Зловмисники можуть намагатися зламати або скомпрометувати ці дані, що може призвести до небажаних наслідків для користувачів [3].

Список використаних джерел

1. Saad T. M. Security of Multifactor Authentication Model to Improve Authentication Systems [Електронний ресурс] / Tamara Mohamed Saad // ResearhGate – Режим доступу [URL]: https://www.researchgate.net/publication/336642009_Security_of_Multifactor_Authentication_Model_to_Improve_Authentication_Systems. (дата звернення: 26.05.2023).

2. Sharma S. Double the Protection: The Benefits of Multifactor Authentication Computer NetworkCommunication systemSecurity [Електронний ресурс] / Sudhir Sharma // Tutorialspoint. – 19. – Режим доступу [URL]: https://www.tutorialspoint.com/double-the-protection-the-benefits-of-multifactor-authentication. (дата звернення: 26.05.2023).

3.Multi-Factor Authentication: A Survey [Електронний ресурс] / A.Ometov, S. Bezzatee, N. Mäkitalo, S. Andreev // ResearhGate – Режим доступу [URL]: https://www.researchgate.net/publication/322288752_Multi-Factor_Authentication_A_Survey. (дата звернення: 26.05.2023).

УДК: 004.056.5:658.872

Базелюк М.В.

здобувач вищої освіти

Вінницького національного технічного університету

Науковий керівник **Шелепало Г.В. ,** *к.ф.м.н. доцент кафедри захисту інформації Вінницького національного технічного університету*

ПРАКТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТ- МАГАЗИНІВ В УМОВАХ ВІЙНИ

У сучасному світі електронної комерції, інтернет-магазини стають все більш поширеними та зручними для споживачів. Світова пандемія, військові

конфлікти та багато інших факторів змушують людей віддавати перевагу інтернет-магазинам та мобільним додаткам. Однак, зі зростанням популярності онлайн-торгівлі збільшується й кількість потенційних загроз для безпеки даних користувачів та бізнесу. Інформаційна безпека в інтернет-магазинах стає критично важливим аспектом, який вимагає уваги від власників та розробників веб-сайтів. Ця теза має на меті дослідити ключові аспекти інформаційної безпеки в інтернет-магазинах, включаючи забезпечення безпеки серверів, проведення регулярного аудиту безпеки веб-сайту, захист платіжних транзакцій та даних клієнтів. Метою цієї роботи є надання рекомендацій щодо підвищення рівня безпеки в інтернет-магазинах на основі аналізу сучасних джерел з галузі електронної комерції.

