку та підтверджено його захищеність.

Блокчейн логіка запобігає спробам зловмисників, якщо вони зможуть отримати доступ до бази даних системи, змінити перевірочний код даного документа, тому що цей код використовується в підрахунку перевірочного коду наступних зареєстрованих документів, що призведе до його невідповідності та буде виявлено під час перевірки наступного документа. Змінити перевірочні коди всіх зареєстрованих пізніше документів, щоб приховати зміну зареєстрованого документа, не виявляється можливим, тому що самі документи не зберігаються в системі й вирахувати їх хеш-суми неможливо.

Висновки

В результаті проведеного дослідження можна відзначити, що інтерес до блокчейн технологій продовжує зростати з реформуванням та розвитком всіх сфер української держави, а саме медичної реформи, судової та правоохоронної реформи, розвитком електронної держави, так званої «діджиталізації» держави та в умовах триваючої кібервійни з державою-агресором. Використання блокчейн технологій може вирішити багато проблем, пов'язаних з бюрократією, корупцією, крадіжками та шахрайством.

В ході роботи розроблено та протестовано додаток, що реалізує визначені механізми захисту: використання технології блокчейн, збереження хеш-суми зареєстрованих документів, верифікація зареєстрованих документів та захист від інших вразливостей веб-додатків, налаштування розмежування доступу для збереження конфіденційної та комерційної таємниці в установі.

Отже, застосування блокчейн логіки в системах електронного документообігу надійно запобігає спробам зловмисників змінити зареєстровані документи.

Література

1. Distributed Ledger Technology: Implications of Blockchain for the Securities Industry [Електронний ресурс] // FINRA. – 2021. – Режим доступу до ресурсу: https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf.

2. Marr B. The 5 Biggest Blockchain Trends In 2022 [Електронний ресурс] / Bernard Marr // Forbes. – 2021. – Режим доступу до ресурсу: https://www.forbes.com/sites/bernardmarr/2021/11/19/the-5-biggest-blockchain-trends-in-2022/?sh=2b9f9422247.

3. Goasduff L. Leaders must determine the suitability of blockchain and set the right expectations [Електронний ресурс] / Laurence Goasduff // Gartner. – 2021. – Режим доступу до ресурсу: https://www.gartner.com/en/articles/how-governments-can-successfully-embark-on-any-blockchain-project.

4. Software Advice [Електронний ресурс] – Режим доступу до ресурсу: https://www.softwareadvice.com/.

5. Google Drive [Електронний ресурс] – Режим доступу до ресурсу: https://www.google.com/intl/uA/drive/.

6. Dropbox [Електронний ресурс] – Режим доступу до ресурсу: https://www.dropbox.com/.

7. OneDrive [Електронний ресурс] – Режим доступу до ресурсу: https://www.microsoft.com/uk-ua/microsoft-365/onedrive/online-cloud-storage.

8. Засоби ТЗІ, які мають експертний висновок про відповідність до вимог технічного захисту інформації [Електронний ресурс] // Державна служба спеціального зв'язку та захисту інформації України. – Режим доступу до ресурсу: https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi.

9. MODX [Електронний ресурс] – Режим доступу до ресурсу: https://modx.com/.

10. Tresorit [Електронний ресурс] – Режим доступу до ресурсу: https://tresorit.com/.

11. FileCloud [Електронний ресурс] – Режим доступу до ресурсу: https://filecloud.com/.

12. SmartVault [Електронний ресурс] – Режим доступу до ресурсу: https://smartvault.com/.

13. CleverForms [Електронний ресурс] – Режим доступу до ресурсу: https://clever-forms.com/.

14. Megapolis.DocNet [Електронний ресурс] – Режим доступу до ресурсу: https://megapolis.inbase.com.ua/.

15. Corda [Електронний ресурс] – Режим доступу до ресурсу: https://corda.net/.

16. Waves Enterprise [Електронний ресурс] – Режим доступу до ресурсу: https://wavesenterprise.com/.

References

1. Distributed Ledger Technology: Implications of Blockchain for the Securities Industry [Online] // FINRA. – 2021. – URL: https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf.

2. Marr B. The 5 Biggest Blockchain Trends In 2022 [Online] / Bernard Marr // Forbes. – 2021. – URL: https://www.forbes.com/sites/bernardmarr/2021/11/19/the-5-biggest-blockchain-trends-in-2022/?sh=2b9f9422247.

3. Goasduff L. Leaders must determine the suitability of blockchain and set the right expectations [Online] / Laurence Goasduff // Gartner. – 2021. – URL: https://www.gartner.com/en/articles/how-governments-can-successfully-embark-on-any-blockchain-project.

4. Software Advice [Online] – URL: https://www.softwareadvice.com/.

5. Google Drive [Online] – URL: https://www.google.com/intl/uA/drive/.

6. Dropbox [Online] – URL: https://www.dropbox.com/.

7. OneDrive [Online] – URL: https://www.microsoft.com/uk-ua/microsoft-365/onedrive/online-cloud-storage.

8. Technical information protection tools that have an expert opinion on compliance with the requirements of technical information protection [Online] // State service of special communication and information protection of Ukraine. – URL: https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi.

9. MODX [Online] – URL: https://modx.com/.

10. Tresorit [Online] – URL: https://tresorit.com/.

11. FileCloud [Online] – URL: https://filecloud.com/.

12. SmartVault [Online] – URL: https://smartvault.com/.

13. CleverForms [Online] – URL: https://clever-forms.com/.

14. Megapolis.DocNet [Online] – URL: https://megapolis.inbase.com.ua/.

15. Corda [Online] – URL: https://corda.net/.

16. Waves Enterprise [Online] – URL: https://wavesenterprise.com/.