УДК 004.054; 004.055

АНАЛІЗ МЕТОДІВ І ФУНКЦІЙ ЗАХИСТУ ДАНИХ ДЛЯ РЕСУРСІВ ДИСТАНЦІЙНОГО НАВЧАННЯ

Обривко Є.В.
Харківський національний університет радіоелектроніки
Україна, 61166, Харків, пр. Науки 14
E-mail: yevhen.obryvko@nure.ua

Анотація: В роботі розглянуто актуальне питання підвищення надійності та захисту персональних даних користувачів та закладу освіти для ресурсу дистанційного навчання. Проведено аналіз існуючих методів захисту даних на веб-сторінках, їх ефективності, актуальності та особливостей застосування, також проаналізовано методи захист паролів та їх надійність.

Ключові слова: захист даних, шифрування, ресурс, дистанційне навчання, навантаження, сервер

ANALYSIS OF DATA PROTECTION METHODS AND FUNCTIONS FOR DISTANCE LEARNING RESOURCES

Obryvko E.V.
Kharkiv National University of Radio Electronics
Ukraine, 61166, Kharkiv, Nauky ave. 14
E-mail: yevhen.obryvko@nure.ua

Abstract.The paper considers the current issue of increasing the reliability and protection of personal data of users and educational institutions for a distance learning resource. An analysis of existing methods of data protection on web pages, their effectiveness, relevance and application features, a nd methods of password protection and their reliability are also analyzed.

Keywords: data protection, encryption, resource, distance learning, load, server

АКТУАЛЬНІСТЬ РОБОТИ. З переходом до дистанційних форм навчання питання безпеки даних користувачів набуло ще більшої важливості. Освітні платформи сьогодні об’єднують тисячі користувачів, від студентів до викладачів, що працюють із персональними акаунтами та конфіденційною інформацією [1].

Системи дистанційного навчання зберігають значні обсяги особистої та академічної інформації, яка піддається ризикам зловживань і витоків. Уразливості в захисті даних можуть призвести до серйозних наслідків, як-от витік даних, фінансові втрати або навіть порушення репутації освітнього закладу [2].

Також важливим фактором є відповідність вимогам законодавства про захист даних. Урахування вимог цих законодавств робить впровадження надійних систем захисту [3] ще більш актуальним.

Внаслідок швидкого розвитку технологій та методів атак зловмисники постійно вдосконалюють свої методи для отримання доступу до конфіденційних даних. На додачу, розвиток технологій штучного інтелекту та машинного навчання дозволяє створювати складні атаки, які важко розпізнати без відповідного захисту. У зв’язку з цим аналіз та оновлення методів захисту даних є необхідними для підтримання безпеки освітніх платформ [1].

Отже при розробці подібних системи безпеці даних та захисту персональної інформації має приділятись велика увага з урахування усіх вище перелічених факторів [4].

ВСТУП. Для ефективного забезпечення безпеки важливо розуміти, з якими загрозами стикаються освітні платформи. Основні загрози включають [5-7]:

Витік даних – уразливості в системах безпеки, які можуть призвести до несанкціонованого доступу до персональної інформації, наприклад, облікових записів, результатів навчання або особистих даних студентів.

Фішинг – метод отримання доступу до конфіденційної інформації шляхом шахрайства. Фішингові атаки можуть приймати вигляд електронних листів, що імітують офіційні запити від навчальних платформ, які просять надати логін або пароль.

Атаки «людина посередині» (MITM) – перехоплення даних між сервером та клієнтом, що дозволяє зловмисникам отримати доступ до інформації, яка передається під час роботи з платформою.

DdoS-атаки – масове навантаження на сервер, що може призвести до повної або часткової втрати доступу до освітньої платформи.

МАТЕРІАЛИ ТА РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ.

Шифрування даних.

Шифрування даних є базовим інструментом для захисту конфіденційної інформації. Розглянемо основні методи шифрування:

1) симетричне шифрування (AES) – один ключ використовується для шифрування та розшифрування інформації. AES забезпечує високу швидкість обробки даних і є ефективним для великих обсягів;

2) асиметричне шифрування (RSA) – використовує пару ключів: відкритий для шифрування та закритий для розшифрування. RSA забезпечує високий рівень захисту, однак потребує значних обчислювальних ресурсів, тому його ефективно використовувати лише для захисту невеликих обсягів критичної інформації.

