УДК 004.5:004.942:004.056 DOI: 10.31673/2412-4338.2024.049842

Запорожченко Михайло Михайлович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0000-0003-0182-9497

МОДЕЛЮВАННЯ ПРОФІЛЮ ЗАХИЩЕНОСТІ КОРИСТУВАЧА ДЛЯ ВИЗНАЧЕННЯ ЙОГО ПОТЕНЦІЙНОЇ ВРАЗЛИВОСТІ ДО СОЦІОІНЖЕНЕРНИХ АТАК

Анотація. *Зростаючі загрози соціоінженерних атак (SEA) в умовах активного використання цифрових технологій висувають нові вимоги до захисту корпоративних інформаційних систем (ІС). У статті представлено розробку математичної моделі профілю захищеності користувача, яка спрямована на визначення його потенційної вразливості до SEA. Запропонована модель базується на інтеграції чотирьох ключових факторів: психологічного, організаційного, технічного та інформаційного впливу, що дозволяє проводити комплексний аналіз ризиків.*

Розглянуто існуючі підходи до оцінки вразливості користувачів та виявлено їх недоліки, зокрема обмеженість у врахуванні комплексної взаємодії факторів. Запропонована модель усуває ці недоліки, дозволяючи оцінювати вразливість користувачів у динамічному середовищі з урахуванням змінних зовнішніх умов та індивідуальних особливостей користувачів. Основу підходу становить моделювання процесу реалізації SEA, розділеного на три ключові етапи: доставку атакуючого контенту, взаємодію користувача з цим контентом та уникнення виявлення атаки. Для кожного етапу розроблено відповідні математичні залежності, які враховують взаємодію зазначених факторів.

Результати моделювання дозволяють виявляти групи вразливих користувачів та критичні етапи, на яких користувач або система проявляють найбільшу вразливість до атак. Запропонований підхід також дозволяє адаптувати заходи захисту до реальних умов корпоративних середовищ, забезпечуючи узгодженість між оцінкою ризиків та потребами захисту. Модель може бути використана для розробки цільових заходів попередження SEA та покращення загального стану інформаційної безпеки.

Таким чином, запропонована модель профілю захищеності користувача є універсальним інструментом для прогнозування ризиків SEA у корпоративних ІС. Вона забезпечує можливість аналізу та попередження атак за допомогою кількісного врахування індивідуальних і зовнішніх факторів, що визначають поведінку користувачів. Крім того, модель дозволяє оптимізувати розробку стратегій захисту, забезпечуючи їх гнучкість та адаптивність до змін інформаційного середовища. Це забезпечує системний підхід до оцінки ризиків і дозволяє мінімізувати вразливість ІС до соціоінженерних загроз.

Ключові слова: *соціоінженерні ризики, інформаційна безпека, корпоративні системи, інформаційний вплив, математичне моделювання, адаптивний захист, оцінка вразливості, прогнозування ризиків.*

Zaporozhchenko Mykhailo
State University of Information and Communication Technologies, Kyiv
ORCID 0000-0003-0182-9497

MODELING THE USER'S SECURITY PROFILE TO DETERMINE HIS POTENTIAL VULNERABILITY TO SOCIAL ENGINEERING ATTACKS

Abstract. *The evolving threats of social engineering attacks (SEA) in the context of the active use of digital technologies impose new requirements for the protection of corporate information systems (IS). The article presents the mathematical model of the user's security profile, which is designed to evaluate his potential vulnerability to SEA. The proposed model is based on the integration of four key factors:*

psychological, organizational, technical and informational impact, which enables a comprehensive risk analysis.

The existing approaches to assessing user vulnerability have been reviewed and their limitations have been identified, in particular, the limited consideration of the complex interaction of factors. The proposed model solves these limitations, allowing to assess the vulnerability of users in a dynamic environment, taking into account changing external environment and users' individual characteristics. The approach is based on modeling the SEA process, divided into three key stages: delivery of attacking content, user interaction with this content, and avoidance of attack detection. For each stage, the corresponding mathematical dependencies have been developed that take into account the interaction of these factors.

