be appropriate in its characteristics to the scale of threats and risks. Deviation from this rule will lead to significant losses. Each computer system (CS) must have its own optimal level of cyber security, which must be constantly maintained. Unfortunately, there is still no adequate methodology for assessing the quantitative level of cyber security. The main problems that need to be solved to develop the mathematical foundations of quantitative analysis of cyber security and determine its level are: determining the functional relationship between the methods of attack on the CS and the methods of short circuit; development of a criterion for assessing the level of short-circuit, based on the totality of its quantitative characteristics; determining the methodology for substantiating priority measures aimed at ensuring a given level of cyber security of information. The proposed technique will enable the use of new methods of information processing in order to assess its cyber security, which were not previously used.

Keywords: cybersecurity, computer system, quantitative analysis, criteria for assessing the level of short-circuit, the level of cyber security.

Хорошко Володимир Олексійович, д.т.н., проф., професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Volodymyr Khoroshko, PhD., Professor, Professor, Department of Information Technology Security, National Aviation University.
E-mail: professor@ukr.net.
Orcid ID: 0000-0001-6213-7086.

Хохлачова Юлія Євгеніївна, к.т.н., доц., доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Yuliia Khokhlachova, Ph.D., Associate Professor, Department of Information Technology Security, National Aviation University.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

Вишневська Наталія Сергіївна, старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університету.

Natalia Vishnevska, Senior Lecturer, Department of Information Technology Security, National Aviation University.
E-mail: viserj@ukr.net.
Orcid ID: 0000-0001-9036-6556.

DOI: 10.18372/2410-7840.25.17675
УДК 004.054

ДО ПИТАННЯ БЕЗПЕЧНОЇ БАГАТОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ У ВЕБ-ЗАСТОСУНКАХ

Валерій Дудикевич, Галина Микитин, Володимир Насилевський, Володимир Фігурняк

Розглянуто основні сегменти інфраструктури "розумного міста" із застосуванням автентифікації за вектором безпеки технологій Індустрії 4.0. Проаналізовано підходи до безпечної автентифікації, зокрема у ВЕБ-застосунках. Проведено порівняння способів автентифікації у ВЕБ-застосунках за вимогами та рівнем захищеності даних. Проаналізовано загрози автентифікації, механізми та технології захисту і, на цій основі, створено системну модель безпечної багатофакторної автентифікації у ВЕБ-застосунку на основі концепції "об'єкт – загроза – захист" за структурою "ВЕБ-сторінка – ВЕБ-сервер – база даних". Розроблено алгоритмічно-програмну реалізацію системи безпечної багатофакторної автентифікації у ВЕБ-застосунку на основі застосування криптографічної хеш-функції SHA-1 та симетричного алгоритму шифрування повідомлень AES засобами мови програмування JavaScript. Наведено практичну реалізацію покрокового алгоритму багатофакторної автентифікації у ВЕБ-застосунках за факторами – логін та пароль, відбиток пальця, смартфон.

Ключові слова: *багатофакторна автентифікація, безпека, ВЕБ-застосунок, системна модель, хеш-функція, алгоритм шифрування повідомлень.*

ВСТУП

В Україні ефективно розгортаються процеси інтелектуалізації у просторі Індустрії 4.0, що передбачає: застосування новітніх інформаційних технологій, впровадження автоматизації промислових процесів, використання штучного інтелекту [1]. В цьому напрямі розвиваються підходи до забезпечення безпеки інформаційних, комунікаційних систем та Інтернету речей (IoT), що підтримують функціонування інтелектуальних об'єк-