Формули шифрування на основі відкритого ключа:

$$C = E(K_{pub}, P)$$

де C – зашифрований текст, K_{pub} – відкритий ключ, P – відкритий текст.

Багатофакторна автентифікація.

Одним із найбільш дієвих методів захисту доступу до акаунтів є багатофакторна автентифікація (2FA). Ця система включає використання додаткового коду, який генерується або відправляється через інший канал (наприклад, телефон або електронну пошту), що знижує ризик несанкціонованого доступу. До методів автентифікації належать:

1) TOTP (Time-based One-Time Password) – одноразові паролі з обмеженим часом дії;

2) біометричні дані – відбитки пальців, розпізнавання обличчя, сканування сітківки тощо, що надають найвищий рівень захисту.

Захист від DdoS-атак.

DdoS-атака – напад на комп’ютерну систему з наміром зробити комп’ютерні ресурси недоступними користувачам, для яких комп’ютерна система була призначена. Одним із найпоширеніших методів нападу є насичення атакованого комп’ютера або мережевого устаткування великою кількістю зовнішніх запитів (часто безглуздих або неправильно сформульованих) таким чином атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним.

Для запобігання відмові в обслуговуванні через масові DdoS-атаки ефективними є:

1) балансування навантаження: розподіл запитів на декілька серверів для забезпечення стабільної роботи платформи;

2) фільтрування трафіку на рівні мережі для зменшення впливу небажаних запитів.

Хешування паролів.

Хешування – це процес перетворення пароля на унікальний хеш-код, який зберігається в базі даних замість самого пароля. Коли користувач вводить свій пароль, система хешує його і порівнює з наявним хешем. Якщо хеші збігаються, доступ дозволяється. Найпоширенішими алгоритмами для хешування є SHA-256, bcrypt, Argon2, які забезпечують різні рівні надійності.

1) bcrypt – алгоритм хешування, стійкий до атак підбору, оскільки включає «сіль» (salt) і адаптивний параметр, що уповільнює обчислення;

2) Argon2 – більш сучасний алгоритм хешування, оптимізований для захисту від атак на графічних процесорах, з додатковими параметрами стійкості.

Формула для хешування пароля з використанням «солі»:

$$H = hash(password + salt)$$

де H – хеш, *password* – пароль користувача, *salt* – випадкове значення, що додається до кожного паролю користувача.

У таблиці 1 нижче наведено порівняння методів шифрування та захисту даних і підвищення безпеки системи з точки зору ефективності використання, ефективності та особливестей.

Таблиця 1 – Порівняння основних методів шифрування, захисту та підвищення безпеки системи.

Метод	Ефективність	Вартість впровадження	Особливості
AES шифрування	Висока	Помірна	Підходить для великих обсягів даних
RSA шифрування	Висока	Висока	Ефективний для критичних даних
Багатофакторна автентифікація (2FA)	Висока	Висока	Захищає від крадіжки облікових записів
SSL/TLS сертифікати	Висока	Помірна	Забезпечує захист від MITM-атак
Хешування паролів (bcrypt, Argon2)	Висока	Низька	Забезпечує надійність паролів
Контроль доступу	Висока	Низька	Дозволяє контролювати права доступу користувачів
Балансування навантаження	Середня	Висока	Зменшує швидкість обробки запитів
Фільтрування трафіку	Середня	Висока	Знижує ризик небажаних запитів

Порівняння основних методи шифрування AES та RSA.Оскільки у системі дистанційної освіти передбачено використання великих обсягів даних, таких як навчальні матеріали, оцінки, персональні дані та паролі, то основними критеріями при виборі методу шифрування будуть захист критичних даних та стабільність і швидкість роботи при великих об’ємах інформації. Тому порівняємо два найбільш доречних у цих умовах методи AES шифрування та RSA шифрування при різних обсягах інформації (рис. 1).

