МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ
(зимовий форум)

Одеса, Україна, 14 листопада 2025 р.

Одеса
2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
INTERNATIONAL UNIVERSITY

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025)

Odesa, Ukraine, November 14, 2025

Conference Proceedings
(winter forum)

Odesa
2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ УНІВЕРСИТЕТ

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ПТІКІ'2025)

Одеса, Україна, 14 листопада 2025 р.

Матеріали конференції
(зимовий форум)

Одеса
2025

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025): Conference Proceedings (winter forum). Odesa : International university, 2025, 101 p.

DOI:

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2025): Матеріали конференції (зимовий форум). Одеса : Міжнародний університет, 2025, 101 с.

Збірка містить праці Міжнародної конференції з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

СЕКЦІЇ

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 2. КОМП'ЮТЕРНІ НАУКИ ТА КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

МІРОШНИК М.А. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
РУСУ О.П. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

ЛУНТОВСЬКИЙ А.О. – д.т.н., проф., Державна академія Саксонії «Беруфсакадемія», м. Дрезден, Німеччина.
ЙОНА Л.Г. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ЛЕМЕШКО А.В. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.
ПЕДЯШ В.В. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

КУЧАЙ О.В. - д.п.н., проф., Національний університет біоресурсів і природокористування України.
ЖИГУЛІН О.А. – д.е.н., проф., Міжнародний університет, Одеса, Україна
ГОРБАЧОВ В.Е. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

References:

1. Онацький О. В., Йона Л. Г. Белова Ю. В. Криптографічний захист інформації: навчальний посібник з дисципліни «Криптографічний захист інформації». Держ. ун-т інтелект. технологій і зв'язку. – Одеса: Астропринт, 2023. 252 с.

2. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика: монографія. – Харків: Видавництво «Форт», 2012. 880 с.

3. Paillier P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes // Int. Conf. Theory Appl. Cryptograph. Techn. Adv. Cryptol. (EUROCRYPT), Prague. Czech Republic, May 1999, Pp. 223-238.

4. The Paillier's Cryptosystem and Some Variants. [Electronic resource] – Mode of access: https://scispace.com/pdf/the-paillier-s-cryptosystem-and-some-variants-revisited-186lebbhcg.pdf

Ковальчук Д. А.
здобувач вищої освіти третього (освітньо-наукового рівня)
спеціальності 125 Кібербезпека
denys.kovalchuk1@gmail.com
Науковий керівник: Йона Л. Г.
Кандидат технічних наук,
Доцент кафедри Комп'ютерної інженерії та інноваційних технологій
Міжнародного університету м. Одеса, Україна

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК СКЛАДОВА ГІБРИДНИХ КІБЕРОПЕРАЦІЙ: СУЧАСНІ ТЕНДЕНЦІЇ ТА ВИКЛИКИ БЕЗПЕКИ

***Анотація**. У тезах розглянуто соціальну інженерію як один із ключових інструментів гібридних кібероперацій, що поєднує технічні та психологічні засоби впливу. Проаналізовано сучасні тенденції розвитку соціально-інженерних методів, їх роль у дестабілізації інформаційного простору та підриві довіри до цифрових систем. Визначено основні канали поширення таких атак, а також виклики, що постають перед системами кібербезпеки держави, бізнесу та суспільства. Запропоновано напрями підвищення рівня кіберстійкості та соціальної відповідальності користувачів.*

Вступ

Сучасні гібридні конфлікти характеризуються поєднанням традиційних та кіберінструментів впливу, серед яких соціальна інженерія посідає особливе місце. На відміну від класичних технічних атак, соціально-інженерні операції спрямовані на маніпулювання людською поведінкою, емоціями та когнітивними особливостями. Це робить їх надзвичайно ефективними, адже навіть найзахищеніші інформаційні системи залишаються вразливими через «людський фактор».

В умовах війни, яку веде Російська Федерація проти України, соціальна інженерія використовується не лише для викрадення даних чи фінансових ресурсів, але й як засіб інформаційно-психологічного тиску на населення, деморалізації та дезінформації. З огляду на це, дослідження соціальної інженерії як складової гібридних кібероперацій набуває стратегічного значення для національної безпеки.

Метою роботи є аналіз сучасних тенденцій розвитку соціально-інженерних методів у контексті гібридних кібероперацій та визначення ефективних стратегій протидії таким загрозам.

Сутність соціальної інженерії у контексті гібридних атак

Соціальна інженерія — це сукупність методів психологічного впливу, спрямованих на отримання конфіденційної інформації або спонукання користувача до певних дій, які порушують політику безпеки системи. У гібридних кіберопераціях вона виступає мостом між технічними засобами злому та інформаційно-психологічними кампаніями.

Типовими прикладами є фішинг, спір-фішинг, вішинг, смішинг, використання deepfake-технологій, а також поширення дезінформації у соціальних мережах. Такі атаки часто мають на меті не лише отримання доступу до систем, а й формування певних наративів або створення недовіри до офіційних джерел.

