УДК 004.056.5 **DOI:10.30837/rt.2023.3.214.03**

С.О. КОЛОМІЙЦЕВ, О.В. СЄВЄРІНОВ, канд. техн. наук,
В.М. ФЕДОРЧЕНКО, канд. техн. наук, В.М. СУХОТЕПЛИЙ

АНАЛІЗ ПЛАГІНІВ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ДЛЯ СИСТЕМИ WORDPRESS

Вступ

За даними компаній W3Techs і Website Rating, що займаються веденням статистики різних технологій в Інтернеті, станом на початок 2023 р. в світі нараховується приблизно 1,97 мілрд веб-сайтів і з кожним роком ця кількість зростає [1]. 68,4 % всіх сайтів працюють під управлінням якоїсь системи управління контентом (Content Management System, CMS) [2].

Найпопулярніші CMS представлені в табл. 1 [2].

Таблиця 1

Найпопулярніші системи управління контентом

№ з/п	CMS	Доля ринку	№ з/п	CMS	Доля ринку
1	WordPress	63.1%	6	Drupal	1.7%
2	Shopify	5.8%	7	Adobe Systems	1.6%
3	Wix	3.7%	8	PrestaShop	1.2%
4	Squarespace	3%	9	Google Systems	1.1%
5	Joomla	2.6%	10	Bitrix	1%

Всі інші CMS, яких налічується сотні, мають долю ринка менше 1 %. Як видно зі статистики, WordPress є найпопулярнішою в світі системою управління сайтом. Через таку популярність WordPress також є системою, на долю якої приходиться найбільша кількість атак. Кожного дня відбувається майже 30,000 атак на веб-сайти, 90 % з яких приходиться на WordPress [3, 4]. Для зламу цієї системи розроблено безліч спеціалізованого програмного забезпечення. Загалом, WordPress достатньо надійна і захищена система, але тим не менш, деякі недоліки роблять її вразливою перед такими типами атак, як атака зі словником і атака методом повного перебору. Якщо врахувати використання слабких або розповсюджених паролів, то успішність атак у більшості випадків це лише питання часу. У пошуку варіантів вирішення цієї проблеми, власники або адміністратори сайтів використовують додаткове стороннє програмне забезпечення (плагіни).

Плагін – це додаткове програмне забезпечення, яке написане сторонніми розробниками для додавання нового функціоналу або зміни існуючого [5]. В теорії, плагіни допомагають швидко і безкоштовно вирішити на сайті певні питання. Але на відміну від ядра системи, розробкою якого займається команда професіоналів, розробкою плагінів можуть займатися всі бажаючі. Тобто, програмісти з будь яким рівнем кваліфікації. Це призводить до того, що плагіни нерідко додають в систему нові вразливості і не вирішують або вирішують тільки частково ті задачі, для яких були створенні.

Тільки в офіційному репозиторії WordPress знаходиться близько 60,000 тисяч плагінів [6]. Працівники компанії фізично не мають змоги слідкувати за безпекою і якістю такої кількості плагінів. Під час додавання в репозиторій нового плагіна, співробітниками WordPress виконується лише поверхнева перевірка типових загроз в програмному коді. А після затвердження плагіна, його оновлення і будь які зміни в коді взагалі не перевіряються. Подальша модерація здійснюється лише постфактум, після скарг від користувачів, які вже постраждали.

Всі ці фактори спонукають до ретельного аналізу плагінів перед їх використанням. Особливо це стосується плагінів для двофакторної автентифікації (ДФА), на які покладають

надії у вирішенні питань, пов'язаних з захистом адміністративної частини сайту від несанкціонованого доступу [7].

Метою статті є аналіз існуючих плагінів двофакторної автентифікації для оцінки їх ефективності.

Захищеність WordPress від несанкціонованого доступу

Проведений аналіз показав, що після інсталяції на веб-сервер системи WordPress, за замовчуванням сайт не має суттєвого захисту від несанкціонованого доступу [8]. Крім відсутності механізмів захисту, деякі технічні рішення в цій системі навпаки допомагають зловмисникам пришвидшити процес отримання доступу.

Виявлено наступні проблеми:

1. Відсутність обмежень на кількість спроб авторизації.
2. Підказки на сторінці авторизації, що допомагають перевірити правильність вводу логіна.
3. Доступність до REST API, що допомагає знайти логіни користувачів.
4. XML-RPC, що допомагає перевірити логін і пароль в обхід сторінки авторизації.