The results of the modeling allow to identify groups of vulnerable users and critical stages at which a user or a system is most vulnerable to attacks. The proposed approach also allows to adapt protection measures to the real conditions of corporate environments, ensuring consistency between risk assessment and protection needs. The model can be used to develop targeted SEA prevention measures and improve the overall state of information security.

Thus, the proposed user security profile model is a universal tool for predicting SEA risks in corporate IS. It provides the ability to analyze and prevent attacks by quantifying individual and external factors that determine user behavior. In addition, the model allows to optimize the development of protection strategies, ensuring their flexibility and adaptability to changes in the information environment. This ensures a systematic approach to risk assessment and minimizes the vulnerability of IS to social engineering threats.

Keywords: *social engineering risks, information security, corporate systems, information impact, mathematical modeling, adaptive protection, vulnerability assessment, risk prediction.*

1. Вступ

Проблема захисту корпоративних інформаційних систем (ІС) від соціоінженерних атак (SEA) стає все більш актуальною у зв'язку зі стабільною популярністю та зростаючою складністю цих атак. Одним із ключових викликів є оцінка потенційної вразливості користувачів, що забезпечує основу для побудови ефективних превентивних стратегій захисту. SEA характеризуються високою адаптивністю до умов корпоративного середовища, тому важливою є розробка методів, які дозволяють враховувати множинність факторів захищеності: психологічного, організаційного, технічного та інформаційного впливу.

Зазначене підкреслює *актуальність* створення моделі профілю захищеності користувача, яка дозволить визначити його потенційну вразливість до SEA, а також закласти основу для подальшого впровадження цільових контрзаходів.

2. Аналіз літературних даних і постановка проблеми

У роботі [1] запропоновано модель оцінки вразливості користувачів до SEA у соціальних мережах, яка враховує залученість, мотивацію та компетентність користувачів. Перевагою є багатофакторний підхід, однак модель орієнтована на соціальні мережі та не враховує специфіку корпоративних ІС, де динаміка ризиків складніша. У статті [2] наведено фреймворк аналізу ризиків у хмарних сервісах на основі профілювання користувачів. Модель враховує частоту операцій та рівень обізнаності, забезпечуючи кількісний підхід до оцінки ризиків. Водночас відсутність психологічних характеристик та врахування взаємодії між користувачами обмежує її застосування для багатоетапних SEA.

У роботах [3,4] представлено прогнозування вразливості користувачів до атак за допомогою алгоритмів машинного навчання. В [3] модель враховує демографічні дані, технологічні навички та психологічні характеристики, забезпечуючи персоналізацію оцінки ризиків. Однак її обмежує залежність від контрольованих умов і відсутність врахування зовнішніх впливів. В [4] модель зосереджена на технічних аспектах і не враховує соціально-психологічні фактори та поведінкові моделі користувачів, що обмежує її застосування в багатофакторному аналізі корпоративних систем.

У роботі [5] запропоновано модель SEA на основі дерева атак і Марковської моделі, яка враховує частоту загроз і ефективність методів переконання. Підхід забезпечує класифікацію

загроз за рівнем ризику, але ігнорує когнітивні характеристики користувачів та зовнішні впливи. Використання статичних даних знижує здатність моделі до адаптації в умовах змін корпоративного та зовнішнього середовища. У статті [6] досліджено застосування штучного інтелекту для аналізу поведінкових патернів, виявлення фішингових атак за допомогою NLP та прогнозування загроз. Висока точність систем залежить від регулярного оновлення моделей, відсутність якого обмежує їхню актуальність у динамічному середовищі.

Таким чином, у більшості існуючих підходів враховуються лише окремі аспекти, такі як психологічні та поведінкові особливості користувача, його демографічні ознаки та залученість до соціальних мереж, технічна обізнаність користувача та середня кількість виконуваних ним операцій, впроваджені технічні засоби захисту, ступінь володіння соціальним інженером атакуючими техніками та ступінь відповідних вразливостей користувачів тощо. При цьому в оцінці не враховується фактор інформаційного впливу, який формують політичні, економічні та соціальні умови країни чи регіону, в якому функціонує організація або перебуває користувач. Ці умови мають значний вплив на кількість та складність SEA, ефективність технічних та організаційних заходів захисту в аспекті протидії даним загрозам та психологічний стан та поведінку ключових цілей SEA – користувачів – що обмежує комплексність такої оцінки і адаптацію до конкретного середовища.

