Ефективна стратегія безпеки вебресурсів включає в себе правильну обробку введених даних, використання сучасних методів шифрування, впровадження багаторівневої автентифікації, постійний моніторинг активності та регулярні оновлення програмного забезпечення. Також важливо застосовувати надійні механізми захисту від атак, зокрема апаратні та хмарні рішення, що здатні мінімізувати ризики компрометації даних.

Захист вебсайтів є безперервним процесом, який потребує не лише технічних заходів, а й підвищення рівня обізнаності розробників та користувачів. Лише дотримання найкращих практик кібербезпеки дозволяє забезпечити стабільну та безпечну роботу вебресурсів, зберігаючи довіру користувачів і захищаючи критично важливі дані від зловмисників.

Abstract. The article discusses a comprehensive approach to website security, including protection against hacker attacks, data leakage, and malware. The main cyber threats, such as SQL injections, XSS attacks, DDoS attacks, and zero-day exploits, are investigated. Methods of vulnerability analysis, risk assessment, and implementation of cybersecurity best practices, including multi-level authentication, encryption, and intrusion detection systems, are applied. The main results demonstrate the effectiveness of a combined approach to protecting web resources, which significantly reduces the likelihood of attacks and ensures the security of user data.

Keywords: website security, hacker attacks, data leakage, cyber threats, encryption.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Найкращі методи створення безпечних веб-сайтів. *Whileweb.* 01.08.2023. URL: Найкращі методи створення безпечних веб-сайтів | While Web Production (дата звернення: 06.03.2025).

2. Шакуров Є. О. Шляхи захисту змістової частини Web-сайту. *Безпека соціально-економічних процесів в кіберпросторі:* матеріали Всеукр. наук.-практ. конф. (Київ, 27 берез. 2019 р.). Київ: Київ. нац. торг.-екон. ун-т, 2019. С. 130–131. URL: 250dafc576ffd3c6a92546eebacc834d.pdf (дата звернення: 06.03.2025).

3. Найпоширеніші атаки ін'єкцій – CoreWin. *CoreWin.* 29.10.2024. URL: Найпоширеніші атаки ін'єкцій – CoreWin (дата звернення: 07.03.2025).

4. How To Prevent SQL Injection Attacks? Best Practices. *GlobalDots.* 30.06.2023. URL: https://www.globaldots.com/resources/blog/how-to-prevent-sql-injection-attacks/ (дата звернення: 08.03.2025).

5. Jatana N., Agrawal A., Sobti K. Post XSS Exploitation: Advanced Attacks and Remedies. P. 9.

6. Безпека та захист сайту. Як не втратити свій сайт. WEB ROOM. URL: Безпека та захист сайту. Як не втратити свій сайт? (дата звернення: 09.03.2025).

7. Шпінталь М. Я., Орловський Н. М. Методи захисту робочих станцій від DDoS-атак. *ACIT'2014.* Тернопіль (16–17 травня 2014). С. 230–231. URL: Шпінталь М.Я., Орловський Н.М..pdf (дата звернення: 09.03.2025).

8. Reddick C. G. Public administration in the digital age: A review of research and practice. International *Journal of Public Administration.* 2013. Vol. 36(2). P. 77–90.

9. Pigarev Yu., Kosteniuk N. Digitalization of public administration as a factor of digital transformation of Ukraine. Actual problems of public administration. 2021. Vol. 2. P. 92–96. URL: http://uran.oridu.odessa.ua/article/view/237257 (Accessed 01 June 2023).

10. Денисюк В. В., Зелінська О. В. Важливість кібербезпеки в сучасному світі. *Комп'ютерні технології обробки даних:* матеріали II Всеукраїнської науково-практичної конференції (м. Вінниця, 10 грудня 2021 р.). Вінниця: ДонНУ імені Василя Стуса. URL: https://jktod.donnu.edu.ua/article/view/11614

11. Зелінська О. В., Колосова К. К. Огляд методів UX-досліджень під час створення IT-продуктів. *Вісник студентського наукового товариства Донецького національного університету імені Василя Стуса.* 2022. Вип. 14, т. 1. С. 267–270. URL: https://jvestnik-sss.donnu.edu.ua/article/view/12827

УДК 004.738.5:651.7

СТРАТЕГІЇ ЕФЕКТИВНОЇ ЕЛЕКТРОННОЇ КОМУНІКАЦІЇ ДЛЯ УНИКНЕННЯ СПАМУ

І. С. Шпикуляк, О. В. Прігунов

Анотація. У статті розглядаються ефективні стратегії запобігання потраплянню електронних листів до папки «Спам». Описуються технічні аспекти, зокрема налаштування записів SPF, DKIM та DMARC, а також важливість ретельного оформлення тексту листів і врахування поведінки одержувачів. Визначено ключові стратегії, як-от використання релевантних тем, оновлення списків розсилки, налаштування процедури відписки, а також використання онлайн-сервісів для перевірки листів на ризик потрапляння до спаму. Підкреслюється важливість постійної адаптації стратегій електронної комунікації з огляду на еволюцію методів спам-фільтрації.

