УДК 004.056.53(045)
DOI https://doi.org/10.32782/IT/2024-3-9

Анна КОРЧЕНКО
доктор технічних наук, професор, професор кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, Дніпро, Україна, 49005
***ORCID:** 0000-0003-0016-1966*
***Scopus Author ID:** 56029291400*

Сергій МАЦЮК
кандидат технічних наук, доцент, доцент кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, Дніпро, Україна, 49005, matsiuk.s.m@nmu.one
***ORCID:** 0000-0001-6798-5500*
***Scopus Author ID:** 57189702975*

Кирило ДАВИДЕНКО
аспірант кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, Дніпро, Україна, 49005
***ORCID:** 0009-0001-9209-1274.*

Бібліографічний опис статті: Корченко, А., Мацюк С., Давиденко, К. (2024). Огляд сучасних методів та засобв виявлення соціотехнічних атак. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 88–96, doi: https://doi.org/10.32782/IT/2024-3-9

ОГЛЯД СУЧАСНИХ МЕТОДІВ ТА ЗАСОБВ ВИЯВЛЕННЯ СОЦІОТЕХНІЧНИХ АТАК

Актуальність. *Стрімкий розвиток інформаційних технологій та інтенсивний обмін даними суттєво змінюють сучасне середовище кібербезпеки, створюючи нові загрози у вигляді кібератак та шахрайства. Особливу небезпеку становлять соціотехнічні атаки, які використовують психологічні маніпуляції для отримання конфіденційної інформації або доступу до захищених систем.* ***Мета.*** *З огляду на це, метою роботи є комплексний огляд існуючих рішень, технологій і методів, які можуть допомогти організаціям та приватним користувачам у боротьбі з соціотехнічними загрозами.* ***Методологія.*** *У статті проведено дослідження сучасних методів виявлення соціотехнічних атак, що використовують маніпулятивні техніки. Розглянуті різні підходи до детектування відповідних атак, включаючи сигнатурні, поведінкові, методи машинного навчання, аналіз метаданих, а також соціальні та психологічні підходи. Особливу увагу приділено інтерактивним і симуляційним методам, які дозволяють організаціям перевіряти свою готовність до атак шляхом моделювання реальних умов.* ***Наукова новизна.*** *Описані апаратні та програмні засоби за дев'ятьма критеріями (високий рівень захисту, централізоване управління, простота використання, інтеграція з іншими платформами, штучний інтелект, адаптивність, можливості роботи в офлайн-режимі, висока вартість, складність налаштування) для виявлення та блокування соціотехнічних атак, які надають багаторівневий захист від соціотехнічних загроз.* ***Висновки.*** *Отримані результати показують, що освітні та організаційні заходи залишаються ключовими для підвищення обізнаності користувачів та зменшення ризику успішних атак, а сучасні підходи до захисту від соціотехнічних загроз мають бути комплексними і включати як технічні рішення, так і навчання персоналу. Також є важливим, постійне вдосконалення існуючих заходів забезпечення безпеки і впровадження новітніх технологій для підвищення ефективності захисту інформаційних систем від соціотехнічних атак.*

Ключові слова: *кібербезпека, інформаційна безпека, соціальний інжиніринг, соціотехнічні атаки, методи соціотехнічних атак, класифікація соціотехнічних атак.*

Anna KORCHENKO
Doctor of Technical Sciences, Professor, Professor at the Department of Information Security and Telecommunications, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005,annakor@ukr.net
***ORCID:** 0000-0003-0016-1966*
***Scopus Author ID:** 56029291400*

Sergii MATSIUK
Assistant Professor at the Department of Information Security and Telecommunications, National Technical University Dnipro Polytechnic, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, matsiuk.s.m@nmu.one
ORCID: *0000-0001-6798-5500*
Scopus Author ID: *57189702975*

Kyrylo DAVYDENKO
Postgraduate Student at the Department of Information Security and Telecommunications, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, kirilldavy@gmail.com
ORCID: *0009-0001-9209-1274*

To cite this article: Korchenko, A, Matsiuk S., Davydenko, K. (2024). Ohliad suchasnykh metodiv ta zasobv vyiavlennia sotsiotekhnichnykh atak [Overview of modern methods and means of detecting of sociotechnical attacks]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 88–96, doi: https://doi.org/10.32782/IT/2024-3-9