3. Мета і задачі дослідження

Метою дослідження є розробка моделі профілю захищеності користувача корпоративної ІС, яка включає комплексну оцінку його психологічних характеристик, впроваджених організаційних і технічних заходів захисту, а також фактору інформаційного впливу для визначення потенційної вразливості користувача до SEA.

Для досягнення поставленої мети вирішено такі завдання:

- проаналізовано існуючи підходи до оцінки потенційної вразливості користувача до SEA, визначено їх переваги та недоліки;
- запропоновано та обґрунтовано модель профілю захищеності користувача корпоративної ІС, яка включає сукупність факторів: психологічного, організаційного, технічного та фактору інформаційного впливу;
- розроблено математичну модель оцінки потенційної вразливості користувача до SEA на основі профілю захищеності користувача корпоративної ІС.

4. Результати дослідження

Формування профілю захищеності користувача є основою прогнозування SEA і моделювання їх можливих траєкторій у корпоративних ІС. SEA характеризуються багатовимірним впливом, що потребує інтегрованого підходу до оцінки вразливості користувачів, що передбачає врахування їх індивідуальних психологічних особливостей, організаційного контексту (рівень впровадження організаційних та технічних заходів захисту) та зовнішніх впливів, які формують поведінкові ризики користувачів та здатність впроваджених механізмів захисту виявляти та блокувати потенційні загрози. Таким чином, запропонована модель (рис. 1) враховує психологічний, організаційний, технічний фактори та фактор інформаційного впливу, забезпечуючи комплексну основу для прогнозування ймовірності успішної SEA.

Психологічний фактор оцінює індивідуальні характеристики, що впливають на сприйнятливість до маніпуляцій через почуття терміновості, страху, авторитету та інші види тиску [7,8]. Організаційний фактор включає рівень культури інформаційної безпеки, ефективність навчання, дотримання політик, частоту аудитів та готовність до реагування на інциденти [9]. Інтеграція цих компонентів у модель дозволяє адаптувати оцінку потенційної вразливості залежно від ефективності навчання та змін в організаційних заходах захисту.

Технічний фактор зосереджується на оцінці інструментів захисту, які знижують ймовірність доставки шкідливого контенту і забезпечують виявлення та протидію сучасним

кібератакам. Фактор інформаційного впливу враховує макросередовище, включаючи економічні, політичні й соціальні умови. Під час криз користувачі стають більш уразливими до маніпуляцій через підвищений рівень стресу. Зокрема, під час війни в Україні з 2022 року зловмисники використовували теми, пов'язані з фінансовою допомогою, гуманітарними ініціативами, евакуацією, мобілізацією для поширення фішингових повідомлень [10].

Рис. 1. Модель профілю захищеності користувача корпоративної ІС

Запропоновано математичну модель оцінки потенційної вразливості користувача до SEA, яка інтегрує фактори профілю захищеності для оцінки ймовірності одноетапної SEA (зловмисник → цільовий користувач). Модель базується на формулі:

$$P(U_i) = P_{del} \cdot P_{int} \cdot P_{con}, \quad (1)$$

де P_{del} – ймовірність доставки атаки; P_{int} – ймовірність взаємодії користувача з небезпечним контентом; P_{con} – ймовірність уникнення виявлена після взаємодії.

Модель структурує SEA на три етапи: доставка, взаємодія та уникнення виявлення. При цьому якщо хоча б один з етапів не реалізовано (атакуючий контент не доставлено, користувач не взаємодіяв з контентом або атака була виявлена), SEA вважається неуспішною. Варто зазначити, що атака може бути як виявлена користувачем, так і заблокована засобами захисту:

$$P_{\text{con}} = \bar{P}_{\text{det}} \cdot \bar{P}_{\text{bl}}, \quad (2)$$

де $\bar{P}_{\text{det}}$ – уникнення виявлення користувачем, $\bar{P}_{\text{bl}}$ – уникнення блокування інструментами захисту.