Ключові слова: спам-фільтрація, репутація відправника, персоналізація листів, онлайн-сервіси для перевірки email.

Вступ. У сучасному цифровому світі, незважаючи на зростання популярності месенджерів та соціальних мереж, одним з основних каналів масової комунікації залишається електронна пошта. Повідомлення email широко використовується не лише для персонального листування, а й для організації професійної, освітньої та бізнес-діяльності, забезпечуючи ефективний обмін інформацією, документами та оперативне інформування про події в електронному середовищі: повідомлення у соціальних мережах, підтвердження транзакцій, отримання квитанцій, участь в опитуваннях, нагадування про події або дедлайни. Email став інструментом автоматизованого зв'язку в сервісах електронної комерції, навчальних платформах, державних послугах, CRM-системах, розсилках новин тощо. Завдяки широкому спектру застосування електронна пошта поступово перетворилася з каналу особистої комунікації на інструмент стратегічного значення, що дає змогу підприємствам і організаціям досягати цільових аудиторій незалежно від їх географічного розташування чи технічних обмежень. Усе це підкреслює важливість не лише правильного формулювання контенту повідомлень, а й дотримання технічних вимог, які впливають на їх доставку та сприйняття.

Постановка проблеми. В Україні роль електронної комунікації стала особливо очевидною в умовах кризових ситуацій. Після початку повномасштабного вторгнення Росії кібератаки на урядові вебсайти та поштові сервери ускладнили офіційне спілкування. У цей час електронна пошта та соціальні мережі стали незамінними для української наукової спільноти, даючи змогу вченим координувати дії з міжнародними колегами та організовувати різноманітні заходи [1]. Цей приклад демонструє надійність і адаптивність електронної пошти як засобу комунікації, особливо коли традиційні канали стають недоступними. До того ж Україна здобула визнання за ефективне використання цифрових каналів комунікації на внутрішньому та міжнародному рівнях, що стало можливим завдяки впровадженню надійних заходів із кібербезпеки [2]. У період гуманітарної кризи, спричиненої війною, особисті контакти та електронна пошта стали важливими джерелами інформації для вимушених переселенців, особливо через обмежений доступ до офіційних джерел [3]. Отже, комунікація за допомогою email із різними категоріями населення у кризових ситуаціях набуває особливої ваги, оскільки стає доступним, надійним джерелом достовірної інформації.

Водночас із розширеними можливостями використання електронної пошти зростає й проблема – значна частина повідомлень, особливо масових, ризикує потрапити до спаму. Це створює суттєві перешкоди в комунікації, знижує ефективність електронних розсилок та ускладнює взаємодію з цільовою аудиторією. Підприємства, установи й організації змушені враховувати ці виклики під час реалізації своїх інформаційних стратегій, зокрема впроваджуючи заходи для уникнення фільтрів спаму.

Виклад основного матеріалу. Спам – це небажані електронні повідомлення, які зазвичай надсилаються масово без згоди отримувача. Цілі таких розсилок можуть варіюватися від просування товарів чи послуг до спроб фішингу, розповсюдження шкідливого програмного забезпечення або здійснення шахрайських дій. Існує безліч різних видів спаму, зокрема комерційні рекламні повідомлення, фальшиві попередження про віруси, листи зі сфальсифікованою адресою відправника (спуфінг), повідомлення про виграші в лотереях і різноманітні схеми фінансового шахрайства [4].

Принципи роботи сучасних спам-фільтрів

Сучасні алгоритми фільтрації спаму використовують складну комбінацію методів для виявлення небажаних повідомлень: аналіз вмісту електронного листа, перевірку технічних протоколів автентифікації (SPF, DKIM, DMARC), оцінку репутації IP-адреси та домену відправника, а також реакцію одержувачів на попередні повідомлення [5–15]. На ранніх етапах розвитку фільтри базувалися на пошуку ключових слів, згодом почали застосовувати баєсівський підхід та системи на основі правил. Сьогодні ж домінує багаторівневий підхід із використанням штучного інтелекту (ШІ) та машинного навчання (МН), які дають змогу виявляти не лише окремі слова, а й загальний контекст, тон повідомлення, його семантичне значення та поведінкові ознаки. Завдяки цьому фільтри можуть адаптуватися до нових тактик спамерів [8; 10]. Важливими технічними індикаторами є наявність і правильність налаштування протоколів SPF, DKIM і DMARC. SPF визначає дозволені поштові сервери для домену; DKIM забезпечує циф-