тів, зокрема критичної інфраструктури України [2, 3]. Найактуальнішим сегментом Індустрії 4.0 є Концепція "Розумного міста", яка розгорнута інфраструктурою – "Розумний дім", "Розумний екологічний моніторинг", "Розумна освіта", "Розумна медицина", що вимагає відповідних підходів до безпечного функціонування технологій їх функціонування [4]. Функціонування "Розумного дому", "Розумного екологічного моніторингу" ефективно підтримують багаторівневі кіберфізичні системи, складовою фізичного простору яких є Інтернет речей, як мережа мереж давачів, що контролюють відповідно: параметри функціональних пристроїв, кліматичні параметри, стан зовнішньої і внутрішньої безпеки будинку; екологічні параметри довкілля (води, повітря, ґрунту, лісів) для подальшої обробки, аналізу даних (їх візуалізації) в кібернетичному просторі з метою прийняття управлінського рішення [5]. Розгортаються процеси інтелектуалізації освіти, зокрема у частині функціонування центрів інформаційного забезпечення закладів вищої освіти, що потребує безпечних інформаційно-комунікаційних технологій [6]. Для зручного та ефективного користування інфраструктурою "Розумного міста" ефективно застосовуються ВЕБ-застосунки, для яких актуальна безпека автентифікації. В процесах безпечної інтелектуалізації об'єктів інфраструктури застосовуються: парольна автентифікація, автентифікація з застосуванням генераторів одноразових паролів, автентифікація за підписом, біометрична автентифікація, пасивна автентифікація за геолокацією, зокрема на практиці ефективна багатофакторна автентифікація [7]. Актуальним питанням залишається розвиток ефективних підходів і апаратно-програмних технологій реалізації багатофакторної автентифікації у ВЕБ-застосунках. В роботі [8] запропоновано нову методику, яка використовує графічний пароль з підказкою точки натискання разом з одноразовим сеансовим ключем, що забезпечує високу ефективність та зручність використання системи автентифікації.

Цікавою є система автентифікації для додатків Інтернету речей, що реалізована як багатофакторна та багаторівнева і ґрунтується на взаємодії між пристроями IoT [9]. В праці [10] розглянуто метод автентифікації для регенерації JWT (веб-токен JSON) при кожному клієнтському запиті на основі випадкових значень мітки часу для підвищення автентичності клієнта на сервері. Багатофакторна автентифікація розгорнута новим механізмом на основі браузера, що використовує відбитки пальців і графічні паролі [11]. Розвиток методологій побудови систем багатофакторної автентифікації у ВЕБ-застосунках забезпечить основні профілі безпеки обміну інформації в просторі інтелектуалізації об'єктів, зокрема критичної інфраструктури. Мета роботи – створення системної моделі багатофакторної автентифікації у ВЕБ-застосунках за структурою "ВЕБ-сторінка – ВЕБ-сервер – база даних" і, на цій основі, розроблення алгоритмічно-програмного забезпечення її реалізації у просторі факторів "знання – властивості – володіння".

ОСНОВНА ЧАСТИНА

Елементи систем автентифікації та її основні фактори

Системи автентифікації – це заходи безпеки, які використовуються з метою захисту даних, сервісів, сторонніх систем або за стосунків і на основі додаткових вхідних даних надають можливість переконатися в достовірності користувача.

Основними елементами систем автентифікації у просторі реєстрації у ВЕБ-ресурсі є: суб'єкт – користувач; характеристика – пароль, біометричні дані, код зі смартфону, власник системи – замовник ВЕБ-ресурсу; механізм автентифікації – програмне забезпечення системи багатофакторної автентифікації, механізм керування доступом – обліковий запис, процес реєстрації. У просторі вимог до конфіденційності, захищеності та цілісності інформації використовуються різні фактори автентифікації або їх комбінація: фактор знань – секретна інформація, фактор властивостей – біометрика, фактор володіння – смартфон, генератор одноразових паролів тощо. В табл. 1 наведено способи автентифікації у ВЕБ-застосунках та їх характеристики.

Багатофакторна автентифікація поєднує певну кількість різних способів у довільному порядку. На практиці ефективно використовується поєднання паролю разом з цифровим підписом або разом з смс, або біометрикою, що уможливлює забезпечення конфіденційності для користувача.

Таблиця 1

Порівняльна характеристика способів автентифікації у ВЕБ-застосунках

Спосіб	Вимоги	Захищеність
Пароль	-	Середня
ЕЦП	Файл ЕЦП, спеціально підібраний пароль	Висока
СМС	Телефон, доступ до Інтернету	Висока
Біометрика	Додаток в телефоні, доступ в Інтернет, наявність додаткових засобів	Висока
Геолокація	Наявність спеціалізованих пристроїв	Середня
Технічні засоби	Наявність додаткових засобів	Висока
Пароль + СМС	Телефон, доступ до Інтернету	Висока
Пароль + Біометрика	Наявність додаткових засобів, додаток в телефоні	Дуже висока
Пароль + ЕЦП	Файл ЕЦП, спеціально підібраний пароль	Висока
Біометрика + Технічні засоби	Наявність додаткових засобів	Дуже висока
Пароль + Технічні засоби	Наявність додаткових засобів	Висока

Системна модель безпечної багатофакторної автентифікації у ВЕБ-застосунках

На основі аналізу загроз автентифікації у ВЕБ-застосунках і застосування відповідних технологій їх протидії побудовано системну модель безпечної багатофакторної автентифікації згідно концепції "об'єкт – загроза – захист", яка уможливить безпечний обмін інформації між ВЕБ-сторінкою, ВЕБ-сервером та базою даних, забезпечуючи основні профілі безпеки Індустрії 4.0 [12, 13, 14] (рис. 1).

