УДК 316.776:004.58

Сучасні методи та техніки захисту від атак соціальної інженерії

Тетяна Крижанівська[0009-0002-8036-9539]
Наталія Коршун[0000-0003-2908-970X]

Київський столичний університет імені Бориса Грінченка, Україна

Анотація. У роботі досліджено сучасні методи захисту від атак соціальної інженерії, які спрямовані на маніпулювання людським фактором у кіберпросторі. Проаналізовано основні типи атак, такі як фішинг, вішинг, смішинг, бейтінг, прітекстинг та інсайдерські загрози, визначено їх характеристики та психологічні механізми впливу. Розглянуто комплексні підходи до протидії атакам, що включають освітні заходи, технічні інструменти (багатофакторна автентифікація, фільтрація пошти, моніторинг поведінки користувачів) та використання новітніх технологій, зокрема Big Data.
Ключові слова: соціальна інженерія, кібербезпека, фішинг, інформаційна безпека, людський фактор.

Modern Methods and Techniques of Protection Against Social Engineering Attacks

Tetiana Kryzhanivska[0009-0002-8036-9539]
Nataliia Korshun[0000-0003-2908-970X]

Borys Grinchenko Kyiv Metropolitan University, Ukraine

Abstract. The paper explores modern methods of protection against social engineering attacks aimed at manipulating the human factor in cyberspace. The main types of attacks, such as phishing, vishing, smishing, baiting, pretexting and insider threats, are analyzed, their characteristics and psychological mechanisms of influence are determined. Comprehensive approaches to countering attacks are considered, including educational measures, technical tools (multi-factor authentication, email filtering, user behavior monitoring) and the use of the latest technologies, in particular Big Data.
Keywords: social engineering, cybersecurity, phishing, information security, human factor.

Вступ

Актуальність теми обумовлена тим, соціальна інженерія є однією з новітніх загроз у сучасному кіберпросторі, оскільки спрямована на маніпуляцію людьми. Соціальна інженерія на сьогодні це поширена методика отримання доступу до конфіденційної інформації шляхом маніпуляцій та обману, спрямованих на людей, що полягає у використанні психологічних вразливостей особисті, довірливості, страху, прагнення до швидкого вирішення проблеми чи отримання вигоди. Саме тому атаки соціальної інженерії вважаються одними з найбільш небезпечних та дієвих у сучасному кіберпросторі. Відповідно зростання кількості таких атак пояснюється легкістю впливу на психологічні вразливості людини. Відповідно в умовах глобальної цифровізації

питання розробки та впровадження сучасних методів протидії соціальній інженерії набуває особливої ваги.

Наукова новизна полягає в комплексному аналізі сучасних методів протидії соціально-інженерним атакам, зокрема із залученням новітніх технологій (Big Data, штучний інтелект, чат-боти), що дозволяє забезпечити технічний захист.

Метою роботи є дослідження сучасних методів та технік захисту від атак соціальної інженерії.

Об'єктом дослідження виступає процес здійснення атак соціальної інженерії в інформаційному середовищі.

Предмет дослідження – методи та техніки захисту від соціально-інженерних атак у контексті кібербезпеки організацій.

Завдання дослідження:

1. Проаналізувати сутність і класифікацію основних видів атак соціальної інженерії.
2. Дослідити традиційні методи протидії соціально-інженерним загрозам.
3. Розглянути сучасні технології та інноваційні підходи.
4. Визначити роль освітніх заходів та культури інформаційної безпеки у протидії атакам.
5. Сформулювати рекомендації щодо комплексного захисту від соціальної інженерії.

Методи та моделі

Під час написання даної роботи ми спиралися на дослідження ряду науковців, зокрема: Є. Каплун, В. Соколов, Д. Курбанмурадов, С. Шевченко, Ю. Жданова, П. Складаний, С. Бойко. Основою дослідження стали напрацювання Л. Половенко та С. Мерінова, які проаналізували виявлення ознак соціальної інженерії та технології протидії соціальним хакерам. Крім того, велике значення мали дослідження Ю. Якименко, Д. Рабчун та М. Запорожченка, які визначили місце соціальної інженерії в проблемі витоку даних та організаційні аспекти захисту корпоративного середовища від фішингових атак з використанням електронної пошти.