OVERVIEW OF MODERN METHODS AND MEANS OF DETECTING OF SOCIOTECHNICAL ATTACKS

Relevance. *The rapid development of information technology and intensive data exchange are significantly changing the modern cybersecurity environment, creating new threats in the form of cyberattacks and fraud. Socio-technical attacks that use psychological manipulation to obtain confidential information or access to secure systems are particularly dangerous.* ***Objective.*** *Given this, the purpose of this paper is to provide a comprehensive review of existing solutions, technologies, and methods that can help organizations and private users combat sociotechnical threats.* ***Methodology.*** *The article studies modern methods of detecting sociotechnical attacks that use manipulative techniques. Various approaches to detecting such attacks are considered, including signature, behavioral, machine learning, metadata analysis, as well as social and psychological approaches. Particular attention is paid to interactive and simulation methods that allow organizations to test their preparedness for attacks by simulating real-world conditions.* ***Scientific novelty.*** *Hardware and software tools are described according to nine criteria (high level of protection, centralized management, ease of use, integration with other platforms, artificial intelligence, adaptability, offline capabilities, high cost, complexity of configuration) to detect and block sociotechnical attacks, which provide multi-level protection against sociotechnical threats.* ***Conclusions.*** *The findings show that educational and organizational measures remain key to raising user awareness and reducing the risk of successful attacks, and modern approaches to protecting against sociotechnical threats should be comprehensive and include both technical solutions and staff training. It is also important to continuously improve existing security measures and introduce the latest technologies to increase the effectiveness of protecting information systems from sociotechnical attacks.*

Key words: *cyber security, information security, social engineering, sociotechnical attacks, sociotechnical attack methods, classification of sociotechnical attacks.*

У сучасному кіберпросторі соціотехнічні атаки становлять одну з найбільших загроз для інформаційної безпеки організацій і приватних осіб. Соціотехнічні атаки, що включають фішинг, підробку особистих даних і інші маніпулятивні техніки, намагаються експлуатувати людську психологію для отримання несанкціонованого доступу до конфіденційної інформації та інших ресурсів. З огляду на стрімкий розвиток технологій і зростання кіберзагроз, ефективні методи детектування цих атак стали критично важливими для забезпечення безпеки інформаційних систем.

Актуальність дослідження сучасних методів детектування соціотехнічних атак підтверджується численними публікаціями та дослідженнями, що підкреслюють їх важливість у боротьбі з кіберзагрозами. Зокрема, вчені акцентують увагу на необхідності інтеграції новітніх технологій, таких як штучний інтелект і машинне навчання, для покращення ефективності систем безпеки. Інші джерела також зазначають, що існуючі методи потребують постійного вдосконалення та адаптації до нових тактик, використовуваних кіберзлочинцями.

Методи та засоби виявлення соціотехнічних атак є ключовими елементами захисту інформаційних систем та організацій від маніпуляцій, що спрямовані на людський чинник.

Виявлення соціотехнічних атак є складним завданням через їх орієнтацію на маніпулювання людською поведінкою, а не на прямий технічний вплив. Методи виявлення зазначених атак поділяються на кілька категорій, зокрема: технічні, поведінкові, аналітичні та освітні.

Метою статті є комплексний огляд існуючих рішень, технологій і методів, які можуть допомогти організаціям та приватним користувачам у боротьбі з соціотехнічними загрозами. Розуміння сучасних методів детектування дозволить знизити ризики, пов'язані з кіберзлочинністю, та покращити загальний рівень інформаційної безпеки.

Задача роботи полягає в огляді сучасних методів та засобів детектування соціотехнічних атак, а також у аналізі їх ефективності та обмежень. Пропонується розглянути різноманітні підходи, зокрема технології на основі штучного інтелекту, системи моніторингу та реагування, а також інтерактивні та симуляційні методи.

Далі розглянемо основні методи, які використовуються для виявлення соціотехнічних атак.

Сигнатурні методи базуються на створенні баз даних сигнатур (шаблонів) відомих атак, які порівнюються з вхідною інформацією, наприклад, антивірусні програми або системи виявлення вторгнень (IDS), які шукають специфічні моделі поведінки. Такі методи швидко виявляють відомі загрози, але є неефективними щодо нових або модифікованих атак (А. Корченко, 2019; Scarfone K., 2007).

Поведінкові методи (аналіз поведінки користувачів) направлені на виявлення відхилень у поведінці користувачів або систем, які можуть свідчити про соціотехнічну атаку. Це системи, що відстежують нетипову активність у мережі, наприклад, неочікувані запити на зміну пароля, спроби доступу до конфіденційних даних, раптові зміни в шаблонах роботи користувачів або незвичайні запити до серверів. Такі методи можуть виявити невідомі атаки або атаки, що змінюють поведінку, але вони мають високий рівень хибно позитивних спрацьовувань (Hee-Yong Kwon, 2022).

Методи машинного навчання та штучного інтелекту використовують класифікаційні моделі або нейронні мережі для прогнозування можливих атак на основі аналізу минулих інцидентів. Застосовують алгоритми машинного навчання для аналізу великих обсягів даних та пошуку аномалій або небезпечних патернів. Також, мають здатність до самонавчання і виявлення складних атак, що може бути недоступним для інших методів. Але зазначені методи потребують велику кількості даних для навчання, що спричиняє можливість появи хибних спрацьовувань (Hee-Yong Kwon, 2022; Moustafa N., 2019).