Рис. 1. Системна модель безпечної багатофакторної автентифікації у ВЕБ-застосунках

Використання багатофакторної автентифікації унеможливить перехоплення зловмисником паролю або логіну, оскільки окрім парольної автентифікації йому для несанкціонованого доступу необхідні будуть біометричні дані та смартфон користувача або токен, що практично не підлягає реалізації. Використання захищених протоколів OAuth, OpenID з відомими провайдерами сервісу автентифікації (Google, Facebook, Twitter) допоможе замінити імплементацію власних систем на користь безпечних, професіональних і перевірених. В системах автентифікації у ВЕБ-застосунках ефективно використовуються криптографічні алгоритми симетричного шифрування, серед яких AES – алгоритм блокового шифрування повідомлень. Найпопулярнішими криптографічними хеш функціями є: сімейство MD, сімейство криптоалгоритмів SHA, HAVAL, Whirlpool.

Криптографічні протоколи в системах автентифікації

На рис. 2 наведена класифікація протоколів автентифікації.

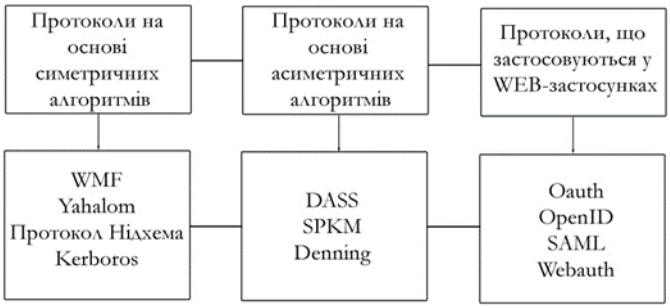

Рис. 2. Види протоколів автентифікації

У ВЕБ-застосунках найчастіше застосовуються протоколи OAuth2 та OpenID, побудовані на основі OAuth, які використовують як блокові симетричні алгоритми, так і хеш-функції. Для верифікації повідомлень від клієнтів, протокол OAuth2 підтримує два методи автентифікації: HMAC-SHA1 і RSA-SHA1. Оскільки при хешуванні паролів часто використовується хеш-функція SHA, то для автентифікації між ВЕБ-сервером та базою даних в протоколі SCRAM використовується функція хешування HMAC, за допомогою якої також генеруються стійкі одноразові паролі для додаткової автентифікації через мобільний додаток. Розглянемо алгоритмічно-програмну реалізацію безпечної багатофакторної автентифікації у ВЕБ-застосунках на основі застосування криптографічної хеш-функції SHA-1 та алгоритму симетричного шифрування AES-256 засобами JavaScript.

Алгоритм системи багатофакторної автентифікації

В алгоритмі системи багатофакторної аутентифікації у ВЕБ-застосунку (рис. 3) використовуємо три фактори: фактор знань – логін та пароль; фактор властивостей – відбиток пальця; фактор володіння – смартфон. Для початку користувач проходить реєстрацію в системі. Під час реєстрації він повинен надати такі дані: ім'я, логін та електронну скриньку. Надалі користувачу пропонується відсканувати відбиток пальця для збереження в системі.