Кожен етап моделюється з урахуванням сукупності факторів профілю захищеності користувача, що дозволяє оцінити внесок кожного фактору у реалізацію атаки та визначити критичні етапи, які потребують посиленої уваги фахівців. До того ж, деталізація етапів сприяє розробці й адаптації цільових заходів захисту, спрямованих на мінімізацію ризиків конкретних етапів атаки, до динамічного контексту і специфіки поведінки користувачів.

Ймовірність доставки атакуючого контенту P_{del} визначається взаємодією першого компонента технічного фактору T_{del} (оцінка засобів захисту, спрямованих на запобігання доставці потенційно небезпечного контенту – фільтрів та систем захисту електронної пошти) та фактору інформаційного впливу E. Формалізація залежності представлена формулою:

$$P_{del} = 1 - T_{del} \cdot e^{\left(d_{T_{del},E} - k_{E_{del}}\right)(E-1)}, \quad (3)$$

де $T_{del}, E \in [0; 1]$ – оцінки відповідних факторів (1 відповідає максимальному захисту/стабільному середовищу); $d_{T_{del},E}$ – динамічна складова коефіцієнта впливу E на T_{del}; $k_{E_{del}}$ – статична складова коефіцієнта впливу, яка використовується для адаптації ймовірності доставки для граничних умов ($T_{del} = 1$ та $E = 0.1$).

При цьому у стабільних зовнішніх умовах ($E = 1$) ймовірність доставки атакуючого контенту залежить виключно від технічних засобів захисту ($P_{del} = 1 - T_{del}$) . У несприятливих умовах ($E < 1$) технічні засоби можуть втрачати свою ефективність, залежно від інтенсивності впливу зовнішнього середовища, яке моделюється коефіцієнтом ($d_{T_{del},E} - k_{E_{del}}$).

Динамічна складова коефіцієнту впливу $d_{T_{del},E}$ була введена для вирішення проблеми недостатнього врахування динамічної взаємодії між факторами у випадку використання статичних коефіцієнтів, що може призводити до спотворення результатів оцінки. Змінні умови, зокрема посилення зовнішніх загроз або зниження ефективності технічних засобів, вимагають адаптивного підходу, який більш точно відображає взаємодію між факторами. Таким чином, коефіцієнти впливу включають динамічну складову, яка змінюється залежно від значень основного та коригуючого факторів:

$$d_{base,cor} = \min(base, cor)^{\max(1-base,1-cor)}, \quad (4)$$

де $d_{base,cor}$ – динамічна складова коефіцієнта впливу, яка при низьких значеннях факторів підсилює їх взаємний вплив, $base$ – оцінка основного фактору, cor – оцінка коригуючого фактору.

Запропонований підхід забезпечує експоненційне зменшення впливу факторів при низьких їх значеннях, що дозволяє більш точно відобразити вразливість користувача або системи в умовах недостатньої захищеності або сильного інформаційного впливу.

Так, у формулі (3) динамічна складова ($d_{T_{del},E}$) визначається залежно від співвідношення значень факторів: якщо $T_{del} < E$, тоді $d_{T_{del},E} = T_{del}^{(E-1)}$, якщо $T_{del} > E$, тоді $d_{T_{del},E} = E^{(T_{del}-1)}$.

Залежність значення динамічної складової коефіцієнтів впливу від оцінок факторів наведена на рис. 2.

