УДК 004.056
DOI https://doi.org/10.32851/tnv-tech.2022.4.4

АСПЕКТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНИХ CRM-СИСТЕМАХ В ЕПОХУ ДІДЖИТАЛІЗАЦІЇ ЕКОНОМІКИ ТА БІЗНЕСУ

Янко А. С. *– кандидат технічних наук, доцент,*
доцент кафедри комп'ютерних та інформаційних технологій і систем
Національного університету «Полтавська політехніка імені Юрія Кондратюка»
ORCID ID: 0000-0003-2876-9316

Шахно В. О. *– магістр спеціальності 122 – «Комп'ютерні науки»*
кафедри комп'ютерних та інформаційних технологій і систем
Національного університету «Полтавська політехніка імені Юрія Кондратюка»
ORCID ID: 0000-0003-1827-8281

Предметом статті є застосування систем класу CRM у сучасній економіці. В умовах інформатизації економічних даних всіх підприємств, не залежно від форм власності, значущість застосування CRM-систем стрімко зростає. Сучасні CRM-системи дозволяють бізнесу приймати якісні та своєчасні управлінські рішення на основі отриманих даних із систем класу CRM. Звичайно не потрібно забувати про інформаційну безпеку, що полягає у захищеності даних від несанкціонованого доступу. Захист даних є один із головних параметрів, за яким варто вибирати CRM-систему. Тому, як наслідок, виникає проблема систем CRM, що полягає у пошуку компромісу між характеристиками безпеки та зручності використання, тому ціллю даної статті є саме досягнення необхідної захищеності інформації при максимальному комфорті користувачів даної системи. У статті досліджено особливості діджиталізації економічного сектору шляхом поєднання CRM-систем з сучасними фреймворками та технологіями IT-безпеки. Проаналізовано особливості функціонування сучасного цифрового ринку, CRM-систем та технологій безпеки. Розглянуто основні сучасні технології, стандарти та протоколи безпеки в умовах діджиталізації. Виділено принципи безпеки та зручності, на які повинні спиратися CRM-системи. В даному дослідженні перевагу в ефективності, зручності, безпеці та захищеності було надано протоколу Oauth2 та технології, що його реалізує Keycloak. Безпека даних у запропонованій CRM-системі забезпечується гнучкими налаштуваннями доступу. Ці два потужні інструменти дозволяють захистити будь-який ресурс від неавторизованого доступу, не передаючи важливі дані користувача іншій стороні та надають досить зручні можливості та альтернативи для авторизації. Використання цих технологій при розробці власних CRM або їх інтеграція до вже готової системи є чи не найкращим безпековим рішенням.

Ключові слова: *діджиталізація економіки, інформаційна безпека, неавторизований доступу, протокол авторизації, CRM-платформа, CRM-система.*

Yanko A. S., Shakhno V. O. The aspect of information security in modern CRM-systems in the era of digitalization of the economy and business

The subject of the article is the application of CRM class systems in the modern economy. In the conditions of informatization of economic data of all enterprises, regardless of the forms of ownership, the importance of using CRM-systems is growing rapidly. Modern CRM-systems allow businesses to make high-quality and timely management decisions based on data received from CRM-class systems. Of course, one should not forget about information security, which consists in the protection of data from unauthorized access. Data protection is one of the main parameters for choosing a CRM-system. Therefore, as a result, the problem of CRM-systems arises, which consists in finding a compromise between security characteristics and ease of use, so the goal of this article is precisely to achieve the necessary information security with the maximum comfort of users of this system. The article examines the peculiarities of digitalization of the economic sector by combining CRM-systems with modern frameworks and IT-security technologies. The features of the functioning of the modern digital market, CRM-systems and secu-

rity technologies are analyzed. The main modern technologies, standards and security protocols in the conditions of digitization are considered. The principles of security and convenience, on which CRM-systems should be based, are highlighted. In this study, the advantage in terms of efficiency, convenience, safety and security was given to the Oauth2 protocol and the technology implemented by Keycloak. Data security in the proposed CRM-system is ensured by flexible access settings. These two powerful tools allow you to protect any resource from unauthorized access without transferring important user data to another party and provide quite convenient options and alternatives for authorization. Using these technologies when developing your own CRM or integrating them into an already ready system is almost the best security solution.