ровий підпис листа, що гарантує його цілісність і справжність; DMARC координує політику обробки листів, які не пройшли автентифікацію, та забезпечує звітність (табл. 1) [11; 12]. Неправильні налаштування цих записів, використання шаблонних слів у темі чи тексті листа, низька репутація IP-адреси, розсилки на неактивні адреси або відсутність реакції одержувачів можуть призвести до автоматичного потрапляння навіть важливих листів до папки «Спам» [12; 14]. Розвиток спам-фільтрів є динамічним процесом, у якому нові захисні механізми постійно створюються у відповідь на еволюцію стратегій спамерів. Завдяки цьому сучасні системи досягають високої точності та ефективності у виявленні небажаних повідомлень.

Таблиця 1

Технічні аспекти автентифікація електронної пошти за допомогою протоколів [9]

Протокол	Опис	Перевага
SPF	Перелік авторизованих поштових серверів для вашого домену в DNS	Запобігає підробці спамерами адреси відправника вашого домену, покращуючи доставляння
DKIM	Додає цифровий підпис до листів, який можна перевірити за допомогою відкритого ключа в DNS	Забезпечує цілісність листа та підтверджує автентичність відправника, знижуючи ймовірність потрапляння до спаму
DMARC	Визначає, як обробляти листи, що не пройшли перевірку SPF або DKIM, та надає звітність	Підвищує безпеку домену від спуфінгу та фішингових атак, покращує репутацію відправника та доставляння листів

Отже, існує кілька основних причин, через які важливі та прийнятні електронні листи можуть потрапляти до папки «Спам»:

– відсутність або неправильне налаштування записів SPF, DKIM та DMARC для домену відправника;

– використання в темі або основному тексті листа певних тригер-слів і фраз, які автоматично розпізнаються фільтрами як підозрілі;

– низька репутація IP-адреси або домену, з яких надходить лист, що може бути наслідком великої кількості скарг від одержувачів на попередні розсилки;

– надсилання листів на велику кількість неактивних або неіснуючих електронних адрес (що призводить до високого рівня відмов);

– реакції одержувачів на попередні повідомлення, зокрема, низькі показники відкриття та переходів за посиланнями;

– неправильне форматування HTML-коду листа;

– наявність великої кількості вкладень і посилань на вебсайти з низькою репутацією.

Дієві стратегії для запобігання потраплянню листів у спам

Щоб запобігти потраплянню важливих і прийнятних електронних листів до папки «Спам», необхідно враховувати кілька ключових аспектів і уникати типових помилок. Перевірити правильність налаштування або наявність записів SPF, DKIM та DMARC для домену відправника можна за допомогою онлайн-сервісів, як-от mxtoolbox.com або mail-tester.com, які допомагають оцінити спам-рейтинг листа. Фрази або тригер-слова, наприклад, «Отримай 1 000 грн прямо зараз!» чи «Клікни тут, щоб виграти приз!», можуть бути автоматично визначені фільтрами як підозрілі. Прийнятним для фільтрів варіантом буде фраза «Новини нашої компанії: спеціальна пропозиція для вас». Для перевірки тексту на спам-фрази можна скористатися сервісами, як-от emailspamwords.com чи sendcheckit.com. Також важливо стежити за репутацією IP-адреси або домену, з яких надсилаються листи. Якщо з домену раніше надсилали спам або масові листи без згоди, це може призвести до блокування (потрапляння в чорний список). Перевірити репутацію домену та IP можна за допомогою інструментів talosintelligence.com чи senderbase.org. Очистити бази контактів від застарілих або неактивних адрес допоможуть сервіси для валідації email-адрес, наприклад, neverbounce.com або zerobounce.net. У випадках, коли одержувачі масово ігнорують або видаляють листи, це сигналізує про погану репутацію відправника. Покращити взаємодію та підвищити довіру допоможе персоналізація звернень, наприклад, використання імені одержувача. Однак невдало виконана персоналізація або її надмірне використання не допоможуть вирішити проблему спаму (рис. 1).

