Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

рівень вищої освіти другий (магістерський)

Метод двофакторної автентифікації на CMS WordPress
(тема)

Виконав: Акшенцев М.О.
(прізвище, ініціали)

студент 2 курсу, групи БДІРм-20-1

Спеціальність 125 Кібербезпека
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва освітньої програми)

Керівник Зав. каф. Халімов Г.З.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Халімов Г.З.
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)
Кафедра Безпеки інформаційних технологій
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна, або освітньо-наукова)

Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав.кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Акшенцеву Максиму Олександровичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Метод двофакторної автентифікації на CMS WordPress*
затверджена наказом по університету від "29" листопада 2021 р. № 1801Ст
2. Термін подання студентом роботи до екзаменаційної комісії _____
3. Вихідні дані до роботи
1) Існуючі плагіни безпеки для CMS WordPress, алгоритми двофакторної автентифікації.
2) 20. Дослідження зі зручності використання п'яти методів двофакторної автентифікації / [К. Різ, Т. Сміт, Д. Датсон та ін.] // П'ятнадцятий симпозіум на приватності та безпеці, що можливо використовувати / [К. Різ, Т. Сміт, Д. Датсон та ін.]. – Санта-Клара, Каліфорнія: USENIX, 2019. – С. 357–370..
4. Перелік питань, що потрібно опрацювати в роботі
1) Плагіни безпеки CMS WordPress
2) Методи забезпечення безпеки веб-сайтів на основі CMS WordPress
3) Захист веб-сайтів на основі CMS WordPress від атак грубою силою
4) Механізми однофакторної автентифікації
5) Механізми двофакторної автентифікації
6) Зручність використання методів двофакторної автентифікації
7) Опис програмної реалізації плагіну безпеки для WordPress
5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій
5.1. Інтерфейс імітованого банківського веб-сайту
5.2. Час, необхідний для автентифікації при використанні
5.3. Оцінка SUS для п'яти других факторів автентифікації
5.4. Час налаштування п'яти других факторів автентифікації
5.5. Меню встановлення плагінів
5.6. Активація плагіну

5.7. Меню налаштування ReCaptcha до отримання ключів
5.8. Налаштування модулю ReCaptcha
5.9. Меню, де зберігаються ключ сайту та секретний ключ
5.10. Меню адміністраторської панелі для ключів
5.11. Меню зміни посилань
5.12. Додаток Google Authenticator
5.13. Меню створення користувача
5.14. Оновлена сторінка входу з полем для двофакторної автентифікації
5.15. Сторінка налаштування двофакторної автентифікації
5.16. Меню додатку Google Authenticator
5.17. Меню Google Authenticator з активованою автентифікацією

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Отримання завдання*	01.09.2021	
2	*Пошук літератури*	02-16.09.2021	
3	*Аналіз зібраних даних*	17.09-01.10.2021	
4	*Аналіз плагінів безпеки*	02-16.10.2021	
5	*Аналіз алгоритмів двофакторної автентифікації*	17-31.10.2021	
6	*Програмна реалізація плагіну безпеки*	01-15.11.2021	
7	*Оформлення пояснювальної записки*	17.09-30.11.2021	

Дата видачі завдання _01_ ___вересня____2021 р.

Студент _____
(підпис)

Керівник роботи (проекту)_____ Зав. каф._Халімов Г.З._
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить: 95 сторінок, 17 рисунків, 9 таблиць, 1 додаткок, 40 джерел.

Об'єктом дослідження є засоби забезпечення безпеки веб-ресурсів на основі системи управління вмістом WordPress, зокрема, програмні додатки для них – плагіни.

Предметом досліджень є двофакторна автентифікація для забезпечення безпеки веб-сайтів, що базуються на CMS WordPress.

Метою дипломної роботи є розробка програмних додатків, що підключаються до системи управління вмістом WordPress для захисту інтернет-сторінок та двофакторної автентифікації як одного з найбільш ефективних засобів захисту.

Методи дослідження: порівняльний аналіз, програмна реалізація плагіну безпеки WordPress.

Проведено аналіз існуючих плагінів безпеки WordPress, їхньої функціональної складової та цінової політики. Також було досліджено ефективність двофакторної автентифікації як методу забезпечення безпеки веб-сайтів.

Відповідно до поставленої мети у дипломній роботі вирішуються такі задачі:

1) Вивчення засобів забезпечення безпеки, необхідних для розуміння переваг плагінів перед іншими засобами;
2) Аналіз безпосередньо плагінів безпеки;
3) Дослідження алгоритмів двофакторної автентифікації, у тому числі у порівнянні зі звичайною;
4) Реалізація плагіну безпеки WordPress та опис його переваг перед існуючими додатками.

Ключові слова: WORDPRESS, ПЛАГІН БЕЗПЕКИ, ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ, АТАКА ГРУБОЮ СИЛОЮ, ЗАХИСТ ПАНЕЛІ АДМІНІСТРУВАННЯ.

ABSTRACT

The explanatory note contains: 95 pages, 17 figures, 9 tables, 1 appendix, 40 sources.

The object of research of this work are security tools for web resources based on the WordPress content management system, in particular, software applications for them - plugins.

The subject of research is two-factor authentication in the context of security of websites based on CMS WordPress.

The purpose of the work is to develop software applications that connect to the WordPress content management system to protect web pages and two-factor authentication as one of the most effective means of protection.

Research methods: comparative analysis, software implementation of WordPress security plugin.

The analysis of existing WordPress security plugins, their functional component and pricing policy is carried out. The effectiveness of two-factor authentication as a method of ensuring the security of websites was also investigated.

In accordance with the goal in the diploma work, it provides solutions for the following tasks:

1) Analysis of the security tools needed to understand the advantages of plugins over other tools;

2) Analysis of security plugins themselves;

3) Research of algorithms of two-factor authentication, including the comparison with the usual authentication;

4) Implementation of the WordPress security plugin and description of its advantages over existing ones.

Key words: WORDPRESS, SECURITY PLUG, TWO-FACTOR AUTHENTICATION, BRUTE FORCE ATTACK, ADMINISTRATION PANEL PROTECTION.

ЗМІСТ

ВСТУП 8
1 ПЛАГІНИ БЕЗПЕКИ CMS WORDPRESS 11
1.1 Актуальність плагінів безпеки 11
1.2 Порівняльна характеристика плагінів безпеки 16
1.2.1 Плагіни без двофакторної автентифікації 16
1.2.2 Плагіни з двофакторною автентифікацією 25
1.3 Висновки 36
2 СИСТЕМИ АВТЕНТИФІКАЦІЇ У СУЧАСНИХ ПЛАГІНАХ БЕЗПЕКИ ... 38
2.1 Механізм роботи алгоритмів однофакторної автентифікації та їхні недоліки 38
2.1.1 Автентифікація за паролем 40
2.1.2 Автентифікація за смарт-картою та електронним ключом 41
2.1.3 Автентифікація за біометричними параметрами 42
2.1.4 Автентифікація за цифровим сертифікатом 43
2.2 Механізм роботи алгоритмів багатофакторної автентифікації 45
2.2.1 SMS-автентифікація 47
2.2.2 TOTP-автентифікація 47
2.2.3 Автентифікація на основі попередньо згенерованих кодів 48
2.2.4 Автентифікація на основі push-повідомлень 49
2.2.5 Автентифікація на основі ключів безпеки U2F 50
2.3 Висновки 50
3 ОЦІНКА ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ 51
3.1 Умови проведення дослідження 51
3.2 Залежність часу перебування у дослідженні від часу на здійснення автентифікації 57
3.3 Опитування SUS 59
3.4 Опитування учасників 61
3.5 Додаткове лабораторне дослідження 67
3.6 Висновки 73

4 ПРОГРАМНА РЕАЛІЗАЦІЯ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ЯК ПОСЛУГИ ПЛАГІНУ БЕЗПЕКИ 74
4.1 Особливості алгоритму автентифікації, що використовується у плагіні 74
4.2 Переваги програмної реалізації перед існуючими 76
4.3 Налаштування оновленого програмного додатку 77
ВИСНОВКИ 86
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 87
ДОДАТОК А 91

ВСТУП

Негативні наслідки порушення безпеки веб-сайту можуть бути величезними незалежно від розміру бізнесу. За нещодавніми оцінками щоденно зламується 30000-50000 веб-сайтів [1] – і ця кількість підвищується, тому важливість їхньої безпеки стрімко зростає. Забезпечення онлайн-безпеки є життєво важливим для захисту власного веб-сайту та даних на ньому.

Сьогодні більшість людей залежать від веб-сайтів. Вони надають власні імена, дані банківських карток, дати народження, а іноді й паспорти чи ідентифікаційні коди – все це є привабливою метою для кіберзлочинців. Крім того, злам веб-сайту дозволятиме перенаправити трафік користувачів з метою зараження шкідливим програмним забезпеченням. Від захищеності веб-ресурсу також залежіть безпека фізичного обладнання, де той розташовано. За умови його некоректного налаштування злочинці можуть здійснити зараження комп'ютера, що може призвести до великих збитків, оскільки знадобиться як мінімум оплатити послуги з видалення шкідливого програмного забезпечення, а як максимум – повністю замінити обладнання.

Втім, віруси – не єдина причина, за якої безпека веб-сайту має значення. Будь-який злам негативно вплине на репутацію як бізнесу в цілому, так й його власника зокрема. До того ж це грозить великою кількістю простоїв та втратою продуктивності, а звідси – до впущеного прибутку (навіть не враховуючи сценарій, за яким зламаний веб-сайт видаляється з усіх пошукових систем).

Отже, слід запроваджувати проактивні заходи безпеки для забезпечення присутності в Інтернеті. Особливо це стосується веб-ресурсів на базі системи управління вмістом (CMS) WordPress, оскільки вони складають найбільшу частину мережі Інтернет. Для наочності слід навести, що станом на 2021 рік 42.7% усіх веб-сайтів використовували саме WordPress [2]. Крім того, щомісяця вони переглядаються близько 22.17 мільярда разів, коментуються 46.6 мільйона разів, а пошукові запити відносно CMS здійснюються 2.7 мільйона разів [3].

Існує декілька причин такої популярності WordPress:

1) Ця система управління вмістом є відкритим та безкоштовним програмним забезпеченням, що надає можливість кожному користувачу застосувати та налаштувати власний веб-сайт без надлишкових витрат.
2) Вона дозволяє створити будь-який веб-сайт, починаючи з блогів та закінчуючи інтернет-магазинами або повноцінним мережевим

представництвом торгівельного або промислового підприємства. За допомогою додаткових тем та плагінів стає можливим оформити веб-ресурс на будь-який погляд власника, незалежно від бюджету.

3) Редагування в межах WordPress здійснюється за так званим принципом «WYSIWYG», за яким контент має виглядати однаково як для редактора на інформаційній панелі, так й для кінцевого користувача на веб-сайті, що опубліковано. Цей підхід великою мірою спрощує процес його створення та оновлення, підвищуючи його відвідуваність.
4) Робота з веб-сайтом не вимагає від власника жодних навичок програмування, не дивлячись на те, що сама система WordPress використовує чотири мови програмування – HTML, CSS, JavaScript та PHP. Це підвищує кількість її потенційних користувачів, знижуючи поріг входу.

Але популярність системи має свої недоліки – будучи найбільш широко використовуваною CMS у всьому світі, веб-ресурси на її основі є настільки ж популярною мішенню для крадіжки, спроб зламу, встановлення зловмисного програмного забезпечення та атак троянських програм.

Статистика показує, що кожну хвилину кіберзлочинці атакують 90 тисяч веб-ресурсів на основі CMS WordPress, а 83% всіх зламаних веб-сайтів, що використовують системи управління вмістом, мали саме WordPress. Серед зламаних веб-сайтів 8% мали слабкі паролі від облікових записів адміністраторів, 61% використовували застарілі версії системи, 52% використовували небезпечні чи підроблені плагіни, а 11% – ненадійні теми. [4]

Не враховуючи втрату відвідувачів та зараження їхніх комп’ютерів через недогляд власника веб-ресурсу, подібні злами загрожують його повним видаленням зі списку видач пошуковими системами на кшталт Google. За статистикою, ця компанія щотижня заносить в чорний список 70 тисяч веб-сайтів через проблеми з безпекою [4].

Отже, важливість забезпечення безпеки веб-сайтів є прямо пропорційною популярності компонентів, що використовуються при їхньому створенні, та самих веб-сайтів – особливо на основі CMS WordPress. Тому в цій роботі буде представлено власний плагін безпеки, що включає в себе провідну технологію багатофакторної автентифікації.

Об’єктом дослідження роботи є засоби забезпечення безпеки веб-ресурсів на основі системи управління вмістом WordPress, зокрема, програмні додатки для них – плагіни.

Предметом досліджень є двофакторна автентифікація для забезпечення безпеки веб-сайтів, що базуються на CMS WordPress.

Метою роботи є розробка програмних додатків, що підключаються до системи управління вмістом WordPress для захисту інтернет-сторінок та двофакторної автентифікації як одного з найбільш ефективних засобів захисту.

Використано такі методи дослідження, як порівняльний аналіз та програмна реалізація плагіну безпеки WordPress.

Проведено аналіз існуючих плагінів безпеки WordPress, їхньої функціональної складової та цінової політики. Також було досліджено ефективність двофакторної автентифікації як методу забезпечення безпеки веб-сайтів. Відповідно до поставленої мети у роботі вирішуються такі задачі:

1) Вивчення засобів забезпечення безпеки, необхідних для розуміння переваг плагінів перед іншими засобами;
2) Аналіз безпосередньо плагінів безпеки;
3) Дослідження алгоритмів двофакторної автентифікації, у тому числі у порівнянні зі звичайною;
4) Реалізація плагіну безпеки WordPress та опис його переваг перед існуючими додатками.

1 ПЛАГІНИ БЕЗПЕКИ CMS WORDPRESS

1.1 Актуальність плагінів безпеки

Плагіни – це програмне забезпечення, що підключається, використовуване для розширення чи покращення існуючого функціоналу того чи іншого додатку. Тема або «скін» – це різновид плагіну, що містить додаткові або змінені деталі графічного вигляду, націлені на поліпшення графічного інтерфейсу користувача, який можливо застосувати до певного програмного забезпечення та веб-сайтів, щоб відповідати цілям, темі або смакам різних користувачів.

Основна програма надає функціонал, який є доступним для використання плагіном, включаючи спосіб реєстрації плагінів у головній програмі та протокол для обміну даними з плагінами. Плагіни залежать від функцій, які надає головна програма, і зазвичай не працюють самі по собі. І навпаки, хост-додаток працює незалежно від плагінів, що дає кінцевим користувачам можливість динамічно додавати та оновлювати плагіни без необхідності вносити зміни до основної програми.

Програмісти зазвичай реалізують плагіни як спільні бібліотеки, які динамічно завантажуються під час виконання. Програмне забезпечення для організації інформації HyperCard підтримувало таку функцію, але частіше включала код плагіна власне у її документи. Таким чином, плагін HyperCard став самостійним додатком, який можливо розповсюджувати як єдину сутність, яку кінцеві користувачі могли запускати без необхідності додаткових кроків встановлення.

Програми можуть підтримувати плагіни для таких цілей, як:

- можливість розширити програму для сторонніх розробників;
- підтримка легкого додавання нових функцій;
- зменшення розміру програми без завантаження невикористаних функцій;
- відокремлення вихідного коду від програми через несумісні ліцензії на програмне забезпечення.

До прикладів програмного забезпечення, що підтримує плагіни, відносяться наступні:

- Цифрові робочі аудіостанції та програмне забезпечення для редагування звуку використовують аудіоплагіни для створення, обробки або аналізу звуку. Прикладами таких систем є Ardour, Audacity, Cubase, FL Studio, Logic Pro X і Pro Tools;

- Поштові клієнти використовують плагіни для розшифровки та шифрування електронної пошти. Прикладом таких плагінів є Pretty Good Privacy;
- Емулятори відеоігрових консолей часто використовують плагіни для модуляції окремих підсистем пристроїв, які вони прагнуть емулювати. Наприклад, емулятор PCSX2 використовує відео, аудіо, оптичні тощо плагіни для відповідних компонентів PlayStation 2;
- Графічне програмне забезпечення використовує плагіни для підтримки форматів файлів і обробки зображень. Це може зробити плагін Photoshop;
- Медіаплеєри використовують плагіни для підтримки форматів файлів і застосування фільтрів. foobar2000 (sic), GStreamer, Quintessential, VST, Winamp, XMMS є прикладами таких медіаплеєрів;
- Сніфери пакетів використовують плагіни для декодування форматів пакетів. OmniPeek є прикладом такого аналізатора пакетів;
- Програми дистанційного зондування використовують плагіни для обробки даних від різних типів датчиків; наприклад, Opticks;
- Текстові редактори та інтегровані середовища розробки використовують плагіни для підтримки мов програмування або покращення процесу розробки, наприклад, додатки підтримки Visual Studio, RAD Studio, Eclipse, IntelliJ IDEA, jEdit та MonoDevelop. Сама Visual Studio може бути підключена до інших програм за допомогою Visual Studio Tools for Office і Visual Studio Tools for Applications;
- Веб-браузери історично використовували виконувані файли як плагіни, хоча зараз вони здебільшого не підтримуються. Приклади включають Adobe Flash Player, віртуальну машину Java (для аплетів Java), QuickTime, Microsoft Silverlight та Unity Web Player. (Розширення для браузера, які є окремим типом встановлюваного модуля, все ще широко використовуються.)

Стосовно ж CMS WordPress, плагіни безпеки є одним з найбільш ефективних засобів захисту веб-ресурсів на її основі, але не єдиним. Тому є доцільним навести інші шляхи захисту, а також порівняти їхню ефективність.

В загальному вигляді список методів захисту виглядає так:

1) Безкоштовні плагіни безпеки;
2) Платні плагіни безпеки;

3) Поради з налаштувань, що знаходяться у відкритому доступі у мережі Інтернет;
4) Використання послуг установки та налаштування веб-сайтів.

Далі буде надано характеристику кожного з методів, наведено їхні переваги та недоліки, після чого – порівняно за такими критеріями, як вартість, ступінь безпеки, зручність у використанні користувачем, захист від доступу до панелі адміністрування (як найбільш ймовірна мета зловмисників) та наявність додаткових опцій для підвищення безпеки.

Безкоштовний плагін надає ефективний захист на базовому рівні, не передбачаючи при цьому захисту від специфічних вразливостей, є зручним для користувача, не вимагає від останнього навичок програмування, є легким у налаштуванні та безкоштовним. Проблема в тому, що часто розробники приховують основні функції захисту (унеможливлюючи здійснення достатньо просунутого налаштування), тому плагін може не спрацювати проти досвідченого кіберзлочинця. До того ж безкоштовні плагіни є некомерційною розробкою, отже, вони нерідко не мають підтримки, своєчасних оновлень і поліпшень, а також в них можуть бути допущені вразливості.

Крім того, велика частина плагінів є складною у використанні і займає значний час для налаштування. Вони можуть вимагати певного рівня технічних навичок, щоб почати працювати очікуваним образом, а оскільки такий плагін не має необхідного рівня документації та підтримки, залишається сподіватися на допомогу інших користувачів. Запуск такого плагіна може вимагати величезних витрат з точки зору часу, що витрачається, тому користувачі й розглядають їхні платні альтернативи. Втім, для деяких країн з невеликим рівнем доходу подібна опція не є релевантною, навіть якщо розглядати комерційні організації.

Таким чином, безкоштовні плагіни найкраще підходять для невеликих сайтів з малим об’ємом трафіку для фільтрування ботів, що сканують сайт з метою знайти вразливості у ньому. Втім, при цілеспрямованому зламі вони можуть не допомогти [5].

Платні плагіни надають більш ефективний захист, ніж безкоштовні, а також мають велику кількість додаткових функцій, наприклад, для захисту від DDoS-атаки або несанкціонованого редагування файлів налаштування. Втім, часто такі плагіни містять занадто багато налаштувань, коректне встановлення яких займає великий обсяг часу та є обов’язковим для їхньої ефективної роботи. Основною ж проблемою є вартість платних плагінів – в

середньому вона складає від 700 до 13000 гривень на рік, що і є основним стримуючим фактором при виборі цього засобу забезпечення безпеки, оскільки для жителів України це неприпустимо велика ціна. [6, 7] Отже, велика кількість власників веб-сайтів надає перевагу безкоштовним плагінам, не дивлячись на менші функціональні можливості.

Отже, платні плагіни є ефективними, мають велику (часто – занадто велику) кількість захисних опцій, роблячи його громіздким, але здатним забезпечити безпеку на високому рівні. Основним недоліком є велика вартість поданого типу плагінів, а також їхнє розповсюдження за моделлю підписки, що часто зустрічається, тобто замість одноразового придбання клієнт матиме сплачувати велику суму щомісячно або щорічно [7].

До того ж існують частково безкоштовні плагіни. Вони надають певну частину функцій захисту безкоштовно, але для отримання іншої частини доведеться здійснити декілька платежів за моделлю підписки. У списку плагінів, що буде представлено у наступному підрозділі, цінність таких додатків буде розглядатися з точки зору функціональності, що доступна безкоштовно.

Безкоштовні поради з налаштувань, що знаходяться у відкритому доступі мережі Інтернет надають слабкий захист від зламу, а також додають незручності середньому користувачеві. Так, часто надаються рекомендації встановлювати складні, довгі логіни та паролі, не зберігаючи їх на комп’ютері або папері, а також не використовувати підозрілі плагіни. Ці поради дійсно підвищують безпеку веб-ресурсу, але можуть виявитися занадто важкими на практиці – наприклад, є важким запам'ятання довгих та складних паролів без їхнього зберігання, але його зберігання спрощує злам. Аналогічно некоректно обраний плагін є здатним зробити веб-ресурс вразливим, але для захисту від існуючих вразливостей CMS WordPress чи атаки грубою силою плагін все одно є необхідним.

Тому хоча наведені (та схожі за змістом) поради й є ефективними, на практиці їхня реалізація стає вкрай складною або неможливою для звичайного користувача. До того ж, часто способи атаки кіберзлочинців, що включають в себе соціальну інженерію, оновлюються швидше, ніж ці поради, тому навіть за умови їхнього виконання існує сценарій, за яким втратити веб-сайт можливо через один електронний лист, складений особливим чином, знову доказуючи ненадійність людського фактору [8].

Що стосується встановлення та налаштування систем безпеки веб-сайту фахівцями – за статистикою середній спеціаліст вимагає від 500 до

1000 гривень за послугу, що включає в себе встановлення безкоштовного плагіну безпеки, а також застосування декількох порад з відкритого доступу, наведених вище, оскільки фахівці мають відповідні технічні навички та досвід [8].

Це може спрацювати для невеликих веб-сайтів, але не дивлячись на невелику ціну та те, що платіж є одноразовим, результатом стають всі недоліки, властиві безкоштовним плагінам, та, іноді, недостатньо захищена панель адміністрації, що є неприпустимим з точки зору захисту важливих веб-ресурсів.

Існують навіть організації, що спеціалізуються на безпеці веб-сайтів на основі WordPress. Наприклад, компанія WishDesk пропонує:

1) Оновити систему управління вмістом WordPress, що встановлено на веб-сайті, а також плагіни та теми до нього;
2) Надати окремий хостинг для баз даних веб-сайту та настроїти права доступу до неї (якщо існує декілька облікових записів);
3) Видалити шкідливе програмне забезпечення;
4) Надати захист від атак грубою силою через двофакторну автентифікацію, зміну логіну та паролю адміністратора, а також встановити плагін безпеки;
5) Робити щоденні резервні копії;
6) Здійснювати моніторинг веб-сайту [10].

Надання цього пакету послуг безпеки, які користувач здебільшого може виконати самостійно і безкоштовно (або встановити відповідний безкоштовний плагін), коштує близько 500 гривень на годину – це невиправдано велика вартість навіть у порівнянні з платними плагінами. Хоча такі коштовні пропозиції є виключенням з правил, список послуг, що надається, залишатиметься приблизно однаковим у всіх фахівців (нерідко – навіть меншим).

Таким чином, послуги фахівців у середньому стоять дешевше, ніж платні плагіни, але їхня якість відповідає програмному забезпеченню та порадам, використати які можливо без надлишкових трат.

Щоб підвести підсумки переваг та недоліків кожного з представлених засобів забезпечення безпеки веб-сайтів, є доцільним навести наступну таблицю оцінювання, де оцінка «1» – найменша, а «5» – найвища. Засоби буде порівняно за такими критеріями, як вартість засобу, ступінь захисту, що може бути забезпечено ним, а також зручність його використання та/або впровадження:

Таблиця 1.1. Оцінювання засобів забезпечення безпеки веб-сайтів

Засіб	Безкоштовний плагін	Платний плагін	Поради з відкритих джерел	Послуги фахівців
Вартість	5 (безкоштовно)	1 (700-13000 гривень/рік)	5 (безкоштовно)	2 (500-1000 гривень)
Ступінь захисту	4	5	1	4
Зручність	5	3	1	5
Захист від несанкціонованого доступу до панелі адміністрування	3	5	4	3
Додаткові функції з забезпечення безпеки	2	5	2	3
Оцінка	3.8	3.8	2.6	3.4

1.2 Порівняльна характеристика плагінів безпеки

В поданій роботі будуть порівнюватися найбільш популярні плагіни безпеки, але перевага надаватиметься безкоштовним або таким, що пропонують більшу частину функцій захисту безкоштовно, оскільки саме від доступності для кінцевого користувача залежить, чи буде той користуватися засобом, що пропонується. Як було наведено вище, ця причина робить платні плагіни непридатними до використання. Нижче буде розглянуто 24 плагіни, здатні підвисити безпеку веб-ресурсу на основі CMS WordPress у різні шляхи.