Звісно, всі ці проблеми мають варіанти вирішення, але для цього, по-перше, треба знати про їх наявність, а по-друге, мати навички з програмування на PHP і досвід роботи з самою системою WordPress. А так як WordPress позиціонується як “рішення з коробки”, для людей без спеціальної технічної підґотовки всі його типові проблеми можна в повному обсязі виявити на абсолютній більшості веб-сайтів.

На рис. 1 зображено приклад того, як зловмисник може перевірити логін користувача на сторінці авторизації.

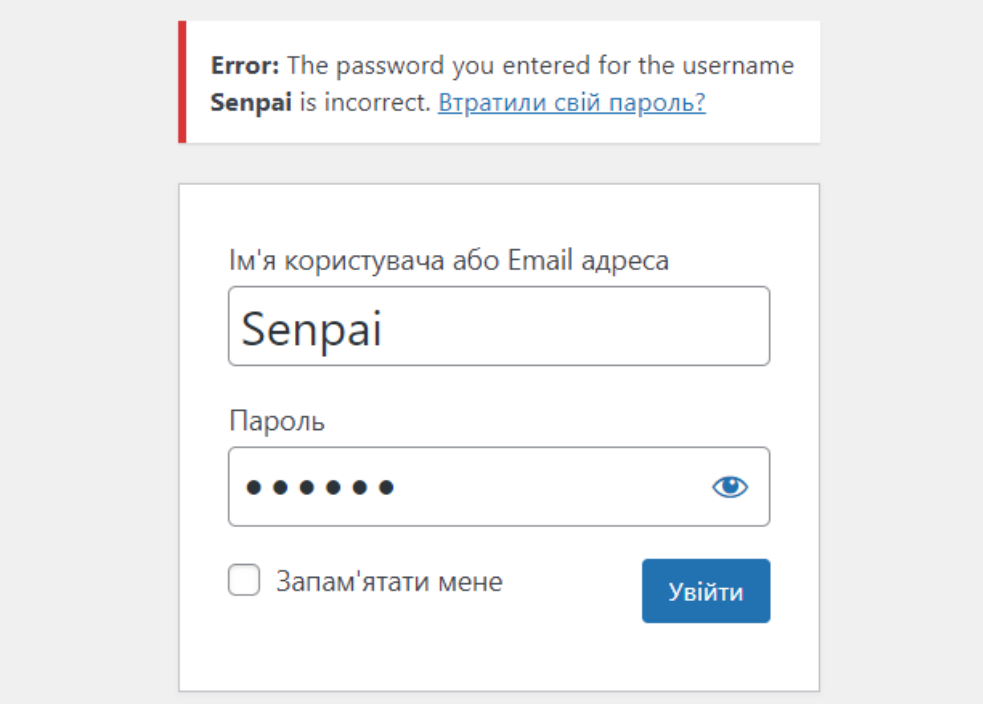

Рис. 1. Підказки на сторінці авторизації

Якщо було введено невірний і логін і пароль, зловмисник побачить повідомлення про те, що користувача з таким логіном в системі не існує. Але якщо логін вірний, то зловмисник побачить повідомлення про те, що для користувача з таким логіном введено невірний пароль. Таким чином, використовуючи підказки, зловмисник може дізнатися логіни всіх користувачів і адміністраторів сайту. Знаючи вірний логін і не маючи обмежень у кількості спроб авторизації, зловмисник отримує достатньо високу імовірність на підбір пароля і отримання несанкціонованого доступу.

Розробники WordPress знають про таку проблему, але навмисно її не виправляють. На їх думку, такі підказки допомагають справжнім користувачам, які забули свої дані, і користі від цих повідомлень більше ніж проблем.

На рис. 2 зображено приклад того, яким чином можна прямо в браузері перевірити існуючих користувачів, просто відкривши певну технічну сторінку.