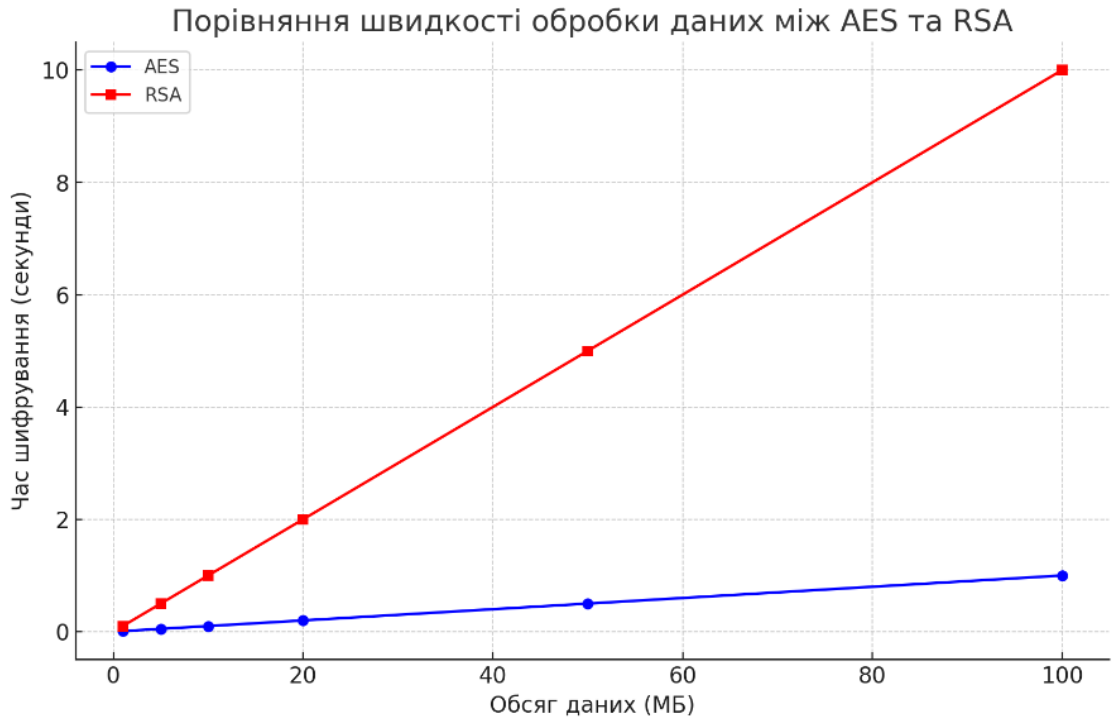

Рисунок 1 – Порівняння швидкості обробки даних між алгоритмами AES та RSA при різних обсягах інформації

На графіку видно, що AES має значно вищу швидкість обробки даних порівняно з RSA, особливо при більших обсягах даних, що робить його більш ефективним для великих інформаційних масивів.

Оскільки у системі дистанційної освіти передбачено використання великих обсягів даних, таких як навчальні матеріали, оцінки, персональні дані та паролі то доцільніше з точки зору вартості впровадження та ефективності буде використовувати метод AES шифрування.

Для ілюстрації основних етапів обробки інформації в системі дистанційного навчання та подальшого визначення для них відповідних методів захисту, створимо схему потоку даних у системі (рис. 2).