Основними критеріями для порівняння плагінів безпеки виступають відомість, оскільки велика кількість користувачів стимулює розробників відповідальніше ставитися до свого програмного забезпечення, а також наявність двофакторної автентифікації як найбільш ефективного засобу захисту адміністративної панелі – найважливішої складової веб-ресурсу.

1.2.1 Плагіни без двофакторної автентифікації

1) All In One WP Security & Firewall

Цей плагін має за мету надати максимальну кількість функцій безпеки. Наприклад, він включає в себе:

- захист облікового запису користувача;
- відстеження невдалих спроб входу від імені власника веб-ресурсу;

- відстеження невдалих спроб входу від імені іншого користувача;
- забезпечення безпеки конфігураційних файлів;
- заборону на використання облікового запису адміністратора, якщо він має стандартний логін – «admin»;
- заборону на використання облікових записів, де логін та ім’я, що відображується, співпадають;
- інструмент для вимірювання вразливості паролів;
- захист від атак грубою силою за таймером, лімітуванням кількості спроб входу та cookie-файлами;
- насильний вивід користувачів з їхніх облікових записів за розкладом;
- моніторинг та журналювання;
- капчу;
- систему ручного ухвалення реєстрації акаунтів;
- резервне копіювання веб-сайту;
- перевірку прав доступу до файлів конфігурації;
- створення чорного списку IP-адрес;
- систему запобігання спаму;
- антивірусне програмне забезпечення;
- блокування копіювання тексту з веб-сайту;
- приховування версій ядра CMS WordPress, плагінів та тем до неї;
- брандмауер;
- захист бази даних.

До того ж розробники акцентують увагу на простому інтерфейсі та безкоштовності. Втім, хоча плагін захищає користувача від атак грубою силою, він не передбачає використання двофакторної автентифікації, що залишає власника веб-сайту вразливим до крадіжки його облікового запису та його неправомірного використання [11].

2) BulletProof Security

BulletProof Security позиціонується як плагін для просунутих користувачів, що пропонує такі функції, як:

- карантин шкідливих програм;
- захист від спаму;
- моніторинг входу;
- автоматичне переривання сесії неактивного користувача;
- резервне копіювання бази даних;
- антивірусне сканування;
- журналювання безпеки та помилок HTTP;

- вбудовані теми;
- автоматичне оновлення ядра WordPress, плагінів та тем до нього;
- заборону слабких паролів;
- сповіщення електронною поштою.

Але він передбачає встановлення великої кількості налаштувань в разі необхідності максимальної захищеності, а також є платним (хоча платіж – одноразовий), що робить його непридатним для середнього користувача. Також не містить функцій двофакторної автентифікації [11].

3) Security Ninja

Security Ninja, окрім іншого, спеціалізується на тестуванні безпеки веб-сайтів та простоті у використанні. Всього плагін пропонує більш за 50 тестів, серед яких:

- тестування на стійкість до атак грубою силою;
- тестування коректності конфігурації веб-сайту;
- тестування на прихованість версії WordPress та плагінів (з метою знизити ймовірність пошуку вразливостей під їхню конкретну версію);
- тестування на актуальність версії WordPress та інших плагінів;
- інші.

Розробники офіційно позиціонують його як «зовсім не складний». Втім, безкоштовно користуватися ним можливо лише 14 днів [11].

4) WP fail2ban

WP fail2ban було створено як плагін для захисту від атак грубою силою. Він підтримує нестандартні для інших додатків функції на кшталт:

- трьох рівнів фільтрації користувачів – м’якого, жорсткого та довільного;
- блокування ботів без логіну (що використовуються для здійснення DDoS-атак);
- підтримки декількох веб-сайтів на основі CMS WordPress одночасно;
- можливості блокування авторизації за логіном;
- можливості блокування користувачів з певними логінами, використовуючи регулярні вирази;
- фільтрації спроб здійснення входу до системи з пустим логіном;
- інтеграції з певними плагінами для текстових форм та проксі-серверами;

- логування коментарів;
- логування повідомлень про цитування коментарів;
- просунуте журналювання (платне).

Інших функцій, включаючи двофакторну автентифікацію, не має [11].

5) iThemes BackupBuddy

Плагін, єдина функція котрого – систематично робити резервні копії веб-сайту в хмарне сховище, що надається розробниками. Це дозволяє швидко відновити його після зламу будь-якого ступеня серйозності. Хоча й позиціонується як плагін безпеки, не має інших функцій та є платним [11].

6) VaultPress

Цей плагін:

- робить щоденні резервні копії за інкрементальною моделлю, тобто за умови існування однієї копії до неї додаються нові та оновлені файли веб-сайту – замість повторного повного копіювання, що підвищує швидкість цього процесу;
- надає власне сховище для резервних копій;
- надає захист від спаму у коментарях та формах для контактування;
- дозволяє здійснювати пошуки по веб-сайту;
- автоматично перевіряє активність на веб-ресурсі на підозрілість на щоденній основі;
- зберігає статистику такої активності для власника веб-сайту.

Зручний у користуванні, але несумісний з актуальними версіями WordPress [11].

7) Astra Web Security

Цей плагін має за мету надати наступний функціонал:

- брандмауер веб-додатків;
- встановлення на веб-сайті як розширення, через що перестає бути потрібним змінювання налаштування DNS;
- захист від SQL-ін’єкцій, атак XSS, LFI та понад 100 інших загроз у режимі реальному часі;
- сканування та видалення вірусних програм;
- блокування ботів;
- блокування та створення білого списку країн;
- блокування та створення білого списку діапазонів IP-адрес;
- профілювання та відстеження IP-адрес;

- запобігання завантаженню шкідливих файлів;
- можливість встановлення обмежень на допустимий розмір файлів, що завантажуються;
- можливість встановлення обмежень на допустимі розширення файлів, що завантажуються;
- ведення обліку активності власника та/або адміністраторів веб-ресурсу;
- блокування автоматичних сканерів вразливостей;
- захист панелі адміністрування від атак грубою силою;
- блокування фальшивих пошукових роботів;
- захист від ін'єкції файлів з використанням Webshell;
- захист від ін’єкції коду;
- захист від несанкціонованого перегляду каталогів;
- захисту від DDoS-атак на прикладному рівні OSI;
- розумна система «honeypot» для перехоплення запитів та маніпуляцій кіберзлочинців;
- обмеження швидкості здійснення веб-запитів;
- автоматичне блокування спаму;
- запобігання крадіжці вмісту веб-ресурсу;
- запобігання спаму коментарів;
- забезпечення безпеки конфігураційного файлу htaccess;
- відсутність затримок при скануванні веб-сайту;
- вбудоване антивірусне програмне забезпечення;
- виправлення наслідків SEO-спаму та SEO-отруєння (включає японські, фармацевтичні або атаки тарабарщиною);
- виправлення несанкціонованих перенаправлень веб-сайту;
- виправлення зламу панелі адміністратора;
- виправлення злому кредитної картки та сторінки оформлення платежу;
- виправлення веб-сайтів, що зазнали атаки «дефейс»;
- видалення бэкдорів;
- забезпечення безпеки бази даних;
- проста у використанні панель управління;
- аналітика загроз;
- погодинна статистика успішних та невдалих спроб отримання доступу до панелі адміністрування;
- можливість створювання білого та/або чорного списків припустимих URL-посилань на веб-ресурсі, а також запитів «GET» та «POST» до нього;

- зберігання інформації про країну походження загрози, браузер, пристрій кіберзлочинця тощо;
- щоденні звіти електронною поштою, що містять підсумок атак, зупинених плагіном;
- сповіщення Slack, що налаштовуються;
- можливість запустити програму «Bug Bounty», що дозволятиме зовнішнім спеціалістам з кібербезпеки проаналізувати веб-ресурс та повідомити його власника без наслідків.

Не дивлячись на наведені переваги, не має безкоштовних планів та двофакторної автентифікації [11].

8) PatchStack

Антивірусне програмне забезпечення з функціями брандмауеру. При встановленні плагін:

- виявляє загрози від інших плагінів та тем;
- здійснює моніторинг вразливостей з інших джерел;
- надає сповіщення про існуючі в межах веб-сайту в режимі реального часу;
- надає пропозиції з покращення безпеки;
- автоматично вирішує знайдені проблеми;
- надає аналітичні дані у вигляді звітів;
- надає доступ до додаткового програмного забезпечення від авторів цього плагінів;
- підтримує декілька веб-сайтів від одного власника, у противагу частому правилу «один користувач – один веб-сайт»;
- активує брандмауер;
- підтримує можливість налаштовувати повідомлення про знайдені та потенційні загрози;
- надає захист від десяти найбільш відомих загроз, що мають статус нульового дня (тобто таких, що офіційно не мають виправлень);
- аналіз заголовків безпеки HTTP;
- аналіз закінчення терміну дії доменного імені та сертифіката SSL.

Має безкоштовний 7-денний пробний період, в іншому також є платним. Не використовує двофакторну автентифікацію [11].

9) MalCare Security WordPress Plugin

Цей плагін також спеціалізується на пошуку та видаленні вірусного програмного забезпечення. Серед можливостей має:

- автоматичне щоденне сканування файлів веб-ресурсу без додаткових дій власника;
- надання власних серверів для сканування з метою запобігти сповільненню роботи веб-сайту;
- автоматичне видалення знайдених вірусних файлів;
- брандмауер;
- обмеження спроб входу з метою захисту від атак грубою силою;
- надання інформаційної панелі для управління користувачами, плагінами та темами;
- маскування даних про плагін безпеки з метою протидії кіберзлочинцям;
- моніторинг швидкості та безперебійності роботи веб-сайту.

Плагін є частково безкоштовним, знижуючи список доступних послуг на безоплатній основі. Не має двофакторної автентифікації [11].

10) Hide My WP

Плагін Hide My WP приховує факт використання системи управління вмістом WordPress, а також включає в себе детектор вторгнень (IDS) для блокування атак на кшталт SQL-ін’єкцій, XSS та інших у реальному часі. Загальний список функцій виглядає так:

- приховування назви теми, плагінів;
- зміна постійних посилань;
- приховування сторінки «wp-admin», URL-адреси для входу тощо;
- блокування прямого доступу до файлів PHP;
- очистка імен класів WordPress;
- дезактивація списку каталогів;
- повідомлення про будь-яку потенційно небажану поведінку на веб-сайті з повною інформацією про ймовірного кіберзлочинця, включаючи ім’я користувача, його IP-адресу, дату підозрілої події тощо;
- автоматичне блокування трафіку, що надходить з підозрілих IP-адрес;
- простота у використанні завдяки серії готових налаштувань для розгортання в один клік;
- можливість використання на багатьох веб-сайтах одразу;
- сумісність з apache, Nginx, IIS, темами та іншими плагінами безпеки.

Плагін є платним та не передбачає двофакторної автентифікації.

11) WebDefender

Частково безкоштовний багатофункціональний плагін, що пропонує:

- приховування веб-сайту та версій WordPress, плагінів та тем до нього від ботів;
- установку в один клік;
- брандмауер, який виявляє та блокує трафік ботів;
- відстеження веб-трафіку від ботів, його фільтрація та блокування;
- фільтрацію коментарів, вставлених ботами;
- виявлення спроб ботами здійснити атаку грубою силою;
- антивірусний сканер, що включає в себе наступне:
    - сканування бази даних,
    - сканування ZIP-файлів,
    - виявлення рекламного, шпигунського та спаму посилань,
    - потужний та простий у використанні інструмент для видалення шкідливих програм,
    - аналітика та рекомендації щодо посилення безпеки,
    - оновлення сигнатур зловмисного програмного забезпечення в режимі реального часу,
    - налаштування планувальника сканувань;
- сканування баз даних на вразливість до SQL-ін’єкцій;
- сканування розміщених посилань на потенційно фішингові веб-сайти;
- сканування плагінів і тем на вразливості;
- перевірку на блокування веб-сайту пошуковими веб-ресурсами;
- автоматичне оновлення ядра WordPress, плагінів і тем;
- управління файлами cookie згідно закону GDPR.

Плагін не передбачає використання двофакторної автентифікації, а захист від атак грубою силою опирається на відкриті дані про підозрілі IP-адреси замість лімітування спроб входу.

12) Akismet

Кращий плагін для фільтрування спаму, який було встановлено 5 мільйонів разів.

Спеціалізується на:

- фільтрації спаму в коментарях веб-сайту;
- перехопленні потенційно небезпечних посилань при використанні механізму звернень до сторонніх веб-ресурсів Trackback;
- блокуванні спаму при відправці повідомлень у формах зворотного зв’язку;

- наданні програмного інтерфейсу для інших плагінів, що реалізовують коментарі або форми зворотного зв’язку.

Є частково безкоштовним та не має інших функцій, окрім фільтрації спамових повідомлень та коментарів.

13) WPBruiser

Плагін WPBruiser поєднує в собі захист від спаму та атак грубою силою. Його функції:

- інтеграція зі стандартними формою входу, реєстрації, сторінки «Забули пароль?» та коментарів WordPress без капчі;
- можливість встановити максимальну кількість символів для кожного поля коментаря;
- логування з можливістю його ввімкнення/вимкнення;
- автоматичне блокування IP-адрес;
- автоматичне очищення старих журналів;
- налаштування білого та чорного списків IP-адрес за протоколами IPV4 та IPV6;
- коректне визначення IP-адреси користувача під час використання сервісів CloudFlare, Sucuri CloudProxy, AWS ELB тощо;
- надання статистики, звітів та діаграм з усіма заблокованими спробами розповсюдження спаму;
- придатність до використання багатьма веб-сайтами за один раз;
- сумісність з плагінами кешу (WP Super Cache, W3 Total Cache, ZenCache, WP Fastest Cache тощо);
- невидимість для користувачів (через працю у фоновому режимі);
- відсутність впливу на час завантаження сторінки;
- автоматичне виявлення атак грубою силою;
- можливість автоматичного блокування IP-адрес;
- можливість блокувати IP-адреси, що використовують TOR;
- дезактивація протоколу XML-RPC;
- сповіщення електронною поштою при виявленні атаки грубою силою.

Не підтримує двофакторну автентифікацію, алгоритм захисту від атак грубою силою не є достатньо прозорим, а сам плагін не отримує оновлень упродовж одного року.

1.2.2 Плагіни з двофакторною автентифікацією

1) iThemes Security Pro

Плагін iThemes Security Pro рекламується як програмне забезпечення, що здатне захистити веб-сайт більш ніж 30 засобами. До основних відносяться:

- сканування інших встановлених на веб-сайті плагінів на наявність вразливостей;
- перевірка версій WordPress та плагінів на актуальність та застарілість;
- аналіз паролів на стійкість до атак грубою силою;
- автоматичний захист від таких атак за IP-адресами;
- надання готових шаблонів налаштувань для шести типів веб-ресурсів;
- можливість блокування небажаних користувачів;
- перевірка цілісності файлів ядра WordPress, плагінів та тем до системи управління вмістом;
- примусове використання протоколу SSL;
- здійснення резервних копій бази даних;
- перевірка прав доступу до файлів конфігурації;
- зміна посилання на сторінку для входу до сайту;
- двофакторна автентифікація.

Це перший плагін у списку, що надає можливість встановити двофакторну автентифікацію. Але безкоштовний план передбачає захист лише одного веб-сайту, а також відсутність актуальних оновлень, що підвищує вразливість самого плагіну [11].

2) Jetpack

Програмний додаток від розробників самої системи управління вмістом WordPress. Переважно використовується через наступні функції:

- автоматичне резервне копіювання веб-сайту в режимі реального часу з власним необмеженим сховищем;
- покращена навігація для міграції на новий хост, переміщення файлів теми та плагіни до іншої бази даних, дублювання та резервних копій баз даних тощо;
- перегляд кожної зміни сайту та її ініціаторів через вбудований журнал активності;

- автоматичне сканування зловмисного програмного забезпечення та безпеки для виявлення інших загроз, що реалізовуються через програмний код;
- інтеграція з плагіном для захисту від спаму Akismet;
- захист від атак грубою силою;
- відстеження часу роботи та простою веб-сайту;
- сповіщення електронною поштою про такі простої;
- автоматичне оновлення інших плагінів;
- інтеграція з фреймворком Google AMP;
- прискорення завантаження статичних файлів на кшталт зображень та кодових файлів за допомогою CDN;
- блокування спроб завантажити всі зображення одночасно для більш плавного перегляду веб-сайту;
- власний високошвидкісний відеохостинг без реклами;
- настроюваний користувацький пошук по веб-сайту та фільтрація товарів (при використанні плагіну WooCommerce);
- вбудовані теми;
- автоматичне відображення пов’язаних дописів для користувачів;
- інструменти для галереї та слайд-шоу;
- можливість для користувачів здійснити підписку на веб-сайт;
- контактні форми;
- підтримка модулю oEmbed для роботи зі зображеннями, публікаціями та посиланнями з Facebook та Instagram;
- просунута інтеграція з WooCommerce;
- інтеграція з аналітичним модулем Google Analytics;
- інтеграція зі соціальними мережами Instagram, Facebook, Twitter, LinkedIn;
- готові елементи для налаштування веб-сайту для взаємодії з Pinterest, Whatsapp, а також програвач подкастів, GIF-файли, карти, плиткова галерея, слайд-шоу;
- інтеграція з платіжними сервісами Stripe та PayPal для комерції та прийому пожертвувань;
- інтеграція з плагінами для кешування Automattic’s WP Super Cache і Cloudflare;
- можливість активувати двофакторну автентифікацію для будь-якої кількості веб-сайтів.

Але його використання передбачає активацію протоколу віддалених процедур XML-RPC. Його використання не тільки спрощує проведення атаки DDoS на порядки, але й дозволяє здійснити атаку грубою силою в обхід

інструментів безпеки. Це становить велику загрозу, тому поданий плагін також не рекомендовано до використання. До того ж, частина функцій є платною [11].

3) SecuPress

Розробники плагіну SecuPress роблять акцент на:

- блокуванні користувачів з певних країн;
- двофакторній автентифікації;
- брандмауері;
- наданні звітності;
- захисту від атак грубою силою;
- автоматичному блокуванні наведеного вище протоколу XML-RPC.

Але тільки останні дві можливості передбачено безкоштовною версією програмного додатку, інше є недоступним без оплати. [11]

4) SiteLock Security

Плагін SiteLock Security:

- відстежує файли та дані веб-сайту, попереджуючі про будь-які загрози, які він знайде, працюючи як антивірусне програмне забезпечення;
- захищає платежі, що є більш актуальним для інтернет-магазинів;
- здійснює резервне копіювання веб-сайту;
- надає брандмауер;
- надає захист від DDoS-атак;
- здіснює автоматичне оновлення ядра системи управління вмістом WordPress, плагінів та тем до неї;
- перевіряє, чи є веб-сайт заблокованим пошуковими веб-ресурсами;
- має двофакторну автентифікацію.

Вважається одним з найбільш просунутих плагінів безпеки, але не має безкоштовних планів та навіть безкоштовних пробних періодів, а двофакторну автентифікацію передбачено лише при використанні організаціями (тарифи для яких є найвищими з тих, що пропонуються) [11].

5) Sucuri

Відомий плагін, який встановили більш за 800 тисяч користувачів. Його розробила однойменна дочірня компанія одного з найбільших реєстраторів доменних імен, GoDaddy. Цей плагін підтримує такі функції:

- підтримка безпечного протоколу HTTPS/SSL з використанням брандмауеру;
- підтримка окремих сертифікатів SSL;
- прикладний програмний інтерфейс для взаємодії з панеллю управління плагіном;
- підтримка декількох веб-сайтів одночасно;
- сканування безпеки, що включає в себе:
    - виявлення шкідливого програмного забезпечення,
    - виявлення аномалій безпеки,
    - моніторинг заблокованих списків,
    - виявлення змін файлів,
    - моніторинг DNS,
    - моніторинг SSL,
    - надання миттєвих сповіщень власнику веб-сайту;
- управління журналюванням подій безпеки за технологією управління SIEM;
- обмеження пропускної здатності;
- брандмауер веб-додатків;
- система виявлення вторгнень;
- пом'якшення DDoS-атак;
- захист від атак грубою силою;
- блокування спроб зламу;
- запобігання вразливостям нульового дня;
- захист окремих сторінок веб-сайту;
- евристичний механізм кореляції;
- балансування навантаження та відмова при його перевищенні;
- набори спеціальних правил;
- виділені мережеві ресурси;
- спеціальна сторінка блокування брандмауера;
- підтримка корпоративних сервисів захисту від DDoS-атак;
- відновлення веб-сайту після зламу та шкідливих програм, а також їхнє видалення;
- лімітування запитів на видалення шкідливих програм;
- видалення попереджень про блок-лист;
- автоматичне очищення;
- ескалація певних подій безпеки при аналітичному аналізі;
- повне очищення сайту;
- видалення бэкдорів;
- здійснення резервних копій;
- звіт після очищення;

- повний огляд журналу та інцидентів;
- дослідження щодо першопричин;
- підтримка технології розподілення навантаження CDN;
- прискорення завантаження сторінок;
- зменшене навантаження на сервер;
- параметри розумного кешування.

Більшість з функцій, включаючи двофакторну автентифікацію, є платними, що знижує його цінність [11].

6) Wordfence Security

Wordfence Security – це ще відоміший плагін, ніж Sucuri, що було встановлено 4 мільйона разів. Він безкоштовно пропонує:

- захист від атак грубою силою методом лімітування спроб входу;
- захист від запитів, що містять вірусний вміст або код;
- антивірусний сканер тем, плагінів, посилань в межах веб-сайту тощо;
- перевірку цілісності файлів ядра WordPress, плагінів та тем до нього шляхом порівняння із копіями у репозиторіях WordPress, а також перезапис підроблених;
- перевірку плагінів на підтримуваність розробниками;
- двофакторну автентифікацію;
- капчу на сторінці входу;
- моніторинг трафіку;
- фільтрування коментарів;
- блокування адміністраторів з паролями, що зазнали виток;
- повідомлення власника веб-сайту про події шляхом електронної пошти чи смс-повідомлень, у тому числі на щоденній основі;
- підтримку декількох веб-сайтів одразу;
- брандмауер.

Але через особливості реалізації останнього плагін може сповільнювати роботу веб-сайту (за умови недостатньої потужності апаратного забезпечення) та пропустити певну частину DDoS-атак. Тому з долею ймовірності власнику веб-ресурсу доведеться оплатити перехід на хостинг з покращеним сервером у випадку, якщо той розраховуватиме на стабільну роботу з цим плагіном [11].

7) Defender

Defender поєднує в собі наступні безкоштовні функції:

- двофакторна автентифікація через коди, що надсилаються на мобільні пристрої;
- маскування сторінки входу шляхом змінення стандартного посилання на інше;
- захист від атаки грубою силою шляхом встановлення лімітованої кількості невдалих спроб входу;
- заголовки безпеки HTTP для додаткового рівню захисту від поширених атак, таких як XSS, ін'єкції коду тощо;
- автоматичне блокування за IP-адресою ботів, що намагаються дістатись до сторінок з кодом 404;
- опція експорту та імпорту створених конфігурацій плагіну при наявності декількох веб-ресурсів;
- блокування користувачів на основі місцезнаходження та країни за IP-геолокацією;
- брандмауер;
- дезактивація спамових трекбеків та пінгбеків;
- періодична перевірка актуальності версій ядра WordPress, плагінів та тем до системи;
- дезактивація редагування файлів конфігурації;
- приховування повідомлень про помилки, що можуть містити чутливу інформацію про веб-сайт;
- періодичне оновлення ключів безпеки;
- скидання ключів безпеки на вимогу власника веб-сайту;
- запобігання розголошенню інформації;
- запобігання несанкціонованому запуску небезпечного зовнішнього програмного коду PHP;
- капча;
- перевірка паролів, що використовуються, на появу у відкритих витоках даних;
- примусове скидання пароля для користувачів із вибраними правами доступу;
- блокування користувачів та ботів за користувацькими агентами браузерів чи іншого програмного забезпечення.

При цьому він має велику кількість налаштувань, некоректне встановлення котрих може погіршити безпеку веб-сайту або сповільнити його роботу [11].