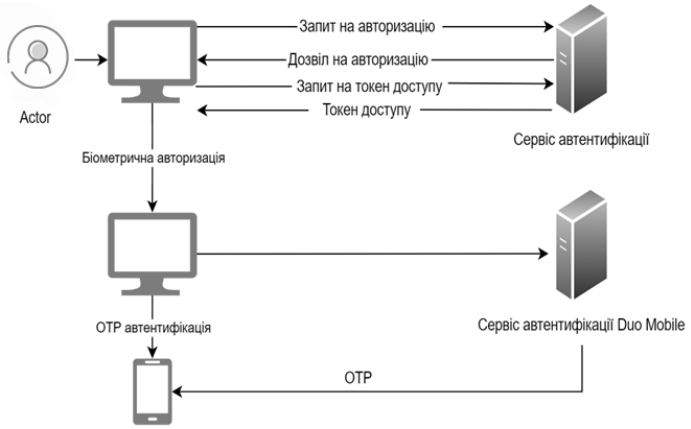

Рис. 3. Структура алгоритму системи багатофакторної автентифікації у ВЕБ-застосунку

Логін та пароль – перший крок авторизації користувача. Завдяки протоколу OAuth2, ми можемо використати сторонні сервіси автентифікації, такі як Google, Facebook, Twitter. Сучасні сервіси автентифікації вимагають використання складних паролів. Мінімальними вимогами до паролів є: наявність восьми символів з верхнього та нижнього регістрів, цифр та спец-символів. Другий крок – біометрична автентифікація із застосуванням протоколу WebAuthn. Користувач повинен буде під'єднати пристрій, що містить сканер відбитків пальців, наприклад смартфон, під'єднаний до браузеру за допомогою Bluetooth, окремий пристрій-сканер або вбудований в ноутбук. Після успішного приєднання користувачу буде запропоновано відсканувати палець. У разі успішної біометричної автентифікації, користувач перейде до

третього кроку – підтвердження через смартфон. Відповідний додаток згенерує стійкий одноразовий пароль, який користувач повинен ввести у полі введення або підтвердити його прямо в додатку.

Програмна реалізація системи багатофакторної автентифікації у ВЕБ-застосунку засобами мови JavaScript

Програмна реалізація системи багатофакторної автентифікації побудована за допомогою парольної, біометричної автентифікації та автентифікації за допомогою додатку на смартфоні. Реалізація системи написана мовою програмування JavaScript. На рис. 4 наведена форма для реєстрації з наступними даними: ім'я користувача, логін (юзернейм) та емейл.

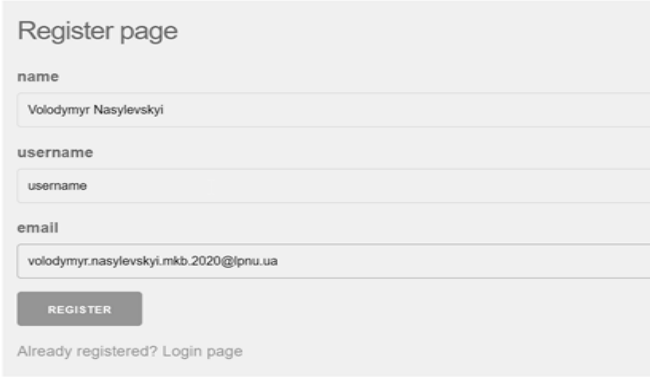

Рис. 4. Реєстрація користувача

При кліку на "Register" для користувача візуалізується віконце біометричної автентифікації з можливістю застосування вбудованого сканера або вибору зовнішнього на смартфоні (рис. 5).

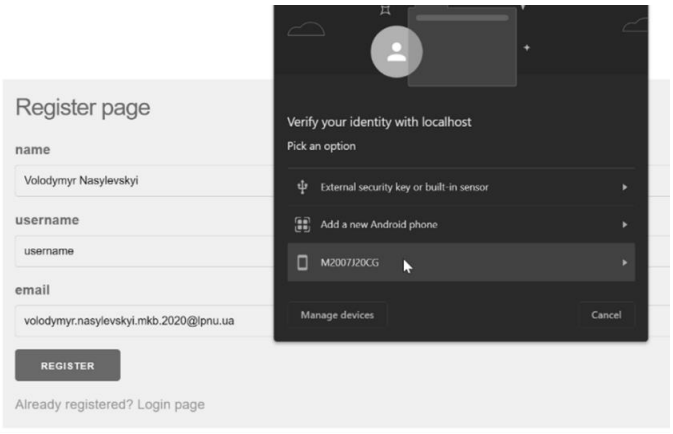

Рис. 5. Вибір пристрою для реєстрації користувача з біометричною автентифікацією

Відбудеться приєднання до вибраного сканера з подальшим запитом щодо надання підтвердження особи за відбитком пальця (рис. 6).