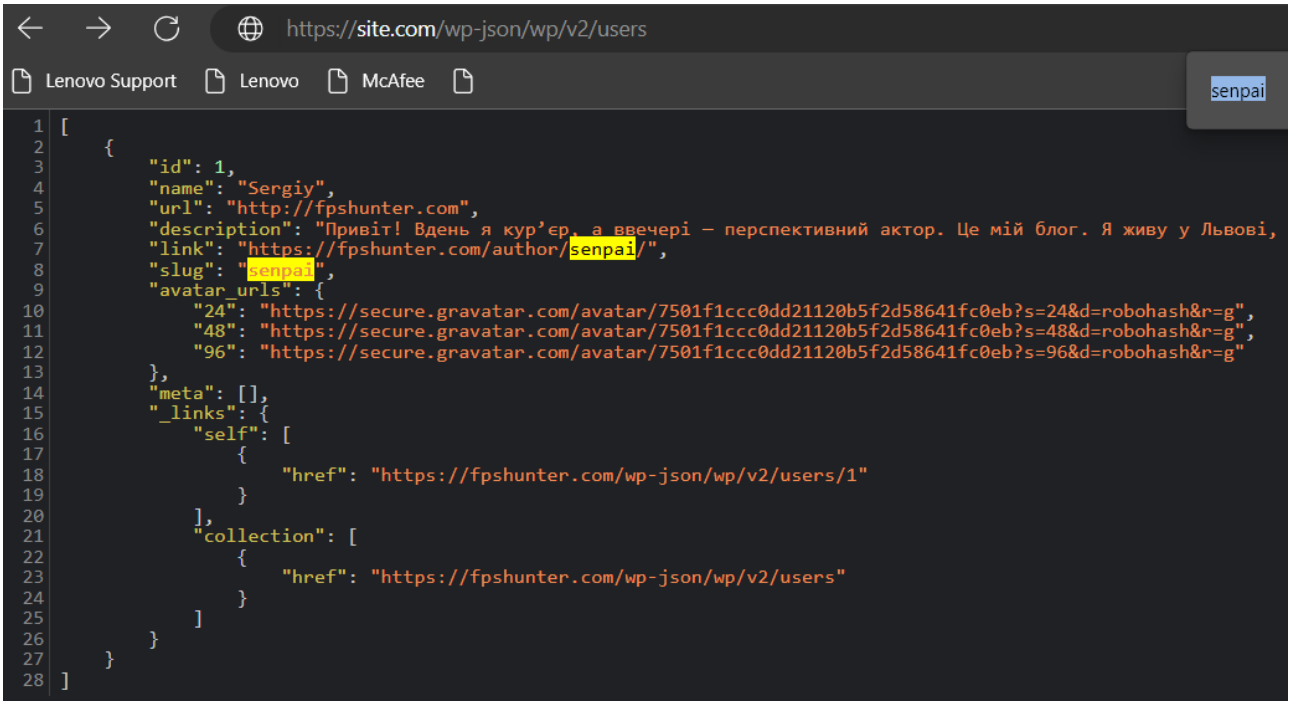

Рис. 2. Пошук логінів користувачів через REST API

Через REST API можна знайти логін користувача і його ідентифікатор в базі даних. Ідентифікатор під номером 1 вказує на те, що це перший зареєстрований користувач, який майже зі стовідсотковою імовірністю має роль адміністратора.

Аналіз плагінів для ДФА

Єдиний спосіб захистити сайт від несанкціонованого доступу – це використання плагінів, що додають двофакторну автентифікацію і виправляють вразливості системи.

Двофакторна автентифікація (ДФА) є типом багатофакторної автентифікації та представляє собою технологію, що забезпечує ідентифікацію користувачів за допомогою комбінації двох різних компонентів [9, 10].

WordPress має велику кількість ДФА плагінів. Але досліджувались тільки ті, що знаходяться в офіційному репозиторії, мають значну кількість користувачів і активно підтримуються розробниками. Кожен з розглянутих плагінів був встановлений на веб-сайт з останньою версією WordPress. Після чого були проведені дослідження з метою оцінити їх ефективність.

Список плагінів над якими проводились дослідження [5]:

1. WP 2FA.
2. Two Factor Authentication.
3. Defender Security.
4. Login Lockdown.
5. Wordfence Login Security.
6. Two Factor (2FA) Authentication via Email.
7. Trusona for WordPress.
8. DoLogin Security.

9. OTP Authenticator.
10. WebAuthn Provider for Two Factor.
11. 1-Click Login.
12. Orion SMS OTP Verification.
13. WP – SMS OTP Login.
14. OwnID Passwordless Login.

При дослідженні для пошуку загроз та вразливостей використовувалась програма WPScan, що входить до дистрибутиву Kali Linux.