8) Shield Security

Розробники цього частково безкоштовного додатку роблять упор на

наступних перевагах:

- механізм виявлення ботів за стандартним алгоритмом;
- виявлення ботів, що спровоковано будь-яким іншим встановленим плагіном безпеки WordPress;
- автоматичне блокування ботів за IP-адресами на основі зовнішньої балової оцінки;
- встановлення захисту від ботів для таких сторінок, як:
    - сторінка входу до веб-сайту,
    - сторінка реєстрації,
    - сторінка скидання пароля;
- інтеграція з плагінами для комерційної діяльності WooCommerce та Easy Digital Downloads
- інтеграція з плагінами для створення членств, навчання та іншої взаємодії з користувачами:
    - Memberpress,
    - LearnPress,
    - BuddyPress,
    - WP Members,
    - ProfileBuilder Security;
- захист від атак грубою силою шляхом лімітування кількості спроб входу та встановлення таймеру між цими спробами
- брандмауер;
- обмеження доступу для адміністратора до деяких функцій налаштування з метою запобігти несанкціонованим змінам сайту навіть з їхнього боку;
- двофакторна автентифікація, яку користувач буде у змозі здійснити у наступні шляхи:
    - електронна пошта,
    - програмний додаток,
    - Yubikey,
    - ключі безпеки U2F,
    - резервні коди безпеки входу,
    - декілька ключів Yubikey для одного користувача;
- опція «Запам’ятати мене» для зменшення кількості необхідних сеансів двофакторної автентифікації та підвищення зручності використання користувачем веб-ресурсу;
- блокування протоколу XML-RPC;
- блокування анонімних запитів RestAPI;

- автоматичне блокування IP-адрес за допомогою системи безпеки на основі точок;
- блокування або дозвіл окремим IP-адресам;
- блокування або дозвіл певним IP-підмережам;
- аналіз безпеки IP-адресів з переглядом статистики;
- виявлення змін файлів шляхом сканування та відновлення основних файлів налаштування WordPress
- виявлення невідомих та підозрілих кодових файлів PHP;
- виявлення плагінів, що не підтримуються;
- антивірусне сканування;
- перевірка цілісності інших плагінів та тем;
- перевірка інших плагінів та тем на відомі вразливості;
- приховування та заміна URL-адреси сторінки входу на іншу;
- виявлення та блокування спаму;
- підтримка капчі;
- автоматичне виявлення та дозвіл взаємодії для офіційних ботів від наступних пошукових систем та сервісів:
    - Google,
    - Bing,
    - DuckDuckGo,
    - Yahoo,
    - Baidu,
    - Apple,
    - Яндекс,
    - ManageWP, iControlWP, MainWP,
    - Pingdom, NodePing, Statuscake, UptimeRobot, GTMetrix,
    - Stripe, PayPal IPN,
    - CloudFlare, SEMRush;
- журналювання активності користувачів та адміністраторів на веб-сайті, що включає в себе наступні пункти:
    - спроби входу та реєстрації у системі,
    - установка, активація та дезактивація певного плагіна та/або теми для CMS WordPress,
    - створення та підвищення прав доступу користувачів,
    - створення, оновлення та видалення сторінки веб-ресурсу або публікації на ньому;
- розширений контроль безпеки сеансів користувача:
    - обмеження входу для кількох користувачів,
    - обмеження сеансів користувачів до IP-адресам,

    - блокування використання паролів, що зазнали витоку та опубліковано у відкритому доступі,
    - дезактивація присвоєння унікальних ідентифікаторів для користувачів,
    - призупинення облікового запису користувача на ручній або автоматичній основі;
- перешкодостійкість механізмів роботи з IP-адресами при використанні користувачами проксі-серверів;
- журналювання трафіку та моніторинг запитів;
- використання безпечних заголовків HTTP;
- використання протоколу політик безпеки вмісту CSP.

Має визнані виробником проблеми з надсиланням листів з кодом автентифікації, а при ненавмисному самоблокуванні від власника знадобиться знання протоколу FTP, що підвищує поріг входу користувачів [11].

9) Duo Two-Factor Authentication

Частково безкоштовний плагін, що спеціалізується на двофакторній автентифікації. До його характеристик відносяться:

- сумісність з програмним додатком;
- додаткова можливість входу до облікового запису за QR-кодом;
- опція використання двофакторної автентифікації для певних рівнів користувачів (наприклад, тільки для адміністраторів);
- налаштування довірених пристроїв, для яких припустима звичайна авторизація;
- можливість здійснити автентифікацію у наступні шляхи:
    - мобільний додаток від розробників плагіну,
    - одноразові коди, що надаються через додаток,
    - одноразові коди, що надаються через SMS,
    - телефонний дзвінок на мобільні телефони,
    - телефонний дзвінок на стаціонарні телефони,
    - одноразові коди, що генеруються апаратними токенами.

Функції сумісності з плагінами для текстових форм, а також настроювання цього плагіну окремо від налаштувань панелі адміністрування доступні тільки в платній версії. До того ж він не надає інших видів захисту [11].

10) WP Cerber Security

Перший плагін у списку, що частково підтримує українську мову.

Забезпечує безпеку у такі шляхи, як:

- лімітування кількості спроб входу для окремих IP-адрес або певних підмереж;
- відстеження входу до веб-сайту, здійсненого за допомогою сторінки входу форм входу, запитів протоколом XML-RPC або файлів cookie для авторизації;
- дозвіл або обмеження доступу шляхом чорних та білих списків для IP-адрес та/або підмереж;
- створення користувацького URL-посилання для входу замість стандартного «wp-login.php»;
- механізм захисту від спаму для контактних та реєстраційних текстових форм;
- автоматичне виявляння та переміщення спамових коментарів в кошик або їхнє повне видалення;
- двофакторна автентифікація;
- журналювання зареєстрованих користувачів, ботів, кіберзлочинців та подій, у тому числі підозрілих;
- сканування для перевірки цілісності файлів конфігурації WordPress, плагінів та тем до системи;
- відстеження змін існуючих файлів та появи нових, а також надання сповіщень та звітів з подібних інцидентів електронною поштою;
- мобільні та електронні сповіщення з набором гнучких фільтрів;
- менеджер сеансів користувачів з підвищеними правами доступу до веб-ресурсу;
- підвищення захисту сторінок «wp-login.php», «wp-signup.php» та «wp-register.php» від атак;
- приховування панелі адміністрування «wp-admin», якщо користувач не ввійшов у систему;
- негайне блокування IP-адреси кіберзлочинця при спробі увійти з неіснуючим або забороненим ім’ям користувача;
- обмеження реєстрації користувача або входу за допомогою його логіну в залежності від встановлених шаблонів REGEX;
- обмеження доступу до REST API за допомогою власних правил безпеки на основі ролей;
- можливість повністю заблокувати доступ до REST API на основі системи управління вмісту WordPress;
- блокування доступу до протоколу XML-RPC, включаючи пінгбеки та трекбеки;
- дезактивація каналів RSS, Atom та RDF;

- обмеження доступу до XML-RPC, REST API та наведених вище каналів за допомогою білого списку доступу для IP-адрес або їхніх діапазонів;
- режим використання веб-ресурсу лише авторизованими користувачами;
- можливість блокування облікового запису того чи іншого користувача;
- дезактивація автоматичного переспрямування на приховану сторінку входу;
- блокування перерахування користувачів з метою запобігти несанкціонованому витоку даних користувача через REST API;
- проактивне блокування IP-підмережі класу C;
- капча reCAPTCHA для захисту форм входу в WordPress, реєстрації та коментарів;
- reCAPTCHA для форм WooCommerce та WordPress;
- невидима reCAPTCHA для форм коментарів веб-сайту;
- спеціальний режим для масових атак грубою силою;
- інтеграція з плагіном безпеки fail2ban, що дозволяє запис невдалих спроб входу до системного журналу або зовнішнього спеціального файлу журналу;
- фільтрація та перевірка дій за IP-адресою, користувачем, його логіном або певною діяльністю;
- експортування дій користувачів у файл CSV;
- надсилання щотижневих звітів з подій безпеки шляхом використання електронної пошти;
- обмеження спроб входу навіть при використанні користувачем зворотного проксі-серверу;
- надсилання сповіщень про потенційно небезпечні події безпеки шляхом використання мобільних push-повідомлень;
- інтеграція з плагіном автоматизації jetFlow.io;
- захист від DDoS-атак.

Безкоштовний план передбачає тільки захист від спаму та сканування на віруси з використанням апаратних потужностей власника веб-сайту, як й у випадку WordFence, що зменшує кількість потенціальних користувачів. Безкоштовна версія також не передбачає двофакторної автентифікації. До того ж, пропонований переклад українською мовою не є високої якості [11].

Таким чином, з 23 наведених плагінів 12 є частково безкоштовними та ще 3 – повністю безкоштовними (не враховуються тарифи, де єдиною перевагою є послуги служби підтримки). З цих 16-ти двофакторну

автентифікацію мають 8 плагінів, що показує актуальність та надійність цієї технології. Кожен з них має свої переваги та недоліки, але повністю безкоштовних серед них немає. З метою наочності ця статистика буде представлена у вигляді таблиці 1.2.

Таблиця 1.2. Співвідношення плагінів за ціновою політикою та наявністю двофакторної автентифікації

	Кількість	З них з двофакторною автентифікацією
Безкоштовні плагіни	3	0
Частково безкоштовні плагіни	12	7
Платні плагіни (включаючи плагіни з пробним періодом)	8	3
Загальна кількість	23	10

Це може стати вирішальним критерієм для компаній, де використання безкоштовного програмного забезпечення є важливим, але цей плагін не надає інших послуг, окрім двофакторної автентифікації, що залишає веб-ресурс вразливим до атак грубою силою, маніпуляцій даними на кшталт SQL-ін’єкцій та іншого. Тому у випадках, коли бюджет не передбачає придбання плагінів, дозволених для комерційного використання, не існує достатньо функціонального програмного додатку, здатного захистити веб-ресурс від більшості використовуваних атак.

1.3 Висновки

У цій главі було розглянуто існуючі шляхи забезпечення безпеки для веб-ресурсів, що використовують CMS WordPress. Було показано, що безкоштовні плагіни безпеки є кращим зі шляхів у порівнянні з платними плагінами, порадами у відкритому доступу мережі Інтернет та послугами фахівців.

Було наведено список популярних плагінів, здатних підвисити безпеку веб-ресурсу. Як було наведено вище, в рамках цієї роботи кращими вважаються такі плагіни, що:

1) Є безкоштовними, у тому числі для комерційного використання;
2) Надають кінцевому користувачеві простий та зрозумілий інтерфейс;
3) Захищають від атак грубою силою як найчастіших;
4) Підтримують двофакторну автентифікацію.

Спираючись на список, наведений вище, можливо зробити висновок, що немає плагінів, що підходять для всіх ситуацій. Певні з них надаються лише на платній основі, деякі є частково безкоштовними (але кількість безкоштовних функцій варується від одного плагіну до іншого), а повністю безкоштовних – меншина. Деякі частково безкоштовні плагіни надають достатній функціонал для захисту, але не завжди є простими у налаштуванні.

До інших недоліків наведених плагінів відноситься той факт, що хоча частково безкоштовні додатки можуть бути використані при створені веб-сайтів фізичними особами, але у випадку комерційних проектів це може призвести до неузгоджених трат, а тому не є доцільним. Крім того, лише один з 20 наведених плагінів перекладено українською мовою – і цей переклад за якістю знаходиться на рівні інтернет-перекладачів, що негативно впливає на зрозумілість наданої інформації, налаштувань тощо.

Якщо розглядати цілком безкоштовні плагіни, то вони діляться на дві групи – такі, що захищають від атак на веб-сайт (у тому числі грубою силою) та такі, що надають можливість застосувати двофакторну автентифікацію – і в поданому випадку ці групи не перетинаються. Плагін, що буде представлено далі в роботі, має за мету об’єднати переваги обох груп, залишаючись при цьому повністю безкоштовним. Він не вимагає від кінцевого користувача спеціальних знань або надлишкового настроювання, надаючи оптимальні налаштування та знижуючи людський фактор як такий, що підвищує ймовірність зламу веб-сайту. До того ж його було локалізовано у зрозумілий для місцевого сегменту користувачів шлях. Стисле порівняння плагіну, що буде представлено, та існуючих виглядає так:

Таблиця 1.3. Порівняння представленого плагіну безпеки з існуючими

	Новий плагін	Існуючі плагіни
Легкість у використанні	1	0.5
Захист від несанкціонованого доступу до панелі адміністрування	1	1
Наявність двофакторної автентифікації	1	0.5
Додаткові опції забезпечення безпеки	1	1
Оцінка	4	3

У наступній главі буде розглянуто двофакторну автентифікацію. Це включає в себе порівняння її зі стандартною автентифікацією, наведення механізмів роботи обох алгоритмів та обґрунтування її ефективності у сучасних плагінах безпеки.

2 СИСТЕМИ АВТЕНТИФІКАЦІЇ У СУЧАСНИХ ПЛАГІНАХ БЕЗПЕКИ

2.1 Механізм роботи алгоритмів однофакторної автентифікації та їхні недоліки

Автентифікація – це захід або комплекс заходів, що мають за мету перевірку особи користувача. Як механізм підтвердження особистості вона почала своє існування ще у XX сторіччі [19]. Хронологія її розвитку виглядатиме наступним чином:

1) У 1961 році Фернандо Корбато винайшов концепцію паролів під час роботи над операційною системою реального часу CTSS;
2) У 1974 році було розроблено перше криптографічне програмне забезпечення – Crypt, що підтримувало гешування паролів;
3) У 2003 році стало масовим використання двофакторної автентифікації на основі апаратного забезпечення;
4) У 2005 році було розроблено алгоритм генерації одноразових паролів HOTP, що використовується у сучасних сервісах двофакторної автентифікації;
5) У 2011 році було офіційно стандартизовано покращений алгоритм генерації одноразових паролів TOTP, що додатково використовує заданий момент часу як параметр генерації та також є присутнім в сервісах двофакторної автентифікації;
6) У 2012 році було засновано «Альянс FIDO» – некомерційну організацію, що розробила та стандартизувала протокол U2F, використовуваний при двофакторній автентифікації на основі електронного ключа;
7) У 2013 році корпорація Apple представила перший смартфон зі сканером відбитків пальців, почавши розповсюдження біометричних методів автентифікації;
8) У 2018 році стандарт безпарольної інтернет-автентифікації WebAuthn став дозволеним до використання у більшості сучасних інтернет-браузерів.

Незалежно від механізму, автентифікація базується на однаковому для всіх випадків алгоритмі – при отриманні інформації про користувача, її порівнюється зі записами, що містяться у базі даних [12]. Якщо інформація співпадає, користувачеві надається доступ до захищеної частини системи. Механізми автентифікації традиційно розділяються за типами на три категорії:

1) Автентифікація на основі того, що користувач знає (пароль);

2) Автентифікація на основі того, що користувач має (фізичний доступ до пристрою, цифровий сертифікат, смарт-карта, електронний ключ);
3) Автентифікація на основі біометричних властивостей користувача (відбиток пальцю, зображення сітківки ока, голос).

Кожен тип механізмів автентифікації дозволяє користувачеві отримати доступ до системи, але всі вони працюють у різні шляхи. Втім, вона не є єдиною частиною алгоритму розподілення доступу – він також передбачає ідентифікацію, авторизацію та ведення електронної звітності.

Ідентифікація відбувається, коли користувач вводить власний ідентифікатор (логін, ID-номер тощо), а система безпеки перевіряє його валідність – чи існує він та обліковий запис з ним у базі даних. Деякі системи безпеки генерують випадкові ідентифікатори, не дозволяючи користувачам обирати власні (і часто ненадійні з точки зору криптографічної стійкості) дані.

Процес авторизації має за мету встановити рівень доступу, що відповідає автентифікованому користувачу, та здійснюється на трьох рівнях – рівні користувача, рівні груп користувачів (наприклад, адміністратори мають мати більше прав, аніж звичайні користувачі) та на рівні систем, якщо таких є декілька. У сценаріях, де певний обліковий запис є дійсним, але його було заблоковано або зламано, саме механізми авторизації мають перевірити ризики його використання та відкликати попередньо наданий рівень доступу.

Нарешті, ведення електронної звітності передбачає автоматичне записування всіх подій для кожного з компонентів системи в окремий текстовий файл. Зокрема це включає спроби увійти до того чи іншого облікового запису зі зазначенням результату та, іноді, даних про електронний пристрій, з якого здійснено таку спробу (IP-адрес, місцезнаходження, дані про апаратне забезпечення тощо).

Слід зазначити, що в тій чи іншій мірі всі з цих механізмів реалізовано в системи управління вмістом WordPress без зовнішнього програмного забезпечення – не враховуючи те, що журналювання слід попередньо активувати.

Далі буде розглянуто сутність, переваги та недоліки різних типів автентифікації, що включають до себе парольну, автентифікацію за смарт-картою, біометричну та автентифікацію за цифровим сертифікатом.

2.1.1 Автентифікація за паролем

Цей тип автентифікації базується на інформації, що імовірно знає тільки користувач. У цьому сценарії від користувача вимагається надати логін та пароль – секретну комбінацію слів та/або цифр, після чого система гешує останній та порівнює з існуючим гешованим паролем у базі даних. Якщо вони співпадають – користувачу надається доступ.

Перевагами цього механізму автентифікації є простота в реалізації для веб-ресурсів – включаючи такі, що базуються на CMS WordPress – і те, що достатньо складний пароль є стійким до атак грубою силою. Наприклад, для здійснення такої атаки на обліковий запис з паролем з дванадцяти символів, що включає великі та маленькі літери, цифри та спеціальні символи, потребуватиме 55 днів за наявності сучасних суперкомп'ютерів, або близько 3000 років при використанні середньостатистичного персонального комп'ютера. Існують веб-сайти, що надають приблизну часову оцінку успішної атаки грубою силою на той чи інший пароль (без врахування атак за словником найчастіших паролів), що наочно мотивує використовувати унікальні складні паролі [13].

Але навіть за умови встановлення такого паролю, що неможливо «перебрати» у розумні строки, існують інші загрози безпеці облікового запису при використанні однофакторної автентифікації. До таких відносяться:

- Сніффінг – прихований аналіз трафіку користувача, що має за мету перехопити певні дані (у поданому випадку – пароль);
- Крадіжка паролю, що записано на фізичному (папір) або електронному рівні;
- Соціальна інженерія – психологічна маніпуляція, що використовує неуважність або страх користувача, що призводить до розголошення паролю ним самим;
- Втрата доступу до облікового запису через забуття паролю (або відповіді на секретне питання для його відновлення, логіну тощо).

Продовжуючи тему слабких паролів та атак грубою силою, слід зазначити, що велика частина систем безпеки веб-сайтів приймає пароль із восьми символів. Є три фактори, які визначають міцність пароля – довжина, кількість допустимих символів та ентропія. Чим більше різних символів дозволено застосовувати, тим складніше перебрати пароль – звідси розповсюджена вимога використовувати літери у різних регістрах, цифри та спеціальні символи. Ентропія – це міра невизначеності присутності кожного

окремого символу у складі їхньої множини (наприклад, у середньому українському реченні літера «Ґ» зустрічатиметься рідше, ніж «А», така визначеність зменшує ентропію). Застосування генератору паролів, що базується на надійному генераторі псевдовипадкових чисел, підвищує ентропію у порівнянні зі середнім користувацьким паролем. Враховуючи це, згенерований таким чином пароль з 8 символів, обраних з діапазону 94 допустимих символів, може бути знайдено за 20 хвилин з використанням персонального комп'ютеру або 0.07 секунди за наявності суперкомп'ютеру [14].

Для запобігання перебору та крадіжці паролю слід використовувати надійніший пароль. Окрім великої довжини та діапазону символів, є також доцільним не включати до паролю особисту інформацію на кшталт дати народження чи улюблених знаменитостей, а також не застосовувати статистично найчастіші паролі (наприклад, «password» чи «iloveyou»). При наявності сторонніх осіб клавіатуру слід прикривати рукою чи тілом, а підозрілі телефонні дзвінки, електронні листи та веб-сайти з некоректними URL-адресами – уникати, особливо за умови відсутності антивірусного програмного забезпечення. Якщо система безпеки дозволяє використання графічних паролів [14] – краще встановити такий замість текстового. Нарешті, для підвищення безпеки кількість спроб введення пароля має бути обмежена системою.

2.1.2 Автентифікація за смарт-картою та електронним ключом

Автентифікація за допомогою смарт-карти базується на використанні того, що має тільки користувач. Смарт-карта має розмір кредитної картки та має вбудований сертифікат, що використовується для підтвердження особи її власника. Користувач може вставити картку в пристрій зчитування смарт-карт [12], після чого, залежно від її налаштування, йому може знадобитися ввести її PIN-код, що забезпечує двофакторну автентифікацію, оскільки йому необхідно мати певну річь та знати певну інформацію, щоб підтвердити свою особу [12, 14]. Більш розповсюдженим аналогом є електронні USB-ключі, що працюють аналогічним чином, але не вимагають додаткових пристроїв зчитування. Втім, такі ключі мають високу ціну, через що більшістю веб-сайтів такий механізм автентифікації не передбачено. Нижче смарт-карти та такі ключі буде розглянуто як рівноцінні пристрої безпеки.

Однією з переваг смарт-карт є те, що вони поставляється в двох різновидах. Перша версія має вбудовану карту пам'яті з даними, що забезпечують двофакторну автентифікацію, а друга оснащена мікропроцесором, що генерує нові ключі автентифікації, роблячи її

надійніше. Смарт-карта з мікропроцесором зберігає сертифікати відкритого та приватного ключа. Обидві версії пристрою блокуються, якщо PIN-код введено неправильно після кількох спроб, запобігають атакам на словники та перехопленню ключових даних [15], а також є портативними та можуть легко переноситися користувачами [12].

Серед недоліків смарт-картки:

- Її крадіжка надає зловмиснику повний доступ, якщо використання PIN-коду не передбачено;
- Людський фактор – певні користувачі не запам’ятовують PIN-код, тому вони записують його на самій картці [14]. Крадіжка такої картки зводить безпеку нанівець;
- Велика кількість провалених спроб ввести код блокує картку не тільки для зловмисників, але й для його власника;
- Код також можливо вкрасти, використовуючи соціальну інженерію [16] або підглянути.

Тому для подібних пристроїв безпеки залишається актуальною порада прикрити клавіатуру, де вводиться PIN-код, а також активувати режим автентифікації через криптографічний протокол SSL. Іншим рішенням може бути поєднання смарт-карт із технологією радіочастотної ідентифікації RFID, але пристрої, що підтримують її, матимуть ще вищу ціну.

2.1.3 Автентифікація за біометричними параметрами

Біометричні методи автентифікації базуються на унікальних для певного користувача фізичних або поведінкових характеристиках. На фізичних особливостях ґрунтуються сканування відбитків пальців, що активно використовуються у сучасних смартфонах, а також розпізнавання обличчя, сканування райдужної оболонки ока, геометрії руки та сітківки ока. На поведінкових характеристиках базуються розпізнавання голосу, ходи, сканування натискань клавіш та сканування підпису [17]. Сканування відбитків пальців є найбільш широко використовуваним біометричним методом, що підтримується більшістю ноутбуків та певними USB-флеш-накопичувачами. Біометрична автентифікація має такі переваги, як:

- Відсутність необхідності згадувати пароль при кожному вході в систему;
- Підвищена складність здійснення несанкціонованого доступу;
- Прискорення входу в систему у порівняння з попередніми механізмами автентифікації;

- У випадку відбитків пальців – мала коштовність сканерів споживчого класу [14, 17];
- У випадку сканування сітківки ока – точність ідентифікації користувачів, що підвищує ймовірність отримання доступу з першої спроби.

Буде розглянуто сканер відбитків пальців як найбільш поширений. Цей пристрій сканує зображення на пальці користувача, а потім порівнює його з даними, що зберігаються у базі даних в закодованому вигляді. Безпека механізму ґрунтується на тому, що кожен користувач має різні відбитки пальців [17].

Цей механізм забезпечує високий рівень безпеки, оскільки важко вгадати малюнок відбитків пальців. Втім, він є схильним до помилок – стаються випадки, коли система помилково відхиляє відомого користувача та приймає його за невідомого (помилка 1 типу) або коли система помилково ідентифікує невідомого користувача як відомого (помилка 2 типу). Чутливість більшості біометричних систем можливо налаштувати, але якщо зробити це недостатньо ретельно, то сканер може стати схильним до помилок того чи іншого типу. Крім того, сканування відбитків пальців не має загального стандарту, тому реалізація, наявність документації та якість кожного окремого сканеру залежить від виробника. Грає роль також психологічний фактор, оскільки в деяких користувачів сканування відбитків асоціюється з криміналістичною процедурою дактилоскопії [14]. Також травма на пальцях може заважати процесу сканування. Нарешті, більшість веб-сайтів не підтримують біометричні методі автентифікації через необхідність додаткового обладнання, а втрата флеш-накопичувача або комп’ютеру з модулем біометрії призведе до втрати доступу та інформації, що зберігається.

Таким чином, біометрична автентифікація зменшує вплив людського фактору, але є вразливою до помилок двох типів. Для зменшення ймовірності технічних перешкод можливо поєднувати різні біометричні дані користувача або використовувати ДНК для автентифікації, але для звичайних веб-сайтів коштовність цього методу перевищує потребу у безпеці.

2.1.4 Автентифікація за цифровим сертифікатом

Цифровий сертифікат – це технологія шифрування, яка працює аналогічно інтернет-версії паспорта. Використовуючи інформацію відкритого та закритого ключа, цифрові сертифікати по суті гарантують одержувачу повідомлення, що повідомлення надходить від конкретної особи

– в даному випадку вони дозволяють переконати систему безпеки, що доступ намагається отримати дійсний користувач.

Відкритий та закритий ключі використовуються разом, щоб закодувати інформацію про користувача в унікальний для нього шлях та захистити її від перехоплення. Іншими словами, цифрові сертифікати працюють не лише на автентифікацію відправника, а й одержувача [18]. Наприклад, електронна пошта, надіслана з використанням цифрових сертифікатів, шифрується з моменту відправлення до моменту, коли цільовий одержувач відкриває повідомлення. Якщо одержувач не має інформації про приватний ключ, зазначений у цифровому сертифікаті, він не зможе відкрити повідомлення.

Найбільшими перевагами автентифікації на основі цифрових сертифікатів є конфіденційність, оскільки за умови їхнього використання буде захищено дані про користувача та відвернено модифікацію інформації сторонньою особою. Системи цифрових сертифікатів також зручні для користувачів, зазвичай працюють автоматично і вимагають мінімальних дій або участі як відправників, так і одержувачів, а сервери сертифікатів дешевші та легші в управлінні, ніж інші центри сертифікації або системи, що використовуються для шифрування [18].