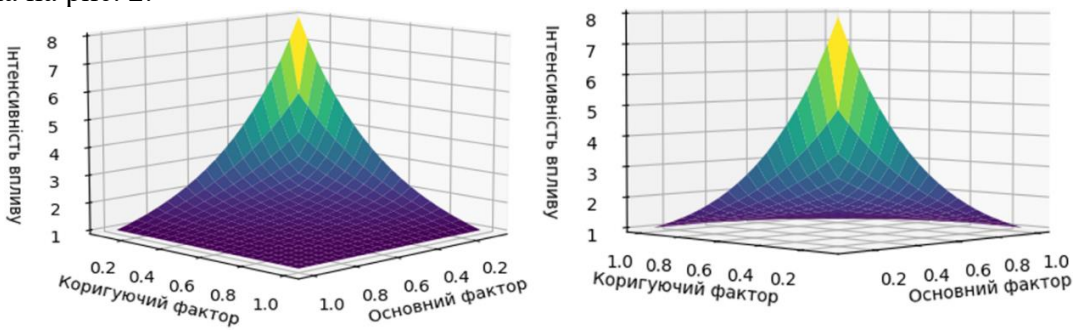

Рис. 2. Залежність значення динамічної складової коефіцієнтів впливу від оцінок факторів

Статичні складові виконують роль базових параметрів, які адаптують початкові оцінки на кожному етапі з урахуванням специфіки впливу факторів та їх взаємозалежності. На рис. 3 наведено розподіл ймовірностей для етапу взаємодії користувача з потенційно небезпечним контентом з урахуванням тільки динамічних складових коефіцієнтів впливу ($k = 0$) – ліворуч, та з урахування динамічних та статичних складових ($k_{O_{int}} = 0.75$, $k_{E_{int}} = 0.43$) – праворуч:

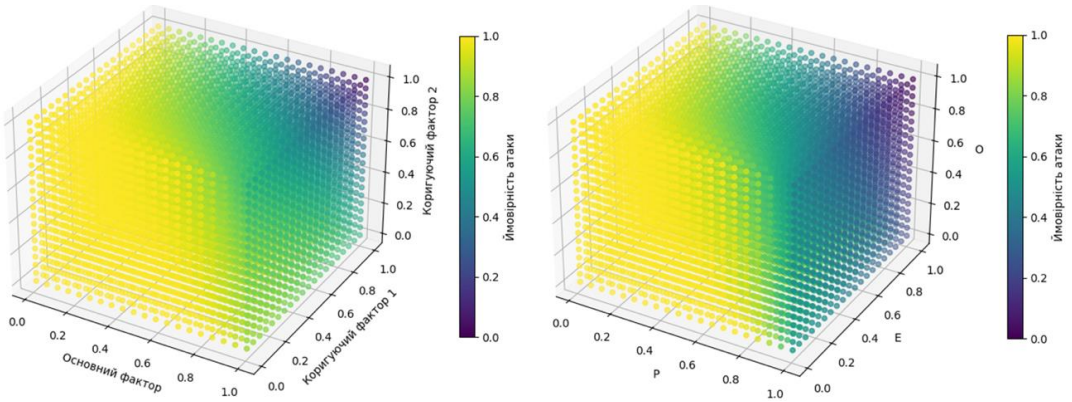

Рис. 3. Розподіл ймовірностей взаємодії користувача з потенційно небезпечним контентом

Аналогічно може бути оцінена ймовірність взаємодії користувача з потенційно небезпечним контентом – як залежність від психологічного фактору користувача, модифікованого організаційним фактором та фактором інформаційного впливу:

$$P_{int} = 1 - P \cdot e^{\left(d_{P,O} - k_{O_{int}}\right)(O-1) + \left(d_{P,E} - k_{E_{int}}\right)(E-1)}, \quad (5)$$

де $d_{P,O}$ та $d_{P,E}$ – динамічні складові коефіцієнтів впливу O на P та E на P відповідно; $k_{O_{int}}$ та $k_{E_{int}}$ – відповідні статичні складові коефіцієнтів впливу, що дозволяють адаптувати початкове значення ймовірності взаємодії (P_{int}) для граничних умов.