WPScan – розроблена виключно для аналізу сайтів, що працюють на системі WordPress і має найбільшу базу загроз та вразливостей, що стосуються цієї системи. Програма створена для спеціалістів з кіберзбезпеки, але через свою ефективність, найбільшу популярність отримала саме серед кіберзлочинців.

Під час дослідження після встановлення кожного плагіна виконувались нова перевірка і спроба атаки зі словником. Мета – перевірити саму можливість проведення атаки, яку і повинні заблокувати ДФА плагіни. Тому, для зменшення часу роботи програми пароль навмисно обирався простим.

На рис. 3 зображено приклад налаштування і запуску WPScan.

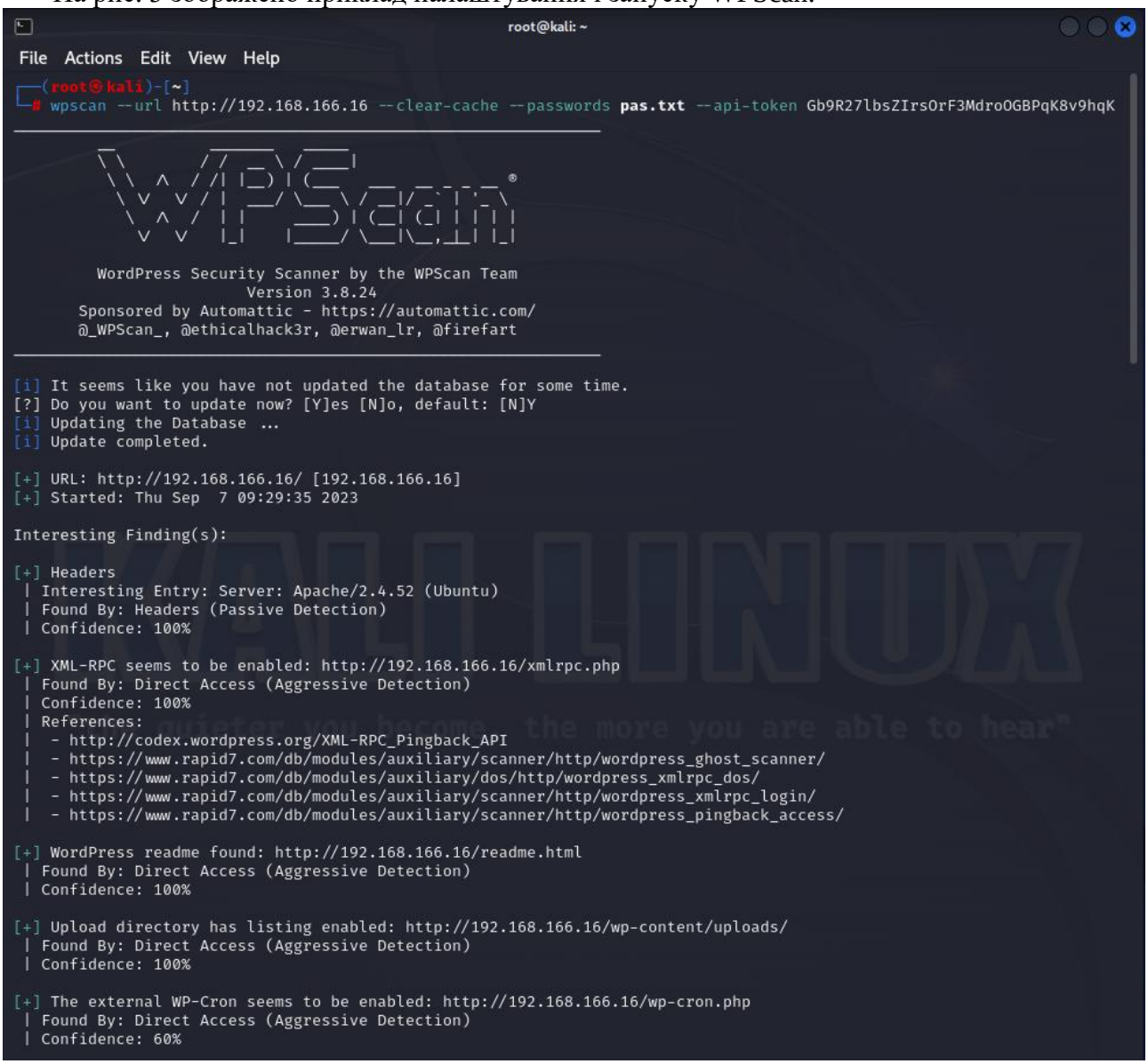

Рис. 3. Запуск роботи WPScan

WPScan вміє проводити атаку зі словником двома методами. Перший – атака безпосередньо на сторінку авторизації: відправка запитів на файл wp-login.php. Другий – атака через протокол XML-RPC: відправка запитів на файл xmlrpc.php. За замовчуванням, WPScan атакує сторінку авторизації, але якщо такий спосіб заблоковано, програма автоматично перемикається на другий метод. Можна обрати і конкретний метод проведення атаки.