Хоча ідея цифрових сертифікатів полягає в тому, щоб заблокувати стороннім користувачам можливість перехоплення ваших повідомлень, система не є безпомилковою. У 2011 році, наприклад, кіберзлочинці здійснили злам голландського центру цифрових сертифікатів DigiNotar [18]. Оскільки центри сертифікації відповідають за видачу цифрових сертифікатів (що фактично є електронною версію паспортів), кіберзлочинці часто атакують ці органи, щоб маніпулювати інформацією сертифікатів. У результаті, коли центр сертифікації скомпрометовано, вони можуть створювати веб-сайти або надсилати електронні листи, які виглядають справжніми та проходять тести на сертифікацію, але насправді є шахрайськими.

Центри цифрових сертифікатів постійно оновлюють своє програмне забезпечення, щоб переконатися, що такі загрози безпеці зведені до мінімуму, але загрози безпеці все ще залишаються ймовірними. У 2013 році компанія Forbes зазначила [18], що цифрові сертифікати стали основною ціллю кіберзлочинців, акцентуючи цінність інформації, що вони захищають. Тому програмне забезпечення центрів сертифікації вимагає постійної пильності, щоб захист користувачів від кіберзлочинів залишався на високому рівні.

Отже, цифрові сертифікати є простими у використанні, але їхня безпека залежить від захищеності центрів цифрової сертифікації. Тому слід відповідально обирати такий центр при створенні сертифікату.

Таким чином, існує декілька типів автентифікації, що варуються за простотою у використанні та рівнем безпеки, що вони надають. Автентифікація за паролем залишається найбільш розповсюдженим механізмом для веб-сайтів, але вона не надає задовільний захист, тому слід звернутися до методів, що забезпечують кращий рівень безпеки, залишаючись простим для користувачів.

2.2 Механізм роботи алгоритмів багатофакторної автентифікації

Достатньо простим та надійним методом безпеки може стати двофакторна автентифікація, що захищає від компрометації облікового запису, використовуючи два окремих механізму однофакторної автентифікації разом. Обліковий запис, захищений за допомогою двофакторної автентифікації, зазвичай вимагає від особи автентифікацію за допомогою чогось, що він знає – наприклад, паролю – пароля, а також чогось, що у нього є (наприклад, мобільного телефону або апаратного токена). Багато методів двофакторної автентифікації, які широко використовуються сьогодні, не були піддані належному тестуванню на зручність використання. Тому у наступному розділі буде наведено статистичні дані двотижневого дослідження американської асоціації «USENIX» відносно зручності п’яти методів двофакторної автентифікації для користувачів [20]. В ньому прийняли участь 72 учасника, що входили на імітований банківський веб-сайт майже щодня з використанням того чи іншого методу двофакторної автентифікації та виконували призначене завдання. Загалом учасники дали високі оцінки вивченим методам та висловили зацікавленість у використанні двофакторної автентифікації для забезпечення більшої безпеки своїх конфіденційних онлайн-рахунків. Додаткове дослідження [20] передбачало 30 учасників, що мали оцінити загальну зручність процедури налаштування для згаданих п’яти методів і хоча деякі з них зіткнулися з труднощами з налаштуванням апаратного токена та одноразового пароля, загалом користувачам було легко здійснити налаштування.

Як було наведено вище, паролі є найпоширенішою формою автентифікації користувачів в мережі Інтернет [21]. Хоча було запропоновано багато схем заміни паролів, жодна з них не конкурує зі

зручністю розгортання та використання паролів [22].

Нещодавно великі постачальники послуг, включаючи Google, Facebook і Microsoft, розгорнули додатковий рівень двофакторної автентифікації як частину власних процесів автентифікації для захисту від компрометації облікового запису. Двофакторна автентифікація вимагає від користувачів надати два з наведених вище типів (того, що користувач знає, має або що є частиною користувача).

Використовується кілька методів двофакторної автентифікації типу «те, що користувач має». Такі методи, як SMS, TOTP (одноразовий пароль на основі часу) та апаратні генератори коду (наприклад, RSA SecurID), вимагають від користувача ввести одноразовий код разом із паролем. Ці коди або надсилаються користувачеві через окремий канал, або генеруються на льоту пристроєм користувача. У комерційних та державних установах смарт-картки є часто використовуваним другим фактором, який вимагає від користувача вставити ідентифікаційний бейдж у пристрій для зчитування карт, підключений до комп'ютера. Системи онлайн-банкінгу, особливо у Великобританії, часто використовують варіанти апаратних генераторів коду та зчитувачів карт у своїх реалізаціях двофакторної автентифікації. Компанії, включаючи Google, Dropbox і Github, розгорнули апаратні токени USB (такі як ключі безпеки), такі як YubiKey, внутрішньо [23].

Двофакторна автентифікація забезпечує надійний захист від компрометації облікового запису. Кількість витоків бази паролів підкреслює ризик компрометації облікового запису – оскільки користувачі мають тенденцію повторно використовувати одне й те саме ім'я користувача та пароль на кількох сайтах [24], витік пароля з одного сайту може призвести до ланцюгової реакції компромісу облікового запису, оскільки зловмисники отримують доступ до інших облікових записів з тими ж обліковими даними [25]. Навіть якщо зловмисник вкраде або вгадає пароль користувача, зловмисник має скомпрометувати телефон користувача або вкрасти інший фізичний пристрій-ключ, щоб отримати доступ до облікового запису. Таким чином, віддаленому зловмиснику значно важче зламати обліковий запис, захищений другим фактором автентифікації.

Далі буде порівняно п'ять поширених методів двофакторної автентифікації, що використовують:

1) SMS-повідомлення;
2) Алгоритм TOTP;
3) Попередньо згенеровані коди;

4) Push-повідомлення;
5) Ключі безпеки U2F.

Відмінності між дослідженням USENIX та попередніми аналогічними роботами полягають у тому, що перші вивчають всі п’ять методів у контексті єдиного змодельованого веб-додатка, щоб зменшити потенціал спотворюючих факторів та мати можливість виміряти час для автентифікації за допомогою кожного методу. Вони також відокремлюють налаштування та щоденне використання, а їхнє дослідження є першим, що включає попередньо згенеровані коди. Нижче буде описано кожен метод та його властивості безпеки.

2.2.1 SMS-автентифікація

Одним з найбільш поширених методів двофакторної автентифікації є SMS. Користувачеві надсилається одноразовий код підтвердження (зазвичай довжиною шість цифр) через текстове повідомлення на свій мобільний телефон. Широке поширення частково пояснюється тим, що більшість споживачів вже мають мобільний телефон, здатний отримувати текстові повідомлення — 99% американців згідно з недавнім дослідженням [20]. Потенційні проблеми зі зручністю використання можуть включати затримку доставки, відсутність стільникового зв’язку (наприклад, в іноземній країні чи віддаленому місці) та неправильне копіювання коду з телефону на комп’ютер.

Автентифікація на основі SMS є вразливою на кількох етапах. Мобільні мережі не шифрують повідомлення під час передачі, що дозволяє зловмисникам здійснювати атаки типу «людина всередині». Особливе занепокоєння викликає добре задокументована атака заміни SIM-карт [34, 35]. Крім того, сервер (або довірена сторона) повинен надійно зберігати одноразовий код, поки SMS-повідомлення надсилається, отримується користувачем і вводиться назад на сайт для перевірки. Для запобігання випадкової крадіжки код можливо було б підсолювати та гешувати, але кіберзлочинець може легко провести атаку грубою силою на вкрадений гешований код, враховуючи відносно невелику кількість кодів. Зловмисники також можуть викрасти SMS-коди за допомогою цілеспрямованих фішингових атак. Деякі способи пом’якшення цих загроз полягають у тому, щоб зробити код недійсним через короткий проміжок часу та обмежити кількість невдалих спроб увійти за допомогою коду.

2.2.2 TOTP-автентифікація

Щоб налаштувати TOTP, користувач спочатку синхронізує секретний

ключ, згенерований провайдером, зі своїм смартфоном, зазвичай шляхом сканування QR-коду. Програма генерує код підтвердження, об'єднуючи секрет зі скороченою міткою часу, гешуючи значення та обрізаючи результат, щоб отримати код підтвердження (як у SMS, зазвичай довжиною 6 або 7 цифр). Сервер перевіряє код, наданий користувачем, використовуючи цей самий метод. Перевага використання програми генератора коду TOTP полягає в тому, що після синхронізації секрету з телефоном користувачеві не потрібно покладатися на постачальника стільникового зв'язку для доставки одноразових кодів, що усуває як потенційний вектор атаки, так і проблему зі зручністю використання. Однак, якщо кіберзлочинець викрадає секретний код TOTP із сервера або телефону, він може видати себе за користувача.

Кожен код є дійсним протягом встановленого інтервалу часу, зазвичай лише 30 секунд, після чого має бути згенерований новий код. Смартфон і сервер повинні мати годинник, який є достатньо синхронізованим. Сервер приймає маркери для поточного 30-секундного вікна, а також 30-секундних проміжків безпосередньо перед і після поточного, щоб врахувати зсув годинника. Важливо, що це означає, що користувачі можуть мати лише 30 секунд для введення коду, оскільки коди можуть бути згенеровані в будь-який час протягом 30-секундного інтервалу. Як і у випадку з SMS, коди підтвердження все одно повинні бути введені користувачем вручну, залишаючи додатковий простір для помилок користувача. За даними досліджень [20], 77% американців мають смартфони, а це означає, що TOTP не так широко розгортається на всіх клієнтських базах, як SMS. TOTP вимагає спільного секретного ключа між сервером і мобільним пристроєм користувача. Цей секрет повинен бути надійно збережений, але односторонній механізм гешування не є корисним, оскільки секрет є вхідними для процесу генерації коду та перевірки.

На стороні сервера загальний секрет може бути зашифрований за допомогою пароля користувача, щоб запобігти випадковій крадіжці. За умови безпечного зберігання спільного секрету як на стороні клієнту, так й серверу, TOTP має значну перевагу перед SMS-кодами, оскільки він не покладається на незахищену мобільну мережу для доставки коду, таким чином усуваючи весь ймовірний вектор атаки.

2.2.3 Автентифікація на основі попередньо згенерованих кодів

Попередньо згенеровані коди часто є резервним методом двофакторної автентифікації на випадок, якщо користувач не може отримати доступ до свого основного методу автентифікації. Реалізація є простою та описується наступним чином:

1) Постачальник послуг генерує список кодів підтвердження і змушує користувача друкувати або записувати коди;
2) Довжина самого списку є змінною;
3) Коди зазвичай складаються з 8 цифр;
4) Коди можуть використовуватися в будь-якому порядку і повинні зберігатися в безпеці як сервером, так і користувачем, щоб запобігти крадіжці.

Оскільки ці коди зазвичай є довшими за коди, надіслані через SMS або згенеровані за допомогою TOTP, існує додатковий простір для помилок користувача під час введення кодів. Крім того, користувач повинен бути обережним, щоб не втратити носій, на який він записав коди. Друковані коди зазвичай використовуються як резервний механізм автентифікації і повинні зберігатися на сервері протягом тривалого часу. Навіть якщо застосувати механізм гешування, який обговорювався для SMS-кодів, нетерміновий характер кодів зробить їх уразливими для офлайн-атаки грубою силою. Незважаючи на те, що наступний метод є технічно складнішим для реалізації, одним із засобів зниження ймовірності успішної атаки грубою силою було б гешування резервного коду разом з паролем користувача. Так чи інакше, з боку користувача, надруковані коди повинні надійно зберігатися з використанням традиційних заходів фізичної безпеки.

Відкритим питанням є те, як користувачі вважають за краще зберігати такі резервні коди – чи вважають за краще користувачі зберігати коди при собі для зручності (можливо, зберігаючи коди в гаманці чи гаманці), чи вони вважають за краще вживати більш суворих заходів безпеки для захисту коди.

2.2.4 Автентифікація на основі push-повідомлень

При використанні методу push-повідомлень користувач отримує попередньо налаштоване push-повідомлення на свій смартфон, яке дозволяє користувачеві схвалити або відхилити спробу входу натисканням однойменних кнопок. Push-автентифікація вимагає доступу до Інтернету. Ця техніка підтримується у ряді комерційного програмного забезпечення на кшталт Authy OneTouch і Duo Mobile. Перевага цього методу полягає у зменшенні ймовірності помилки з боку користувача, оскільки немає необхідності копіювати число з екрана телефону. Припускається, що відсутність необхідності вводити цифри, як того вимагають інші методи двофакторної автентифікації, є швидшим і сприймається учасниками як більш зручне для використання.

Push-автентифікація не вимагає явного зберігання секретного ключа,

однак сервер повинен переконатися, що push-повідомлення надсилаються на правильний пристрій, що передбачає, що має відбутися певна форма двосторонньої перевірки клієнта та сервера. Крім того, зв'язок між пристроєм користувача та сервером має бути захищеним, наприклад, за допомогою криптографічного протоколу TLS. Найвідоміші методи автентифікації на основі push-повідомлень є запатентованими, що ускладнює перевірку точних заходів безпеки та вимагає неявної довіри третій стороні. Автентифікація на основі push-повідомлень ще не була добре вивчена спільнотою безпеки.

2.2.5 Автентифікація на основі ключів безпеки U2F

Спочатку розроблений у співпраці з Google і Yubico, а тепер спонсорований Альянсом FIDO, протокол «Universal 2nd Factor» (він же U2F) є відкритим стандартом для автентифікації за допомогою апаратного USB-пристрою. Для автентифікації за допомогою ключа безпеки користувач повинен підключити пристрій до свого комп'ютера та активувати пристрій, коли з'явиться запит на веб-сайті.

Стандарт U2F був розроблений так, щоб бути високозахищеним, але при цьому мав гарну зручність використання [20]. На відміну від інших чотирьох методів двофакторної автентифікації, описаних вище, сам стандарт U2F було розроблено для запобігання фішинговим атакам і забезпечення більшої безпеки та захисту конфіденційності, ніж інші форми двофакторної автентифікації. Автентифікація U2F вимагає, щоб сервер зберігав відкритий ключ, який користувач генерує під час реєстрації – секретний ключ ніколи не покидає пристрій U2F. Основний ризик полягає в тому, що користувач може втратити свій пристрій U2F, але втрата пристрою також є ризиком для інших чотирьох методів двофакторної автентифікації.

2.3 Висновки

У поданому розділі розглянуто однофакторну та двофакторну автентифікації. Було наведено декілька типів автентифікації – за паролем, смарт-карткою та електронним ключом, біометричними параметрами та цифровим сертифікатом. Автентифікація за паролем залишається найбільш розповсюдженим механізмом для веб-сайтів, але вона не надає задовільний захист, що робить двофакторну автентифікацію більш переважною.

Після цього наведено механізми двофакторної автентифікації, що найчастіше використовуються у системах безпеки сучасних веб-сайтів.

3 ОЦІНКА ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

3.1 Умови проведення дослідження

Незважаючи на привабливі переваги безпеки двофакторної автентифікації, її вплив на користувацький досвід залишається неясним. Попередні дослідження двофакторної автентифікації дали результати, які можуть здатися суперечливими. У той час як одна група досліджень [26-29] прийшла до висновку, що двофакторна автентифікація є абсолютно непридатною до використання, інші [23, 30] виявили, що деякі її методи є достатньо вартими. Важко зробити загальні висновки з цих попередніх опитувань і досліджень через дуже різні умови.

Ці фактори ускладнюють визначення того, як різні методи порівнюються з точки зору зручності використання. Компанією «USENIX» проведено двотижневе дослідження юзабіліті між суб'єктами п'яти поширених методів двофакторної автентифікації за участю 72 учасників, де було зібрано як кількісні, так і якісні дані. Учасники входили на імітований банківський веб-сайт майже щодня за допомогою двофакторної автентифікації та виконували призначене завдання. Наявність в усіх учасників досвіду двофакторної автентифікації в контексті однієї програми зменшує незрозумілі фактори, які зазвичай присутні при порівнянні результатів різних методів двофакторної автентифікації в дослідженнях зручності використання. Загалом учасники дали високі оцінки вивченим методам, і багато хто висловив зацікавленість у використанні двофакторної автентифікації для забезпечення більшої безпеки своїх конфіденційних онлайн-рахунків.

Було навмисно проігнорувано проблеми з налаштуванням під час початкового дослідження, щоб не упереджувати учасників щодо повсякденної зручності використання одного з факторів на основі поганого досвіду налаштування. Однак багатообіцяючі результати двотижневого дослідження залишають відкритим питання про те, чи є обнадійливі результати для даного фактора неповними, якщо існує пов'язана з цим перешкода зручності використання для встановлення цього фактора. Щоб зрозуміти це питання, було проведено лабораторне дослідження процесу налаштування п'яти методів двофакторної автентифікації. Хоча деякі учасники зіткнулися з труднощами з налаштуванням апаратного токена та одноразового пароля, загалом користувачам було легко налаштувати методи.

Попередні дослідження досліджували можливість використання методів двофакторної автентифікації за допомогою лабораторних досліджень та опитувань. В одному з них [31] вивчалося налаштування та вхід в систему чотирьох методів двофакторної автентифікації. Виявлено, що учасники зазнали багато невдач і виявили, що систему двофакторної автентифікації важко використовувати. Порядок переваг чотирьох систем, про які йдеться в дослідженні, точно відповідає порядку переваг цих чотирьох систем у дослідженні USENIX, але результати налаштування суттєво відрізняються. Це частково пояснюється тим, що дослідники вимірювали налаштування двофакторної автентифікації та вхід в систему з тими ж учасниками в одному дослідженні. Крім того, змінено інструкції щодо налаштування у проміжку між їхнім дослідженням та дослідженням USENIX, що може пояснити більш позитивні результати налаштування в останньому.

В іншому дослідженні [29] автори порівняли зручність використання трьох апаратних генераторів коду, які оцінювались банком у Великобританії. Користувачі віддали перевагу найзручнішій системі, а не системам з більшим рівнем безпеки. Вони також провели лабораторне дослідження трьох систем автентифікації, включаючи двофакторні системи на основі SMS-повідомлень та апаратного генератора коду. Найбільшого успіху учасники досягли саме за допомогою системи на основі SMS-повідомлень.

Додатково [23] звітується про внутрішнє розгортання ключів безпеки своїм співробітникам. Дослідники повідомляють про довгострокове скорочення кількості запитів на підтримку, пов’язаних з автентифікацією, після розгортання апаратних ключів. Крім того, вони демонструють значне скорочення загального часу автентифікації в порівнянні з іншими методами на основі одноразового коду.

Було проведено два одночасних дослідження [32], які вимірюють як зручність використання, так і прийнятність використання YubiKey (апаратного токена, сумісного з FIDO U2F) як другого фактора захисту облікового запису. Використовуючи протокол обдумування вголос, дано деякі рекомендації Yubico (виробнику YubiKey) на основі загальних моментів плутанини. Через рік дослідники повторили дослідження з новою групою користувачів і виявили, що, хоча багато з попередніх проблем щодо зручності використання були вирішені, багато користувачів все ще не бачили необхідності у використанні YubiKey. Постульовано, що така неприйнятність частково пояснюється неусвідомленням ризиків, які пом’якшуються використанням YubiKey.

Нарешті, описуються два дослідження зручності використання

YubiKeys [33]. Дослідження виявило багато проблем з використанням процесу налаштування YubiKey, але виявилося, що повсякденна зручність використання була значно вищою. Подібно до дослідження USENIX, учасники використовували YubiKey протягом кількох тижнів, хоча у першому випадку вони вивчали YubiKey у поєднанні з кількома іншими методами двофакторної автентифікації. Додатково було проведено інтерв'ю з 21 особою, що використовували двофакторну автентифікацію як частину процесу входу в кілька банків Великобританії. Учасники використовували різноманітні двофакторні методи, включаючи зчитувачі карток, апаратні генератори кодів, SMS, телефонні дзвінки та програми для смартфонів, які генерували одноразові коди. Особливо учасникам не сподобалися апаратні генератори коду; фактично кілька осіб змінили банки через складність використання токенів. Після цього було проведено опитування [28] через сервіс «Amazon Mechanical Turk» серед учасників, які мають досвід використання апаратних генераторів кодів, одноразових кодів через SMS та електронну пошту, а також програм для створення кодів для смартфонів. Виявлено, що електронні листи або SMS-повідомлення були найбільш часто використовуваним другим фактором для фінансових або особистих сайтів, а апаратні токени були найпоширенішими для роботи. Кожен із методів отримав вищі оцінки зручності використання.

Duo — це комерційний продукт двофакторної автентифікації, який підтримує автентифікацію другого фактора за допомогою смартфона, телефонні дзвінки, U2F та кілька інших методів. Було вивчено перехід від системи двофакторної автентифікації на основі токенів до Duo для співробітників за допомогою опитування в Університеті штату Пенсільванія. Так було виявлено, що співробітники віддавали перевагу попередній системі на основі токенів, ніж використанню програми Duo. На переваги деяких співробітників вплинуло їхнє невдоволення тим, що вони змушені використовувати персональні пристрої для роботи. Також було проведено широкомасштабне опитування викладачів і студентів Університету Карнегі-Меллона під час розгортання системи Duo двофакторної автентифікації на всьому кампусі. Результати показали, що багато учасників опитування визнали переваги безпеки від використання двофакторної автентифікації. Вони також виявили проблеми зі зручністю використання під час розгортання Duo. Відмінності у сприйнятті зручності використання між користувачами, які добровільно прийняли двофакторної автентифікації, і тими, від яких потребували її використання, були досить незначними, і багато учасників, яким було необхідно використовувати її, повідомили, що вона є простішою, ніж вони очікували.

Дослідження двофакторної автентифікації USENIX проводилося два тижні в Університеті Бригама Янга. Метою дослідження було порівняти зручність використання п’яти поширених методів двофакторної автентифікації, описаних у розділі вище.

Всього 72 учасники були розділені на 6 груп по 12 учасників у кожній. П’ять груп були призначені до певного методу двофакторної автентифікації, а останньою групою була контрольна група, яка використовувала лише паролі без другого фактора. Кожен учасник спочатку зустрівся з координатором дослідження, щоб створити обліковий запис на веб-сайті дослідження. Під час цієї зустрічі учаснику було надано список з 12 завдань, які потрібно виконати на веб-сайті дослідження протягом наступного двотижневого періоду (при цьому не більше одного завдання на день). Під час виконання кожного завдання кожен учасник входив на веб-сайт дослідження, використовуючи призначений їм механізм автентифікації. Через два тижні учасники повернулися на вихідну співбесіду з координатором дослідження. Використовуючи комбінацію даних про час автентифікації, відповідей на опитування та якісних даних, зібраних під час вихідних інтерв’ю, було порівняно зручність використання різних методів автентифікації, що тестувалися, та зроблено спостереження та рекомендації на основі цих даних.

Тестовим сценарієм передбачалося, що учаснику потрібно ввійти в інтерфейс онлайн-банківської системи та виконати завдання, наприклад переказувати гроші між рахунками або оплачувати рахунок онлайн. Для підтримки цього сценарію було створено імітований інтерфейс онлайн-банкінгу, як показано на рисунку 2.1, де підтримувалася автентифікація за допомогою тільки пароля або пароля разом з одним з п’яти методів двофакторної автентифікації, описаних раніше.

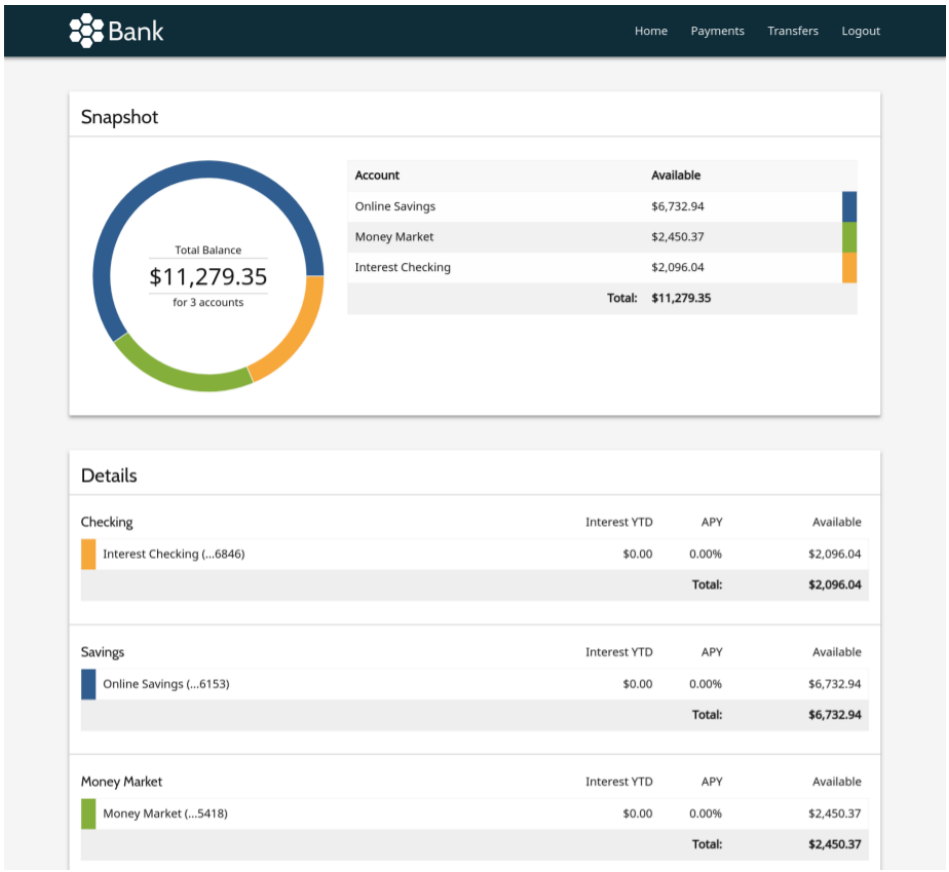

Рисунок 2.1 – інтерфейс імітованого банківського веб-сайту

Було набрано 72 учасники [20] за допомогою листівок, розклеєних по всьому кампусу Університету. Майбутнім суб'єктам було повідомлено, що їм знадобиться щоденний доступ до комп'ютера, під'єднаного до мережі Інтернет, із браузером Google Chrome. Chrome було обрано, оскільки це єдиний основний браузер, що за замовчуванням підтримує ключі безпеки U2F. Щоб отримати право на участь у дослідженні, потенційні учасники заповнили коротке опитування, щоб повідомити, чи є у них смартфон Android чи iOS, та/або чи є у них телефон, який може отримувати текстові повідомлення.