Результати

Соціальна інженерія на сьогодні відіграє важливу роль для кожного з нас. Через її розвиток за інтеграцію, класифікація атак соціальної інженерії проводиться за: особливостями впливу, формою реалізації, цілями й середовищем, у якому вони відбуваються. Серед найпоширеніших типів таких атак є:

– смішинг, який відбувається через надсилання фальшивих електронних листів або повідомлень. При цьому зловмисники маскуються під надійні джерела, щоб змусити користувача розкрити конфіденційну інформацію або завантажити шкідливе ПЗ;

– вішинг, при якому атака через телефон, коли зловмисник видає себе за працівника банку чи іншої організації та намагається отримати персональні дані;

– смішинг, де відбувається використання SMS з посиланнями на шкідливі ресурси;

– бейтинг, для якого є характерним використання фізичних або онлайн-приманок для отримання доступу до системи жертви;

– прітекстинг, за якого зловмисник вигадує ситуацію, щоб завоювати довіру жертви і перспективі отримати конфіденційну інформацію або спонукати до певних дій [1].

Захист від соціально-інженерних атак є багаторівневим процесом, що потребує поєднання різних методів і засобів для зменшення ризиків, підвищення стійкості

інформаційних систем. Оскільки основною мішенню таких атак є людина, ефективна протидія має охоплювати не лише технічні інструменти, але й освітні заходи.

Ключову роль у протидії атакам відіграє навчання персоналу та формування культури безпечної поведінки. Відповідно працівники організацій повинні бути ознайомлені з найпоширенішими видами соціальної інженерії та мати навички розпізнавання потенційних загроз. Регулярні заняття й тренінги з кібергігієни допоможуть підвищити уважність співробітників, зменшити ймовірність розголошення конфіденційних відомостей невідомим особам або відкриття шкідливих посилань. Крім того, імітаційні перевірки, зокрема тестові фішингові розсилки, дозволяють оцінити рівень підготовки колективу та виявити найбільш вразливі місця.

Відповідно важливим стає впровадження внутрішніх політик інформаційної безпеки, що мають чітко визначати правила роботи з конфіденційними даними, порядок створення і зберігання паролів, а також алгоритми дій у разі отримання підозрілих запитів.

Технічні засоби захисту є невід'ємною складовою комплексної безпеки. Зокрема, впровадження багатофакторної автентифікації значно ускладнює несанкціонований доступ до систем, навіть якщо пароль став відомим зловмиснику. Вона передбачає підтвердження особи за допомогою кількох незалежних факторів, наприклад, комбінації пароля, біометричних даних (відбиток пальця) або одноразового коду, надісланого на мобільний пристрій. Такий підхід суттєво зменшує ймовірність успішної атаки, навіть коли користувач піддається обману.

Інформаційні системи повинні бути оснащені сучасними інструментами для фільтрації електронної пошти, які дозволяють виявляти та блокувати фішингові листи. Такі фільтри аналізують вміст повідомлень і виявляють характерні ознаки шахрайства, наприклад, спроби видаватися за відомі організації або службові особи [2].

Не менш важливим елементом захисту є контроль доступу до фізичних об'єктів, таких як робочі місця, серверні приміщення та архіви. Тому використання електронних пропусків і систем відеоспостереження дозволяє ефективно відстежувати переміщення співробітників в офісі, що зменшує ризик витоку інформації. Також важливим аспектом є формування в організації культури інформаційної безпеки, що передбачає регулярне інформування працівників про значення захисту даних та впровадження механізмів, що заохочують дотримання правил безпеки [3].

Сучасні технології стрімко змінюють сферу інформаційної безпеки, тому методи соціальної інженерії постійно еволюціонують. Крім того, зловмисники впроваджують нові інструменти та підходи, зокрема автоматизацію та штучний інтелект, що ускладнює їхнє своєчасне виявлення та блокування. У відповідь на це організації повинні залишатися гнучкими та оперативно адаптувати свої системи захисту до нових загроз.

Одним із перспективних методів протидії соціальній інженерії є аналіз великих обсягів даних з метою виявлення аномалій у поведінці користувачів.

Використання технологій Big Data дозволяє відстежувати типові поведінкові патерни та своєчасно ідентифікувати підозрілу активність, яка може свідчити про спробу атаки. Наприклад, якщо працівник несподівано намагається отримати доступ до конфіденційної інформації, яка не входить до його посадових обов'язків, це може сигналізувати про потенційну загрозу. Крім того, віртуальні помічники та чат-боти на базі штучного інтелекту можуть надавати оперативні консультації користувачам при підозрілих запитах, що допомагає визначити автентичність запиту та рекомендує відповідні дії для захисту інформації. Це особливо ефективно для великих організацій, де велика кількість внутрішніх взаємодій робить традиційні методи контролю менш ефективними [4].

Ефективний захист від соціальної інженерії також передбачає використання сучасних технологій шифрування для збереження конфіденційності даних навіть у разі їх потрапляння до зловмисників, адже протоколи шифрування суттєво ускладнюють подальше використання компрометованої інформації. Водночас працівники повинні знати і дотримуватися правил безпечного зберігання та передачі зашифрованих даних, аби уникати помилок і випадкових витоків інформції.