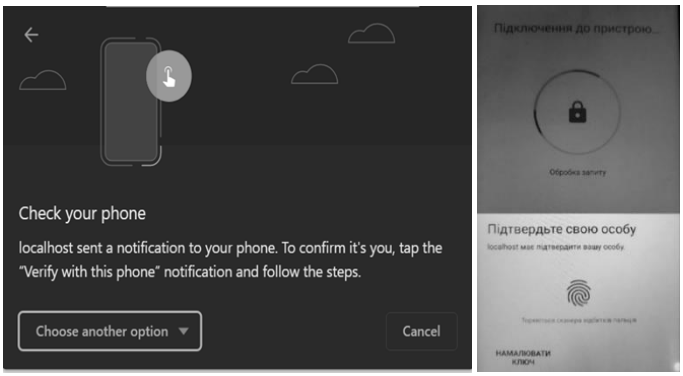

Рис. 6. Підтвердження особи за допомогою смартфона

Після реєстрації здійснюється вхід до аккаунту, користувача буде перенаправлено на сторінку першого етапу автентифікації у ВЕБ-застосунку (рис. 7).

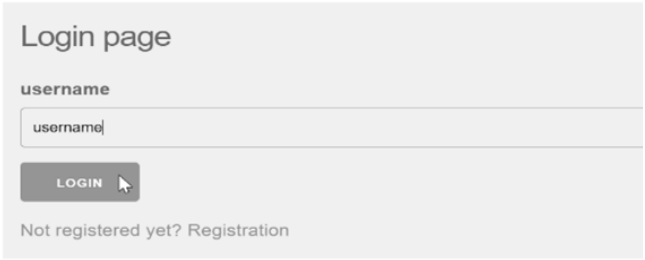

Рис. 7. Спроба входу до ВЕБ-застосунку із зареєстрованим користувачем

Для автентифікації використовуємо надійний та перевірений сервіс Google (рис. 8).

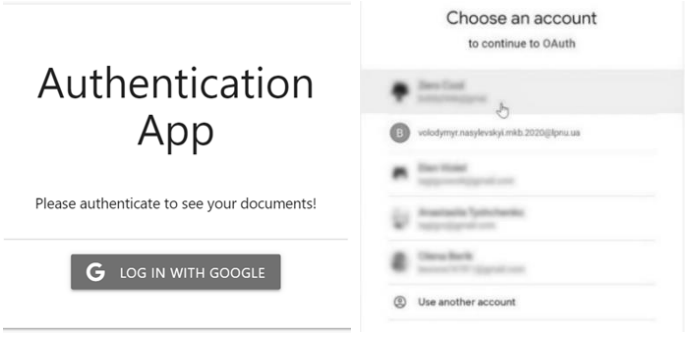

Рис. 8. Вибір Google-аккаунту для автентифікації

Після першого успішного кроку, реалізується запит на біометричну автентифікацію (рис. 9).

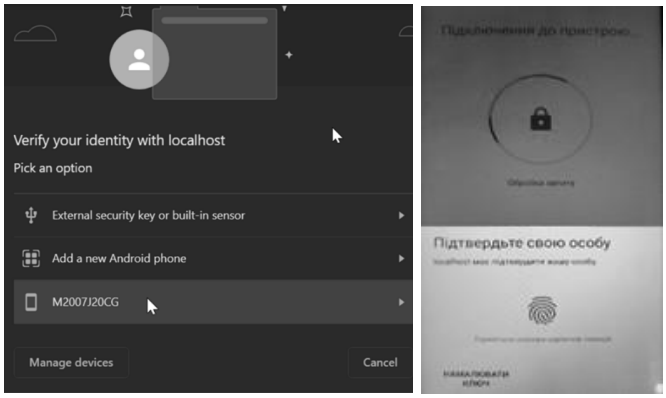

Рис. 9. Підтвердження особи за допомогою біометричної автентифікації

Після проходження біометричної автентифікації користувачу надходить на додаток у смартфоні згенерований одноразовий код (рис. 10).