Потім учасники були випадковим чином розподілені до досліджуваної групи, залежно від наявності пристрою – наприклад, один учасник не мав смартфона і був випадковим чином віднесений до групи дослідження, яка не вимагала використання смартфона. Коли група досягла 12 учасників, її видалялося зі списку потенційних груп, до яких було б припустим призначити додаткового учасника.

Статистика учасників дослідження [20] виглядає наступним чином:

1) Було трохи більше жінок (38 осіб, 55%), ніж чоловіків (31 особа, 45%);
2) Учасниками були переважно підлітки та дорослі:

   а) 18–19 років (3 особи, 4%);
   б) 20–29 років (61 особа, 88%);
   в) 30–39 років (5 осіб, 7%).
3) Понад дві третини учасників (49 осіб, 71%) закінчили той чи інший коледж, але ще не отримали диплом;
4) Рівень комп'ютерних знань учасників за їхньою власною оцінкою:
   а) Набагато вище середнього (13 осіб, 19%);
   б) Дещо вище середнього (28 осіб, 41%);
   в) Середній (25 осіб, 36%);
   г) Трохи нижче середнього (3 особи, 4%).

Учасники запланували попередню зустріч з координатором дослідження. Під час першої зустрічі координатор дослідження допоміг їм створити рахунок в інтерфейсі онлайн-банкінгу. Було дозволено учасникам обирати свої логін та пароль, з єдиним обмеженням, що пароль повинен мати довжину не менше восьми символів.

Якщо учасник належав до однієї з груп дослідження, що тестували методи двофакторної автентифікації, координатор також допоміг їм налаштувати її у своєму обліковому записі для веб-сайту дослідження. Залежно від досліджуваної групи, це включало допомогу учаснику в установці будь-яких необхідних програм для push-повідомлень, TOTP тощо, перевірку їх номера телефону, видачу учаснику пристрою U2F (було використано апаратні токени «YubiKey NEO») або роздрукування резервних кодів. Нарешті, координатор дослідження допоміг учасникам виконати перше з переліку завдання під час початкової зустрічі, залишивши учаснику 11 завдань для виконання самостійно.

Для цього дослідження було вирішено зосередитися лише на щоденному використанні методів двофакторної автентифікації і не змішувати ці результати з будь-якими негативними обставинами, які виникають через зручність процесу налаштування. Нещодавні роботи вивчали налаштування двофакторної автентифікації для токенів YubiKey [32, 35] і стверджували, що дослідники повинні досліджувати налаштування та повсякденне використання окремо. Якщо повсякденне використання є прийнятним і перспективним для користувачів, це може надати більшу мотивацію для вирішення проблемних процедур налаштування.

Протягом наступних двох тижнів учасникам було запропоновано виконувати не більше одного завдання на день у порядку, зазначеному в їхньому списку завдань. Щоб виконати кожне завдання, учаснику потрібно буде відвідати симульований веб-сайт онлайн-банкінгу та увійти,

використовуючи раніше вибране ім’я користувача та пароль. За винятком контрольної групи, яка використовує лише пару «логін-пароль», учасник також має автентифікуватися за допомогою призначеного їм методом другого фактора для кожного входу. Після входу учасник переходить на сторінку «Платежі» або «Перекази» і виконує «банківську» частину завдання. Мета полягала у тому, щоб учасники виконали завдання, пов’язане з банківськими послугами, після входу в систему (на відміну від того, щоб просто ввійти в систему і нічого не робити), – для того, щоб спонукати користувача діяти більш природно під час процесу входу та зробити моделювання більш реалістичним, наскільки це можливо.

Через два тижні учасники повідомили про вихідну співбесіду з координатором дослідження. Координатор спочатку попросив учасника пройти коротке опитування, щоб зібрати невелику кількість демографічних даних. Учасники також пройшли оцінку SUS («System Usability Scale», оцінку зручності використання системи) веб-сайту в цілому та методу автентифікації, який вони використовували під час дослідження.

Після цього координатор провів напівструктуроване інтерв’ю з учасником, щоб зібрати додаткову інформацію про те, як учасник ставиться до веб-сайту в цілому, а також до процесу входу. Зокрема, учасникам було поставлено запитання про їх загальну позицію безпеки в Інтернеті, щоб краще зрозуміти їхнє походження та почуття щодо безпеки в Інтернеті. За згодою кожного учасника було здійснено аудіозапис кожного інтерв’ю. Два кодери прослухали записи та закодували кожне інтерв’ю, обговорюючи кожну відповідь до досягнення згоди. Загальні теми, визначені із записів, будуть обговорюватися пізніше.

Після участі в дослідженні учасники отримували компенсацію в розмірі до 25 доларів США відповідно до багаторівневої компенсаційної структури на основі загальної кількості завдань, виконаних через банківський інтерфейс.

3.2 Залежність часу перебування у дослідженні від часу на здійснення автентифікації

Вимірювався час для входу з паролем і час для двофакторної автентифікації на стороні сервера на основі подій, надісланих від клієнта. Відрахування пароля починалося, коли сторінка розпочинала завантажуватися, і закінчувалася, коли користувач вводив пароль. Хронометраж двофакторної автентифікації починався, коли було

завантажено підказку двофакторної автентифікації, і закінчився, коли двофакторну автентифікацію було перевірено (або відхилено). Було записано часові позначки на сервері, оскільки кожен клієнт може мати дещо інший годинник.

Завдяки порівнянню суміжних подій з мітками часу, стало можливим обчислити загальний час здійснення входу. Можливо, користувачі витратили час на отримання свого пристрою двофакторної автентифікації, перш ніж отримати доступ до сторінки входу, що не враховується в наведених даних про час.

Було обчислено кореляцію між кількістю часу, протягом якого особа перебувала в дослідженні, та кількістю часу, необхідного їй для автентифікації. Використовується методика кореляції повторних вимірювань «rmcorr» [36], щоб оцінити загальний нахил регресії для кожного методу двофакторної автентифікації в дослідженні. Припускається, що учасники з часом стануть швидше, оскільки вони ближче знайомляться з методом двофакторної автентифікації. Було знайдено статистично значущу ($p < 0,05$) підтримку цієї гіпотези як для push-повідомлень, так і для ключів безпеки U2F (див. таблицю 2.1).

Таблиця 2.1. Кореляція повторних вимірювань «rmcorr» між кількістю часу участі в дослідженні та кількістю часу на автентифікацію

Метод двофакторної автентифікації	Коефіцієнт p	Коефіцієнт r	Коефіцієнт df	Довірчий інтервал (95%)
SMS	0.280	-0.097	124	(-0.269, 0.081)
TOTP	0.586	-0.049	122	(-0.225, 0.129)
Push-повідомлення	0.029	-0.204	113	(-0.374, -0.020)
U2F	<0.003	-0.269	118	(-0.429, -0.093)
Попередньо згенеровані коди	0.426	-0.076	110	(-0.260, 0.113)

Для порівняння часу, необхідного для двофакторної автентифікації, було застосовано односторонній дисперсійний аналіз Краскала-Уолліса та виявлено, що існує значна різниця ($p < 0,001$, $\alpha = 0,05$) у середньому часі автентифікації між методами. Не включено час, який знадобився користувачеві, щоб ввести свій пароль; спостережувані часи автентифікації, зазначені тут, включають лише час проходження кроку автентифікації другого фактора. Пристрої з ключем безпеки (U2F) мали найшвидший середній час автентифікації, за якими слідували push-повідомлення. Ці результати зведені в таблиці 2.2 та рисунку 2.2.

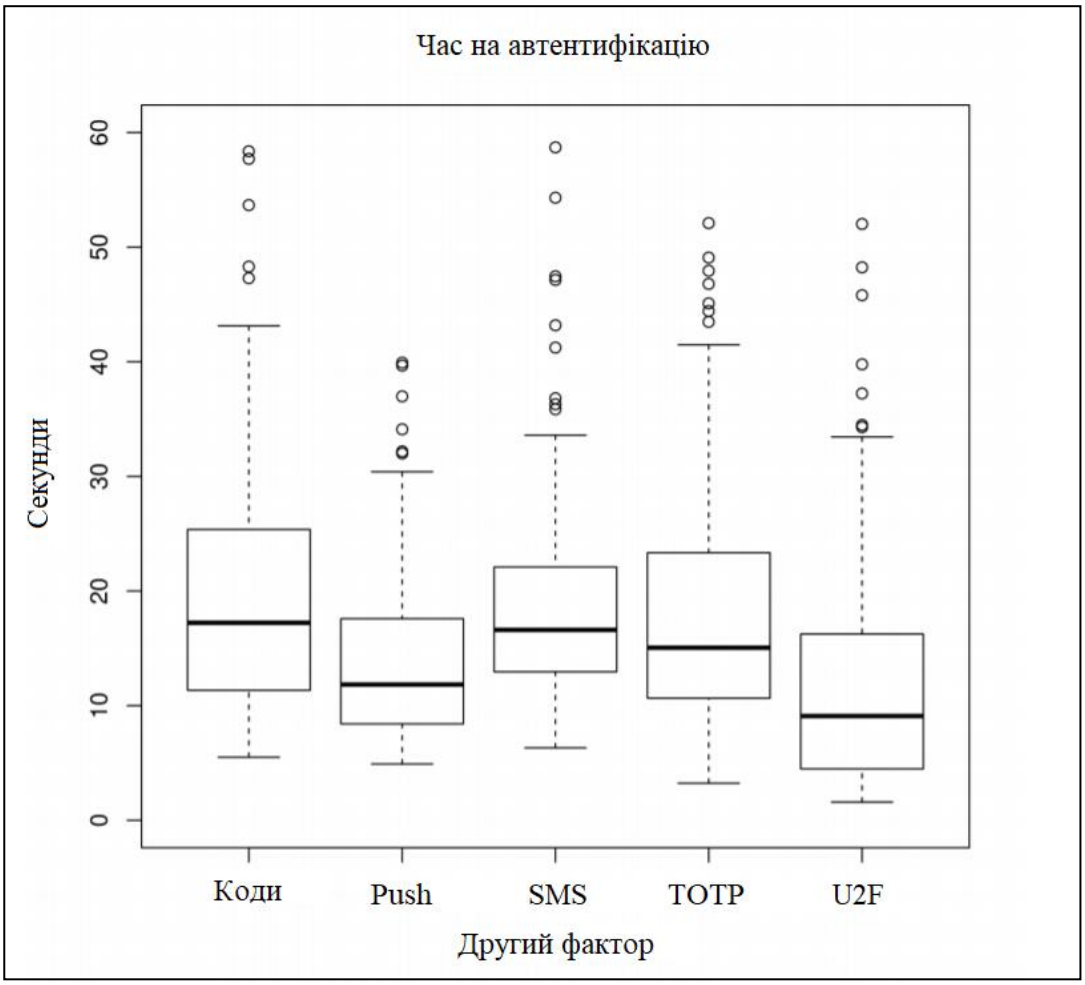

Рисунок 2.2 – час, необхідний для автентифікації при використанні п’яти різних других факторів

Таблиця 2.2. Час автентифікації (секунди), зведена статистика

Метод автентифікації	Q1	Медіана	Середнє значення	Q3
Попередньо згенеровані коди	11.3	17.2	28.0	25.4
Push-повідомлення	8.4	11.8	16.1	17.6
SMS	13.0	16.6	18.5	22.1
TOTP	10.7	15.1	23.9	23.3
U2F	4.5	9.1	13.0	16.3

3.3 Опитування SUS

Було проведено два опитування SUS для учасників на початку кожного вихідного інтерв’ю. Перше опитування розглядало зручність використання банківського веб-сайту в цілому, а друге – лише зручність використання системи входу. Мета проведення двох опитувань полягала в тому, щоб

визначити, наскільки великий вплив мав сам банківський веб-сайт на відчуття учасників щодо методу автентифікації. Крім того, вважалося, що учасники були б точнішими у своїх думках про метод двофакторної автентифікації, якби вони мали можливість розглянути та висловити свої почуття щодо системи в цілому; якби було проведено лише опитування SUS щодо методу автентифікації, учасники можуть з більшою ймовірністю (неправильно) висловитися щодо непов'язаних функцій веб-сайту.

Оцінки SUS для методів автентифікації підсумовано в таблиці 2.3 та на рисунку 2.3. Було проведено односторонній дисперсійний аналіз Крускала-Уолліса і визначено, що використаний метод автентифікації був статистично значущим ($p = 0{,}02579$, $\alpha = 0{,}05$) предиктором медіанної оцінки SUS при використанні методів двофакторної автентифікації. Також обчислено значення $\rho = 0{,}7576$ для коефіцієнта рангової кореляції Спірмена і підтверджено, що існує значна ($p < 0{,}001$) кореляція між загальними оцінками SUS веб-сайту та оцінками SUS окремих методів автентифікації. Паролі без використання другого фактора мали найвищий середній бал SUS із середнім балом 95, за яким слідував протокол одноразових ключів TOTP, який мав середній бал SUS 88,75.

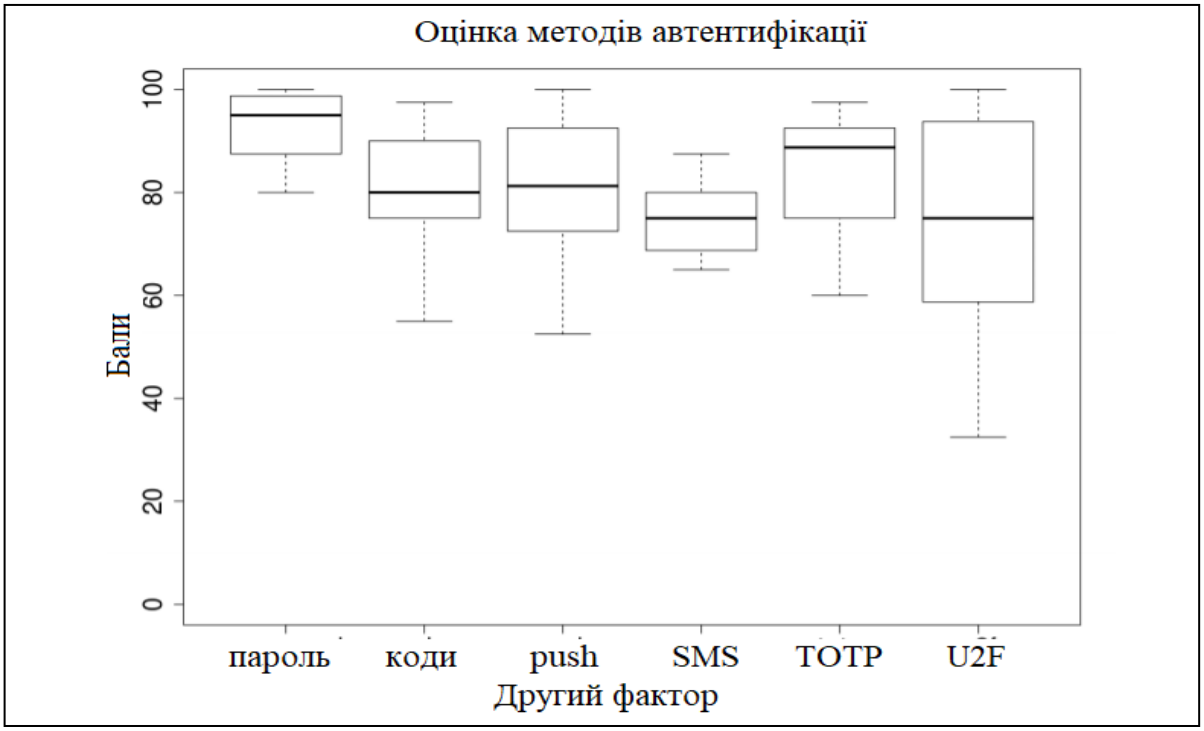

Рисунок 2.3 – оцінка SUS для п'яти других факторів автентифікації

Таблиця 2.3. Оцінки SUS для кожного методу, підсумкова статистика

Метод автентифікації	Q1	Медіана	Середнє значення	Q3
Пароль	87.5	95.0	92.5	98.8
Попередньо згенеровані коди	75.0	80.0	80.2	90.0

Продовження таблиці 2.3

Push-повідомлення	72.5	81.3	81.0	92.5
SMS	68.8	75.0	75.0	80.0
TOTP	75.0	88.8	83.1	92.5
U2F	61.9	75.0	73.1	93.1

3.4 Опитування учасників

Було здійснено опитування учасників відносно того, чи є вхід з використанням другого фактору перевірки більш безпечним. Більшість учасників відчували себе більш захищеними, хоча 3 з 12 учасників, які використовували надруковані резервні коди, не відчували, що коди додають додатковий захист методу. Далі будуть наведені цитати учасників дослідження.

Учасник 6: «Мені здавалося, що коди ні до чого не призвели, тому що це просто більше паролів — будь-хто міг їх відгадати».

Було також опитано учасників відносно того, чи буде додаткова безпека вартою додаткового часу входу або незручностей, з якими вони можуть зіткнутися під час використання методу двофакторної автентифікації. Кілька людей (20 осіб, 29%) сказали, що додаткова безпека, безумовно, є вартою компромісу, а учасники додаткової групи (25 осіб, 36%) заявили, що вони готові використовувати двофакторної автентифікації залежно від важливості облікового запису.

Учасник 25: «На мій погляд, це може бути трохи нав’язливим для всього, але банківські справи – це те, для чого я дійсно хочу певної автентифікації. Я майже хотів, щоб це була вимога, про яку банк сказав би: «О, ось, налаштуйте [двофакторну автентифікацію]. Тому що тепер, коли я думаю про це, я не знаю, як налаштувати двофакторну автентифікацію зі своїм банком. Якби це був варіант, я б точно використав її».

Учасник 33: «Це було досить швидко, так що це було добре. Я не відчував, що мені довелося обходити багато перешкод. Я можу уявити, що було б приємно мати додаткову стіну безпеки, якщо це ваша банківська інформація. Якщо хтось інший отримає ваш пароль, він не зможе зламати ваш обліковий запис, оскільки у нього немає [ключа безпеки]».

Деякі учасники були особливо стурбовані центральним (для них) значенням і важливістю свого облікового запису електронної пошти, особливо враховуючи потенційно велику кількість конфіденційних даних, що зберігаються там. Наприклад, одна учасниця повідомила, що вона вже

ввімкнула двофакторну автентифікацію для свого облікового запису Gmail, щоб отримати додатковий захист.

Учасниця 24: «Я використовую свою електронну пошту для всього, і тому я подумала, що не завадить мати додатковий захист. Думка про те, що хтось зробив би злам [мого облікового запису] і зробив усе вразливим… краще перестрахуватися, ніж шкодувати».

Інші учасники (9 осіб, 13%) прямо заявили, що вони не хотіли б використовувати двофакторну автентифікацію для отримання додаткової безпеки, оскільки незручності були надто високими.

Учасник 37: «Я не знаю, наскільки мій рівень зручності та моя потреба в рівні безпеки будуть збалансовані, тому що для мене мати те, що зручно і є під рукою, майже важливіше, ніж мати щось більш безпечне… Я знаю, що якщо люди зламають ваші кредитні картки, то банк подбає про це і поверне гроші, тому наявність додаткової безпеки робить мене менш дбайливим про наявність другого фактора».

Кожен учасник дослідження в одній із груп двофакторної автентифікації був зобов’язаний використовувати якесь зовнішнє обладнання для свого комп’ютера для входу, будь то аркуш паперу з надрукованими кодами, YubiKey або їхній телефон. Багато учасників (24 особи, 35%) зазначили, що не мають негайного доступу до другого фактора, коли їм потрібно було ввійти.

Учасник 8: «У мене не завжди телефон при собі, і тому, якщо я щось роблю на комп’ютері, я зазвичай роблю домашнє завдання, тому я насправді намагаюся тримати телефон подалі від себе».

Учасниця 42: «Чесно кажучи, коли я вдома, я просто відклала телефон і іноді забувала, куди я його поклала, тому це було трохи важко… Мені потрібно було знайти свій телефон і відкрити програму».

Хоча учасники, які використовували TOTP, загалом дуже позитивно оцінили свій досвід, 8 з 12 учасників зазначили, що у них виникли проблеми з введенням шестизначного коду підтвердження до того, як минув час очікування.

Учасник 30: «Мені потрібно ввести ці цифри дуже швидко, інакше вони зникнуть».

Учасники висловили широкий спектр поглядів на те, яку цінність вони надають своїм онлайн-рахункам. Деякі учасники (9 осіб, 13%) вважали, що їм нема чого захищати і тому не стануть мішенню злочинців.

Учасник 5: «Можливо, тому, що мені нема чого захищати… Я перебуваю на такому етапі свого життя, коли ніщо, чим я володію, не є настільки цінним, і жодна моя інформація не є такою, щоб вона мала значення».

Учасниця 8: «Ви багато чуєте про те, що в когось щось було зламано. Я просто не думаю, що у мене є щось, що люди хотіли б забрати від мене, тому я думаю, що через це я не дуже хвилювалась про це».

Учасник 30: «Наразі у мене на рахунках не так багато грошей, тому якби хтось вкрав мої гроші, це було б погано, але недостатньо, щоб відчувати кінець світу, якщо я втратив усі ці гроші… Я не відчуваю себе мішенню для когось, щоб мої речі викрадали. Але я можу уявити, що в майбутньому, якби у мене був величезний пенсійний фонд чи щось таке, я б хотів, щоб це було більш безпечним».

Було здійснено опитування кожного учасника цього дослідження, чи були коли-небудь скомпрометовані їхні онлайн-акаунти. Кілька учасників (26 осіб, 38%) описали досвід з віддаленими кіберзлочинцями, які захопили їхні онлайн-акаунти, а кілька людей (7 осіб, 10%) згадали, що хтось із їхніх знайомих зламав один з їхніх облікових записів. Хоча це не є прямою формою компрометування облікового запису в Інтернеті, деякі учасники також згадали про досвід фінансової крадіжки через викрадення номера їхньої кредитної чи дебетової картки або викрадення облікових даних банківського рахунку. Інші згадали, що їхня особиста інформація була викрадена в рамках однієї або кількох подій, пов’язаних із порушенням даних, включаючи широко розголошене компанією «Equifax» компрометування мільйонів особистої інформації людей [37]. Коли їх запитали, як вони помітили, що їхній обліковий запис зламано, більшість учасників відповіли, що отримали електронний лист із зазначенням нового входу з підозрілого місця.

Припускалося, що учасники з попереднім досвідом скомпрометованого облікового запису з більшою ймовірністю вважатимуть, що використання другого фактора автентифікації є вартим будь-яких додаткових незручностей. Використовуючи дані, отримані з кодування інтерв’ю (див. таблицю 2.4 та рисунок 2.4), було використано як критерій хі-квадрат Пірсона з двома ступенями свободи, щоб перевірити залежність цих змінних. Не всі учасники прямо говорили про обидві ці змінні; таким чином проаналізовано лише учасників, для яких були закодовані дані для обох змінних.

Таблиця 2.4. Співвідношення учасників зі скомпрометованими обліковими записами та відношенням до незручностей двофакторної автентифікації

«Чи є двофакторна автентифікація вартою незручностей?»	Учасники, що зазнали злам	Учасники, що не зазнали злам
Безперечно	11	9
Іноді	6	19
Ніколи	4	5

Не помічено жодного статистично значущого зв'язку між попередньою історією учасника з компромісом облікового запису та їхньою думкою про те, що двофакторна автентифікація варта незручностей (з урахуванням коефіцієнтів $\chi = 4.6332$, $p = 0.0986$, $\alpha = 0.05$). Одним з обмежень цього аналізу є те, що він не враховує точний характер компрометування попереднього рахунку (наприклад, чи мала місце фінансова втрата). Проте зазначається, що багато людей незалежно заявили, що вони вважають використання двофакторної автентифікації вартим незручностей принаймні невеликий проміжок часу, особливо для банківських або фінансових рахунків.

Нижче додатково буде висвітлено деякі з найцікавіших результатів дослідження USENIX та обговорено їх значення в контексті придатних для використання методів двофакторної автентифікації.