Контекстуальні методи базуються на аналізі контексту взаємодій і комунікацій, таких як аналіз змісту повідомлень електронної пошти, соціальних мереж, телефонних розмов тощо. Відповідні методи включають аналітичні інструменти для перевірки достовірності повідомлень і виявлення підозрілих або шахрайських комунікацій. Вони можуть ідентифікувати соціотехнічні атаки, такі як фішинг або шахрайство, але потребують складних алгоритмів для точного аналізу контенту і часто залежать від контексту застосування (Kisiel J., 2018).

Методи аналізу метаданих базуються на аналізі адрес електронної пошти, IP-адрес, шаблонів дзвінків та інших сигналів, які можуть вказувати на підозрілу активність, також орієнтовані на виявлення підроблених електронних листів шляхом аналізу метаданих повідомлень. Вони допомагають у швидкому виявленні несанкціонованих або підроблених комунікацій, але не завжди можуть бути точними, наприклад, якщо метадані підробляються (Кузьма К., 2017).

Соціальні та психологічні методи базуються на оцінці психологічних та соціальних аспектів поведінки працівників, що можуть бути використані зловмисниками для реалізації атак. Також, вони використовують опитування та соціальну інженерію для виявлення співробітників, які можуть бути більш вразливими до маніпуляцій. Дозволяють розпізнати потенційні уразливості, пов'язані з людським чинником але мають труднощі у вимірюванні психологічних показників та потребують необхідності у регулярному оновленні знань (Kevin D., 2003; Rahman T., 2021).

Методи на основі аналізу соціальних мереж направлені на виявлення шахрайських облікових записів або підозрілих повідомлень, що спрямовані на збір персональних даних. Також, включають аналіз поведінки користувачів у соціальних мережах для виявлення соціотехнічних атак, таких як фішинг або соціальні маніпуляції. Вони дозволяють ефективно аналізувати широкі потоки інформації у відкритих джерелах але працюють з великою кількістю даних і мають труднощі у відслідковуванні всіх можливих джерел (Войтович О.П., 2023).

Освітні та організаційні методи орієнтовані на навчання співробітників і користувачів щодо виявлення соціотехнічних атак та способів їх уникнення. Проводяться навчання співробітників, щодо розпізнавання ознак фішингових атак або інших типів шахрайства. В результаті їх використання зменшуються ризики реалізації атак через підвищення обізнаності користувачів але вони залежать від постійної підтримки та оновлення знань (Cyber.academy, 2024).

Інструменти моніторингу та реагування складаються з технічних рішень, які забезпечують безперервний моніторинг систем для виявлення підозрілої активності та негайного реагування. До них відносяться системи SIEM (Security Information and Event Management), які аналізують журнали подій у режимі реального часу. Вони мають високу оперативність виявлення атак, але потребують значних ресурсів для обробки значних обсягів даних (González-Granadillo G., 2021).

Інтерактивні та симуляційні методи (соціальна інженерія через симуляцію атак) використовують симуляції для створення довкілля, де проводяться тренування та тести для виявлення соціотехнічних атак, наприклад, проведення «фішингових тестів» для співробітників компанії або надсилання фальшивих фішингових листів для оцінки того, скільки працівників переходять за посиланням чи вводять свої облікові дані. Мають можливість оцінки реальної готовності організації до протидії атакам, а також значний ризик хибних висновків, якщо симуляції не відображають реальних умов (Bamanga Ahmad M., 2023; Forbes Advisor, 2024).

Ці методи часто використовуються в комбінації для підвищення ефективності та створення багаторівневої системи захисту від соціотехнічних атак, оскільки вони спрямовані на виявлення як технічних, так і людських аспектів цих загроз.

Існує низка програмних і апаратних засобів для виявлення та блокування соціотехнічних атак, які використовуються для захисту від кіберзагроз, таких як фішинг, спуфінг, маніпуляції та інші види атак, що враховують людський чинник.

Далі, порведемо огляд програмних та апаратних засобів для виявлення та блокування соціотехнічних атак.

Програмні засоби

1. Proofpoint – це комплексне рішення для захисту електронної пошти та запобігання фішинговим атакам, спаму та компрометації електронної пошти. Виявляє та блокує фішингові атаки, спуфінг, шкідливі вкладення та URL-адреси, а також забезпечує навчання користувачів для підвищення обізнаності про кіберзагрози (Proofpoint, 2024).

Перевагами зазначеного рішення є високий рівень захисту, що включає використання машинного навчання для виявлення фішингових атак та спроб компрометації електронної пошти. Має централізоване управління і пропонує єдину панель для управління безпекою електронної пошти та іншими загрозами. Забезпечує глибокий аналіз загроз з детальними звітами.