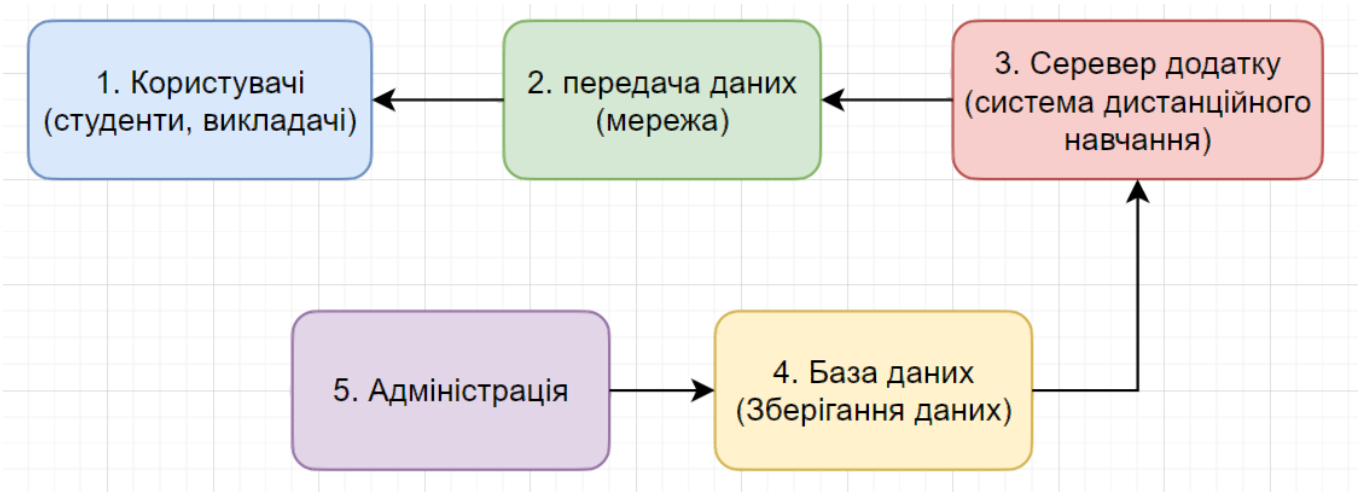

Рисунок 2 – Схема потоку даних у системі дистанційного навчання

Як бачимо на рис. 2, у системі є 5 основних етапів обробки інформації:

– Користувачі (студенти, викладачі);
– Передача даних (мережа);
– Сервер додатку;
– База даних;
– Адміністрація.

Для забезпечення найвищого рівня безпеки даних, кожному з етапів обробки інформації бажано мати свій метод захисту для системи в нашому випадку, базуючись на попередньому аналізі методів та засобів, можна зробити наступний розподіл етапів потоку даних та засобів захисту для них (рис. 3).

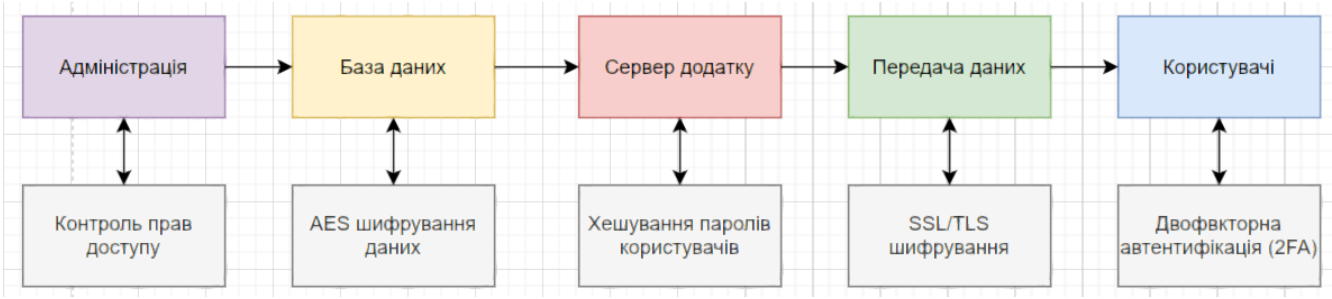

Рисунок 3 – Розподіл етапів потоку даних та засобів захисту

ВИСНОВКИ. Для поставлених задач системи більш за все підходить метод AES шифрування, проте поєднання методів шифрування, багатофакторної автентифікації та захисту від DdoS-атак дозволяє досягти високого рівня безпеки для ресурсів дистанційного навчання. Доцільно впроваджувати багатошарову систему захисту, яка охоплює шифрування даних, автентифікацію користувачів і систему фільтрації трафіку. Використання штучного інтелекту для аналізу загроз у реальному часі може стати наступним кроком у забезпеченні безпеки освітніх платформ. Інтеграція інтелектуальних систем моніторингу дозволить не тільки реагувати на кіберзагрози, а й прогнозувати їх.

ВИКОРИСТАНА ЛІТЕРАТУРА.

1. Anees, A., Hussain, I., Khokhar, U. M., Ahmed, F., & Shaukat, S. (2022). Machine learning and applied cryptography. *Security & Communication Networks*.

2. Віртуальне навчальне середовище: Вікіпедія. URL: https://uk.wikipedia.org/wiki/DoS-атака (дата звернення: 27.10.2024).

3. Tibouchi, M., & Wang, X. (2023). Applied cryptography and network security. In *Proceedings of the 21st International Conference on ACNS* (Vol. 13906).

4. William Stallings. Cryptography and Network Security: Principles and Practice // Prentice Hall. 1999. – С. 118-154.

5. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2021). Handbook of applied cryptography. *Instructor, 202101*.

6. Шифрування. Типи і алгоритми: hostpro.ua. URL: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/ (дата звернення: 29.10.2024).