Хоча автентифікація як на основі push-повідомлень, так й ключів безпеки U2F мали швидший середній час автентифікації, жоден із цих методів не отримав найвищого середнього бала SUS. І навпаки, TOTP був найвищим методом другого фактора, який тестувався, але середній час автентифікації був повільнішим, ніж методи на основі push-повідомлень або U2F. З проведених вихідних інтерв'ю було знайдено деякі пояснення цьому результату. По-перше, деякі учасники, які отримували push-запити через Authy, не завжди отримували запит на автентифікацію у своїй області сповіщень, і замість цього доводилося відкривати програму та затверджувати запит вручну. Було незрозуміло, чи це була помилка в Authy, чи результат налаштування сповіщень на телефонах деяких учасників. Кілька учасників U2F, які використовують операційні системи Windows і Mac, повідомили про низку незначних проблем із тим, щоб YubiKey працював зі своїми комп'ютерами (можливо, тому, що вони підключили його в неправильному напрямку). Однак інші учасники повідомили про відсутність проблем із використанням YubiKey. Зрештою, учасники, які використовують TOTP, повідомили, що їм подобається відносна простота програми. Додаток

функціонував дуже подібно до SMS, методу двофакторної автентифікації, з яким багато учасників вже були знайомі, при цьому не вимагаючи від них завжди мати доступ до послуги стільникового зв'язку [20].

Ймовірно, незначні проблеми, з якими стикаються учасники за допомогою програми Authy та YubiKey, пояснюють більшість нижчих балів, які вони отримали. Тим не менш, жоден метод автентифікації, який тестувався, не отримав погану оцінку зручності використання, що свідчить про те, що, хоча є помітний вплив на зручність використання через необхідність двофакторної автентифікації, її наявність сама по собі не прирікає метод в цілому на погану зручність використання.

Додатковим аспектом дослідження є те, що учасники використовували свій другий фактор неодноразово протягом двох тижнів замість того, щоб використовувати його лише один раз у лабораторних умовах. Симульований веб-сайт навмисно не передбачав опцію «Запам'ятати мене», тому від учасників неконтрольних груп вимагалося щодня використовувати свій другий фактор. В рамках дослідження вважається, що деякі впливи на зручність використання другого фактора можливо пом'якшити, якщо ввести другий фактор лише на нових комп'ютерах або після виходу з системи. Вимагання рідшого входу в систему двофакторної автентифікації забезпечить подібний рівень захисту від віддалених кіберзлочинців, в основному дозволяючи користувачам безперешкодний доступ до своїх облікових записів. Деякі системи надають доступ протягом обмеженого періоду часу (наприклад, 30 днів) без використання другого фактора на тому ж апаратному забезпеченні. Учасники з попереднім досвідом використання таких систем (як правило, систем для входу до університету) зробили деякі зауваження щодо того, що вони ніколи не були впевнені, коли знадобиться другий фактор. Одним із рішень цієї проблеми було б показувати користувачеві невеликий зворотний відлік, який розповідає, скільки днів залишилося, доки їм знову потрібно буде вказати другий фактор, щоб уникнути ефекту «засідки» [38]. Необхідно провести подальші дослідження, щоб визначити правильний баланс того, коли запитати користувача про другий фактор знову, якщо він уже ввійшов у систему раніше на тій же машині.

Враховуючи слабкі результати попередніх досліджень двофакторної автентифікації щодо зручності використання, в USENIX очікувалася погана загальна реакція щодо зручності використання. Під час вихідних співбесід вони були здивовані кількістю учасників, які повідомили про загальний позитивний досвід використання двофакторної автентифікації. Багато

учасників хотіли використовувати двофакторну автентифікацію для деяких своїх фактичних онлайн-облікових записів, але або не знали, що цей варіант є припустим, або не знали, як його налаштувати.

Хоча учасники, як правило, менше дбали про безпеку своїх акаунтів у соціальних мережах, багато хто висловив стурбованість безпекою своїх банківських та фінансових рахунків. Були неоднозначні відчуття щодо часто використовуваних облікових записів, таких як облікові записи електронної пошти, зокрема, щодо балансу, чи варто використовувати двофакторну автентифікацію для таких облікових записів. Учасники загалом погодилися, що вони не хочуть, щоб вони використовували свій другий фактор для входу до свого облікового запису електронної пошти з відомого комп'ютера. Інші учасники вважали, що у них немає конфіденційної інформації в електронній пошті, і що наявність другого фактора не є вартою додаткового кроку входу. Загалом, чим вище сприймається значення облікового запису, тим більша ймовірність того, що учасник захоче використовувати двофакторну автентифікацію для облікового запису.

Дослідження USENIX має ряд обмежень.

1) Учасників не запитували про те, чи вони використовували раніше двофакторну автентифікацію. Користувач, призначений до другого фактору, з яким він уже був знайомий, міг схилити результати.
2) Учасниками були студенти університетів, які були молодшими та більш технічно підкованими, ніж загальне населення. Студенти також мають більшу ймовірність мати менше матеріальних цінностей, про які потрібно зайнятися, як зазначено в якісних результатах.
3) Було свідомо вирішено не дозволяти учасникам самостійно встановлювати механізм двофакторної автентифікації, щоб поганий досвід налаштування не негативно впливав на повсякденне використання. Це рішення означає, що повсякденні результати зручності використання можуть бути більш упереджені в порівнянні з користувачами, яким доведеться налаштувати власноруч та використовувати двофакторну автентифікацію.
4) Оскільки були необхідними дані про час автентифікації, учасникам не дозволялося використовувати дійсну банківську систему або існуючий онлайн-рахунок, оскільки це могло змінити їхню поведінку.
5) По-п'яте, учасники повинні були використовувати двофакторну автентифікацію для кожної спроби отримання доступу, що,

можливо, змусило їх звикнути до використання двофакторної автентифікації занадто швидко.

6) Дискусії учасників щодо необхідності двофакторної автентифікації та онлайн-безпеки могли б відрізнятися, якби веб-сайт імітував соціальну мережу замість сторінки банку.
7) Маючи лише 12 учасників у кожній дослідницькій групі, існує ймовірність не досягти достатнього насичення в якісних даних, які були зібрані. Навіть якщо це не так, обмежені демографічні показники дослідження все одно вимагають подальших досліджень із більш широким населенням.

Було навмисно проігноровано етап налаштування під час двотижневого дослідження [20], щоб уникнути поганого досвіду налаштування, який може негативно вплинути на оцінку учасниками щоденної зручності використання одного з факторів. Однак багатообіцяючі результати дослідження викликають питання про те, чи є результати неповними, і чи упускають вони важливу пов'язану перешкоду зручності використання для встановлення цього фактора. Щоб розібратися в цьому питанні, представниками USENIX було проведено лабораторне дослідження з метою порівняти зручність фази налаштування для п'яти методів двофакторної автентифікації. Виходячи з первинного огляду процесу налаштування на деяких популярних веб-сайтах, не очікувалося, що виникнуть значні проблеми зі зручністю налаштування п'яти методів двофакторної автентифікації.

3.5 Додаткове лабораторне дослідження

Кожен учасник отримав завдання налаштувати п'ять методів двофакторної автентифікації з настільного комп'ютера за допомогою наданого облікового запису Google. Google було обрано через відомість та професійну підтримку безпеки для своїх клієнтів і співробітників. Налаштування ключів безпеки було вивчено раніше, і на основі цих результатів було внесено покращення [32, 33].

Мета додаткового лабораторного дослідження полягала в тому, щоб спостерігати загальну зручність процесу налаштування, а не зосереджуватись на деталях, що стосуються постачальника, оскільки не порівнювалося налаштування між кількома постачальниками. Учасники отримали телефон на базі Android та апаратний токен «YubiKey NEO» для методів, які потребують фізичного пристрою. Тестування для кожного можливого порядку налаштування п'яти методів вимагає 120 процедур. Щоб скоротити

час і витрати на наше дослідження, було створено неповну врівноважену міру, призначену для пом'якшення спотворень через порядок встановлення учасниками кожного з методів двофакторної автентифікації. Використовувались два збалансованих латинських квадрата п'ять на п'ять, щоб створити десять різних упорядкувань налаштування методів автентифікації, щоб урівноважити послідовні ефекти, викликані цими упорядкуваннями [39]. Кожне з десяти завдань було виконано три рази протягом дослідження. Після кожної спроби налаштувати другий фактор учасникам пропонувалося заповнити єдине опитування про легкість «SEQ», щоб виміряти складність кожного завдання. SEQ — це стандартна анкета щодо зручності використання з одним запитанням – «Загалом, наскільки важко чи легко було виконати завдання?», оціненим за 7-бальною шкалою. Хоча опитування містить лише одне запитання, було виявлено, що SEQ працює достатньо надійно та забезпечує достовірні відповіді від осіб, що опитуються [40]. SEQ було обрано для того, щоб уникнути втоми від опитування, оскільки учасники повинні були оцінити п'ять різних методів. Таким чином дослідники використали дані часу та відповіді SEQ, щоб порівняти зручність налаштування для п'яти методів.

Листівки було розміщено у згаданому раніше кампусі Університету, щоб набрати 30 учасників, що вміли працювати з обліковими записами Google і телефонами на базі Android. Коли кожен учасник зустрівся з координатором дослідження, вони спочатку підписали форму згоди. Після завершення дослідження учасникам було виплачено 10 доларів США. Після цього учасників було розподілено на десять латинських квадратів у порядку кругової системи.

Координатор надавав учаснику телефон на базі Android, апаратний токен YubiKey та інформаційний лист із зазначенням номера мобільного телефону та пароля блокування екрана. Було зроблено аудіозапис словесних коментарів кожного учасника разом із відеозаписом екрану комп'ютера. Не дозволялося налаштовувати автентифікацію за резервними кодами, push-сповіщеннями або TOTP без попереднього налаштування методів на основі SMS або U2F. Щоб перевірити кожен метод незалежно, використовувався один обліковий запис Google для налаштування SMS і окремий обліковий запис для інших чотирьох варіантів. Координатори дослідження перейшли на сторінку налаштування двофакторної автентифікації у браузері Chrome, а потім проінструктували учасників, у якому порядку налаштувати п'ять других факторів. Координатори також переходили між двома обліковими записами Google до та після SMS-повідомлення про налаштування учасника. Після того, як учасник виконав завдання або не зміг завершити

налаштування, координатор запропонував учаснику пройти опитування SEQ. Соіл зазначити, що координатори не допомагали учасникам у встановленні жодного з других факторів.

Нижче наведено короткий опис кожного завдання налаштування.

1) SMS. Учасникам було запропоновано ввести номер телефону. Після цього Google надсилав на вказаний номер текст підтвердження, що містить шестизначний код. Учасник завершує налаштування, ввівши код на веб-сторінці Google.
2) TOTP. Учасникам надали телефони Android без встановленого додатка автентифікації. Передбачалося, що учасники завантажили б програму у рамках налаштування через припущення, що типовий користувач Google не встановлює цю програму на своєму телефоні. Телефон був налаштований за допомогою програми PlayStore на домашній сторінці для легкого доступу. Було доручено учасникам встановити програму за допомогою PlayStore, а потім відсканувати QR-код, показаний на веб-сторінці. Після сканування QR-коду учасники завершили налаштування, ввівши шестизначний код із програми на веб-сторінку.
3) Попередньо згенеровані коди. Автоматично генерується десять резервних кодів за запитом. Учасники не повинні були друкувати або завантажувати ці коди, але координатор запитав, як вони зберігатимуть ці коди, якби вони використовували власний обліковий запис Google. Деякі учасники поділилися, що вирішили б сфотографувати коди за допомогою камери на телефоні, а інші сказали, що запишуть коди та збережуть їх у безпечному місці. Для даних часу було здійснено вимірювання, починаючи від першої секунди виконання учасником завдання та закінчуючи відображенням на екрані резервних кодів. Незважаючи на опитування учасників про їхній ймовірний метод зберігання резервних кодів, у дані про час налаштування не було включено час, необхідний для зберігання кодів, оскільки він сильно різниться залежно від вибраного методу зберігання.
4) Push-повідомлення. Для push-повідомлень потрібно, щоб учасник через телефон увійшов в обліковий запис Google. Телефон, наданий учасникам, уже мав доступ до системи через припущення, що звичайний користувач Google уже має доступ до свого облікового запису на його телефоні. Коли телефон підключено до Інтернету та облікового запису, а у нього ввімкнено блокування екрана,

надсилається push-сповіщення, яке можливо схвалити, розблокувавши телефон і натиснувши кнопку «Так» у сповіщенні.

5) Ключ безпеки U2F. Учасникам було надано апаратний токен «YubiKey NEO». Надано інструкцію вставити ключ безпеки у відкритий USB-порт, а потім натиснути золоту кнопку на ключі. Перш ніж пристрій можливо було розпізнати, учасники повинні були відхилити сповіщення з браузера з проханням дозволу побачити марку та модель пристрою U2F. Незалежно від того, дозволяє користувач або відхиляє цей запит, пристрій U2F реєструється та за бажанням отримує назву. Оскільки процедура отримання імені не є обов'язковою, час для неї було виключено з даних.

Для вимірювання часу налаштування кожного методу двофакторної автентифікації використовувався відеозапис екрана. Час вимірювався в секундах від моменту, коли учасник розпочав завдання налаштування, до моменту, коли учасника сповіщено про успішне налаштування. Випадки, коли учасник не зміг завершити налаштування, не буде включено до даних, отриманих під час аналізу часу. Помилка налаштування сталася двічі з пристроєм U2F і двічі з програмою TOTP. Підсумок результатів наведено в таблиці 2.5 та на рисунку 2.4.

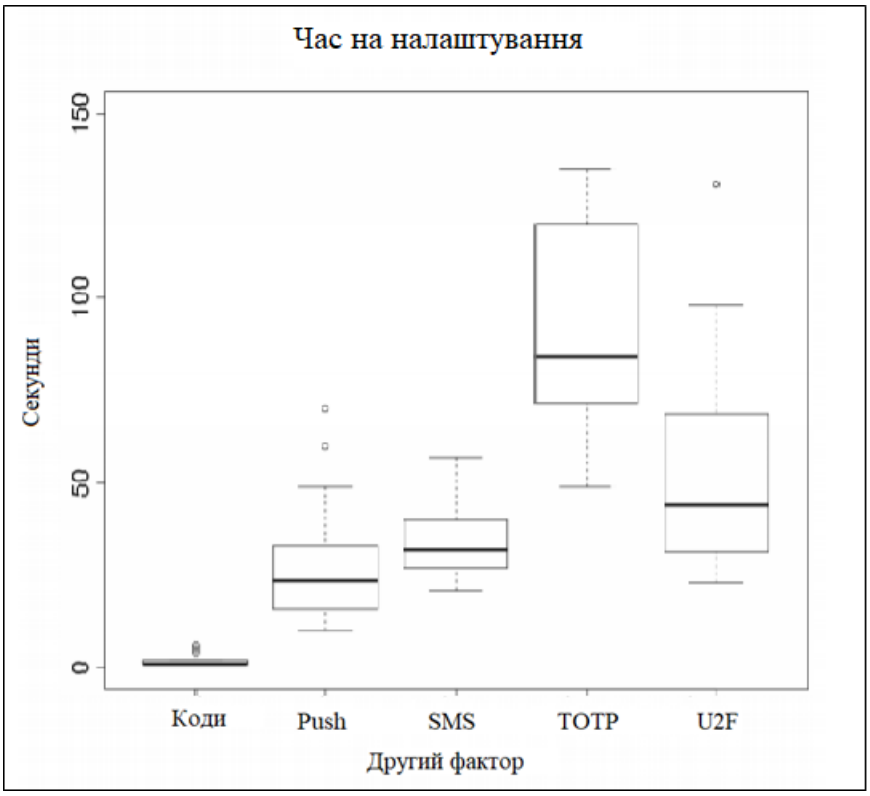

Рисунок 2.4 – час налаштування п'яти других факторів автентифікації

Таблиця 2.5. Час налаштування (у секундах), підсумкова статистика

Метод автентифікації	Q1	Медіана	Середнє значення	Q3
Попередньо згенеровані коди	1.0	1.0	2.2	2.0
Push-повідомлення	16.0	23.5	27.3	33.0
SMS	27.5	32.0	34.5	40.0
TOTP	73.3	84.0	109.6	120.0
U2F	31.8	44.0	57.8	67.8

Як і очікувалося, резервні коди мали найшвидший час налаштування, оскільки все, що було задіяно, це натискання кнопки веб-сторінки для створення кодів. Проте резервні коди мали найдовший середній час автентифікації в щоденному дослідженні, за якими слідували push-сповіщення та SMS-повідомлення. У той час як пристрої U2F мали найшвидший середній час автентифікації в дослідженні, вони мали другий за довжиною середній час налаштування. TOTP мав найповільніший середній час налаштування.

Учасники відповідали на питання SEQ після того, як виконали (або не змогли завершити) кожен метод двофакторної автентифікації. Середні показники SEQ наведено в таблиці 2.6. За винятком резервних кодів, рейтинг найкращого SEQ до гіршого відповідає рейтингу часу на встановлення, тобто чим швидше налаштування, тим вище середній показник SEQ. Дослідників здивувало, що резервні коди отримали нижчий рейтинг, оскільки налаштування не передбачало нічого іншого, як натискання кнопки. Ймовірно, уявлення учасників про повсякденну зручність використання методу двофакторної автентифікації вплинуло на їх оцінку SEQ, навіть якщо їм було доручено оцінити лише зручність використання завдання налаштування.

Таблиця 2.6. Середній бал в опитуванні SEQ

Push-повідомлення	SMS	Згенеровані коди	U2F	TOTP
6.7	6.2	5.9	4.7	4.5

Дослідження показує, що коли налаштування двофакторної автентифікації можливо реалізувати добре, користувачам зазвичай це легко зробити. Кожен із п’яти других факторів мав середній бал, ближчих до оцінки «легко», ніж до оцінки «важко». Це є примітним, враховуючи, що координатори дослідження не надавали допомоги під час налаштування, і багатьом учасникам потрібно було встановити другі фактори, які були їм незнайомі (наприклад, пристрій U2F або генератор TOTP). Автентифікація

SMS є однією з найпоширеніших форм двофакторної автентифікації, і знайомство з використанням SMS як другого фактора, ймовірно, вплинуло на його оцінку SEQ.

Збій налаштування стався двічі з TOTP і двічі з U2F. Обидва збої в TOTP відбулися, коли учасник негайно спробував відсканувати QR-код камерою телефону, замість того, щоб завантажити програму для сканування коду. Ще двоє учасників спочатку спробували відсканувати QR-код камерою телефону, але зрозуміли свою помилку та успішно завершили налаштування після завантаження програми. Обидва збої в U2F сталися, коли учасник не помітив сповіщення браузера із запитом на дозвіл побачити марку та модель пристрою U2F. Не вимагається марка чи модель для автентифікації пристрою, тому пристрій U2F буде зареєстровано незалежно від того, дозволив користувач чи відхилив запит веб-переглядача. Однак учасники, які взагалі не помітили сповіщення, не змогли завершити налаштування. На основі спостережень представлено дві рекомендації щодо зменшення помилок налаштування облікових записів Google.

1) Користувачі з меншою ймовірністю пропустять встановлення програми, якщо інструкції зі встановлення містяться в підказці окремо від QR-коду.
2) Оскільки сповіщення браузера U2F виникає у багатьох браузерах, які підтримують U2F (включаючи Chrome, Opera та Firefox), постачальники двофакторної автентифікації повинні сповіщати користувачів про сповіщення під час процесу налаштування. Yubico робить це на своїй сторінці підтримки, у такій формі: «Доторкніться до YubiKey, коли з’явиться запит, і, якщо запитають, дозвольте йому побачити марку та модель пристрою».

Учасники дослідження були набрані в Університеті Бригама Янга, а тому результати не можуть бути узагальнені для широкої популяції. Протестовано налаштування на настільному комп’ютері, і процес налаштування може відрізнятися при використанні телефону як основної обчислювальної платформи. Дані про час для резервних кодів не включали час, необхідний для зберігання кодів. На дані про час і результати SEQ може негативно вплинути незнайомство учасників із наданим телефоном. Якби учасники використовували особистий телефон, вони, ймовірно, швидше б виконали завдання, для яких потрібен телефон (наприклад, ввести номер телефону або розблокувати його). Хоча дослідження не зосереджувалося на деталях, пов’язаних із постачальником, впровадження налаштувань двофакторної автентифікації вплинуло на сприйняття користувачів.

3.6 Висновки

Проаналізовано два просунутих дослідження компанії USENIX, здійснених з метою оцінки повсякденної зручності використання кількох методів двофакторної автентифікації. В його рамках учасникам запропоновувалось входити на імітований банківський веб-сайт майже щодня протягом двох тижнів і виконувати призначене банківське завдання. Завдяки тому, що всі учасники випробовують метод двофакторної автентифікації в контексті одного додатка, зменшується кількість незрозумілих факторів, які зазвичай присутні під час порівняння результатів різних методів двофакторної автентифікації в дослідженнях зручності користування.

Загалом учасники поставили високі оцінки вивченим методам, і багато хто висловив інтерес до використання двофакторної автентифікації для своїх конфіденційних онлайн-рахунків. Проте близько третини учасників повідомили про те, що їх пристрій другого фактора не був негайно доступним, коли їм це було потрібно.

З двотижневого дослідження було винесено ряд висновків. Учасники, які використовували push-повідомлення та ключі безпеки U2F, скоротили час входу, оскільки вони набули досвіду роботи з методом. Дві третини учасників, які використовували TOTP, мали проблеми з введенням шестизначного коду до того, як минув час очікування. Приблизно 25% учасників, які використовували надруковані резервні коди, не відчували, що коди додають додатковий захист системі – їм здавалося, що це просто ще один пароль, який зловмисник може скомпрометувати. Дослідники також порівняли зручність етапу налаштування для кожного з п’яти методів двофакторної автентифікації. Хоча деякі учасники зіткнулися з труднощами з налаштуванням U2F і TOTP як других факторів, загалом користувачі знайшли ці методи легкими у налаштуванні. Разом ці два дослідження показують, що добре реалізовані методи двофакторної автентифікації можливо налаштувати та використовувати щодня без особливих труднощів.

4 ПРОГРАМНА РЕАЛІЗАЦІЯ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ЯК ПОСЛУГИ ПЛАГІНУ БЕЗПЕКИ

4.1 Особливості алгоритму автентифікації, що використовується у плагіні

Завдяки проведеному аналізу даних про існуючі плагіни безпеки та методи двофакторної автентифікації було вирішено розробити власний плагін для веб-сайтів на основі CMS WordPress. Створення та використання паролю залишається обов'язковою мірою безпеки, але додатково плагін вимагатиме від користувача ввести одноразовий код, створений за протоколом TOTP. Його використання спрощує настроювання плагіну, а також виключає оплату послуг сервісів відправки SMS-повідомлень, підвищуючи таким чином ефективність та дозволяючи його безкоштовне використання. Він інтегрує сумісний додаток з веб-ресурсом, до якого підключається, але додатково плагін дозволяє активацію двофакторної автентифікації для того чи іншого користувача.

Задля забезпечення додаткової безпеки в плагіні було реалізовано наступний функціонал:

1) Лімітування кількості спроб входу

Після встановлення система WordPress, за умови відсутності додаткових плагінів, не обмежує кількість спроб входу в систему. Розроблений плагін вирішує цю проблему, надаючи опцію на налаштування допустимої кількості спроб та час, на який буде заблоковано обліковий запис користувача, що перевищив ліміт. Це вирішує одну з найбільших проблем безпеки (зокрема, для веб-сайтів на основі WordPress) – можливості здійснити атаку грубою силою на паролі та логіни, що підвищує ймовірність несанкціонованого отримання кібелзлочинцем прав адміністратора, що призводить до ймовірного неправомірного використання, розміщення забороненого інформаційного вмісту, реклами або переправлень до інших веб-ресурсів.

2) Зміна URL-посилання сторінки входу до панелі адміністрування

Подана функція відокремлює від дійсних користувачів ботів – програмне забезпечення, що автоматично шукає вразливі веб-ресурси, а також здійснює атаки грубою силою. Принцип роботи таких ботів опирається на відомість стандартних URL-посилань системи WordPress, зокрема на панель адміністрування «site.com/wp-admin» та часто використовувані альтернативи на кшталт «site.com/admin» або «site.com/login».

Плагін безпеки дозволяє редагувати стандартне посилання на адміністраторську панель, через що зменшується ймовірність її знаходження та зламу ботами.

3) Приховування версії WordPress, встановлених зовнішніх додатків та тем для CMS

Часто власники веб-ресурсів на основі системи управління вмістом WordPress не займаються своєчасним оновленням її та плагінів, що надає кіберзлочинцям додатковий вектор атак, оскільки чим старіша версія, тим більше вразливостей вона має. Чотири рази на рік в мережі Інтернет стають опублікованими нові вразливості для різних версій CMS WordPress, плагінів та тем для неї. Тому наявність інформації за умови знання версії системи (або додатків до неї) будь-хто може з легкістю використовувати вразливість та отримати доступ до системи.

Для запобігання цьому сценарію плагін безпеки приховує версію системи управління вмістом та додатків до неї, що робить неможливим аналіз налаштування системи, а також підбор придатних до експлуатування вразливостей.

4) Дезактивація застарілого протоколу віддаленого управління XML-RPC

З перших версій WordPress мала XML-RPC – протокол віддаленого управління веб-сайтом через передачу закодованого (через XML) текстового пакету налаштувань. Це було проривним рішенням через повільне інтернет-з’єднання, що запобігало редагуванню веб-сайту через адміністративну панель, але тепер він надає додатковий вектор атак. По-перше, через необхідність у прискореної автентифікації існує вимога включити до текстового файлу логін та пароль користувача з відповідними правами, що надає простір для атаки грубою силою (оскільки за замовчуванням обмежень на кількість спроб відправити такі файли не існує). По-друге, при певній конфігурації відправки таких файлів кіберзлочинець може здійснити DDoS-атаку на веб-ресурс та вивести його з ладу. Тому плагін автоматично дезактивує XML-RPC. Це не приносить незручності, оскільки у WordPress реалізовано альтернативний функціонал віддаленого доступу, що було інтегровано безпосередньо у прикладний програмний інтерфейс.