Інструменти та канали реалізації соціально-інженерних впливів

Соціальні платформи, електронна пошта та месенджери є основними каналами поширення соціально-інженерних атак. В умовах глобальної цифровізації користувачі щодня отримують сотні інформаційних повідомлень, що створює ідеальні умови для маніпуляцій.

Атакувальники активно застосовують методи OSINT (розвідка відкритих джерел) для збору персональних даних, які потім використовують для індивідуалізації атак. Широке використання генеративного штучного інтелекту, зокрема для створення фейкових зображень, аудіо та текстів, суттєво підвищує рівень достовірності таких впливів.

Виклики для системи кібербезпеки

Основною проблемою протидії соціальній інженерії є складність виявлення атак, що не містять безпосередніх технічних ознак злому. Більшість інцидентів відбувається через помилки користувачів, які піддаються психологічному тиску або довіряють неправдивій інформації.

Для держави та організацій це означає потребу у зміні підходів до кіберзахисту: від технічної до комплексної соціотехнічної моделі безпеки, що враховує людський чинник. Значну роль відіграють навчальні програми з кіберграмотності, тестування персоналу на стійкість до фішингу та розвиток культури кібербезпеки.

Шляхи протидії соціально-інженерним загрозам

Протидія соціальній інженерії потребує синергії технологічних і поведінкових стратегій. До ефективних напрямів належать:

- впровадження програм постійного навчання працівників із моделюванням реальних сценаріїв атак;
- моніторинг і аналіз поведінкових аномалій користувачів у корпоративних мережах;
- використання систем штучного інтелекту для виявлення фішингових повідомлень і deepfake-контенту;
- розвиток державних інформаційних кампаній з підвищення обізнаності населення щодо кіберзагроз.

Важливо, щоб кіберзахист розглядався не лише як технічне завдання, а як соціальний процес, що охоплює освіту, етику, психологію та комунікацію.

Висновки

Соціальна інженерія є однією з ключових складових сучасних гібридних кібероперацій, оскільки дозволяє зловмисникам впливати на свідомість і поведінку людей, обходячи технічні засоби захисту. Її особливість полягає у використанні психологічних прийомів, емоційного тиску, дезінформації та маніпуляцій довірою, що робить людину найслабшою ланкою у системі кібербезпеки.

У контексті повномасштабної війни, розв’язаної Російською Федерацією проти України, соціальна інженерія стала одним із головних інструментів інформаційного та

кібернетичного впливу. Російські кіберактивності часто поєднують класичні технічні атаки (злами, DDoS, крадіжки даних) із кампаніями психологічного тиску, спрямованими на деморалізацію населення, поширення панічних настроїв та підрив довіри до державних інституцій.

Приклади таких дій включають фішингові розсилки, що імітують офіційні повідомлення державних органів, створення фейкових сторінок благодійних фондів, а також масштабні кампанії з дезінформації в соціальних мережах, спрямовані на спотворення сприйняття подій на фронті.

Досвід України демонструє, що протидія соціально-інженерним загрозам має не лише технічний, а й національно-безпековий характер. Формування культури кіберграмотності серед громадян, підвищення обізнаності про механізми інформаційного впливу та розвиток державних комунікаційних стратегій є необхідними умовами кіберстійкості країни.

Комплексна система протидії соціальній інженерії повинна поєднувати технологічні, психологічні, освітні та правові інструменти. Зокрема, ефективною є інтеграція штучного інтелекту для виявлення маніпуляцій, проведення тренінгів для державних службовців і критичної інфраструктури, а також співпраця між державними органами, науковими установами та громадським сектором у сфері інформаційної безпеки.

Отже, соціальна інженерія у гібридних кібероперaціях є не лише технічною проблемою, а складним соціально-психологічним викликом, що загрожує національній безпеці. Подальші дослідження мають бути спрямовані на розробку моделей оцінювання ризиків соціально-інженерних атак у контексті воєнного протистояння, формування ефективних стратегій кіберосвіти та створення адаптивних систем захисту, здатних враховувати людський чинник у цифровому середовищі.

Література

1. Sarker H. I. AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability. 2024.

2. Gray J. Practical Social Engineering: A Primer for the Ethical Hacker. 2022.

3. Hamid Jahankhani, Babak Akhgar, Peter Cochrane, Mohammad Dastbaz “Policing in the Era of AI and Smart Societies”.

4. Cyble. (2024). Ukraine's Cyberthreat Landscape 2024. URL: https://cyble.com/blog/ukraine-cyberthreat-landscape-2024/.

5. European Parliament. (2025). Cybersecurity: main and emerging threats. URL: https://www.europarl.europa.eu/topics/en/article/20220120STO21428/cybersecurity-main-and-emerging-threats.