7. Хешування паролів: використання солі та bcrypt: drukarnia.com.ua. URL: https://drukarnia.com.ua/articles/kheshuvannya-paroliv-vikoristannya-soli-ta-bcrypt fsme-#heading-3-350 (дата звернення: 29.10.2024).

8. Yevsieiev V. Ecosystem Model of the Concept of Industry 5.0 / V. Yevsieiev // Digital innovation & sustainable development 2024 : Proceedings of I-st International Conference, November 15, 2024. – Kharkiv, 2024. – P. 12-13.

9. Moiseev, M., Maksymova, S., Yevsieiev, V., & Alkhalaileh, A. (2024). Program Algorithm for Monitoring System Development. *Journal of universal science research*, *2*(7), 33-43.

10. Abu-Jassar, A. T., Attar, H., Yevsieiev, V., Amer, A., Demska, N., Luhach, A. K., & Lyashenko, V. (2022). Electronic User Authentication Key for Access to HMI/SCADA via Unsecured Internet Networks. Computational Intelligence and Neuroscience, 2022, Article ID 5866922. https://doi.org/10.1155/2022/5866922.

11. Lyashenko, V., Abu-Jassar, A.T., Yevsieiev, V., Maksymova, S. Automated Monitoring and Visualization System in Production, Int. Res. J. Multidiscip. Technovation, 5(6) 2023 09-18. https://doi.org/10.54392/irjmt2362

12. Amer Abu-Jassar, Vladyslav Yevsieiev, & Svitlana Maksymova. (2024). The Optical Flow Method and Graham's Algorithm Implementation Features for Searching for the Object Contour in the Mobile Robot's Workspace. Journal of Universal Science Research, 2(3), 64–75.

13. Vladyslav Yevsieiev, Samariddin, S. M., Nikolay Starodubtsev, & Amer Abu-Jassar. (2024). ACTIVE CONTOURS METHOD IMPLEMENTATION FOR OBJECTS SELECTION IN THE MOBILE ROBOT'S WORKSPACE. Journal of Universal Science Research, 2(2), 135–145.

14. Svitlana Maksymova, Vladyslav Yevsieiev, & Ahmad Alkhalaileh. (2024). The Monitoring System Architecture Development. Journal of Universal Science Research, 2(1), 69–79.

15. Andrii Bondariev, Svitlana Maksymova, & Vladyslav Yevsieiev. (2023). Automated Monitoring System Development for Equipment Modernization. Journal of Universal Science Research, 1(11), 6–16. Retrieved from https://universalpublishings.com/index.php/jusr/article/view/2484

16. Yevsieiev, V. Comparative Analysis of the Characteristics of Mobile Robots and Collaboration Robots Within INDUSTRY 5.0. / V. Yevsieiev, D. Gurin // In the VI International Scientific and Theoretical Conference, September 8, 2023. Chicago, USA. P.92-94

17. Yevsieiev, V., & et al. (2024). Object Recognition and Tracking Method in the Mobile Robot's Workspace in Real Time. Technical science research in Uzbekistan, 2(2), 115- 124.

18. Gurin, D., & et al. (2024). Effect of Frame Processing Frequency on Object Identification Using MobileNetV2 Neural Network for a Mobile Robot. Multidisciplinary Journal of Science and Technology, 4(8), 36-44.

19. Yevsieiev, V., & et al. (2024). Building a traffic route taking into account obstacles based on the A-star algorithm using the python language. Technical Science Research In Uzbekistan, 2(3), 103-112

20. Gurin, D., & et al. (2024). MobileNetv2 Neural Network Model for Human Recognition and Identification in the Working Area of a Collaborative Robot. Multidisciplinary Journal of Science and Technology, 4(8), 5-12.

21. Yevsieiev, V., & Uskov, S. (2024). *Development of the Layout Concept of a Small-Dimensioned Mobile Robot With Increased Accessibility* (Doctoral dissertation, International Scientific Unity).

22. Yevsieiev, V., & Gurin, D. (2024). *New Concepts of Human Interactions and Collaborative Robot-Manipulators in the Concepts of Industry 5.0* (Doctoral dissertation, Collection of scientific papers «SCIENTIA»).

Науковий керівник: *Демська Наталія Павлівна, доцент, кандидат технічних наук, доцент кафедри КІТАР Харківського національного університету радіоелектроніки*