Key words: *digitalization of the economy, information security, unauthorized access, authorization protocol, CRM-platform, CRM-system.*

Вступ. Перехід до цифрової економіки – це необхідна вимога сьогоднішнього дня. Діджиталізація економіки дає можливість людині полегшити вирішення багатьох завдань, пов'язаних з роботою, з пошуком інформації, буденними справами з якими він неодноразово стикається. Діджиталізація відкриває для людини широкі можливості в розвитку бізнесу. Особливе значення тут набувають комунікативні можливості цифрових каналів. Велика швидкість, зручність, безпечність, перспективність, досконалість, захищеність цифрового середовища, дозволило з'явитися сотням нових видів давно вже відомих напрямків бізнесу. Бізнес, який зараз не дивиться в сторону інформатизації неминуче рано чи пізно або все ж таки звернеться до послуг ІТ сектору, або втратить клієнтів, прибуток та будь-яку перспективу для розвитку У світі, де люди вже давно звикли отримувати товари та послуги в декілька "кліків миші", зменшуючи до мінімуму спілкування з іншими людьми та економлячи свій час. У світі, де інформаційні технології вже давно диктують світовий розвиток людства, розвиток всіх світових ринків, будь-яких галузей. Тому, ідеальною моделлю цифрової економіки є модель, при якій бізнес прагне відповідати сучасним вимогам цієї економіки та рівням надання онлайн послуг шляхом інформатизації, діджиталізації, захищеності даних, звертається до ІТ сектору за отриманням послуг та рішень, які зможуть достатньою мірою «оцифрувати» та вивести їхнє підприємство чи організацію на новий рівень бізнес стосунків та надання якісних, сучасних, безпечних та зручних послуг. І тут отримуємо таку собі синергію, ІТ сектор прагне задовольнити клієнта, збільшити йому прибуток, кількість клієнтів, масштабність, охоплення, а клієнт своєю чергою виступає, як рушійна сила економіки, одночасно інвестує як в ІТ сектор, рішення та послуги якого пропорційно інвестиціям та капіталізації збільшують його привабливість так і в економіку держави, адже створює вже власні послуги, товари та робочі місця.

Місце безпеки в сучасних CRM-системах. Та що є одним із найважливіших аспектів при переході в інформаційно технологічний світ? Безпека… Саме безпека та захищеність викликає найбільше запитань, адже будь-хто, може запропонувати своє рішення тієї чи іншої бізнес задачі, але чи буде воно достатньо безпечним та відповідати всім нормам та стандартам інформаційної безпеки та захищеності даних? Щоб відповісти на це питання потрібно добре розумітися в ІТ безпеці, основних вразливостях ІТ систем, баз даних, веб-ресурсів та в багато чому іншому. Це своєю чергою породжує ненадійність таких рішень та вимагає чималих ресурсів при розробці програмного забезпечення «з нуля», покликаного стати надійним, відмовостійким та безпечним. Проте, ІТ ринок за десятиліття свого існування, створив десятки тисяч готових рішень [1, с. 42–45]. Ці рішення пройшли тестування на десятках клієнтів і багато з них, можливо, і не принесли належної користі та потрібних рішень своїм бізнесам та врешті решт і самі створили для них проблеми. Та саме це дозволило ринку шляхом спроб та невдач,

накопичити достатньо досвіду, щоб створити та перевірити найдієвіші рішення, технології, фреймворки. Одним з таких рішень є CRM-платформа(Customer Relationship Management – управління відносинами з клієнтами).