5) Заборона на редагування файлів через панель адміністрування

Подана функція має дві мети – вона захищає систему, її конфігурацію, плагіни та теми як від зловмисника, навіть якщо той зумів здійснити злам веб-ресурсу, так й від його власника (чи його колег). Якщо адміністратор не

має достатнього досвіду настроювання веб-ресурсів, він є у змозі порушити конфігурацію до такого ступеню, що відновленню сайт вже не підлягатиме. Плагін також передбачає такий сценарій, тому опція редагування відповідних файлів через панель адміністратора також деактивується автоматично.

6) Відключення небезпечних підказок WordPress на сторінці входу

За замовчуванням, система управління вмістом при вході в обліковий запис повідомляє користувача, чи існує введений логін. Втім, ця інформація може допомогти зловмиснику прискорити процес атаки грубою силою – підібравши логін, він не матиме шукати інші та почне перебір паролів. Плагін вирішує цю проблему заміною повідомлення «некоректний пароль» на «некоректний логін або пароль».

7) Автоматичне оновлення WordPress та додатків до нього

Як наводилось вище, оновлення CMS, плагінів та тем для неї – це один з найголовніших факторів безпеки, який часто ігнорують власники веб-сайтів. Для усунення цієї проблеми плагін підтримує можливість автоматично оновлювати наведене програмне забезпечення, що запобігає використанню ряду вразливостей та, в свою чергу, підвищує безпеку веб-ресурсу. Цей функціонал залишається актуальним через масштабні злами, що періодично здійснюються через несвоєчасно оновлене програмне забезпечення та призвело до втрати чуттєвих даних, а також до появи на веб-сайтах протиправного вмісту.

4.2 Переваги програмної реалізації перед існуючими

Оскільки більшу частину системи управління вмістом WordPress було розроблено в 2003-2004 роках, система не зазнавала великих модифікацій системи безпеки – окрім виправлення найбільш критичних вразливостей. Подібне відношення розробників до функціональних оновлень системи залишає вразливості у її безпеці.

На даний момент система управління вмістом є схильною до найголовнішої проблеми – можливості здійснення атаки грубою силою. На жаль, її розробники не передбачили будь-якого обмежуючого функціоналу у цій частині системи. Втім, вони дозволили вироблення зовнішнього програмного забезпечення – плагінів, у тому числі таких, що може вирішити цю проблему. Завдяки цьому стало можливим розробити плагін, що є здатним забезпечити повноцінний захист системи доступу до веб-ресурсу у першу чергу, а також його удосконалення за допомогою двофакторної

автентифікації у подальшому.

У порівнянні з іншими плагінами безпеки, розроблене у рамках поданої роботи програмне забезпечення має такі переваги, як:

1) Поєднання захисту від атак грубою силою із механізмом двофакторної автентифікації, що зводить нанівець крадіжку облікового запису адміністратора. До того ж плагін забезпечує якнайшвидше закриття вразливостей системи через автоматичні оновлення, а також запобігає скороченню часу цих атак через те, що кіберзлочинцю стане необхідним додатково знайти логін (у той час як без плагіну він, дізнавшись правильний логін, мав би знайти тільки пароль);
2) Можливість безкоштовного комерційного використання, на відміну від більшості інших плагінів. Це дозволяє корпораціям встановити та застосовувати плагін без необхідності переузгоджувати бюджет та взагалі сплачувати його, таким чином підвищуючи безпеку їхніх веб-сайтів та, опосередковано, мережі Інтернет у цілому;
3) Відкритий початковий код – ця особливість підвищує довіру користувачів до плагіну, надаючи можливість переконатися у його надійності;
4) Простота – плагін починає захист з моменту його підключення до веб-сайту, без необхідності встановлювати або редагувати велику кількість налаштувань. До того ж він базується на мобільному програмному додатку, що встановлюється, через що користувач не має оплачувати та налаштовувати приймання кодів шляхом SMS-повідомлень та дзвінків;
5) Зрозуміла для українського сегменту користувачів локалізація – в той час, як більшість аналогів використовують тільки англійську мову, розроблений плагін було перекладено, що вкупі з невеликою кількістю налаштувань поліпшить досвід використання.

4.3 Налаштування оновленого програмного додатку

Далі буде представлено кроки для налаштування плагіну з описом його функціональних особливостей. Для активації програмного додатку необхідно відкрити адміністративну панель веб-сайту, перейти в розділ «Плагіни» та встановити плагін «Frity Security», що розташовано у відповідному zip-архіві.

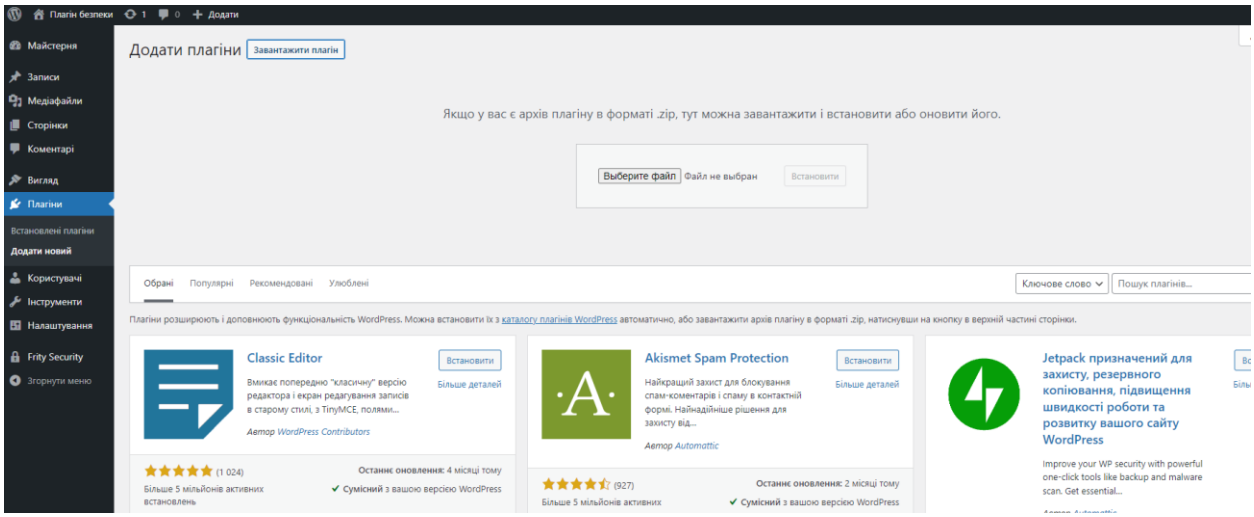

Рисунок 3.1 – меню встановлення плагінів

Після встановлення плагін необхідно активувати. Для цього достатньо натиснути на кнопку «Активувати», як показано на зображенні нижче.

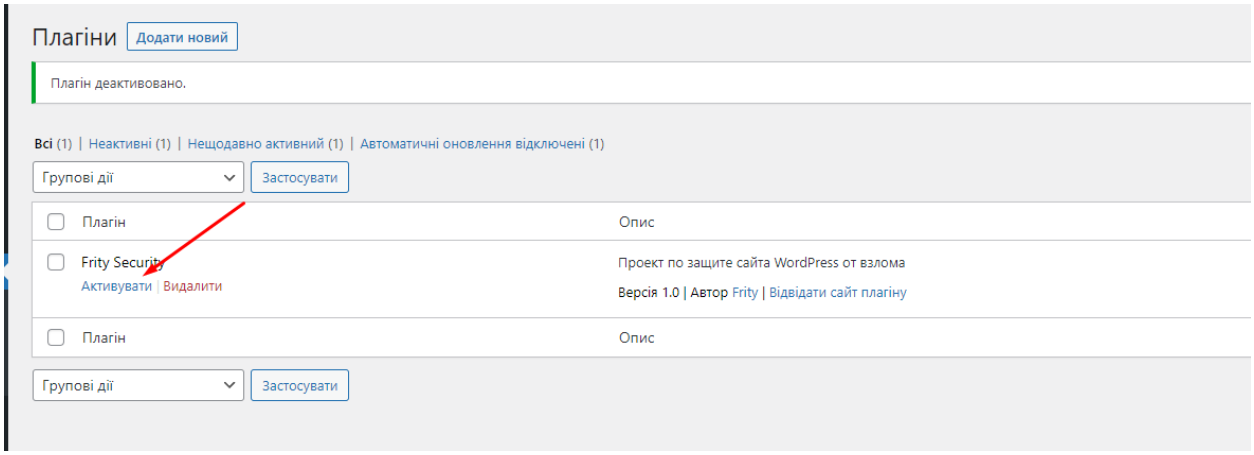

Рисунок 3.2 – активація плагіну

Слід помітити, що програмний код плагіну є об'ємним, але його реалізовано у такий шлях, щоб користувачеві було легше працювати з плагіном. Наприклад, сторінку налаштувань відображено у зрозумілий шлях та автоматизовано, до того ж вона не перетинається з панеллю адміністрування. Остання лише дозволяє здійснювати функціональні налаштування на кшталт підключення модулю капчі «ReCaptcha», додавання ключів, конфігурації двофакторної автентифікації шляхом підключення через смартфон тощо. Для налаштування ReCaptcha необхідно:

1) Перейти в розділ «Frity ReCaptcha» та перейти за посиланням для отримання ключів;

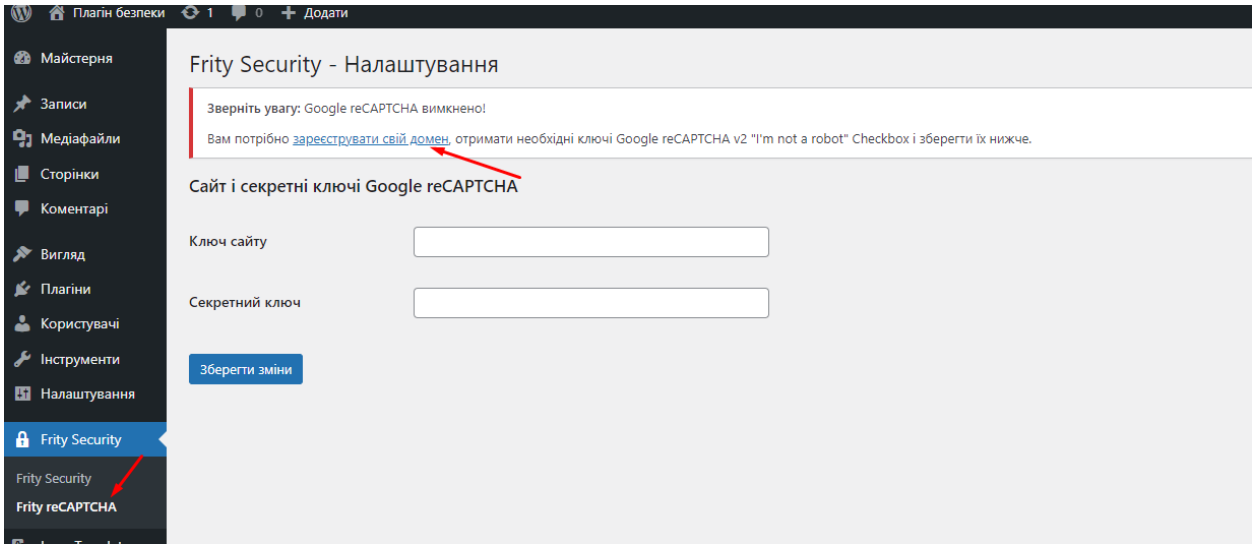

Рисунок 3.3 – меню налаштування ReCaptcha до отримання ключів

2) Вказати адресу сайту та обрати тип «Версія 2», вказати адресу сайту ще раз, прийняти угоду та натиснути кнопку «Відправити»;

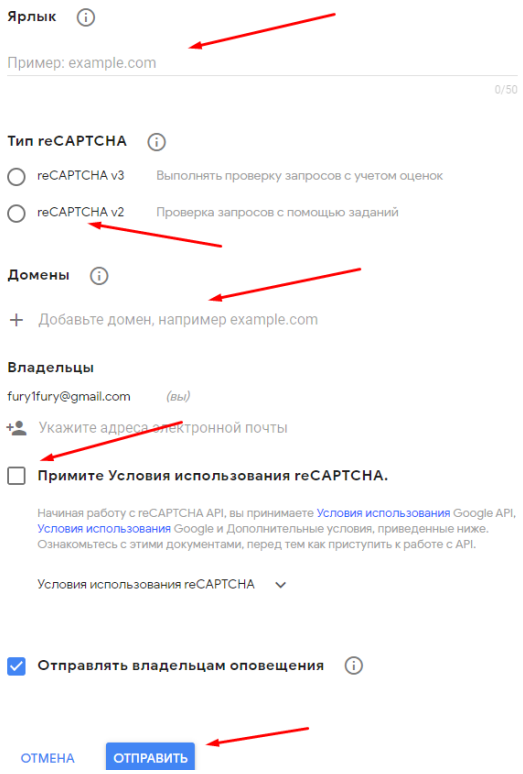

Рисунок 3.4 – налаштування модулю ReCaptcha

3) Скопіювати ключ сайту та секретний ключ;

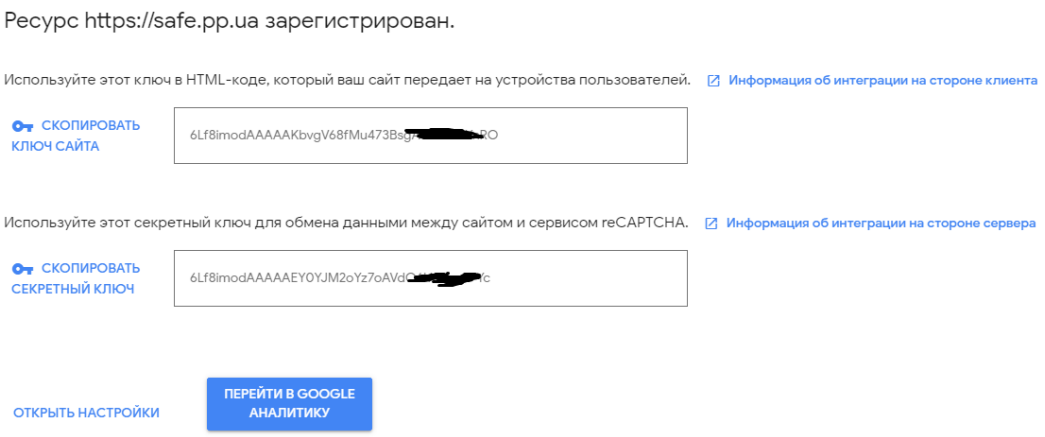

Рисунок 3.5 – меню, де зберігаються ключ сайту та секретний ключ

4) Вказати отримані ключі у відповідному меню адміністраторської панелі.

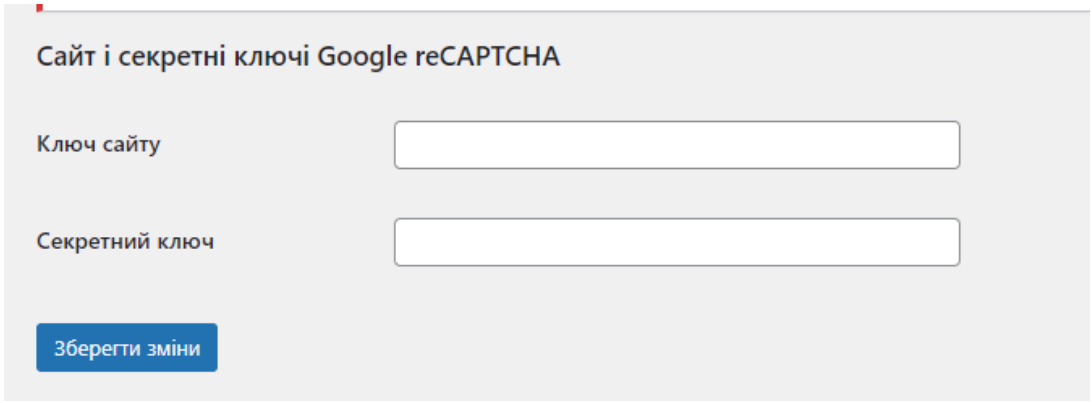

Рисунок 3.6 – меню адміністраторської панелі для ключів

Після збереження налаштувань на сторінці входу до системи стане активним модуль ReCaptcha, що буде блокувати 99% ботів, які сканують веб-сайти на основі WordPress на вразливості.

Для зміни посилань на критичні сторінки веб-сайту необхідно перейти в розділ «Постійні посилання» та знайти пункт «Перейменування».

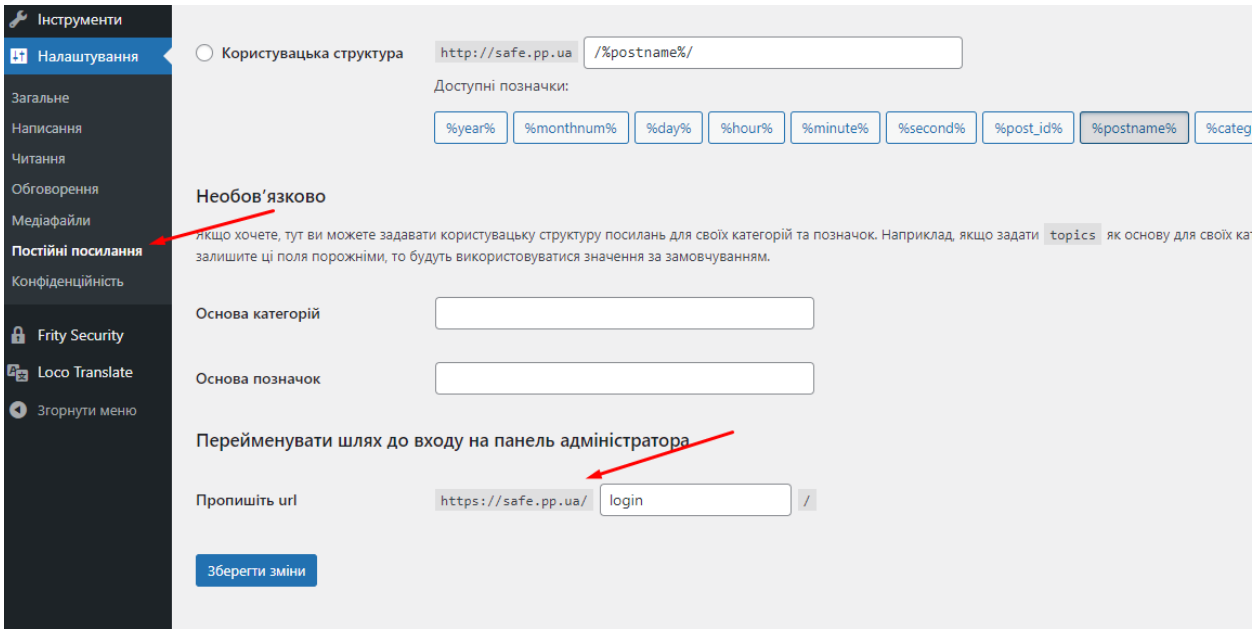

Рисунок 3.7 – меню зміни посилань

Після зміни доступ до сторінки стане можливим тільки за вказаним посиланням, таким чином використання нестандартного посилання запобігатиме її знаходженню людьми та ботами, а отже, несанкціонованому доступу до панелі адміністрування.

Що стосується налаштування захисту від атак грубою силою, з метою підвищення зручності використання було виміряно та встановлено оптимальну конфігурацію, а додаткові її налаштування видалено. На звичайного користувача це ніяк не вплине, оскільки він не помітить системи, але це стане перешкодою для ботів та сканерів – навіть якщо атака цілеспрямована, умовний бот використовуватиме систему розпізнавання капчі та знайде потрібне посилання, то все одно він зіштовхнеться з обмеженням у три спроби входу до системи. Перевищення цієї кількості призведе до блокування такого боту.

Це не гарантує абсолютний захист, але більш просунуті сценарії зламу вимагають від кіберзлочинця великої кількості ресурсів, що зводить ймовірність успішної атаки нанівець.

Для налаштування двофакторної автентифікації необхідно завантажити програму Google Authenticator з додатків Play Market або App Store на смартфон.

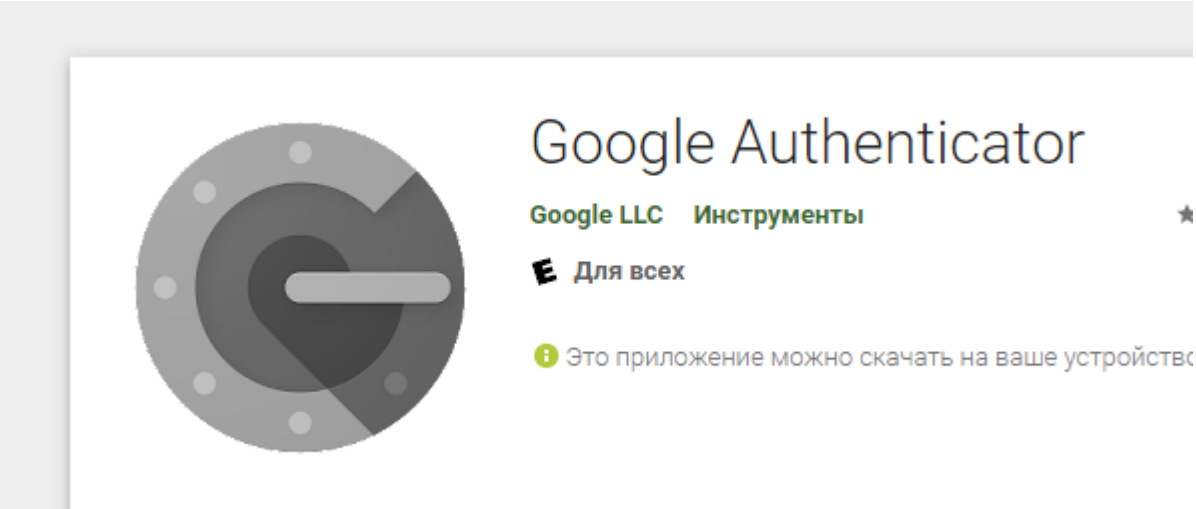

Рисунок 3.8 – додаток Google Authenticator

Налаштування здійснюється адміністратором для кожного користувача окремо, таким чином кожен користувач, що має дозвіл на вхід до системи, зможе зробити це незалежно від інших.

Для початку необхідно створити користувача стандартними методами WordPress. Для цього слід відкрити меню «Користувачі -> Додати», зазначити ім’я, електронну пошту, пароль, задати роль «Адміністратор» та додати його.

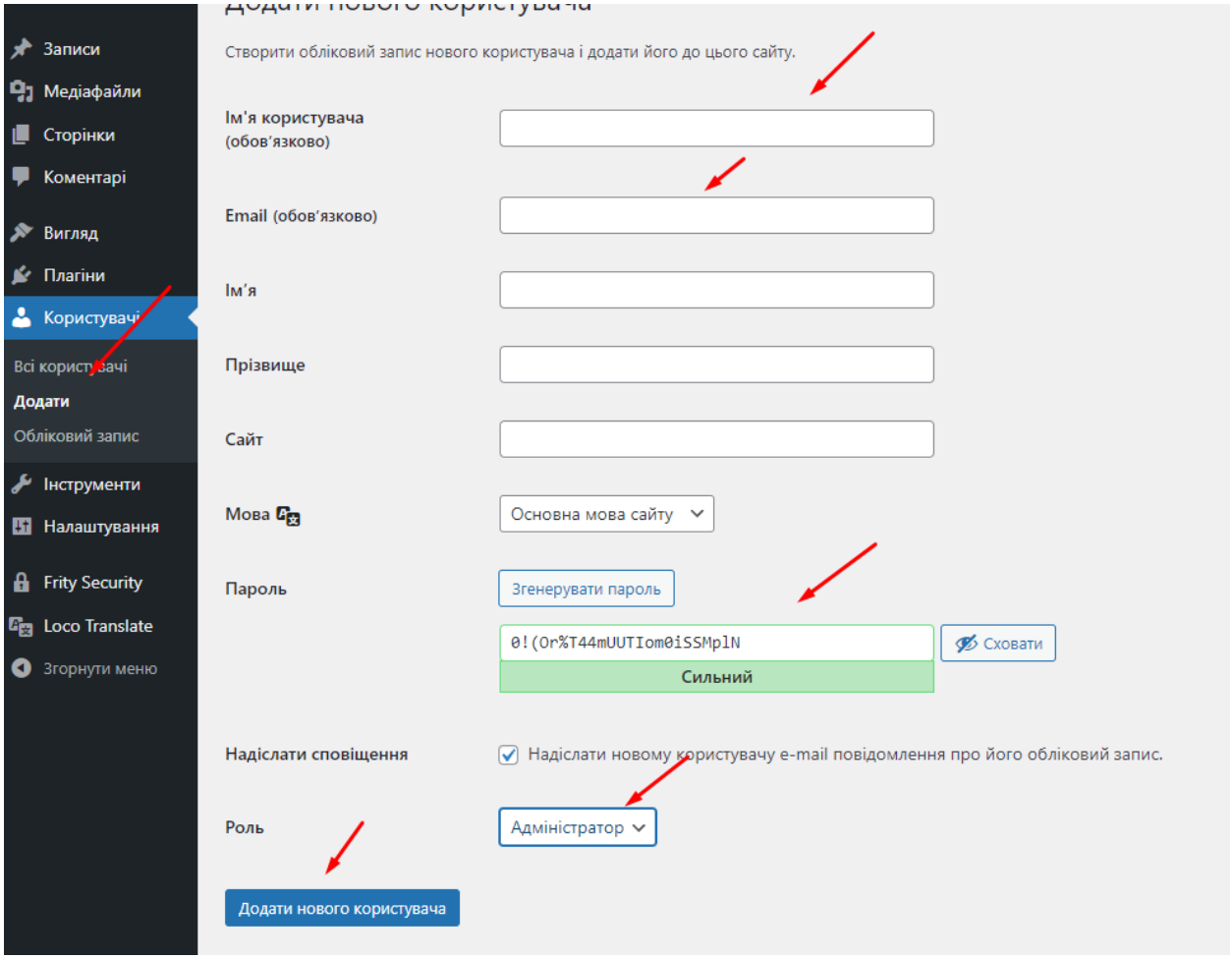

Рисунок 3.9 – меню створення користувача

Тепер необхідно увійти до системи, використовуючи щойно створений обліковий запис адміністратора. Код двофакторної автентифікації для нього не потрібен.

