УДК 004.7

ЗАХИСТ КОМПЮТЕРНИХ МЕРЕЖ ВІД АТАК МЕТОДОМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ У ВОЄННИЙ ЧАС

Ромашук Роман
здобувач першого (бакалаврського) рівня вищої освіти,
Приватного вищого навчального закладу
«Міжнародний економіко-гуманітарний університет
імені академіка Степана Дем'янчука» (м. Рівне, Україна)

Науковий керівник **Лотюк Ю. Г.,**
кандидат педагогічних наук, завідувач кафедри
інформаційних систем та обчислювальних методів
Приватного вищого навчального закладу
«Міжнародний економіко-гуманітарний університет
імені академіка Степана Дем'янчука» (м. Рівне, Україна)

Анотація. *У статті розглянуто загрози інформаційної безпеки, що виникають у воєнний час, зокрема – атаки методом соціальної інженерії. Аналізуються типові методи впливу на користувачів, такі як фішинг, психологічний тиск, маніпуляція довірою, deepfake-технології та використання фальшивих мобільних застосунків. Значна увага приділена практичним прикладам використання соціальної інженерії під час російсько-української війни, зокрема атакам на військових, волонтерів і державні структури. Визначено основні напрями захисту від зазначених загроз, що включають як технічні, так і освітні заходи. Стаття підкреслює необхідність комплексного підходу до забезпечення кібербезпеки в умовах інформаційної війни.*

Ключові слова: *інформаційна безпека, соціальна інженерія, фішинг, кіберзагрози, інформаційна війна, комп'ютерні мережі, кіберзахист.*

Abstract. *The article examines the threats to information security that emerge during wartime, particularly those involving social engineering attacks. It analyzes common techniques used to influence users, including phishing, psychological pressure, trust manipulation, deepfake technologies, and the deployment of fake mobile applications. Considerable attention is devoted to practical examples of social engineering employed during the Russian-Ukrainian war, especially attacks targeting military personnel, volunteers, and government institutions. The study identifies the main directions for countering these threats, encompassing both technical and educational measures. The article emphasizes the necessity of a comprehensive approach to cybersecurity in the context of information warfare.*

Keywords: *information security, social engineering, phishing, cyber threats, information warfare, computer networks, cyber defense.*

Інформаційна безпека – це комплекс заходів, спрямованих на захист інформації від несанкціонованого доступу, модифікації, розголошення або знищення. В умовах війни цей аспект набуває особливого значення, оскільки інформаційні ресурси стають ключовими об'єктами атак.

Інформаційна безпека базується на трьох основних принципах:

− Конфіденційність – гарантує, що інформація доступна лише тим особам, які мають відповідні права доступу.

− Цілісність – забезпечує незмінність та достовірність даних, запобігаючи їх випадковому чи навмисному спотворенню.

− Доступність – означає, що інформація повинна бути доступною для авторизованих користувачів у потрібний момент.

Під час війни інформація стає не лише стратегічним ресурсом, але й об’єктом цілеспрямованих атак з боку супротивника, що може призвести до дестабілізації ситуації в державі, порушення координації військових дій, економічних збитків та паніки серед населення.

Під час військових конфліктів інформаційна безпека охоплює:

− Захист державних інформаційних систем.

− Безпеку військових комунікацій.

− Захист критичної інфраструктури (банків, енергомереж, медичних установ).

− Контроль за розповсюдженням чутливої інформації серед цивільного населення.

Захист інформації у воєнний час стикається з рядом критичних загроз, які можуть впливати на державні установи, військові структури та цивільну інфраструктуру. Розглянемо основні види атак, їхні методи та потенційні наслідки:

− DDoS-атаки DDoS (Distributed Denial of Service) – це масовані атаки на сервери, які спрямовані на перевантаження мережевого каналу або ресурсів обробки даних;

− Перехоплення трафіку (Man-in-the-Middle, MITM) цей тип атак дозволяє зловмисникам вставлятися між користувачем і сервером для прослуховування або зміни переданих даних;

− Злами мережевих пристроїв. Хакери використовують вразливості в маршрутизаторах, комутаторах та серверах для отримання доступу до критичних систем.