Під CRM-платформою потрібно розуміти саме веб-додаток, адже сьогодні веб має набагато більше переваг перед звичайними додатками для тієї чи іншої операційної системи. Така платформа не є зараз чимось новим, навпаки такі галузі як маркетинг, фінанси, продажі, логістика та багато інших вже давно успішно використовують це рішення. Вона об'єднує різні відділи, від маркетингу до продажу та обслуговування клієнтів, та поєднує їх нотатки, дії та показники в єдину зв'язкову систему. Кожен користувач має простий доступ до потрібних клієнтських даних в режимі реального часу [2, с. 203–207]. Це не тільки забезпечує безпрецедентну координацію між командами та відділами, а й дозволяє компанії надавати своїм клієнтам щось екстраординарне: персоналізовані індивідуальні взаємодії з клієнтом. Якщо порівняти це з обмеженою функціональністю старих аналогових та застарілих систем, то отримаємо щось здатне революціонізувати спосіб зв'язку з клієнтами. Також неможливо використовувати CRM, не беручи до уваги SaaS та хмарні обчислення, які працюють разом, щоб платформи CRM були доступні скрізь, де користувач має Інтернет.

Понад 39% компаній, які впровадили CRM-платформи, називають свої дані конкурентною перевагою або стратегічним активом. CRM-система дозволяє більшості компаній значно збільшити кількість потенційних клієнтів, виторг від продажу та утримання клієнтів [3, с. 1–3].

Сучасні безпекові рішення для інтеграції з CRM-системами. Повертаючись до питань безпеки та захищеності потрібно сказати, що є достатньо велика кількість фреймворків та технологій захисту даних, які використовуються при розробці CRM-систем або інтегруються з ними уже на етапі користування. Візьмемо для прикладу одну з найпопулярніших на сьогодні мов програмування Java. Ця мова програмування теж пройшла десятиліття розвитку, спроб та невдач. Був накопичений неоціненний досвід розробки «ентерпрайз» проектів, тобто великих проектів, де кінцевим користувачем є корпоративний клієнт. Саме через це досить велика кількість банківських там CRM-систем написані на Java та підтримуються довгі роки. Java має досить велику кількість фреймворків, але в рамках цього дослідження потрібно виділити такий потужний фреймворк, як "Spring Security", який забезпечує аутентифікацію, авторизацію та інші функції безпеки для корпоративних програм. Spring підтримує сучасний та популярний стандарт захисту – JWT [4, с. 2–4]. Розглянемо спрощену схему роботи наведену на рис. 1, авторизації клієнта з використанням JWT.

На схемі можемо побачити наступні етапи авторизації:

1) користувач POST запитом відправляє на сервер свій логін та пароль;

2) сервер авторизації, яким виступає Spring, перевіряє отримані дані, та якщо вони вірні надає та повертає користувачеві токен доступу (закодований рядок символів, що створюється сервером і підписується секретним ключем);

3) користувач відправляє GET запит на отримання профілю своєї сторінки з вже отриманим JWT в хедері запиту;

4) сервер авторизації тепер вже перевіряє лише раніше випадний токен доступу;

5) якщо токен доступу вірний та дійсний, користувач отримує запитану сторінку з інформацією.

Навіть на такому простому прикладі видно, що цей стандарт надає значно більшу захищеність ніж звичайний логін та пароль, але на реальних проєктах ніхто