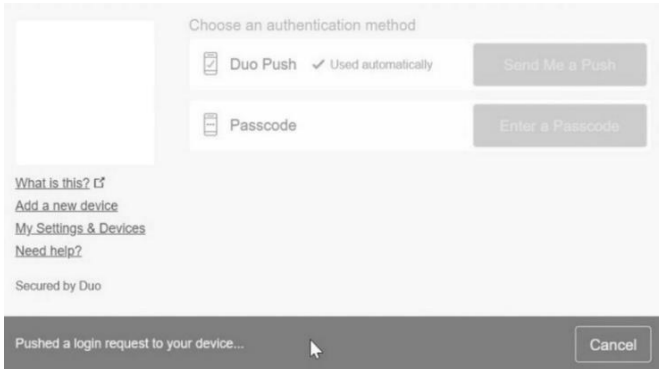

Рис. 10. Генерування коду за допомогою Cisco Duo

Після цього користувач отримує доступ до власного облікового аккаунту з секретною інформацією (рис. 11).

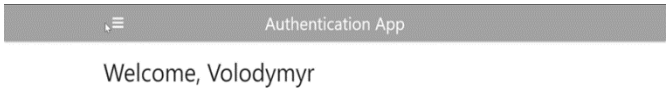

Рис. 11. Обліковий запис користувача після успішної автентифікації

ВИСНОВКИ

Розгорнуто актуальність використання багатофакторної автентифікації у ВЕБ-застосунках в технологіях Індустрії 4.0. Проаналізовано розвиток підходів до реалізації багатофакторної аутентифікації у ВЕБ-застосунках. Проаналізовано основні загрози системі аутентифікації та відповідні механізми і технології безпеки на їх протидію і, на цій основі, створено системну модель багатофакторної безпечної автентифікації у ВЕБ-застосунку. Розглянуто види криптографічних протоколів автентифікації у ВЕБ-застосунках, застосування яких уможливить безпечний обмін даних за профілем конфіденційності. Представлено алгоритмічно-програмну реалізацію системи безпечної багатофакторної автентифікації у ВЕБ-застосунках за трьома факторами: знань, властивостей, володіння мовою програмування JavaScript.

ЛІТЕРАТУРА

[1] Yurchak Oleksandr. "Ukrayins'ka stratehiya Industriyi 4.0 – 7 napryamiv rozvytku" [Електронний ресурс] Режим доступу: https://industry4-0-ukraine.com.ua / 2019 / 01 / 02/ukrainska-strategiya-industrii-4-0-7-napriamkiv-rozvutku.

[2] Стратегія кібербезпеки України. [Електронний ресурс]. Режим доступу: https: // zakon.rada.gov.ua/ laws/show/447/2021#n12.

[3] Програма EU4Digital: Кібербезпека – Схід. [Електронний ресурс]. Режим доступу: https://eufordigital.eu / uk / discover-eu/eu4digital-improving-cyber-resilience- in - the - eastern - partnership - countries/.

[4] Дудикевич В.Б. Системна модель інформаційної безпеки “розумного міста” / В.Б. Дудикевич, Г.В. Микитин, М.О. Галунець // Системи обробки інформації. 2020. Випуск 2(161). С. 93-98.

[5] Дудикевич В.Б. Елементи безпеки “розумного дому” / В.Б. Дудикевич, Г.В. Микитин, Д.В. Васильєв // Сучасна спеціальна техніка. 2020. № 4. С. 35-47.

[6] Yuriy Bobalo, Valeriy Dudykevych, Galyna Mykytyn, Taras Stosyk Paradigm of Safe Intelligent Ecological Monitoring of Environmental Parameters.CEUR Workshop Proceedings, 2021, pp. 244-249 (Proceedings of the 3rd International Conference on Information Security and Information Technologies (ISec-IT 2021) co-located with 1st International Forum "Digital Reality" (DRForum 2021), Odesa, Ukraine, September 13-19, 2021 (pp. 244-249) // http://ceur-ws.org/Vol-3200/; [Електронний ресурс] Режим доступу: http: / / ceur-ws.org / Vol-3200 / paper35. pdf].

[7] Дудикевич В.Б. Захищений обмін інформацією в безпровідних мережах центру інформаційного забезпечення / В.Б. Дудикевич, Г.В. Микитин, М.В. Ленник // Сучасна спеціальна техніка. 2021. № 2. С. 7-19.