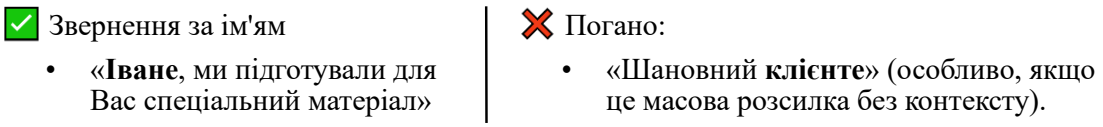

Рис. 1. Приклади персоналізації звернень до одержувача

Варто також зазначити, що існують системи автоматизації розсилки, які дають змогу персоналізувати звернення та контент (наприклад, Mailchimp, eSputnik). До некоректного форматування HTML-коду листа, що може стати причиною блокування, належить відсутність текстової частини повідомлення або використання непарних тегів. Перевірка здійснюється інструменти на зразок mailtrap.io чи litmus.com. Важливо також стежити за балансом тексту і графічних елементів у листі. Рекомендується, щоб текст складав 60 % від загального обсягу листа, а графіка – не більше 40 %. Використання лише одного великого зображення може бути розцінене спам-фільтрами як спроба обійти текстовий аналіз. Для всіх зображень необхідно додавати альтернативний текст (alt-text), а файли зображень мають бути оптимізовані для швидкого завантаження. Треба бути обережним, якщо використовуються вкладення, оскільки вони суттєво збільшують загальний розмір листа, що підвищує ймовірність його блокування. Особливо спам-фільтри підозріло ставляться до виконуваних файлів (.exe) або архівів (.zip, .rar). Якщо потрібно надіслати великі файли, краще використовувати посилання на файли у хмарних сховищах, як-от Google Drive, Dropbox або OneDrive. Фінальним етапом перед масовою розсилкою є проведення пробної відправки електронного листа на платформу https://mail-tester.com. Цей інструмент дає змогу оцінити загальний бал листа та виявити потенційно небезпечні фактори [9; 12; 16–25].

Висновки. Підсумовуючи вищесказане, можна зробити висновок про те, що ефективна стратегія запобігання потраплянню електронних листів до спаму вимагає комплексного підходу. Він включає в себе не лише ретельне оформлення та написання листів з урахуванням рекомендацій щодо структури, стилю та змісту, але й обов’язкове налаштування технічних аспектів, як-от записи SPF, DKIM та DMARC, а також постійне врахування очікувань та поведінки одержувачів.

Для підвищення ефективності обміну інформацією та підтримки позитивної репутації відправника необхідно дотримуватися низки ключових стратегій. Це включає в себе створення чітких та релевантних тем листів, регулярне оновлення списків розсилки і видалення неактивних користувачів, забезпечення простої та зручної процедури відписки від розсилок, обов’язкове зазначення контактної інформації відправника у кожному листі, а також використання спеціалізованих онлайн-сервісів для перевірки повідомлень на ризик потрапляння до спаму перед їх відправкою.

Враховуючи постійну еволюцію методів спам-фільтрації і тактик спамерів, важливо постійно навчатися та адаптувати свої стратегії електронної комунікації. Комплексний підхід, який поєднує в собі уважність до деталей під час написання листів, належну технічну конфігурацію та орієнтацію на потреби та очікування одержувачів, є запорукою успішної та ефективної електронної комунікації, яка дасть змогу уникнути небажаної папки «Спам» і забезпечити надійне доставляння важливої інформації.

Abstract. The article discusses effective strategies for preventing emails from landing in the «Spam» folder. It describes technical aspects, including the configuration of SPF, DKIM, and DMARC records, as well as the importance of careful email content formatting and considering recipient behavior. Key strategies are identified, such as using relevant subject lines, updating mailing lists, setting up unsubscribed procedures, and using online services to check emails for the risk of being marked as spam. The importance of continuously adapting email communication strategies considering the evolution of spam filtering methods is emphasized.

Keywords: spam filtering, sender reputation, email personalization, online services for email checking.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ukraine: how can the scientific community help scholars at risk? *World economic forum.* URL: https://www.weforum.org/stories/2022/03/ukraine-scientific-community-scholars-at-risk/ (дата звернення: 18.02.2025).

2. Peter Schrijver. Ukraine's Fight on the Front Lines of the Information Environment. *Modern War Institute*. URL: https://mwi.westpoint.edu/ukraines-fight-on-the-front-lines-of-the-information-environment/ (дата звернення: 16.02.2025).

3. Christine Fricke, Nataliia Gusak and Andrii Kryshtal. Effective support for people fleeing the war in Ukraine requires an understanding of their language and communication needs and preferences. *Forced Migration Review*. URL: https://www.fmreview.org/ukraine/fricke-gusak-kryshtal/ (дата звернення: 18.02.2025).

4. What is Spam Mail in Email? *Darktrace.* URL: https://darktrace.com/cyber-ai-glossary/email-spam (дата звернення: 21.02.2025).

