

2. Стець В. В. Органи місцевого самоврядування як особливі суб'єкти забезпечення кібербезпеки України. Матеріали Міжнародної наук.-практ. конференції "Україна у сучасному міжнародному просторі" «УКРАЇНА У СУЧАСНОМУ МІЖНАРОДНОМУ ПРОСТОРИ». Україна : Одеса 2021 С. 56 – 58 URL: http://dspace.op.edu.ua/jspui/bitstream/123456789/12143/1/09_Full_Block_ (дата звернення: 18.05.2023).

3. Козюра В.Д., Хорошко В.О., Система кібернетичної безпеки в Україні. Науково-практичний журнал. Сучасна спеціальна техніка. 2017. №4 (51) С. 34 – 41 URL:

<http://elar.naiu.kiev.ua/bitstream/123456789/13635/1> (дата звернення: 19.05.2023).

4. Проект Закону України від 14.04.2016 № 2126а “Про основні засади забезпечення кібербезпеки України” URL: <https://ips.ligazakon.net/document/JH1N268B?an=3> (дата звернення: 21.05.2023).

5. Закон України № 2469 VIII (2021). Про національну безпеку. URL: <https://zakon.rada.gov.ua/laws/show/2469-19> (дата звернення: 22.05.2023).

6. Янковський О. Україні потрібна нова кіберстратегія. Українська правда. 2019. URL: <https://www.pravda.com.ua/rus/columns/2019/09/14/7226291/> (дата звернення 22.05.2023)

Вітковський А.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*

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ШЛЯХОМ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

В сучасному цифровому світі, де персональні дані стають все більш цінними та піддатливими на атаки зловмисників, забезпечення безпеки та

конфіденційності персональних даних стає надзвичайно важливою задачею. Одним із найефективніших методів захисту є багатофакторна аутентифікація, яка використовує комбінацію різних факторів для підтвердження ідентичності користувача. У цьому документі будуть розглянуті основні аспекти багатофакторної аутентифікації та її роль у захисті персональних даних [1].

Багатофакторна аутентифікація є процесом перевірки ідентичності користувача, використовуючи комбінацію різних факторів. Це означає, що для підтвердження ідентичності необхідні не лише пароль або ідентифікаційний код, а й додаткові фактори, такі як фізичний об'єкт (токен або смарт-карта) або біометричні дані (відбиток пальця, розпізнавання обличчя).

Цей процес перевірки використовує комбінацію різних факторів для підтвердження ідентичності користувача. Ці фактори можуть бути класифіковані на три основні категорії: що щось ви знаєте (наприклад, пароль, PIN-код), що щось маєте (наприклад, смарт-карта, USB-ключ), і що щось ви є (наприклад, біометричні дані, такі як відбиток пальця або розпізнавання обличчя). Комбінація цих факторів дозволяє створити більш надійну систему аутентифікації, оскільки зловмисникам буде важче підробити або отримати доступ до всіх необхідних факторів [2].

Безпека персональних даних залежить не тільки від технологій багатофакторної аутентифікації, але й від свідомості та освіти самого користувача. Розуміння принципів та переваг багатофакторної аутентифікації дозволяє користувачам правильно використовувати цей метод і захищати свої особисті дані. Освічені користувачі знають, як обрати надійні паролі, як управляти своїми аутентифікаційними факторами і як реагувати на підозрілі запити на авторизацію. Також, свідомість користувачів щодо потенційних загроз і методів атак допомагає запобігти соціальному інжинірингу та підступам зловмисників.

Вона включає в себе декілька переваг у порівнянні з традиційними методами однофакторної аутентифікації. Перш за все, вона забезпечує вищий

рівень безпеки, оскільки втратити або викрасти всі необхідні фактори набагато складніше, ніж лише пароль або ідентифікаційний код. Додаткові фактори орудують процес зламу аутентифікації значно складнішим для зловмисників.

Існує ряд технологій, які використовуються у багатофакторній аутентифікації. Одним з поширених методів є SMS-підтвердження, де користувачу надсилається одноразовий код на мобільний пристрій. Інші методи включають використання апаратних токенів або програмних токенів, які генерують одноразові паролі, а також використання біометричних методів, таких як сканування відбитку пальця або розпізнавання обличчя.

Впровадження багатофакторної аутентифікації може зіткнутися з деякими викликами. Наприклад, вартість впровадження і підтримки таких систем може бути високою. Деякі методи багатофакторної аутентифікації можуть бути складними для користувачів і вимагати додаткових зусиль для використання. Також існує ризик приватності та безпеки, особливо при збереженні біометричних даних.

Для успішного впровадження багатофакторної аутентифікації рекомендується враховувати контекст і потреби організації або користувачів. Важливо вибрати відповідні технології, забезпечити надійну і безпечну інфраструктуру, а також надати належну підтримку користувачам. У майбутньому багатофакторна аутентифікація може розвиватися за допомогою нових технологій, таких як блокчейн або штучний інтелект, щоб поліпшити безпеку та зручність для користувачів.

Впровадження багатофакторної аутентифікації може виникнути декілька викликів та ризиків. Один з них - складність використання для користувачів. Використання декількох факторів може вимагати додаткових кроків або пристроїв, що може призвести до несправностей або незручностей для користувачів. Крім того, вартість впровадження та підтримки системи багатофакторної аутентифікації також може бути значною. Існує також ризик приватності та безпеки, зокрема при збереженні і обробці біометричних даних.

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 // ResearchGate – 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 // ResearchGate – 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