− Впровадження бекдорів та руткітів. Ці шкідливі програми дозволяють зловмисникам отримати прихований доступ до системи та контролювати її без відома користувачів.

− Фізичні атаки на мережеву інфраструктуру. Знищення фізичних компонентів інфраструктури – це один із найефективніших методів дестабілізації роботи зв'язку.

− Соціальна інженерія. Це форма шахрайства, при якій зловмисник використовує довіру, обман або дезінформацію, щоб змусити людину добровільно розкрити важливі дані або виконати небезпечні дії.

Соціальна інженерія – це метод психологічного впливу на людей з метою отримання конфіденційної інформації, несанкціонованого доступу до ресурсів або маніпуляції поведінкою жертви. Це одна з найбільш небезпечних загроз інформаційній безпеці, оскільки вона використовує не технічні вразливості, а людський фактор. Військові конфлікти лише посилюють роль соціальної інженерії, оскільки ворожі сторони прагнуть отримати стратегічну інформацію, дестабілізувати суспільство або посіяти паніку серед цивільного населення.

Основні механізми соціальної інженерії:

− Використання довіри – зловмисники прикидаються авторитетними особами (співробітниками банку, державними службовцями, військовими) для отримання інформації.

− Терміновість та тиск – створення ситуації, коли жертва повинна швидко реагувати, не маючи часу для аналізу (наприклад, "Ваша картка заблокована! Негайно введіть код для розблокування!").

− Емоційний вплив – маніпуляція страхом, співчуттям або відчуттям обов’язку.

− Стимулювання цікавості – використання привабливих підроблених лінків, файлів або USB-носіїв, які жертва відкриває через цікавість.

− Соціальний доказ – переконання жертви діяти, оскільки "багато інших так роблять" (наприклад, фальшиві відгуки чи маніпулятивні коментарі).

Фішинг – це один із найпоширеніших методів атак у соціальній інженерії, що передбачає обман жертви шляхом надсилання підроблених електронних листів, повідомлень або створення фальшивих веб-сайтів.

Основні види фішингу:

− Email-фішинг – масові розсилки електронних листів, що імітують офіційні установи (банки, держоргани, соціальні мережі).

− Spear Phishing – цілеспрямовані атаки на конкретних осіб або організації.

− Smishing (SMS-фішинг) – атаки через підроблені повідомлення у месенджерах або SMS.

− Vishing (Voice Phishing) – телефонні дзвінки від шахраїв, що видають себе за техпідтримку або банківських співробітників.

Фішингові атаки особливо небезпечні у військовий час, коли хакери можуть маскуватися під урядові організації або військові структури, змушуючи людей передавати конфіденційну інформацію.

Маніпуляції та використання довіри. Зловмисники використовують психологічні методи, щоб змусити жертву довіряти їм:

− Імітація авторитетних осіб – зловмисники видають себе за військових, посадовців або співробітників спецслужб.

− Фальшиві накази та розпорядження – створення підроблених документів, що нібито містять важливі інструкції.

− Використання соціальних зв'язків – атаки через друзів або родичів, наприклад, прохання про допомогу від імені знайомих у соціальних мережах.

Використання технологій у соціальній інженерії

− Deepfake – підроблені відео та аудіозаписи, які можуть імітувати голос або зовнішність людини.

− Масові атаки через соцмережі – використання фальшивих акаунтів для поширення паніки або дезінформації.

− Підроблені мобільні додатки – заражене програмне забезпечення, що краде дані користувачів

Приклади використання соціальної інженерії у військових конфліктах

− Фейкові накази та повідомлення – підроблені документи від імені військових командирів.

− Атаки на військових через соцмережі – виманювання місцезнаходження військових через підставні акаунти в соцмережах.

− Розсилка дезінформації через месенджери – створення паніки серед населення через фальшиві повідомлення.

− Підставні благодійні фонди – фейкові збори коштів для нібито допомоги військовим чи постраждалим.

Приклад 1: Кібератаки на Україну

У 2022 році група APT28 (пов'язана з російською розвідкою) проводила масові фішингові кампанії, надсилаючи підроблені листи нібито від Міністерства оборони України, що містили шкідливі файли для крадіжки інформації. Це призводило до компрометації мереж та витоку критично важливих даних.