При розгляді **недоліків** proofpoint необхідно зауважити, що рішення потребує значних зусиль для початкового налаштування та інтеграції з існуючими системами, а також має високу вартість, що може бути проблемою для невеликих організацій.

2. Mimecast – це хмарна платформа, яка забезпечує багаторівневий захист електронної пошти, включаючи захист від фішингу, спаму, шкідливих програм, соціотехнічних атак **та** включає виявлення компрометації електронної пошти (Mimecast, 2024).

Її **перевагами** є інтуїтивно зрозумілий інтерфейс та легка інтеграція з іншими платформами. Ця платформа доступна з будь-якого місця, що забезпечує її гнучкість (має хмарне рішення). Також, добре зарекомендувала себе у виявленні та блокуванні загроз, пов'язаних з електронною поштою.

До **недоліків** можна віднести – залежність від інтернет з'єднання. Оскільки Mimecast це хмарна платформа, для її роботи потрібен стабільний інтернет. Також, вона має **о**бмежені можливості в офлайн-режимі, тобто не має можливості забезпечити повний захист, якщо підключення до інтернету відсутнє.

3. PhishMe (Cofense) – це платформа для навчання та симуляцій фішингових атак. Навчає співробітників розпізнавати фішингові атаки за допомогою реалістичних симуляцій, а також допомагає виявляти та реагувати на реальні загрози (Cofense, 2024).

Переваги платформи пов'язані з можливістю навчання персоналу, що підвищує обізнаність співробітників про фішингові атаки через регулярні симуляції. Створює фішингові сценарії, які відповідають реальним загрозам. Також, надає детальні звіти про реакцію співробітників на симуляції, що допомагає визначити слабкі місця.

До **недоліків** можні віднести, той факт, що платформа більше орієнтована на навчання, а не на безпосередній захист, а також занадто часті симуляції можуть призвести до «втоми від навчання», коли співробітники почнуть ігнорувати попередження.

4. KnowBe4 – це хмарна платформа для навчання кібербезпеці. Вона пропонує навчальні програми та симуляції соціотехнічних атак, включаючи фішинг, спуфінг та інші методи соціальної інженерії (KnowBe4, 2024).

Серед **переваг** можна виділити наявний широкий спектр тренінгів та симуляцій, що

охоплюють різні типи соціотехнічних атак. **Є** аналіз ефективності, який включає можливість відстеження прогресу співробітників і їхню здатність розпізнавати загрози. Платформа дозволяє адаптувати навчальні програми відповідно до потреб організації.

До **недоліків** можна віднести високу вартість для великих організацій з значною кількістю співробітників. А також, ефективність залежить від активної участі співробітників у навчанні.

5. Barracuda Sentinel – це рішення для захисту електронної пошти, яке використовує штучний інтелект для виявлення фішингових атак, спуфінгу та компрометації електронної пошти у реальному режимі часу (Barracuda, 2024).

Серед **переваг** можна виділити легку інтеграцію з хмарними сервісами Microsoft, що робить його зручним для організацій, які використовують цю платформу. Використання штучного інтелекту, дозволяє автоматично виявляти і блокувати загрози в реальному режимі часу. Також, є можливість виявлення атак на ранніх стадіях, запобігаючи їх поширенню.

До **недоліків** можна віднести залежність від Microsoft 365, тобто відповідне рішення оптимально працює тільки в зазначеному довкіллі, а користувачі інших платформ можуть не отримати всі переваги цього рішення.

6. **Microsoft Defender for Office 365** – це платформа для захисту від фішингу, шкідливих програм, шкідливих URL-адрес та компрометації електронної пошти, інтегрована в екосистему Microsoft (Microsoft, 2024).

До **переваг** можна віднести глибоку інтеграцію з продуктами Microsoft, що дозволяє забезпечити всебічний захист. Платформа використовує різні механізми виявлення загроз, включаючи захист від фішингу та шкідливих програм. Пропонує автоматизовані засоби для виявлення та реагування на загрози.

До **недоліків** можна віднести значну вартість, а повний захист, буде доступний лише у вищих планах підписки Microsoft 365, що може бути дорого для невеликих підприємств. Також є **з**алежність від екосистеми Microsoft, тобто оптимальне функціонування можна отримати тільки в межах Microsoft, що може обмежити його використання іншими користувачами.

7. **Mandiant ATP (advanced threat protection)** – це програмне рішення для виявлення, аналізу та реагування на складні кіберзагрози, здатне детектувати деякі аспекти соціотехнічних атак, але з певними обмеженнями. Це рішення використовує потужні інструменти для аналізу загроз, включаючи технології машинного навчання, розвідку загроз, та аналіз подій безпеки, а також може допомагати виявляти ознаки соціотехнічних атак, таких як фішинг, через аналіз поведінки користувачів і моніторинг мережевого трафіку (Mandiant, 2024).