5. Decoding the Evolution of Spam: From Unsolicited Emails to AI-Driven Filters. *ENAILTREE.AI*. URL: https://emailtree.ai/blog/evolution-of-spam/ (дата звернення: 18.02.2025).

6. Cora Quigley. How AI and machine learning are shaping the future of spam filtering. *Spaceship Blog.* URL: https://www.spaceship.com/blog/ai-spam-filtering/ (дата звернення: 18.02.2025).

7. Mastering Spam Filtering: A Comprehensive Guide. *Abusix.* URL: https://abusix.com/blog/mastering-spam-filtering-a-comprehensive-guide/ (дата звернення: 20.02.2025).

8. Top 40 Latest Anti-Spam Software Statistics, Data & Trends. *9cv9 Career Blog*. URL: https://blog.9cv9.com/top-40-latest-anti-spam-software-statistics-data-trends/ (дата звернення: 20.02.2025).

9. Understanding How Email Spam Filter Works. *Sage Network & Communications.* URL: https://www.sagenet-com.com/blog/how-email-spam-filter-works (дата звернення: 20.02.2025).

10. How AI and machine learning are shaping the future of spam filtering. *Spaceship Blog.* URL: https://www.space-ship.com/blog/ai-spam-filtering/ (дата звернення: 20.02.2025).

11. What Is Anti-Spam? How Anti-Spam Works & Evaluating Solutions. *Perception Point*. URL: https://perception-point.io/guides/email-security/what-is-anti-spam-how-anti-spam-works-and-how-to-evaluate-solutions/ (дата звернення: 20.02.2025).

12. Why are emails going to SPAM/JUNK. *Florida Atlantic University.* URL: https://comsupport.fau.edu/kb/articles/why-are-emails-going-to-spam-junk (дата звернення: 20.02.2025).

13. Mastering Spam Filtering: A Comprehensive Guide. *Abusix.* URL: https://abusix.com/blog/mastering-spam-filtering-a-comprehensive-guide/ (дата звернення: 20.02.2025).

14. 18 Reasons Why Your Email Goes to Spam (+ How to Prevent It). *Omnisend.* URL: https://www.omnisend.com/blog/email-goes-to-spam/ (дата звернення: 21.02.2025).

15. How to avoid spam filters: 16 proven ways. *Omnisend.* 2025. URL: https://www.omnisend.com/blog/how-to-avoid-spam-filters/ (дата звернення: 24.02.2025).

16. Free Email Spam Words Checker. *Warmup Inbox.* URL: https://www.warmupinbox.com/email-spam-words-checker/ (дата звернення: 24.02.2025).

17. What are DMARC, DKIM, and SPF? *Cloudflare.* URL: https://www.cloudflare.com/learning/email-security/dmarc-dkim-spf/ (дата звернення: 24.02.2025).

18. Email Subject Lines: Top Tips & Best Practices. *Salesforce US*. URL: https://www.salesforce.com/marketing/email/subject-lines/ (дата звернення: 25.02.2025).

19. Rachel Rockwell. Don't Be Spammy: 10 Email Body Content Tips to Help Avoid Filters. *THE MARKETING MANAGER.ai* URL: https://www.mirabelsmarketingmanager.com/blog/10-email-body-content-design-tips-to-help-avoid-spam-filters/ (дата звернення: 25.02.2025).

20. 20 Will Sigsworth. How to optimize your email size to avoid spam filters. *Pipedrive*. URL: https://www.pipedrive.com/en/blog/email-size-limits (дата звернення: 25.02.2025).

21. The Risks and Choices of Using Email Attachments in Marketing. *Campaign Refinery.* URL: https://campaignrefinery.com/email-attachments-in-marketing/

22. Effective Email Communication in the Workplace Drives Business. *Ariel.* URL: https://www.arielgroup.com/effective-email-communication/ (дата звернення: 25.02.2025).

23. Rachel Adnyana, Claire Broadley. How AI Spam Filters Work to Protect Your Inbox. *SendLayer*. URL: https://sendlayer.com/blog/how-ai-spam-filters-work-to-protect-your-inbox/ (дата звернення: 25.02.2025).

24. Caroline Henno. Why Easy Email Unsubscribe Boosts Your Brand. *Acoustic.* URL: https://www.acoustic.com/blog/why-an-easy-email-unsubscribe-option-is-actually-good-for-your-brand (дата звернення: 25.02.2025).

25. How to Write a Formal Email. *Spark Mail.* URL: https://sparkmailapp.com/formal-email-template (дата звернення: 25.02.2025).