На рис. 4 зображено результат успішної атаки.

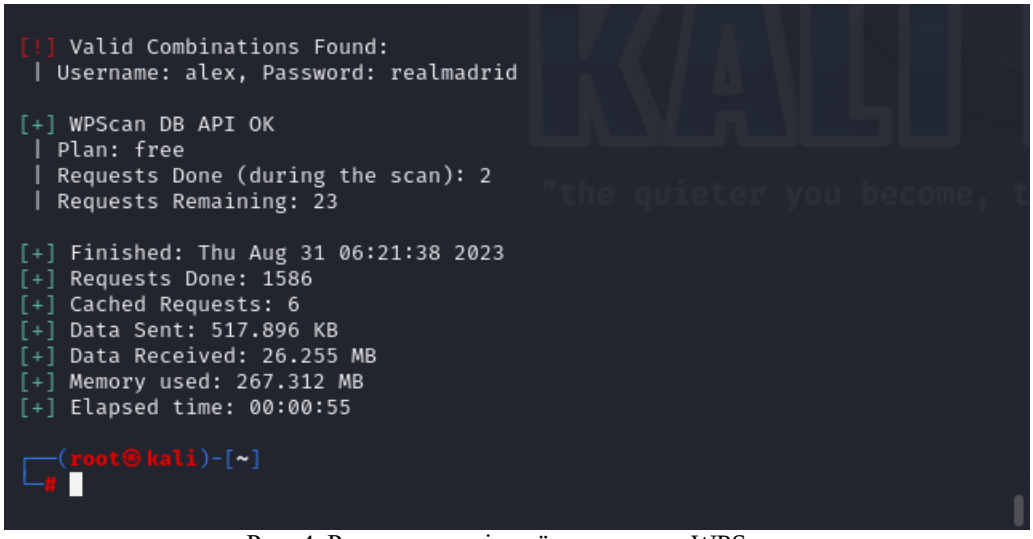

Рис. 4. Результат успішної атаки через WPScan

За результатами досліджень було виявлено наступне. Всі розглянуті плагіни в повній мірі захищають веб-сайт, якщо атака відбувається на сторінку авторизації. Але якщо атака відбувається через протокол XML-RPC, тільки один плагін, а саме Wordfence Login Security, здатен заблокувати таку атаку. У всіх інших випадках результат атаки був успішним.

XML-RPC – це протокол для віддаленого виклику процедур, він зберігся у WordPress з часів повільного інтернету, коли сайтом було простіше керувати через десктопні застосунки. Наразі XML-RPC використовується тільки в окремих випадках, а загалом системою не використовується. Сьогодні це лише додаткова вразливість, яку активно використовують кіберзлочинці. На файл xmlrpc.php можна без обмежень відправляти запити і отримувати відповіді про успішність авторизації. Таким чином, двофакторна автентифікація, яка додається плагінами на сторінку авторизації, ніяк не запобігає можливості провести атаку (рис. 5).