Додатковим елементом захисту є регулярний аудит інформаційної безпеки, що дозволяє своєчасно виявляти вразливості та оцінювати ефективність існуючих заходів. Оскільки соціально-інженерні атаки ґрунтуються на психологічному тиску, створюючи у жертв відчуття страху, терміновості чи провини, необхідно навчати персонал розпізнавати такі маніпуляції, зберігати спокій і за потреби звертатися до спеціалістів з кібербезпеки [5].

Окремим типом фішингових атак є spear-phishing, що націлені на конкретних осіб або організації з метою отримання критично важливої інформації. Ці атаки ґрунтуються на детальному знанні цільової групи та часто використовують внутрішню інформацію компанії для підвищення правдоподібності обману. Через необхідність значної підготовки такі атаки вважаються особливо небезпечними.

Для захисту від соціально-інженерних атак користувачі повинні бути обережними з будь-якими несподіваними електронними повідомленнями. Тому включення прикладів фішингових атак у навчальні програми персоналу допомагає працівникам розпізнавати шахрайство.

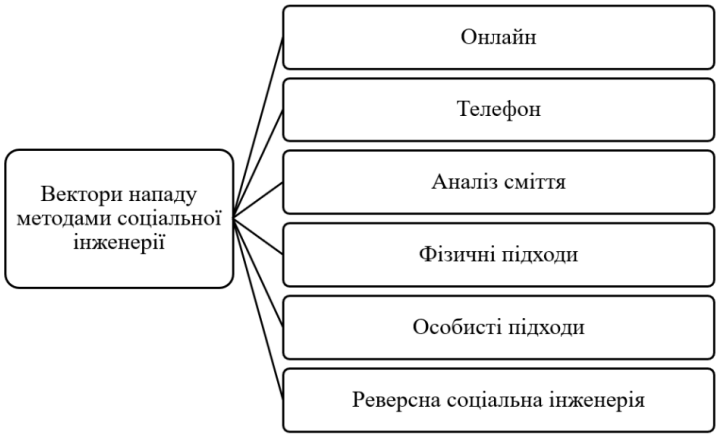

Рис. 1. Вектори нападу при проведенні атак методами соціальної інженерії [1]

Одним із поширених методів маніпуляції є використання спливаючих вікон та діалогових повідомлень на робочому столі. Ефективний захист у даному випадку ґрунтується на підвищенні обізнаності працівників, які мають уникати переходу за підозрілими посиланнями без перевірки у службі підтримки, а також на забезпеченні компанією чітких правил безпечної роботи в мережі та необхідної допомоги.

Телефонний зв’язок також може використовуватися зловмисниками. Анонімність дзвінків дозволяє нападникам видаватися співробітниками компанії та запитувати доступ до систем або конфіденційну інформацію. У разі сумніву жертва може відмовитися або завершити дзвінок, що робить такі атаки відносно безпечними для зловмисника [6, 7].

Захист аналітиків служби підтримки від внутрішніх загроз є складним завданням, оскільки зловмисники-інсайдери добре орієнтуються в корпоративних процесах і можуть використовувати власні знання для створення підроблених запитів з метою отримання інформації. Для зменшення ризиків важливо забезпечити аудит усіх дій співробітників служби підтримки, що дає змогу контролювати їхні операції та своєчасно

виявляти потенційні загрози, а також розробити чіткі процедури обробки користувацьких звернень, які мінімізують можливості маніпуляцій. Дотримання правил та підтримка від керівництва, значно ускладнює дії зловмисників, а ведення журналів подій допомагає як у запобіганні інцидентам, так і в їх розслідуванні [8, 9].

Окремим фактором ризику виступають неналежно утилізовані електронні носії, адже жорсткі диски чи інші пристрої без очищення або знищення можуть містити конфіденційні дані.

Метод особистого отримання інформації залишається одним із найпростіших і найменш затратних для зловмисників, адже існує низка психологічних стратегій та маніпулятивних дій, які допомагають їм завоювати довіру або примусити жертву розкрити потрібні дані. Наприклад, залякування створює тиск і страх, протидія якому полягає у формуванні в організації культури безпеки, коли працівники не бояться помилок і знають, як реагувати на подібні ситуації. Якщо зловмисник потрапляє в штат компанії, знизити ризики допомагає неухильне дотримання політик безпеки всіма співробітниками і відповідальне ставлення до правил. Баланс між захистом і ефективністю роботи служби підтримки досягається через чітко прописані процедури, які дозволяють виконувати обов'язки без шкоди для безпеки, а також регулярні аудити дій та структуровану обробку запитів, що ускладнює використання внутрішніх знань проти компанії.