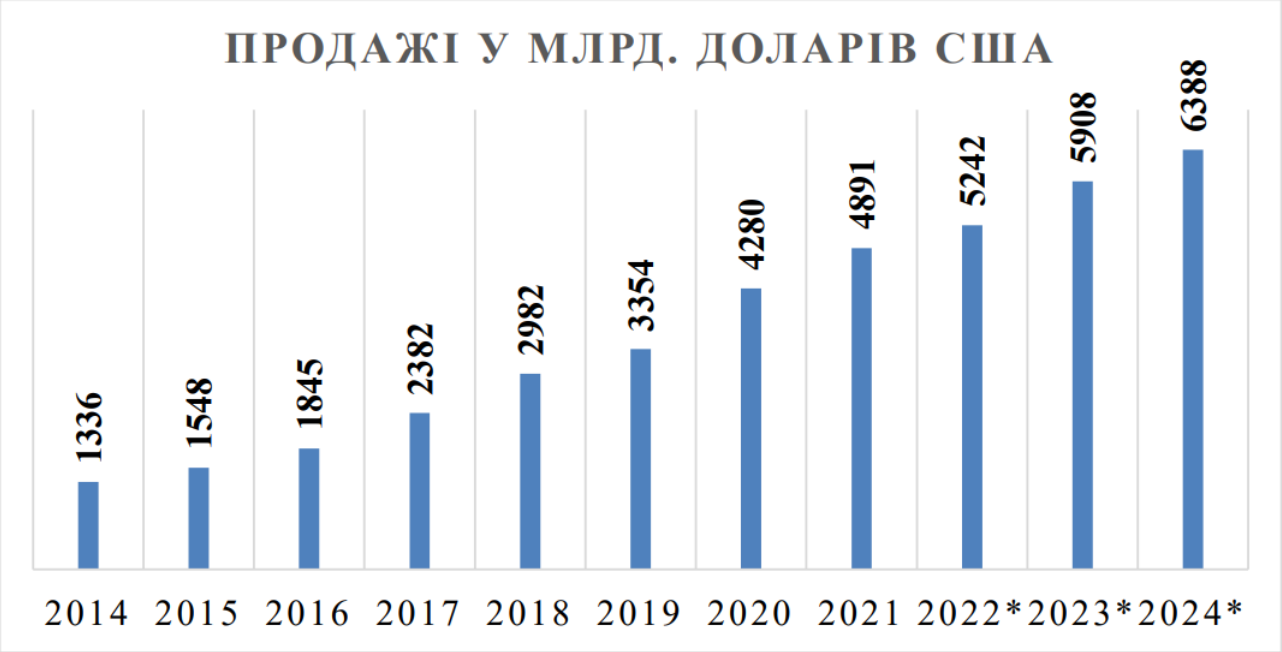
Основна частина

Інформаційна безпека є одним з найважливіших аспектів успішного інтернет- магазину. Забезпечення безпеки даних клієнтів та захист від зловмисників є відповідальністю кожного власника інтернет-магазину. У цій частині було розглянуто результати дослідження світової тенденції розвитку електронної комерції, ключові аспекти інформаційної безпеки інтернет-магазину та рекомендації щодо їх впровадження.

Протягом останніх кількох років електронна комерція стала необхідною складовою глобальної системи роздрібної торгівлі. Подібно до багатьох інших галузей, роздрібна торгівля зазнала значних змін завдяки постійній цифровізації сучасного життя. Споживачі з усього світу мають можливість отримувати вигоди від переваг онлайн-транзакцій. Завдяки стрімкому розширенню доступу до Інтернету і його поширенню по всьому світі, кількість покупців цифрових технологій зростає щороку.

У 2020 році понад два мільярди людей здійснили покупки товарів або послуг в Інтернеті. Протягом того ж року глобальний обсяг електронної роздрібної торгівлі перевищив 4,28 трильйона доларів США. Прогнозоване значення цього обсягу в 2021 році становитиме 4,89 трильйона доларів США, а

вже до 2024 року очікується зростання до 6,3 трильйона доларів США (рис.



1).[1]

Рисунок 1 – Обсяги електронного роздрібного продажу, млрд. доларів США Світовий ринок електронної комерції демонструє перспективне зростання, і до

2023 року очікується, що 22% роздрібних продажів будуть здійснені онлайн (рис. 2).[1]

Рисунок 2 – Частка електронної комерції в роздрібних продажах, %

Першим кроком у забезпеченні безпеки інтернет-магазину є встановлення захисту на рівні сервера. Це включає в себе регулярне оновлення програмного забезпечення, використання файрволів та антивірусних програм, а також моніторинг трафіку на сервері [2]. Окрім того, важливо забезпечити безпеку даних клієнтів, зокрема платіжної інформації. Для цього рекомендується використовувати протокол SSL (Secure Sockets Layer) для шифрування даних, які передаються між сервером і браузером користувача [3]. SSL використовує алгоритми шифрування, такі як AES та RSA, для забезпечення безпечного обміну даними. Вибір між SSL та іншими стандартами шифрування залежить від конкретного застосування та вимог до безпеки. SSL є відмінним вибором для забезпечення безпеки веб-сайтів та онлай- транзакцій, тоді як стандарти шифрування, такі як AES та RSA, можуть бути використані для захисту даних на різних рівнях.[4]

Ще одним важливим аспектом інформаційної безпеки є захист від DDoS-атак (розподілена атака типу "відмова в обслуговуванні"). Ці атаки полягають у перевантаженні сервера великою кількістю запитів, що може призвести до його відмови. Для запобігання DDoS-атакам можна використовувати спеціальні сервіси, які допомагають відфільтровувати легітимний трафік від шкідливого [5].

Для інтернет-магазину важливо забезпечити безпеку платіжних транзакцій та даних клієнтів. Це можна зробити шляхом використання шифрування даних, аутентифікації користувачів та контролю доступу до системи. Згідно з дослідженням української академії, "забезпечення конфіденційності, цілісності та доступності інформації є основними принципами інформаційної безпеки" [5].

Крім того, важливо забезпечити безпеку на рівні веб-додатку. Це включає в себе захист від таких загроз, як SQL-ін'єкції, XSS-атаки (Cross-Site Scripting) та CSRF-атаки (Cross-Site Request Forgery). Для цього рекомендується регулярно проводити аудит безпеки веб-додатку, використовувати безпечні

методи розробки та впроваджувати заходи безпеки, такі як валідація вводу користувача та санітарна обробка даних [6].

Окрім власників бізнесу, проблема захисту своєї інформації також стосується клієнтів. Дослідження "Security Issues For Online Shoppers" [7] розглядає ключові загрози та вразливості, пов'язані з онлайн-покупками, пропонує стратегії і рекомендації для забезпечення безпечного середовища для споживачів та підприємств у галузі електронної комерції. Проблеми безпеки для онлайн-покупців є актуальними та вимагають постійної уваги як від споживачів, так і від підприємств у галузі електронної комерції. Як видно з дослідження, застосування ефективних стратегій забезпечення безпеки та розуміння потенційних загроз може допомогти створити безпечне середовище для онлайн-покупок.[7]

Ключові загрози безпеки для онлайн-покупців:

– Фішинг: Фішингові атаки полягають у відправленні шахрайських електронних листів, які намагаються змусити користувачів розкрити свої особисті дані або паролі. Ці атаки можуть призвести до крадіжки ідентифікаційних даних та фінансових втрат.