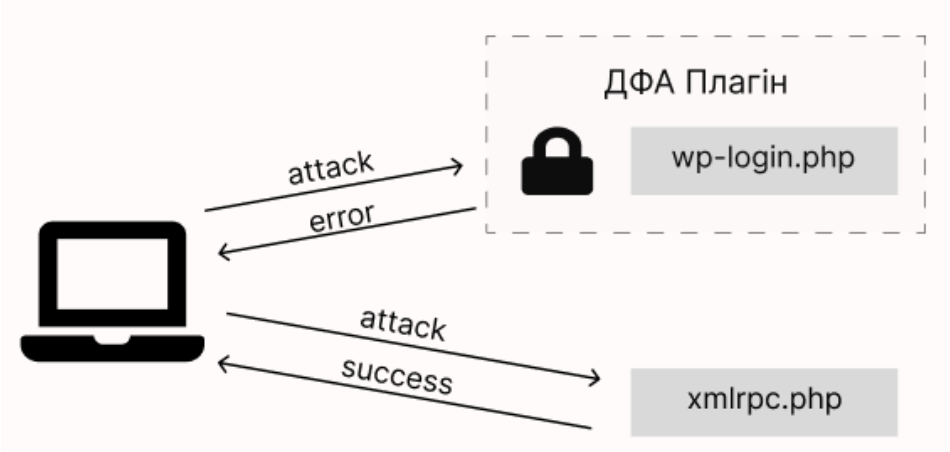

Рис. 5. Вектори атак

Для WordPress існують окремі плагіни, які вирішують виключно проблему XML-RPC. Але середньостатистичний користувач немає уявлення навіть про існування такої проблеми,

тому функціонал для відключення XML-RPC має бути присутнім саме у плагінах для двофакторної автентифікації, бо без цього їх використання не дає повноцінного захисту. Тільки розробники плагіна Wordfence Login Security врахували цю вразливість і реалізували функціонал для її вирішення.

Висновки

Динаміка зростання кількості веб-сайтів і велика доля ринку, що належить системі WordPress, спонукають до необхідності ретельного аналізу плагінів, які повинні забезпечувати захищеність цієї системи. Результати дослідження показали, що більшість ДФА плагінів не забезпечують захист системи в повній мірі. Більшість розробників концентрує увагу виключно на сторінці авторизації. Загалом, всі справляються з її захистом, але разом з цим ігнорують або не знають, як саме програми проводять атаки з технічної точки зору. Це пов'язано з тим, що розробка плагінів, як правило, не є комерційною діяльністю. Розробкою в основному займаються ентузіасти з різним рівнем кваліфікації на добровільній основі і без ретельного вивчення проблеми.

Кожен розглянутий плагін використовується на десятках, а в деяких випадках і на сотнях тисячах веб-сайтів. В результаті сотні тисяч власників сайтів переконані в тому, що вони в повній мірі захищені від несанкціонованого доступу, але як показало дослідження, це не відповідає дійсності.

Список літератури:

1. Website Rating [Електронний ресурс]. Режим доступу: https://www.websiterating.com/research/internet-statistics-facts/
2. W3Techs [Електронний ресурс]. Режим доступу: https://w3techs.com/technologies/overview/content_management
3. Website Rating [Електронний ресурс]. Режим доступу: https://www.websiterating.com/research/cybersecurity-statistics-facts/
4. Сєвєрінов О.В., Хрєнов А.Г., Поляков А.О. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі // Системи обробки інформації. 2015. № 9. С. 101–104.
5. Developer WordPress [Електронний ресурс] Режим доступу: https://developer.wordpress.org/plugins/intro/what-is-a-plugin/
6. Репозиторій плагінів WordPress [Електронний ресурс]. Режим доступу: https://wordpress.org/plugins/
7. Сєвєрінов О.В.; Баклан Я.А. Аналіз рівня безпеки web-ресурсів. 2022. PhD Thesis.
8. Wordpress Codex [Електроний ресурс]. Режим доступа: https://codex.wordpress.org/Main_Page
9. Сєвєрінов О.В., Кліпоносова В.С. Автентифікації користувачів веб-ресурсів. 2022. PhD Thesis.
10. Ayoade O., Afolabi A. S., Awelewa A. T. A Review of Two Factor Authentication // International Journal of Computer Science and Information Security. 2018. Vol. 16, no. 6. P. 35–42,

Надійшла до редколегії 10.09.2023

Відомості про авторів

Коломійцев Сергій Олександрович – Харківський національний університет радіоелектроніки, студент, кафедра безпеки інформаційних технологій; Україна; e–mail: girbest@gmail.com

Сєвєрінов Олександр Васильович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: oleksandr.sievierinov@nure.ua; ORCID: https://orcid.org/0000-0002-6327-6405

Федорченко Володимир Миколайович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри електронних обчислювальних машин, факультет комп'ютерної інженерії та управління, Україна; e-mail: volodymyr.fedorchenko@nure.ua; ORCID: https://orcid.org/0000-0001-7359-1460

Сухотеплий Владислав Миколайович – Харківський національний університет Повітряних Сил імені Івана Кожедуба, старший викладач кафедри радіоелектронних систем пунктів управління Повітряних Сил, Україна; e-mail: vladislav181168@gmail.com; ORCID:https://orcid.org/0000-0002-2566-4167