[8] Kovalan K., Omar S. Z., Tang L., Bolong J., Abdullah R., Ahmad G., Akmar H., Pitchan M. A. A Systematic Literature Review of the Types of Authentication Safety Practices among Internet Users. The Scientific

Annals of Computer Science, 2021, vol 31 (1), pp. 23-29.
[9] Mathew G., Thomas S., PG Scholar. A novel multi-factor authentication system ensuring usability and security, The Journal arXiv of Computer Science, 2021.
[10] AlJanah, S., Zhang, N., & Tay, S. W. A Multifactor Multilevel and Interaction Based (M2I) AuthenticationFramework for Internet of Things (IoT) Applications. IEEE Access, 2022, vol 10, pp. 47965-47996.
[11] Ahmed S., Mahmood Q. An authentication based scheme for applications using JSON web token. International Conference on Computer and Information Sciences (ICCIS), 2021, pp. 1-6.
[12] Drakonakis K., Ioannidis S., Polakis J. The Cookie Hunter: Automated Black-box Auditing for Web Authentication and Authorization Flaws. ACM SIGSAC Conference on Computer and Communications Security (CCS '20), 2020, pp. 1953-1970.
[13] Ben Fredj, Cheikhrouhou O., Krichen M., Hamam H., Derhab A. An OWASP Top Ten Driven Survey on Web Application Protection Methods. International Conference on Cyber Security and Protection of Digital Services (CRiSIS), 2021, pp. 189-201.
[14] Erdodi L., Zennaro F. M. The Agent Web Model: modeling web hacking for reinforcement learning. International Journal of Information Security volume, 2022, vol 21, pp. 293-309.

TO THE ISSUE OF SECURE MULTIFACTOR AUTHENTICATIONIN WEB APPLICATIONS

The main segments of the smart city infrastructure using authentication in the security vector of Industry 4.0 technologies are considered. Approaches to secure authentication, in particular in WEB applications, are analyzed. A comparison of authentication methods in WEB applications by requirements and level of data security is made. Authentication threats, mechanisms and technologies of protection are analyzed and, on this basis, a system model of secure multifactor authentication in a WEB application based on the concept of "object – threat – protection" according to the structure "WEB page – WEB server – database" is created. An algorithmic and software implementation of a secure multi-factor authentication system in a WEB application based on the use of the SHA-1 cryptographic hash function and the AES symmetric message encryption algorithm using the JavaScript programming language is developed. The practical implementation of a step-by-step algorithm for multifactor authentication in WEB applications by factors such as login and password, fingerprint, and smartphone is presented.
Keywords: multifactor authentication, security, WEB application, system model, hash function, message encryption algorithm.

Дудикевич Валерій Богданович, д.т.н., професор, завідувач кафедри Національного університету «Львівська політехніка», Львів, Україна.
Valerii Dudykevych, Doctor of Technical Sciences, Professor, Head of Department of Lviv Polytechnic National University, Lviv, Ukraine.
E-mail: vdudykev@gmail.com.
Orcid ID: 0000-0001-8827-9920.

Микитин Галина Василівна, д.т.н., професор, професор кафедри Національного університету «Львівська політехніка», Львів, Україна.
Halyna Mykytyn, Doctor of Technical Sciences, Professor, Professor of Department of Lviv Polytechnic National University, Lviv, Ukraine.
E-mail: cosmos-zirka@ukr.net.
Orcid ID: 0000-0003-4275-8285.

Насилевський Володимир Павлович, інженер-програміст компанії "SoftServe", Львів, Україна.
Volodymyr Nasylevskyi, Software Engineer at SoftServe, Lviv, Ukraine.
E-mail: bobbyf4de@gmail.com.
Orcid ID: 0009-0003-0203-4087.

Фігурняк Володимир Русланович, Магістрант, Національний університет «Львівська політехніка», Львів, Україна.
Volodymyr Fihurniak, Master's student, Lviv Polytechnic National University, Lviv, Ukraine.
E-mail: volodymyr.fihurniak@gmail.com.
Orcid ID: 0009-0005-6695-0521.

DOI: 10.18372/2410-7840.25.17757
УДК 004.054

МЕТОД ФОРМУВАННЯ ЕТАЛОННОГО СУБДОВКІЛЛЯ ДЛЯ ВИЯВЛЕННЯ ФІШИНГОВИХ URL-АДРЕС

Анна Корченко, Євгенія Іванченко, Сатибалдієва Феруза, Жумангалієва Назим

Збільшення та удосконалення кібератак на інформаційні системи зростає щорічно, а використання сучасних систем виявлення вторгнень дозволяє швидко реагувати на нові види кібератак та вдосконалювати існуючі