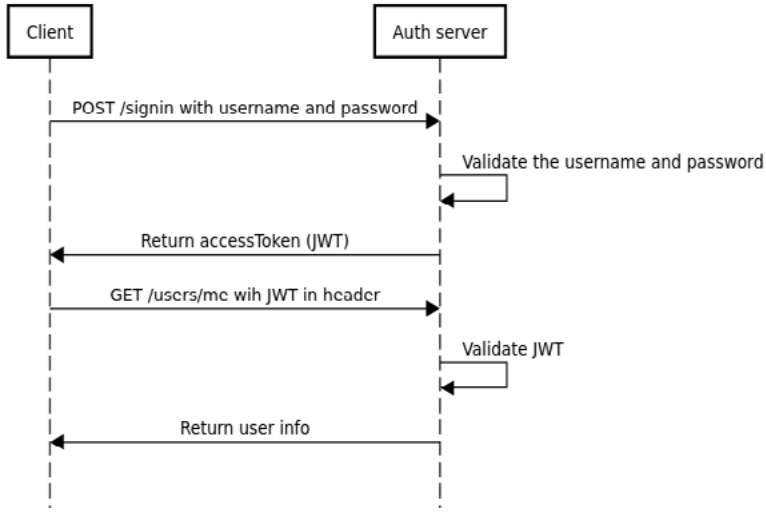

Рис. 1. Схема процесу авторизації клієнта з використанням JWT

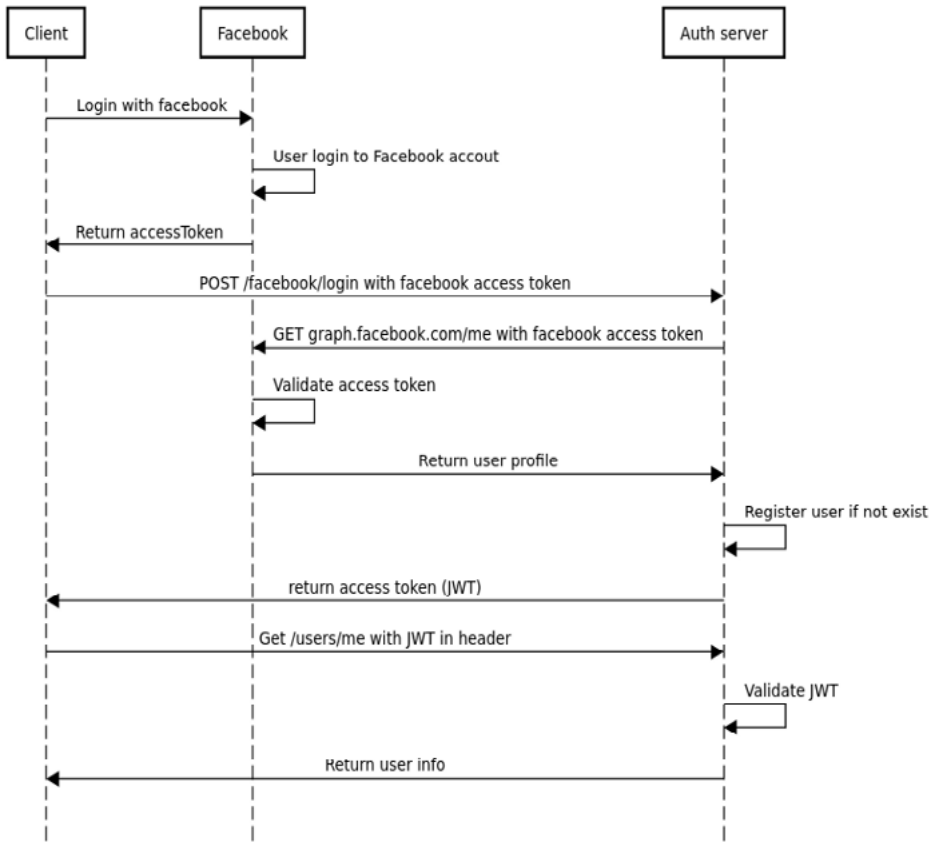

Рис. 2. Схема процесу авторизації з використанням протоколу Oauth

в «чистому» вигляді не використовує JWT. Тут потрібно розуміти, що часто один стандарт використовує або розширює інший, а вже отриманий новий стандарт реалізує якась технологія. Так і вийшло з протоколом авторизації Oauth та його реалізацією Keycloak. Останньою версією є Oauth2 і саме ця версія була взята для дослідження. Oauth – забезпечує надання третій стороні обмежений доступ до захищених ресурсів користувача без передачі їй (третій стороні) логіна та пароля [5, с. 3–8]. Тобто зараз це зручний та один з найбезпечніших засобів авторизації та аутентифікації. Зручний в тому, що користувачеві не обов'язково проходити процес реєстрації, Oauth дає можливість використати будь-яку соціальну мережу для підтвердження даних та і більшість сучасних CRM-систем мають або за замовчуванням Oauth авторизацію або дозволяють її інтегрувати, тобто використати, як сервер авторизації [6, с. 18–23].