Mandiant ATP працює як хмарне або локальне програмне забезпечення, яке можна інтегрувати в існуючі системи безпеки підприємства. Воно надає комплексний набір функцій для виявлення та реагування на кібератаки, включаючи аналіз поведінки, розслідування інцидентів, та забезпечення відповідності стандартам безпеки.

Серед **переваг** Mandiant ATP виділяють легкість інтегруватися з іншими продуктами безпеки, такими як SIEM або інші засоби управління інцидентами, що робить його частиною загальної стратегії кібербезпеки. Має глобальну базу даних загроз, яка постійно оновлюється, що дозволяє виявляти нові та змінювані загрози в режимі реального часу. Програмне рішення використовує передові технології, такі як машинне навчання і поведінковий аналіз, щоб ідентифікувати складні загрози, які можуть залишатися непоміченими іншими системами. Mandiant надає доступ до команди експертів, які можуть допомогти у випадку великих інцидентів, а також проводити аудит безпеки та навчання персоналу.

До **недоліків** можна віднести достатньо високу вартість, складність налаштування та використання, що вимагає високого рівня технічної обізнаності фахівців, залежність від зовнішньої інфраструктури, а також потребує значних обчислювальних ресурсів для аналізу даних, що може вплинути на продуктивність інших систем в організації.

Програмні засоби, такі як Proofpoint, Mimecast, PhishMe (Cofense), KnowBe4, Barracuda Sentinel, і Microsoft Defender for Office 365, Mandiant, пропонують комплексний захист від соціотехнічних атак, включаючи фішинг, спам, шкідливі програми та компрометацію електронної пошти. Вони використовують різні підходи, від машинного навчання і штучного інтелекту до навчання та симуляцій, для виявлення та запобігання загрозам. Хоча ці рішення мають свої переваги, такі як високий рівень захисту та інтуїтивно зрозумілі інтерфейси, їх вартість і залежність від специфічних платформ можуть бути обмеженням для деяких організацій.

Апаратні та апаратно-програмні засоби

1. Cisco Secure Email Gateway (раніше IronPort) – це апаратний шлюз для захисту

електронної пошти. Захищає корпоративну пошту від фішингових атак, спаму, шкідливих програм та інших загроз. Використовує багаторівневий захист для фільтрації вхідної та вихідної пошти (Cisco, 2024).

Серед **переваг** можна виділити високий рівень захисту, який ефективно захищає від складних фішингових атак і шкідливого програмного забезпечення, а також може фільтрувати вміст за різними параметрами, що підвищує загальний рівень безпеки. Засіб є **і**нтегрований з іншими продуктами Cisco та забезпечує гнучкість і ефективність у комплексних рішеннях безпеки.

До **недоліків** можна віднести складність налагодження та супроводу, що вимагає спеціальних знань для налаштування та підтримки. Також, має високу вартість, що може бути дорогим рішенням, особливо для малих і середніх компаній.

2. Palo Alto Networks WildFire – це апаратно-програмний комплекс для захисту від шкідливого програмного забезпечення. Виявляє та блокує шкідливе програмне забезпечення. Використовує технології глибокого аналізу трафіку та машинного навчання для виявлення загроз (Paloaltonetworks, 2024).

Серед **переваг є** використання машинного навчання, що дозволяє швидко ідентифікувати нові загрози. Має інтеграцію з іншими продуктами Palo Alto Networks, що в свою чергу при комплексному використанні забезпечує цілісну систему захисту. Здатен постійно вдосконалюватися завдяки вбудованому механізму самонавчання.

Серед **недоліків** можна виділити високу вартість, тобто є одним з найдорожчих рішень на ринку, а також має високу ресурсоємність, що потребує значних обчислювальних ресурсів для роботи.

3. SonicWall Email Security – це апаратне (або програмне) рішення для захисту та фільтрації електронної пошти, яке встановлюються в мережі і забезпечує захист від фішингових атак, спаму, шкідливих програм та інших загроз, пов'язаних з електронною поштою (SonicWall, 2024). Загалом, SonicWall Email Security пропонує рішення для захисту електронної пошти як у вигляді фізичних пристроїв, так і у вигляді програмних рішень, що дає можливість організаціям вибрати найбільш відповідний варіант для їхніх потреб.

До **переваг** цього рішення можна віднести інтуїтивно зрозумілий інтерфейс та простоту налаштування, високу продуктивність і точність фільтрації електронної пошти, інтеграцію з іншими рішеннями SonicWall для комплексного захисту.

Серед **недоліків** виділяють обмежену функціональність у порівнянні з конкурентами, а також вимагає фізичного простору і обладнання для розгортання і може потребувати обслуговування.