Ймовірність виявлення атаки користувачем (повідомлення в службу ІБ) залежить від організаційного фактору та модифікується психологічним фактором і фактором інформаційного впливу:

$$\bar{P}_{\text{det}} = 1 - O \cdot e^{(d_{O,P} - k_{P_{det}})(P-1) + (d_{O,E} - k_{E_{det}})(E-1)}, \quad (6)$$

де $d_{O,P}$ та $d_{O,E}$ – динамічні складові коефіцієнтів впливу P на O та E на O відповідно; $k_{P_{det}}$ та $k_{E_{det}}$ – статичні складові коефіцієнтів впливу, що дозволяють адаптувати початкове значення ймовірності виявлення користувачем $\bar{P}_{\text{det}}$ для граничних умов.

Ймовірність уникнення блокування атаки технічними засобами розраховується як:

$$\bar{P}_{\text{bl}} = 1 - T_{bl} \cdot e^{(d_{T_{bl},P} - k_{P_{bl}})(P-1) + (d_{T_{bl},E} - k_{E_{bl}})(E-1)}, \quad (7)$$

де $d_{T_{bl},P}$ та $d_{T_{bl},E}$ – динамічні складові коефіцієнтів впливу P на T_{bl} та E на T_{bl} відповідно; $k_{P_{bl}}$ та $k_{E_{bl}}$ – статичні складові коефіцієнтів впливу, що дозволяють адаптувати початкове значення ймовірності блокування атаки технічними засобами захисту $\bar{P}_{\text{bl}}$ для граничних умов.

Підхід до визначення статичних складових коефіцієнтів впливу базується на моделюванні граничних сценаріїв, де максимізується вплив одного фактору за фіксованих протилежних значень інших. Це забезпечує кількісну оцінку взаємодії факторів у несприятливих умовах та адаптивність моделі до специфіки корпоративних систем. Процес оцінки включає такі етапи:

1. Формулювання сценаріїв граничних умов із контекстуальними даними про середовище, типи загроз та потенційні вектори атак;

2. Незалежне оцінювання експертами ймовірності реалізації кожного етапу атаки з урахуванням сценарних обмежень;

3. Узгодження результатів через обговорення або застосування середньозважених значень (в залежності від досвіду, кваліфікації, специфіки діяльності експерта).

Коригувальні коефіцієнти оптимізуються шляхом мінімізації квадратичної похибки між прогнозованими та емпіричними значеннями, з обмеженням $C_{j,min} \leq C_j \leq C_{j,max}$, яке забезпечує відповідність моделі специфіці корпоративного середовища, де C_j – вектор коефіцієнтів для j-го етапу. Для валідації моделі використовується аналіз чутливості, який визначає вплив окремих коефіцієнтів на точність прогнозу. Результати візуалізуються графічно, що дозволяє ідентифікувати найбільш критичні фактори для точного моделювання.

5. Висновки

У статті запропоновано новий підхід до моделювання профілю захищеності користувача корпоративних ІС для оцінки його потенційної вразливості до SEA. Розроблена модель інтегрує психологічні характеристики, організаційні заходи, технічні аспекти безпеки та зовнішні інформаційні впливи, забезпечуючи комплексну оцінку ризиків. Вона дозволяє формалізувати взаємодію зазначених факторів на кожному з ключових етапів атаки: доставки, взаємодії та уникнення виявлення. Математична модель дозволяє кількісно оцінити ризики SEA, враховуючи індивідуальні особливості користувачів, рівень корпоративного захисту та зовнішні умови, забезпечуючи системний аналіз і мінімізацію загроз.

Використання розробленої моделі може дозволити ідентифікувати слабкі місця у системі безпеки та критичні етапи атак, що потребують посилення захисту, персоналізувати заходи безпеки відповідно до індивідуальних оцінок користувачів та адаптувати механізми захисту

до динамічних умов корпоративних систем. Таким чином, практичне застосування моделі сприяє оптимізації управління ризиками та вдосконаленню корпоративних систем кіберзахисту.