– Вразливості веб-сайтів: Недоліки в безпеці веб-сайтів можуть дозволити зловмисникам отримати доступ до особистих даних користувачів або виконати несанкціоновані дії від імені користувачів.

– Мережеві атаки: Атаки типу "-in-the-middle" та "eavesdropping" можуть призвести до перехоплення даних, переданих між користувачем та веб-сайтом, що ставить під загрозу конфіденційність та цілісність даних.[7]

Стратегії забезпечення безпеки для онлайн-покупців:

– Освіта користувачів: Інформування користувачів про потенційні загрози та надання рекомендацій щодо безпечного користування інтернетом може допомогти зменшити ризик стати жертвою шахрайства.

– Застосування протоколів безпеки: Використання протоколів безпеки, таких як SSL/TLS, може забезпечити зашифроване з'єднання між

користувачем та веб-сайтом, що ускладнює перехоплення даних зловмисниками.

– Багаторівнева аутентифікація: Застосування багаторівневої аутентифікації може допомогти зменшити ризик несанкціонованого доступу до облікових записів користувачів.[7]

Узагальнюючи, інформаційна безпека інтернет-магазину є важливим аспектом успішного електронного бізнесу. Забезпечення безпеки серверів, проведення регулярного аудиту безпеки веб-сайту та захист платіжних транзакцій та даних клієнтів є ключовими елементами успішної стратегії інформаційної безпеки. Власники інтернет-магазинів повинні розуміти важливість цих аспектів та приділяти їм належну увагу.

Список використаних джерел

1. Бергер А.Д. та Галета А.С. (2021) Світові тенденції розвитку електронної комерції з урахуванням кризових умов пандемії covid-19. Економіка та суспільство 26(18), 2-5. DOI: 2524-0071 URL https://doi.org/10.32782/2524-0072/2021-26-18 (дата звернення: 07.06.2023)

2. Arno Ham (2022) E-commerce security 101: Essential information for web store owners URL: https://www.sana- commerce.com/blog/ecommerce-security-101/ (дата звернення: 07.06.2023)

3. Nadya Bakhur. How to Protect an Online Store: 7 Ways to Secure eCommerce URL: https://neklo.com/how-to-protect-online-store/ (дата звернення: 07.06.2023)

4. Андрюши В.С. (2016) Огляд криптографічного протоколу SSL. Актуальні задачі та досягнення у галузі кібербезпеки. 72-73. URL: https://core.ac.uk/download/pdf/84825467.pdf (дата звернення: 07.06.2023)

5. Безпека інтернет-магазину: що і чому потрібно захищати URL: https://rau.ua/novyni/bezopasnost-internet-magazina-chto-i- pochemu-nuzhno-zashhishhat/ (дата звернення: 08.06.2023)

6. Jinson Varghese (2022) Ecommerce Security: Importance, Issues & Protection Measures URL; https://www.getastra.com/blog/knowledge-base/ecommerce-security/ (дата звернення: 09.06.2023)

7. Abdulah M. Aseri (2016) Security Issues For Online Shoppers.International Journal of Scientific & Technology Research 10(3).112-116. URL: https://www.researchgate.net/publication/350220654_Security_Issues_For_Online_Sho ppers (дата звернення: 09.06.2023)

УДК: 004.838.2

Римаренко М.В.
здобувач вищої освіти
Вінницького національного технічного університету
Науковий керівник
Шелепало Г.В. , *к.ф.м.н. доцент кафедри захисту інформації*
Вінницького національного технічного університету

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В СУЧАСНОМУ ЖИТТІ

Штучний інтелект - технологія, яка змінює наше життя і спосіб взаємодії зі світом. Завдяки постійному розвитку комп'ютерної науки та високотехнологічних досягнень, штучний інтелект стає все більш присутнім у нашому повсякденному житті. Він перетворює спосіб, яким ми працюємо, виробляємо товари, спілкуємося, розважаємося та приймаємо рішення. Задачі, які раніше здавалися неможливими для виконання комп'ютерами, тепер можуть бути вирішені штучним інтелектом зі швидкістю і точністю, що раніше були недосяжними.

Роль штучного інтелекту стає все більш важливою, відіграючи значущу функцію в різних сферах нашого суспільства. Виробництво, охорона здоров'я, освіта,транспорт, фінанси, медіа - усі ці галузі отримують нові можливості та ефективність завдяки впровадженню штучного інтелекту. Його потенціал у