Безпековий же аспект полягає в тому, що авторизуючись через соціальну мережу або через Keycloak, що реалізує даний протокол, не передається третій стороні (ресурсу до якого хочемо отримати доступ) ніякої інформації крім вже розглянутого токена доступу [7, с. 4–7]. Розглянемо схему процесу авторизації з використанням протоколу Oauth через соціальну мережу Facebook (рис. 2).

На схемі можемо побачити алгоритм схожий до звичайної JWT авторизації, за виключенням того, що користувач спершу проходить авторизацію Facebook, який і надає токен доступу, який потім проходить перевірку як Facebook, так і даного сервера авторизації, яким може виступати Keycloak.

Висновок. Однією з найбільших проблем CRM-систем є компроміс між безпекою та зручністю. І якщо зручності приділяється багато уваги як від розробника, так і від користувача, то безпековий аспект часто схований від користувача. Тут потрібно розуміти, що будь-яка система має свої вразливості, які рано чи пізно знаходяться, але використання останніх протоколів, стандартів, реалізацій цих стандартів, дозволяє посилити захист, як самого програмного продукту, так і персональних даних користувача. В даному дослідженні перевагу в ефективності, зручності, безпеці та захищеності було надано протоколу Oauth2 та технології, що його реалізує Keycloak. Ці два потужні інструменти дозволяють захистити будь-який ресурс від неавторизованого доступу, не передаючи важливі дані користувача іншій стороні та надають досить зручні можливості та альтернативи для авторизації. Використання цих технологій при розробці власних CRM або їх інтеграція до вже готової системи є чи не найкращим безпековим рішенням. CRM-системи, що використовують протокол Oauth2 та технологію Keycloak, здатні забезпечити істотно вищий рівень безпеки. За рахунок того, що CRM поставляється безлічі користувачів по всьому світу, якісний захист робочих документів обходиться значно дешевше, ніж самостійне індивідуальне забезпечення безпеки кожного робочого місця. Протокол Oauth2 відповідає світовим стандартам безпеки, тому йому з упевненістю можна довірити клієнтську базу, фінансову інформацію та інші робочі дані.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. De Capitani di Vimercati S., Foresti S., Samarati P. In Security, Privacy, and Trust in Modern Data Management. Authorization and Access Control / Petković M, Jonker W (eds.), *Springer Berlin Heidelberg*, 2007. P. 39 –53. ISBN: 978-3-540-69860-9. DOI: 10.1007/978-3-540-69861-6_4.

2. Nuñez D., Agudo I. BlindIdM: A privacy-preserving approach for identity management as a service. *International Journal of Information Security*, Apr. 2014, Vol.13(2). P. 199–215. DOI: 10.1007/s10207-014-0230-4

3. What is CRM Software? A Comprehensive Guide and Historical Overview of CRM (Customer Relationship Management) software. *SalesForce* : веб-сайт. URL: www.salesforce.com/crm/what-is-crm-infographic (дата звернення: 20.05.2021).

4. JWT and Social Authentication using Spring Boot. *Medium* : веб-сайт. URL: https://medium.com/javarevisited/jwt-and-social-authentication-using-spring-boot-90e4faaa9204 (дата звернення: 18.08.2020).

5. Campbell B., Mortimore C., Jones M. RFC 7522: Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants. *Technical Report, Internet Engineering Task Force (IETF)*, May 2015. 15 p. https://tools.ietf.org/html/rfc7522.

6. Maler E., Machulak M., Richer J., Hardjono T. User Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization. *Technical Report (Draft, work in Progress), Internet Engineering Task Force (IETF)*, February 2019. 37 p. https://datatracker.ietf.org/doc/html/draft-maler-oauth-umagrant-00.

7. Jones M., Campbell B., Mortimore C. RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants. *Technical Report, Internet Engineering Task Force (IETF)*, May 2015. 11 p. https://tools.ietf.org/html/rfc7523.