Подальші дослідження можуть бути спрямовані на розширення моделі для врахування додаткових аспектів, таких як рівень цифрової грамотності, вплив колективної поведінки співробітників, інтенсивність взаємодії між ними, а також на адаптацію профілю захищеності до специфіки окремих галузей. Перспективним є вдосконалення підходів до оцінки психологічного фактору з використанням сучасних методів психометричного аналізу. Окремий напрям досліджень може бути зосереджений на розробці інтегрованих систем оцінки ризиків SEA у реальному часі на основі технологій штучного інтелекту, які враховують динамічні зміни в поведінці користувачів та зовнішньому середовищі, для побудови прогностичних моделей та автоматизації аналізу.

Список використаної літератури

1. Albladi S., Weir G. Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*. 2020. № 3. 7.
2. Ye Z., Guo Y., Ju A., Wei F., Zhang R., Ma J. A risk analysis framework for social engineering attack based on user profiling. *Journal of Organizational and End User Computing.* 2020. Vol. 32, № 3. P. 37-49.
3. Huseynov F., Ozdenizci Kose B. Using machine learning algorithms to predict individuals' tendency to be victim of social engineering attacks. *Information Development.* 2024. Vol. 40, № 2. P. 298-318.
4. Бохонько О., Лисенко С. Методи виявлення кібератак соціальної інженерії. Вісник Хмельницького національного університету. *Технічні науки*. 2023. Том 327, № 5(2). С. 231-236.
5. Aijaz M., Nazir M. Modelling and analysis of social engineering threats using the attack tree and the Markov model. *International Journal of Information Technology*. 2024. № 16. P. 1231-1238.
6. Fakhouri H.N., Alhadidi B., Omar K., Makhadmeh S.N., Hamad F., Halalsheh N.Z. AI-driven solutions for social engineering attacks: detection, prevention, and response. *2024 2nd International Conference on Cyber Resilience (ICCR).* Dubai, United Arab Emirates. 2024. P. 1-8.
7. Wang Z., Sun L., Zhu H. Defining Social Engineering in Cybersecurity. *IEEE Access*. 2020. Vol. 8, P. 85094-85115.
8. Hadnagy C. Social engineering. The science of human hacking. Indiana: John Wiley & Sons, Inc. 2018.
9. Siponen M., Vance A. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*. 2010. Vol. 34, № 3. P. 487-502.
10. Russia's Cyber Tactics: Lessons Learned 2022 – аналітичний звіт Держспецзв'язку про рік повномасштабної кібервійни росії проти України. *ДССЗЗІ України*.

References

1. Albladi S., Weir G. Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*. 2020. № 3. 7.
2. Ye Z., Guo Y., Ju A., Wei F., Zhang R., Ma J. A risk analysis framework for social engineering attack based on user profiling. *Journal of Organizational and End User Computing.* 2020. Vol. 32, № 3. P. 37-49.
3. Huseynov F., Ozdenizci Kose B. Using machine learning algorithms to predict individuals' tendency to be victim of social engineering attacks. *Information Development.* 2024. Vol. 40, № 2. P. 298-318.
4. Bohonko O., Lysenko S. Methods of detecting social engineering cyberattacks. *Herald of Khmelnytskyi National University. Technical sciences.* 2023. Vol. 327, № 5(2). P. 231-236.
5. Aijaz M., Nazir M. Modelling and analysis of social engineering threats using the attack tree and the Markov model. *International Journal of Information Technology*. 2024. № 16. P. 1231-1238.
6. Fakhouri H.N., Alhadidi B., Omar K., Makhadmeh S.N., Hamad F., Halalsheh N.Z. AI-driven solutions for social engineering attacks: detection, prevention, and response. *2024 2nd International Conference on Cyber Resilience (ICCR).* Dubai, United Arab Emirates. 2024. P. 1-8.
7. Wang Z., Sun L., Zhu H. Defining Social Engineering in Cybersecurity. *IEEE Access*. 2020. Vol. 8, P. 85094-85115.
8. Hadnagy C. Social engineering. The science of human hacking. Indiana: John Wiley & Sons, Inc. 2018.
9. Siponen M., Vance A. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*. 2010. Vol. 34, № 3. P. 487-502.
10. Russia's Cyber Tactics: Lessons Learned 2022 – an analytical report of the SSSCIP on the year of russia's full-scale cyberwar against Ukraine. *SSSCIP*.