4. FortiGate пропонується у вигляді спеціалізованих пристроїв (апаратних брандмауерів), які можна встановити в мережі для забезпечення захисту від загроз. Ці пристрої виконують функції брандмауера, VPN, IPS/IDS, вебфільтрації та багато інших завдань у режимі реального часу.

Fortinet FortiMail – це апаратний шлюз для захисту електронної пошти. Забезпечує захист від фішингу, спаму та інших загроз, пов'язаних із електронною поштою. Використовує багатошарові механізми виявлення (Fortinet, 2024).

До **переваг** можна віднести ефективну фільтрацію та високу ефективність у виявленні та блокуванні небажаних повідомлень. Наявний широкий набір функцій, включаючи антивірусну перевірку, контроль спаму та інші засоби безпеки. Є можливість інтеграції **з** Fortinet Security Fabric, що в комплексному застосуванні підвищує загальний рівень безпеки, інтегруючись із іншими продуктами Fortinet.

Недоліки повязані зі складністю управління, що потребує належного налаштування та підтримки висококваліфікованими спеціалістами. Має обмежену масштабованість, що може бути менш ефективним для великих організацій із значною кількістю користувачів.

5. Sophos XG Firewall – це мережевий брандмауер, який захищає мережу від різних типів атак, включаючи фішинг і соціотехнічні загрози. Використовує глибокий аналіз трафіку та можливості захисту від загроз в режимі реального часу (News.sophos, 2024).

Серед **переваг** виділяють простоту використання та Інтуїтивно зрозумілий інтерфейс і зручність налаштування. Є інтегрована система безпеки яка об'єднує різні засоби захисту в єдиному рішенні. Також, є можливість отримання детальних звітів про загрози та активність в мережі.

До **наявних** недоліків можна віднести обмеження в налаштуванні, тобто засіб **є** менш гнучкий у порівнянні з деякими іншими рішеннями на ринку, а для отримання повного спектра функцій необхідно регулярно оновлювати підписки.

Апаратні засоби, такі як Cisco Secure Email Gateway, Palo Alto Networks WildFire, SonicWall Email Security, Fortinet FortiMail та Sophos XG

Таблиця 1

Порівняльна таблиця засобів виявлення та блокування соціотехнічних атак

№	Засіб	Критерії								
		Високий рівень захисту	Централізоване управління	Простота використання	Інтеграція з іншими платформами	Штучний інтелект	Адаптивність	Можливості роботи в офлайн-режимі	Висока вартість	Складність налаштування
1	Proofpoint	+	+	-	+	+	-	-	+	+
2	Mimecast	+	-	+	+	-	-	-	-	-
3	PhishMe (Cofense)	-	-	-	-	-	+	+	-	-
4	KnowBe4	-	-	-	-	-	+	+	+	-
5	Barracuda Sentinel	+	-	-	+	+	-	-	-	-
6	Microsoft Defender for Office 365	+	+	+	+	+	+	-	+	-
7	Mandiant ATP	+	+	-	+	+	+	-	+	+
8	Cisco Secure Email Gateway	+	+	-	+	-	-	+	+	+
9	Palo Alto Networks WildFire	+	-	-	+	+	+	+	+	-
10	SonicWall Email Security	+	+	+	+	-	-	+	-	+
11	Fortinet FortiMail	+	+	-	+	-	-	+	+	+
12	Sophos XG Firewall	+	+	+	+	+	-	+	-	+

Firewall, є потужними інструментами для забезпечення безпеки, надають комплексний захист від різних загроз, включаючи фішинг, шкідливі програми, атаки соціальної інженерії та мережеві атаки. Вони використовують передові технології, такі як машинне навчання та багатошаровий аналіз, для виявлення і блокування загроз в режимі реального часу. Незважаючи на високу ефективність та інтеграцію з іншими рішеннями безпеки, ці засоби потребують значних інвестицій і спеціалізованих знань для налаштування та підтримки, що може бути викликом для малих та середніх підприємств.

Відповідно до проведеного аналізу в табл. 1 за дев'ятьма критеріями (високий рівень захисту, централізоване управління, простота використання, інтеграція з іншими платформами, штучний інтелект, адаптивність, можливості роботи в офлайн-режимі, висока вартість, складність налаштування) інтегровано характеристики розглянутих засобів де відображається наявність або відсутність переваг та недоліків у відповідних рішеннях («+» означає наявність певного аспекту в продукті, а «-» – його відсутність).

Висновки. Слід зазначити, що програмні засоби виявлення та блокування соціотехнічних атак, часто пропонують більшу гнучкість і легкість використання, але можуть бути обмеженими в офлайн-режимі та залежати від інтернет-з'єднання. Апаратні засоби, з іншого боку, надають більш надійний захист і можуть бути інтегровані з іншими мережевими рішеннями, але вимагають значних фінансових вкладень і складні в налаштуванні.

ЛІТЕРАТУРА:

1. Анна Корченко. Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019. 361 с.

2. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology (NIST). NIST Special Publication 800-94. 2007.

3. Hee-Yong Kwon. Advanced Intrusion Detection Combining Signature-Based and Behavior-Based Detection Methods. Hee-Yong Kwon, Taesic Kim, Mun-Kyu Lee. Electronics 2022, *Special Issue Real-Time Control of Embedded Systems*. Vol. 11(6), Pp 867. doi.org/10.3390/electronics11060867.

4. Moustafa N., Hu J. Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Evaluation. IEEE Access, 2019, Vol. 7, Pp. 104821–104845. URL: https://doi.org/10.1109/ACCESS.2019.2932754 (дата звернення: 21.08.2024).

5. Kisiel J., O'Neill D. Contextual Analysis for Secure Communication: A Survey. *Computers & Security*, 2018, Vol. 74, Pp. 172–191. URL: https://doi.org/10.1016/j.cose.2018.01.002 (дата звернення: 18.08.2024).

6. Кузьма К., Зівенко В. Аналіз методів фільтрації електронної пошти від спаму. *Геометричне моделювання та інформаційні технології*, Миколаїв, № 1 (3), 2017, стр. 84–89.

7. Kevin D. Mitnick, William L. Simon. The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons, 2003. Computers – 368 pages.

8. Rahman T., Rohan R., Pal D. Human Factors in Cybersecurity: A Scoping Review. *In* Proceedings of the 12th International Conference on Advances in Information Technology (IAIT 2021), Bangkok, Thailand. ACM. 2021. URL: https://doi.org/10.1145/3468784.3468789 (дата звернення: 18.08.2024).

9. Войтович О. П., Буда А. Г., Головенько В. О. Дослідження методів аналізу соціальних мереж як середовища інформаційних війн. Сучасні інформаційні технології. 2023, стр. 76–80.

10. Cyber.academy. Підвищуємо кіберобізнаність громадського сектору України (cyber.academy). URL: https://www.cyber.academy/post/cyber_awareness_public_sector-1 (дата звернення: 19.08.2024).

11. González-Granadillo G., González-Zarzosa S., Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors 2021, Vol. 21, Pp. 4759. URL: https://doi.org/10.3390/s21144759 (дата звернення: 19.08.2024).

12. Bamanga Ahmad M., Ahmed Shehu M. Enhancing Phishing Awareness Strategy Through Embedded Learning Tools: A Simulation Approach. *Archives of Advanced Engineering Science*. 2023, Vol. XX. Pp. 1–14. DOI:10.47852/bonviewAAES32021392.

13. Forbes Advisor. Best Phishing Simulators To Prepare Employees And Defend Your Network. URL: https://www.forbes.com/advisor/business/best-phishing-simulators/ (дата звернення: 20.08.2024).

14. Proofpoint. Products. URL: https://www.proofpoint.com/us (дата звернення: 21.08.2024).

15. Mimecast. Our Platform. URL: https://www.mimecast.com (дата звернення: 21.08.2024).

16. PhishMe Cofense. Products. URL: https://cofense.com (дата звернення: 21.08.2024).

17. KnowBe4. Products+Pricing. URL: https://www.knowbe4.com (дата звернення: 21.08.2024).

18. Barracuda. Products. URL: https://www.barracuda.com/ (дата звернення: 21.08.2024).

19. Microsoft. Microsoft Defender for Office 365. URL: https://www.microsoft.com/en-gb/security/business/siem-and-xdr/microsoft-defender-office-365 (дата звернення: 21.08.2024).

20. Mandiant. Products. URL: https://www.mandiant.com (дата звернення: 22.08.2024).

21. Cisco. Configure Cisco Security Awareness Integration with Cisco Secure Email Gateway – Cisco. URL: https://www.cisco.com/c/en/us/support/docs/security/secure-email-gateway/220332-configure-cisco-security-awareness-integ.html (дата звернення: 22.08.2024).

22. Network security. Products. URL: https://www.paloaltonetworks.com/network-security/wildfire (дата звернення: 22.08.2024).

23. SonicWall. Products. URL: https://www.sonicwall.com/products/secure-email/cloud-email-security (дата звернення: 22.08.2024).

24. Fortinet. Products A–Z. URL: https://www.fortinet.com/products/email-securityт (дата звернення: 22.08.2024).

25. Sophos Firewall. Products and Services. URL: https://news.sophos.com/en-us/2020/02/18/xg-firewall-v18-is-now-available/ (дата звернення: 22.08.2024).

REFERENCES:

1. Korchenko, Anna. (2019). Metody identyfikatsii anomalnykh staniv dlia system vyiavlennia vtorhnen [Methods of identifying abnormal states for intrusion detection systems]. Monohrafiia, Kyiv, TsP «Komprynt», 361 s.