Обговорення

Отримані результати підтверджують актуальність проблеми соціальної інженерії як одного з головних векторів кібератак у сучасному інформаційному просторі. Дослідження підтвердило, що сучасна протидія атакам соціальної інженерії повинна бути комплексною та багаторівневою. Вона включає як технічні інструменти (багатофакторна автентифікація, фільтри, системи шифрування, моніторинг та аудит інформаційних процесів), так і організаційні та освітні заходи (формування культури інформаційної безпеки, регулярні тренінги, перевірки, розробка внутрішніх політик та процедур реагування). Особливої ваги набуває розвиток навичок персоналу у розпізнаванні маніпуляцій і здатності зберігати критичне мислення у стресових ситуаціях.

Варто зазначити, що проаналізовані методи захисту не завжди можуть бути однаково ефективними в різних організаціях, оскільки рівень кіберкультури, технічної інфраструктури та фінансових можливостей суттєво відрізняється залежно від компанії чи організації. Крім того, швидкий розвиток технологій зумовлює постійну зміну тактик зловмисників, що потребує регулярного оновлення знань і практик захисту.

Висновки

Соціальна інженерія є однією з ключових кіберзагроз сучасності через орієнтацію на людський фактор. Основні види атак, такі як фішинг, вішинг, смішинг, бейтінг, прітекстинг та інсайдерські загрози, демонструють високу ефективність завдяки використанню психологічних уразливостей користувачів. Виявлено, що найуспішніші стратегії захисту ґрунтуються на комплексному підході, що поєднує технічні, організаційні та освітні заходи.

Аналіз методів протидії показав, що навчання персоналу та формування культури інформаційної безпеки є критично важливими компонентами стратегії захисту, а використання сучасних технологій таких як: багатофакторної автентифікації, систем

моніторингу, Big Data та штучного інтелекту, значно підвищує ефективність захисту навіть у випадках складних цільових атак.

Тому успішна боротьба із соціальною інженерією можлива лише за умови інтеграції технічних, організаційних, освітніх і психологічних методів захисту. Такий комплексний підхід дозволяє не лише мінімізувати ризики витоку даних чи компрометації систем, але й формує в організаціях культуру кіберстійкості, що є ключовим чинником у формуванні та підтримці безпеки в умовах цифрової трансформації суспільства.

Джерела

1. Каплун, Є. В. (2024). Інформаційна технологія захисту від атак соціальної інженерії на основі великих мовних моделей: Робота на здобуття кваліфікаційного ступеня магістра: спец. 122 – комп'ютерні науки / наук. кер. В. В. Москаленко. Суми : Сумський державний університет. https://essuir.sumdu.edu.ua/handle/123456789/97749

2. Sokolov, V. Y., & Kurbanmuradov, D. M. (2018). Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності. Кібербезпека: освіта, наука, техніка, 1(1), 6–16. https://doi.org/10.28925/2663-4023.2018.1.616

3. Shevchenko, S., Zhdanova Y., Skladannyi, P., & Boiko, S. (2022). Інсайдери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність. Кібербезпека: освіта, наука, техніка, 3(15), 175–185. https://doi.org/10.28925/2663-4023.2022.15.175185

4. Дмитрієнко, К., & Коршун, Н. (2025). Застосування вдосконалених моделей курамото для ідентифікації дезінформації у соціальних мережах. Кібербезпека: освіта, наука, техніка, 3(27), 406–416. https://doi.org/10.28925/2663-4023.2025.27.754

5. Половенко, Л. П. & Мерінова, С. В. (2019). Виявлення ознак соціальної інженерії та технологія протидії соціальним хакерам на підприємстві. Підприємство та інновації, 9, 183–187. https://doi.org/10.37320/2415-3583/10.28

6. Савченко, В. А. (2024). Дослідження потенційного впливу соціальної інженерії на процеси цифрової трансформації. Зв'язок, 3, 12–17. https://doi.org/10.31673/2412-9070.2024.031217

7. Жмурко, О. (2024). Соціальна інженерія як загроза кібербезпеці: методи запобігання та захисту. ПедБез, 9(1), 37–42. https://doi.org/10.31649/2524-1079-2024-9-1-037-042

8. Yakymenko, Y., Rabchun, D., & Zaporozhchenko, M. (2021). Місце соціальної інженерії в проблемі витоку даних та організаційні аспекти захисту корпоративного середовища від фішингових атак з використанням електронної пошти. Кібербезпека: освіта, наука, техніка, 1(13), 6–15. https://doi.org/10.28925/2663-4023.2021.13.615

9. Козицька, О. (2021). Використання методу соціальної інженерії в процесі виявлення, розкриття та розслідування кримінальних правопорушень. Юридична психологія, 28(1), 34–40. https://doi.org/10.33270/03212801.34