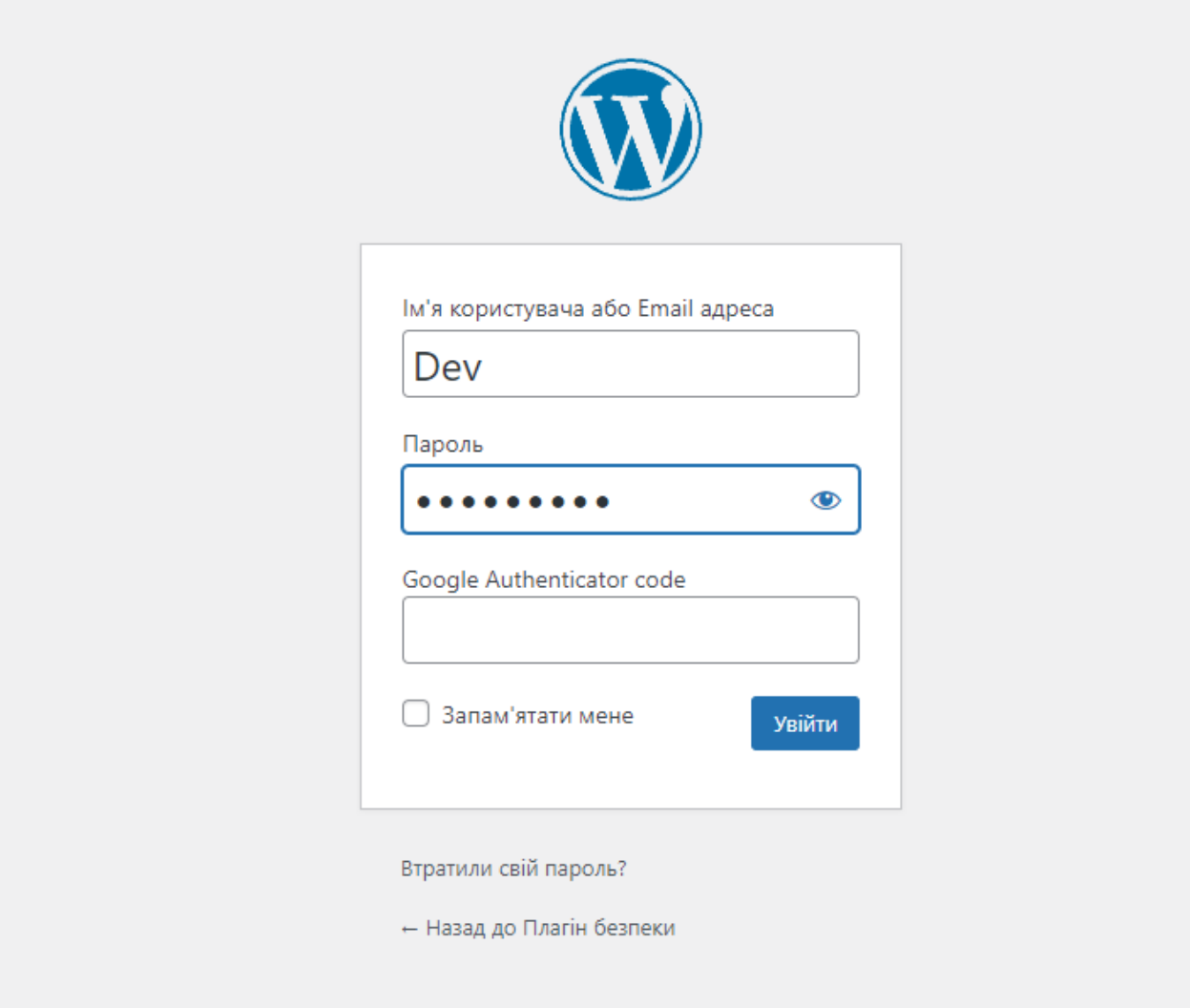

Рисунок 3.10 – оновлена сторінка входу з полем для двофакторної автентифікації

Тепер через меню для перегляду користувачів слід обрати одного та активувати двофакторну автентифікацію для нього. Ключ буде згенеровано попередньо, але передбачено додаткову опцію генерування нового ключа, а також сканування коду.

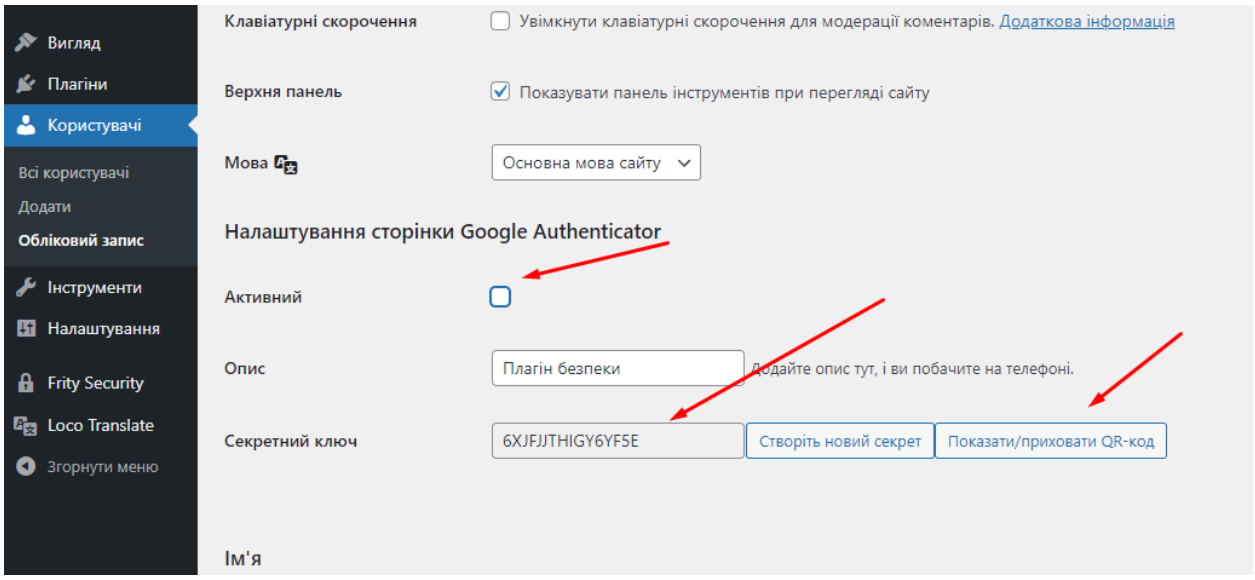

Рисунок 3.11 – сторінка налаштування двофакторної автентифікації

У додатку знадобиться обрати одну з опцій – «Ввести ключ» або «Сканувати код».

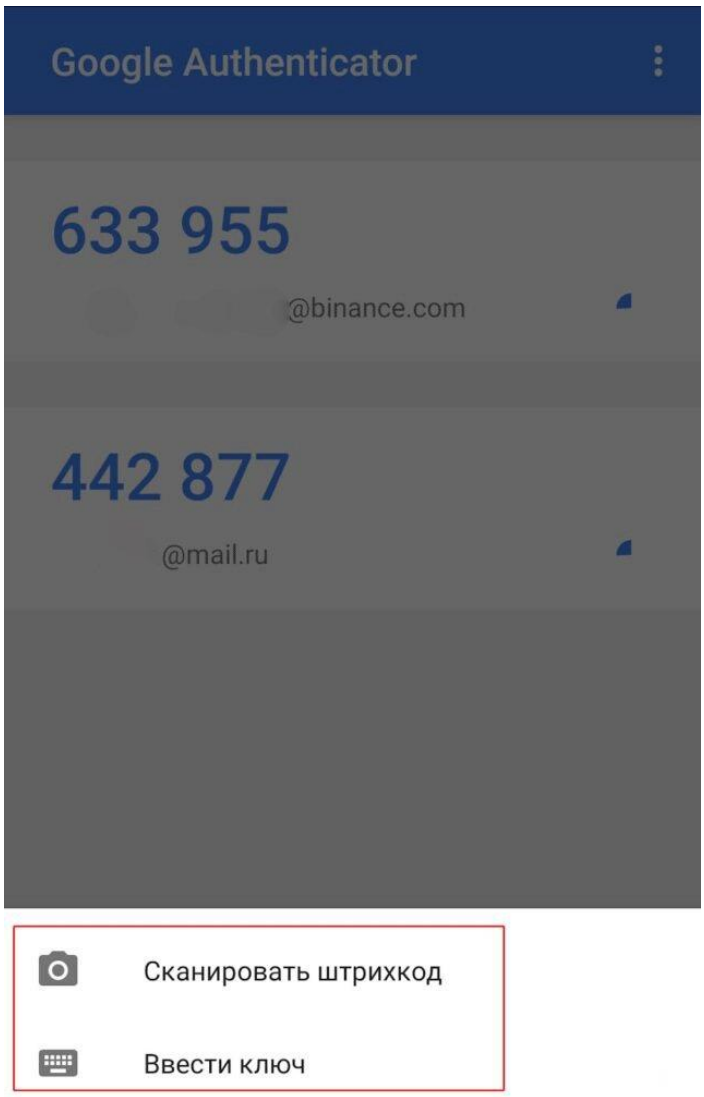

Рисунок 3.12 – меню додатку Google Authenticator

І після сканування (чи введення) коду для поданого веб-сайту його буде автоматично додано, після цього використання смартфону для користувача стає обов’язковим. Ця процедура є ключовою для захисту панелі адміністрування від зламу кіберзлочинцями.

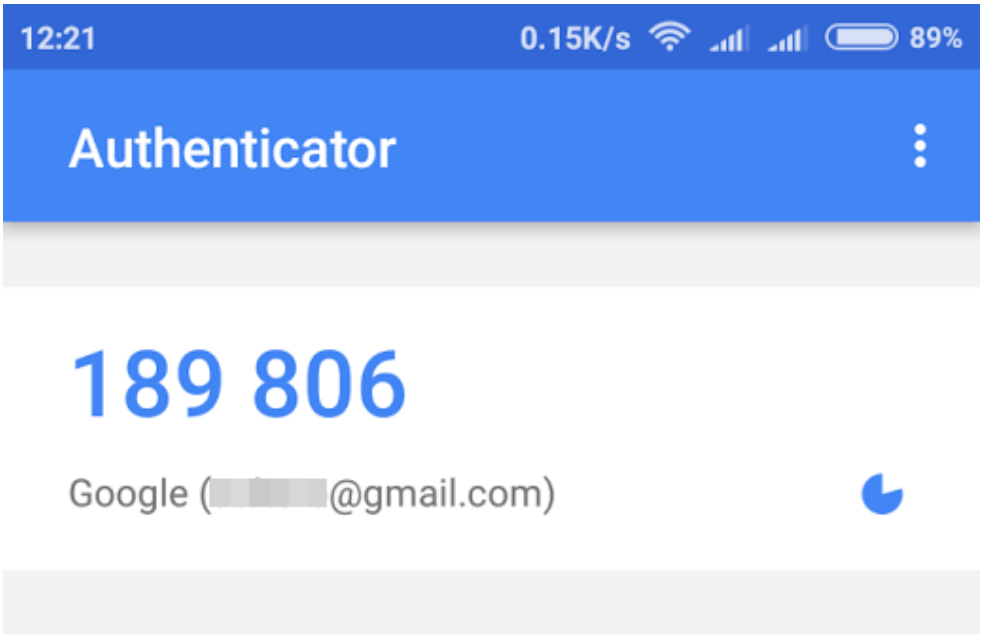

Рисунок 3.13 – меню Google Authenticator з активованою автентифікацією

Для зміни секретного ключа достатнім є вхід до профілю користувача та натискання кнопки «Змінити». Якщо певний адміністратор втратив смартфон, то інший зможе деактивувати двофакторну автентифікацію або створити новий обліковий запис. Якщо ж всі адміністратори втратили доступ до сайту, його можливо деактивувати при використанні протоколу FTP.

Нарешті, серед інших налаштувань безпеки також присутні:

- приховування версії CMS WordPress, а також всіх файлів стилів та файлів з програмним кодом;
- вимкнення протоколу XML-RPC;
- заборона редагування файлів через панель адміністрування;
- вимкнення підказок WordPress на сторінці входу («Логін або пароль не є правильними» замість «Пароль не є правильним для цього користувача»);
- автоматичне оновлення CMS WordPress, тем та плагінів до неї.

Усі наведені налаштування є автоматичними та набувають чинності в момент активації плагіну.

ВИСНОВКИ

У поданій роботі досліджено засоби забезпечення безпеки веб-ресурсів на основі CMS WordPress. Порівняльний аналіз довів, що безкоштовні плагіни є кращим шляхом серед запропонованих. Це зумовлено тим, що безкоштовні плагіни часто мають задовільні функціональні можливості для підвищення рівня захисту, у той час як поради ігноруються більшістю власників веб-сайтів як занадто складні, послуги фахівців не відповідають встановленим ними цінам, а платні плагіни є недоступними для більшості українських користувачів через вартість.

Проаналізовано множину існуючих плагінів безпеки, що включають в себе безкоштовні, частково безкоштовні та платні плагіни для наочного порівняння функціональних можливостей, що надаються залежно від цінової категорії. Більшість плагінів є частково безкоштовними – до того ж, серед них є більша частина таких, що надають опцію двофакторної автентифікації. Втім, вони не є придатними до використання організаціями через необхідність платити за такі плагіни для комерційного використання, та не підходять для великої частини некомерційного українського сегменту користувачів через недостатньо якісний переклад українською мовою. У той же час єдиний безкоштовний плагін, що підтримує цю технологію, не є здатним надати будь-які інші види захисту. Це достатні причини для розробки власного плагіну безпеки.

Досліджено механізм роботи двофакторної автентифікації передбачає використання двох факторів під час підтвердження особи користувача – паролю, що є відомим тільки власнику веб-ресурсу, та додаткового коду підтвердження, що пов’язано лише з його пристроєм. Іноді код замінюється на сканування частини тіла – наприклад, відбиток пальцю або зображення сітківки ока. У порівнянні з однофакторною автентифікацією цей метод безпеки зменшує ймовірність крадіжки або пошкодження веб-сайту, навіть коли кіберзлочинцю є відомим пароль у формі відкритого тексту.

Нарешті, розроблено програмну реалізацію власного плагіну безпеки. Він використовує двофакторну автентифікацію, а також надає захист від атак грубою силою, обмежуючи кількість спроб входу та фільтруючи підозрілі акаунти за IP-адресами та множиною компонентів комп’ютеру, що використовується кіберзлочинцем. Він є повністю безкоштовним, що дозволяє комерційне використання на відміну від частково безкоштовних плагінів, а також надає більші функціональні можливості, ніж в них. До того ж його локалізовано для використання місцевим сегментом користувачів зрозумілим чином.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Практичне розуміння ін'єкцій [Електронний ресурс] // Safe Security. – 2021. – Режим доступу до ресурсу: https://www.safe.security/assets/img/research-paper/pdf/Practical%20Insight%20Into%20Injections.pdf.
2. Статистика використання та ринкова доля WordPress [Електронний ресурс] // W3Techs. – 2021. – Режим доступу до ресурсу: https://w3techs.com/technologies/details/cm-wordpress.
3. Навіщо використовувати WordPress для вашого наступного веб-сайту? [Електронний ресурс] // AppCurate. – 2019. – Режим доступу до ресурсу: https://appcurate.com/blog/why-use-wordpress-for-your-next-website/.
4. Статистика безпеки WordPress [Електронний ресурс] // WP Manage Ninja. – 2020. – Режим доступу до ресурсу: https://wpmanageninja.com/wordpress-security-statistics/.
5. 6 вразливостей плагінів WordPress, зламаних хакерами [Електронний ресурс] // Builtin. – 2020. – Режим доступу до ресурсу: https://builtin.com/cybersecurity/CMS-wordpress-plugins-hacks.
6. Геннаро Л. 8 кращих плагінів безпеки WordPress для захисту вашого веб-сайту [Електронний ресурс] / Ліза Геннаро // WPForms. – 2021. – Режим доступу до ресурсу: https://wpforms.com/best-wordpress-security-plugins/.
7. Платформа безпеки веб-сайтів Sucuri: ціноутворення [Електронний ресурс] // Sucuri. – 2021. – Режим доступу до ресурсу: https://sucuri.net/website-security-platform/signup/.
8. Коннеллі О. Абсолютна безпека WordPress 3 / Оллі Коннеллі. – Бірмінгем: Packt Publishing, 2011. – 408 с.
9. Фрілансери [Електронний ресурс] // Хабр Фріланс. – 2021. – Режим доступу до ресурсу: https://kwork.ru/search?query=wordpress%20вирус&s=x&page=1.
10. Обслуговування безпеки WordPress: чому воно вам потрібно? [Електронний ресурс] // InternetDevels. – 2019. – Режим доступу до ресурсу: https://wishdesk.com/blog/why-you-need-wordpress-security-service.
11. Результати пошуку плагінів безпеки WordPress [Електронний ресурс] // WordPress. – 2021. – Режим доступу до ресурсу: https://wordpress.org/plugins/search/Security/.
12. Вангі Б. Автентифікація [Електронний ресурс] / Біл Вангі // Webopedia. – 2016. – Режим доступу до ресурсу:

http://web.archive.org/web/20161216115208/https://www.webopedia.com/TERM/A/authentication.html.
13. Наскільки безпечним є мій пароль? [Електронний ресурс] // Security.org – Режим доступу до ресурсу: https://howsecureismypassword.net/.
14. Фарік М. Розгляд методів автентифікації / М. Фарік, Н. А. Лал, Ш. Прасад // Міжнародний журнал наукового та технологічного дослідження / М. Фарік, Н. А. Лал, Ш. Прасад. – Чхаттісгарх: IJSR, 2016. – (5). – С. 247.
15. Шнаєр Б. Атаки "Людина всередині" [Електронний ресурс] / Брюс Шнаєр // Schneier on Security. – 2008. – Режим доступу до ресурсу: https://www.schneier.com/blog/archives/2008/07/maninthemiddle_1.html.
16. Уникання атак соціальною інженерією та фішингом [Електронний ресурс] // CISA. – 2009. – Режим доступу до ресурсу: https://us-cert.cisa.gov/ncas/tips/ST04-014.
17. Що таке біометрія - як працює сканер відбитків пальців [Електронний ресурс] // Easy Clocking. – 2021. – Режим доступу до ресурсу: http://www.bioelectronix.com/what_is_biometrics.html.
18. Спектор Х. Якими є переваги та недоліки цифрового сертифікату? [Електронний ресурс] / Харві Спектор // Techwalla. – 2021. – Режим доступу до ресурсу: https://www.techwalla.com/articles/advantages-of-a-digital-certificate.
19. Еволюція автентифікації [Електронний ресурс] // HYPR. – 2019. – Режим доступу до ресурсу: https://www.hypr.com/wp-content/uploads/the_evolution_of_authentication_white_paper.pdf.
20. Дослідження зі зручності використання п'яти методів двофакторної автентифікаці / [К. Різ, Т. Сміт, Д. Датсон та ін.] // П'ятнадцятий симпозіум на приватності та безпеці, що можливо використовувати / [К. Різ, Т. Сміт, Д. Датсон та ін.]. – Санта-Клара, Каліфорнія: USENIX, 2019. – С. 357–370.
21. Бонно Д. Чащоба паролів: технічні та ринкові збої при автентифікації людини в Інтернеті / Д. Бонно, С. Прайбущ. – Арлінгтон, Вірджинія: Economics of Information Security, 2010. – 28 с. – (9).
22. Пошуки заміни паролів: основа для порівняльної оцінки схем веб-автентифікації / Д.Бонно, К. Херлі, П. Ц. Оорщот, Ф. Стаджано // Симпозіум з безпеки та приватності / Д.Бонно, К. Херлі, П. Ц. Оорщот, Ф. Стаджано., 2012. – (IEEE). – С. 553–567.
23. Ключі безпеки: практичні криптографічні другі фактори для сучасної мережі / [Д. Ленг, А. Ческіс, Д. Белфанц та ін.] // Міжнародна конференція з фінансової криптографії та безпеки даних / [Д. Ленг, А.

Ческіс, Д. Белфанц та ін.]. – Люксембург: Springer, 2016. – (FC). – С. 422–440.
24. Заплутана мережа повторного використання паролів / [А. Дас, Д. Бонно, М. Цезар та ін.] // Безпека мереж та розподілених систем / [А. Дас, Д. Бонно, М. Цезар та ін.]. – Сан-Дієго: NDSS, 2014. – С. 23–26.
25. Івс Б. Ефект доміно при повторному використанні паролів / Б. Івс, К. Уолш, Х. Шнайдер. // CACM. – 2004. – №4. – С. 75–78.
26. Уявлення користувачів про безпеку та зручність використання однофакторної та двофакторної автентифікації в автоматизованому телефонному банкінгу / Н.Гансон, Д. Маршалл, Х. Мортон, М. Джек. // Комп'ютери та безпека. – 2011. – №30. – С. 208–220.
27. Джаст М. Про безпеку та зручність використання подвійної автентифікації облікових даних в Інтернет-банкінгу Великобританії / М. Джаст, Д. Аспіналл. // ICITST. – 259–264. – №1. – С. 2012.
28. «Вони привезли жахливу річ для ключів!» Аналізуємо зручність використання двофакторної автентифікації в онлайн-банкінгу Великобританії / К.Крол, Е. Філіппу, Е. Д. Крістофаро, А. М. Сассе. – Меріленд: USEC, 2015.
29. Уявлення користувачів про безпеку, зручність та зручність використання маркерів автентифікації Ebanking / К.Вейр, Г. Дуглас, М. Каррутерс, М. Джек. // Комп'ютери та безпека. – 2009. – №28. – С. 47–62.
30. Порівняльне дослідження юзабіліті двофакторної автентифікації / Е. Д.Крістофаро, Х. Ду, Ж. Фройгер, Г. Норсі. // USEC. – 2014.
31. Двофакторна автентифікація може бути безпечною, але її не можливо використовувати: підсумкова оцінка юзабіліті методів двофакторної автентифікації / К.Ачемян, Ф. Кортум, Д. Сюн, Д. Воллах. // SAGE. – 2018. – №62.
32. Дас С. Чому Джонні не використовує два фактора: двофазне дослідження зручності використання ключа безпеки FIDO U2F / С. Дас, Е. Дінгман, Д. Кемп. // FC. – 2018.
33. Історія двох досліджень: найкращі та найгірші можливості використання YubiKey / [Д. Рейнольдз, Т. Сміт, К. Різ та ін.]. // IEEE. – 2018.
34. Ендрюс Н. «Чи можу я отримати ваші цифри?»: Незаконне придбання бездротових телефонних номерів для атак із заміною SIM-карт і відповідальність постачальника послуг бездротового зв’язку / Натанаель Ендрюс // Північно-західний журнал з технологій та інтелектуальної власності / Натанаель Ендрюс. – Еванстон, Іллінойс: NWJTIP, 2018. – С. 78–106.

35. Одноразові паролі на основі SMS: атаки та захист / К.Маллінер, Р. Боргаонкар, П. Стювін, Ж. Зайферт // Виявлення вторгнень і шкідливих програм, а також оцінка вразливості / К.Маллінер, Р. Боргаонкар, П. Стювін, Ж. Зайферт. – Гайдельберг: Springer, 2013. – С. 150–159.
36. Бакдаш Д. З. Кореляція вимірювань, що повторюються [Електронний ресурс] / Д. З. Бакдаш, Л. Р. Марусіч // Frontiersin. – 2017. – Режим доступу до ресурсу: https://www.frontiersin.org/articles/10.3389/fpsyg.2017.00456/full.
37. Equifax каже, що кібератака могла вплинути на 143 мільйони людей у США [Електронний ресурс] / Т. З.Бернард, Т. Хсу, Н. Перлрот, Р. Лібер // NYTimes. – 2017. – Режим доступу до ресурсу: https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.
38. Сассе М. А. Перетворення «найслабшої ланки» — підхід взаємодії людини та комп'ютера на ефективну та ефективну безпеку / М. А. Сассе, С. Бростофф, Д. Вейріх. // BT Technology Journal. – 2001. – №19. – С. 122–131.
39. Льюїс Д. Пари латинських квадратів для врівноваження послідовних ефектів і поєднання умов і стимулів / Джеймс Льюїс. // Матеріали щорічної зустрічі Товариства людського фактора. – 1989. – №33. – С. 1223–1227.
40. Сауро Д. Порівняння трьох анкет про зручність використання після виконання завдання / Д. Сауро, Д. С. Дюма. // Матеріали конференції SIGCHI про людський фактор у обчислювальних системах. – 2009. – №9. – С. 1599–1608.