2. Scarfone, K., Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology (NIST). NIST Special Publication 800-94.

3. Hee-Yong, Kwon. (2022). Advanced Intrusion Detection Combining Signature-Based and Behavior-Based Detection Methods. Hee-Yong Kwon, Taesic Kim, Mun-Kyu Lee. Electronics. *Special Issue Real-Time Control of Embedded Systems*. Vol. 11(6), Pp 867. doi.org/10.3390/electronics11060867.

4. Moustafa, N., Hu, J. (2019). Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Evaluation. IEEE Access, Vol. 7, Pp. 104821–104845. Retrieved from: https://doi.org/10.1109/ACCESS.2019.2932754 (date of access: 21.08.2024).

5. Kisiel, J., O'Neill, D. (2018). Contextual Analysis for Secure Communication: A Survey. *Computers & Security*, Vol. 74, Pp. 172–191. Retrieved from: https://doi.org/10.1016/j.cose.2018.01.002 (date of access: 18.08.2024).

6. Kuzma, K., Zivenko, V. (2017). Analiz metodiv filtratsii elektronnoi poshty vid spamu [Analysis of email spam filtering methods]. Heometrychne modeliuvannia ta informatsiini tekhnolohii, Mykolaiv, № 1 (3), str. 84–89.

7. Kevin, D. Mitnick, William, L. Simon. (2003). The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons, Computers. 368 pages.

8. Rahman, T., Rohan, R., & Pal, D. (2021). Human Factors in Cybersecurity: A Scoping Review. *In* Proceedings of the 12th International Conference on Advances in Information Technology (IAIT 2021), Bangkok, Thailand. ACM. Retrieved from: https://doi.org/10.1145/3468784.3468789 (date of access: 18.08.2024).

9. Voitovych, O. P., Buda, A. H., Holovenko, V. O. (2023). Doslidzhennia metodiv analizu sotsialnykh merezh yak seredovyshcha informatsiinykh viin [Study of methods of analysis of social networks as an environment of information wars. Suchasni informatsiini tekhnolohii. str. 76–80.

10. Cyber.academy. Pidvyshchuiemo kiberobiznanist hromadskoho sektoru Ukrainy (cyber.academy). Retrieved from: https://www.cyber.academy/post/cyber_awareness_public_sector-1 (date of access: 19.08.2024).

11. González-Granadillo, G., González-Zarzosa, S., Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors. Vol. 21, Pp. 4759. Retrieved from: https://doi.org/10.3390/s21144759 (date of access: 19.08.2024).

12. Bamanga Ahmad, M., Ahmed Shehu, M. (2023). Enhancing Phishing Awareness Strategy Through Embedded Learning Tools: A Simulation Approach. *Archives of Advanced Engineering Science*. Vol. XX. Pp. 1–14. DOI:10.47852/bonviewAAES32021392.

13. Forbes Advisor. Best Phishing Simulators To Prepare Employees And Defend Your Network. Retrieved from: https://www.forbes.com/advisor/business/best-phishing-simulators/ (date of access: 20.08.2024).

14. Proofpoint. Products. Retrieved from: https://www.proofpoint.com/us (date of access: 21.08.2024).

15. Mimecast. Our Platform. Retrieved from: https://www.mimecast.com (date of access: 21.08.2024).

16. PhishMe Cofense. Products. Retrieved from: https://cofense.com (date of access: 21.08.2024).

17. KnowBe4. Products+Pricing. Retrieved from: https://www.knowbe4.com (date of access: 21.08.2024).

18. Barracuda. Products. Retrieved from: https://www.barracuda.com/ (date of access: 21.08.2024).

19. Microsoft. Microsoft Defender for Office 365. Retrieved from: https://www.microsoft.com/en-gb/security/business/siem-and-xdr/microsoft-defender-office-365 (date of access: 21.08.2024).

20. Mandiant. Products. Retrieved from: https://www.mandiant.com (date of access: 22.08.2024).

21. Cisco. Configure Cisco Security Awareness Integration with Cisco Secure Email Gateway – Cisco. Retrieved from: https://www.cisco.com/c/en/us/support/docs/security/secure-email-gateway/220332-configure-cisco-security-awareness-integ.html (date of access: 22.08.2024).

22. Network security. Products. Retrieved from: https://www.paloaltonetworks.com/network-security/wildfire (date of access: 22.08.2024).

23. SonicWall. Products. Retrieved from: https://www.sonicwall.com/products/secure-email/cloud-email-security (date of access: 22.08.2024).

24. Fortinet. Products A-Z. Retrieved from: https://www.fortinet.com/products/email-securityт (date of access: 22.08.2024).

25. Sophos Firewall. Products and Services. Retrieved from: https://news.sophos.com/en-us/2020/02/18/xg-firewall-v18-is-now-available/ (date of access: 22.08.2024).