Приклад 2: Фейковий застосунок "eVorog"

У 2022 році українським військовим і волонтерам пропонували завантажити підроблений застосунок "eVorog", який нібито дозволяв повідомляти про ворожу техніку. Насправді він збирав геолокаційні дані та передавав їх російським спецслужбам. Це дозволяло ворогу відстежувати переміщення українських сил.

Приклад 3: Віруси у месенджерах

Російські хакери створювали заражені документи у форматі Word та PDF, які поширювали через месенджери серед військових. Відкривши файл, жертва активувала шкідливий код, який передавав хакерам вміст пристрою, включаючи паролі та розташування користувача.

Приклад 4: "Знайомство з дівчиною"

Ворог створює фейкові профілі молодих жінок у соціальних мережах, які нібито потребують допомоги або мають особистий інтерес до військових. Під час листування вони витягують важливу інформацію про позиції військ, озброєння, моральний стан бійців.

Приклад 5: Образливий коментар

У соціальних мережах (наприклад Instagram) жертва отримує провокаційний або образливий коментар під своїм постом. У шапці профілю є посилання, наприклад: “переходь в телеграм". Проте насправді людина потрапляє на фішинговий сайт.

Приклад 6: Підроблені програми для волонтерів

Створюється фейковий застосунок, що нібито полегшує передачу гуманітарної допомоги та розподіл ресурсів між волонтерами. Насправді він зчитує всі контакти користувача, повідомлення та відстежує його переміщення, передаючи цю інформацію ворогу.

Методи протидії соціальній інженерії

Освітні заходи та підвищення обізнаності

− Регулярні навчання для військових, співробітників державних установ та громадян щодо методів соціальної інженерії.

− Симуляційні тренінги з фішингу для підвищення пильності користувачів.

− Проведення інформаційних кампаній про типові методи шахрайства.

Технічні методи протидії соціальній інженерії

− Використання багатофакторної аутентифікації (MFA).

− Впровадження антифішингових фільтрів та захисту електронної пошти.

− Автоматизовані системи аналізу поведінки користувачів (UEBA – User and Entity Behavior Analytics).

Соціальна інженерія є однією з найбільш небезпечних форм інформаційних атак, оскільки вона експлуатує людський фактор – емоції, довіру та психологічну вразливість. Використання таких методів, як фішинг, маніпуляції, обман через діпфейки, дозволяє зловмисникам отримати доступ до конфіденційних даних, порушити функціонування критичних систем і вплинути на громадську думку.

В умовах війни соціальна інженерія набуває ще більшої загрози, оскільки вона використовується для інформаційної дестабілізації, деморалізації суспільства та впливу на хід бойових дій. Захист від таких

атак вимагає підвищеної обізнаності користувачів, ретельної перевірки інформації, впровадження багатофакторної аутентифікації та регулярного навчання щодо кібербезпеки. Лише комплексний підхід до інформаційної гігієни може знизити ризики соціальної інженерії та допомогти зберегти безпеку держави та громадян.

ЛІТЕРАТУРА

1.Ганченко М. І. Людський психологічний та біометричний фактор у розвитку та використанні методів соціальної інженерії у мирний та воєнний час. *Військово-науковий вісник*. 2022. № 37. С. 138–146. **2.** Active Social Engineering Defense (ASED). Defense Advanced Research Projects Agency. URL: https://www.darpa.mil/program/active-social-engineering-defense**. 3.** Копча І. І. Інформаційно-психологічна війна та технології соціального інжинірингу. *Інформаційне суспільство.* 2021. № 4(38). С. 48–55. URL: 10.52506/IS.2021.38.6. **4.** Кібербезпека бізнесу під час війни. *Бізнес і безпека*. 2023. № 2. С. 15–22. URL: https://cybersecurityhub.ua/articles/cyberwar2023. **5.** Avoiding Social Engineering and Phishing Attacks / *CISA Cybersecurity & Infrastructure Security Agency*. 2023. URL: https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks