DOI: https://doi.org/10.26565/2304-6201-2025-66-08

УДК (UDC) 004.056

Товкун Юлія Ігорівна
аспірантка кафедри Автоматизації та проектування обчислювальної техніки
Харківський національний університет радіоелектроніки
61166, проспект Науки, 14, Харків, Україна
e-mail: ytovkun@gmail.com
https://orcid.org/0009-0000-5916-2897

Методи кібершпіонажу та їх вплив на міжнародну безпеку

Актуальність дослідження обумовлена зростаючою роллю кібершпіонажу як засобу геополітичного впливу та інструменту для отримання конфіденційної інформації. У сучасних умовах цифровізації державні установи, міжнародні організації та корпоративні структури стають ключовими цілями кібератак, які створюють значні загрози для національної безпеки та глобальної стабільності.
Метою цієї статті є аналіз феномену кібершпіонажу, зокрема, його технічних, організаційних та соціальних аспектів, на основі реальних кейсів. У дослідженні акцентується увага на використанні сучасних методів атак, таких як таргетований фішинг, експлуатація вразливостей програмного забезпечення та впровадження модульного шкідливого програмного забезпечення. Стаття спрямована на визначення спільних характеристик кібершпіонажних кампаній і розробку рекомендацій для протидії таким загрозам.
Під час роботи використано теоретичний методологічний підхід, що поєднує аналіз літератури, кейс-аналіз атак (операція Red October, атака на Офіс управління персоналом США, кібератака на Міжнародний кримінальний суд, операція "Star Blizzard") та системний аналіз факторів, які сприяють успіху кібершпіонажних кампаній.
У результаті дослідження визначено ключові технічні методи атак, їхній вплив на інформаційну безпеку, а також роль людського фактора в успішності кібершпіонажу. Сформульовано рекомендації для посилення кіберзахисту, включаючи технічні, організаційні та міжнародні заходи.
Матеріали статті становлять інтерес для науковців, спеціалістів із кібербезпеки та державних структур, які займаються питаннями захисту інформації, та можуть бути використані для розробки політик протидії кібершпіонажу.

Ключові слова: *кіберзагрози, шпигунське програмне забезпечення, таргетований фішинг, інформаційна безпека, кібершпіонаж.*

Як цитувати: Товкун Ю. І. Методи кібершпіонажу та їх вплив на міжнародну безпеку. *Вісник Харківського національного університету імені В. Н. Каразіна, серія Математичне моделювання. Інформаційні технології. Автоматизовані системи управління*. 2025. вип. 66. С.81-89. https://doi.org/10.26565/2304-6201-2025-66-08

How to quote: Y. Tovkun, “Methods of cyber espionage and their impact on international security”, *Bulletin of V. N. Karazin Kharkiv National University, series Mathematical modelling. Information technology. Automated control systems*, vol. 64, pp. 81-89, 2025. https://doi.org/10.26565/2304-6201-2025-66-08

Вступ

Кібершпіонаж стає дедалі більшою загрозою у сучасному світі, де інформаційні технології відіграють ключову роль у функціонуванні державних установ, міжнародних організацій та бізнесу. Використовуючи уразливості цифрових систем, зловмисники отримують доступ до конфіденційної інформації, що може бути використана для геополітичних маніпуляцій, економічного шантажу чи підриву довіри до ключових міжнародних інституцій.

Сучасний стан дослідження кібершпіонажу підкреслює складність цієї загрози, яка поєднує технічні, організаційні та соціальні аспекти. За останні роки значна кількість досліджень була присвячена аналізу методів, які використовуються зловмисниками. Наприклад, Josh Fruhlinger (2020) вивчає правові аспекти кібершпіонажу, акцентуючи увагу на порушеннях міжнародного права, пов’язаних із втручанням у внутрішні справи держав. Brian Mitchell (2020) досліджує масштаби викрадення інтелектуальної власності через кібератаки та пропонує рекомендації щодо посилення кіберзахисту у корпоративному секторі.

Проблема ускладнюється через еволюцію методів, які використовуються для кібершпіонажу. Зокрема, Abu Samah та Abd Rashid (2024) зазначають, що з переходом на дистанційну роботу

© Товкун Ю. І., 2025
This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0.

ризики зросли через збільшення використання незахищених пристроїв. Автори наголошують, що нові форми кібератак спрямовані не лише на державні установи, але й на приватний сектор, що створює додаткові виклики для забезпечення інформаційної безпеки.

Попри значний прогрес у вивченні цієї теми, залишається недостатньо висвітленим питання про те, як саме поєднуються технічні та організаційні аспекти у реальних кібершпіонажних кампаніях. Аналіз конкретних кейсів, таких як операція Red October, атака на Офіс управління персоналом США чи угруповання "Star Blizzard", дозволяє поглибити розуміння механізмів, що стоять за такими атаками, та їхнього впливу на міжнародну безпеку.

Метою цього дослідження є всебічний аналіз феномену кібершпіонажу на основі конкретних кейсів і розробка рекомендацій для запобігання таким загрозам. У межах роботи ставляться такі завдання: дослідити сучасні методи, які використовуються зловмисниками; виявити спільні риси кібершпіонажних кампаній; оцінити вплив таких атак на міжнародну стабільність; і сформулювати заходи для підвищення ефективності кіберзахисту.

Наукова новизна цього дослідження полягає у міждисциплінарному підході до аналізу кібершпіонажу, який поєднує технічний, правовий і соціальний аспекти. Використання кейс-аналізу дозволяє виявити структурні характеристики кібершпіонажних атак і розробити практичні рекомендації для їхнього запобігання. Таким чином, результати цього дослідження можуть бути корисними для наукової спільноти, фахівців у сфері кібербезпеки та державних органів, які відповідають за захист інформації.

Огляд літератури

Кібершпіонаж залишається однією з найгостріших загроз у сучасному цифровому середовищі, особливо в контексті роботи урядових і корпоративних структур. Різноманітність методів, які застосовують зловмисники, і їхній постійний розвиток ставлять під сумнів традиційні підходи до забезпечення безпеки (Діордіца, 2017) [4]. У цьому контексті література, присвячена кібершпіонажу, пропонує корисні перспективи для розуміння його механізмів і запобігання.

У дослідженні "Military Cybersomethings" (Bellovin, 2013) аналізуються особливості кібершпіонажу у військовій сфері [5]. Автор акцентує увагу на технічній складності атак і зазначає, що більшість успішних операцій залежить від довготривалого доступу до цільових систем і висококваліфікованих ресурсів. Bellovin підкреслює, що технологічний аспект таких операцій часто супроводжується ретельним збором розвідданих про жертву, що дозволяє обійти стандартні методи захисту. Цей підхід резонує з моїм дослідженням, яке зосереджується на аналізі конкретних кейсів, таких як операція Red October, де ключовим елементом успіху було використання модульного програмного забезпечення для довготривалої присутності в системах.

Інше важливе дослідження, "Corporate Cyberespionage: Identification and Prevention" (Mitchell, 2020), присвячене аналізу шпигунства в корпоративному середовищі. Автори виділяють соціальну інженерію як один із головних інструментів зловмисників, підкреслюючи залежність від людського фактора [2]. Дослідження вказує на необхідність впровадження програмного забезпечення для моніторингу поведінки співробітників, що дозволяє ідентифікувати аномалії в мережевому трафіку. Це особливо актуально в контексті кейсів, які я аналізую, наприклад, атака угруповання "Star Blizzard", де фішингова кампанія стала відправною точкою для зламу систем.

Третє дослідження, "Navigating Data Secrecy Challenges: A Study on Cyberespionage Intentions in the WFH Era" (Samah et al., 2024), зосереджується на зміні ризиків у зв’язку з поширенням дистанційної роботи [3]. Автори доводять, що робота з дому створює додаткові вразливості, оскільки співробітники часто використовують незахищені пристрої та домашні мережі. У дослідженні підкреслюється, що систематичне навчання співробітників основам кібербезпеки зменшує успішність атак. Цей висновок корелює з моїм аналізом, який акцентує увагу на важливості людського фактора в успішних кібершпіонажних кампаніях, таких як атака на Офіс управління персоналом США.

Аналіз літератури показує, що кібершпіонаж є не лише технічним, але й соціальним феноменом. Використання уразливостей програмного забезпечення, таргетованих фішингових кампаній та модульного шкідливого програмного забезпечення створює унікальний набір викликів для кібербезпеки. Ці роботи вказують на необхідність інтегрованих підходів, які включають технічні засоби виявлення загроз, навчання співробітників і покращення політик безпеки. Висновки, зроблені в цих дослідженнях, є цінними для мого аналізу кейсів і сприяють розумінню масштабів проблеми.

Методологічна основа

Ця стаття базується на теоретичному аналізі явища кібершпіонажу з акцентом на вивченні реальних кейсів, їхніх технічних та організаційних аспектів, а також на розробці рекомендацій щодо запобігання таким атакам. Методологічна основа дослідження охоплює міждисциплінарний підхід, що поєднує концепції інформаційної безпеки, правового регулювання та соціальної інженерії.

Основою дослідження є огляд літератури, у межах якого були вивчені наукові статті, звіти та дослідження у сфері кібершпіонажу, опубліковані в авторитетних базах даних, таких як Web of Science, Scopus та Google Scholar. Особлива увага приділялася роботам, які аналізують реальні кейси кібершпіонажу (Bellovin, 2013; Mitchell, 2020; Samah et al., 2024) та пропонують рекомендації з удосконалення систем кібербезпеки [2-5].

Методологія також включає кейс-аналіз чотирьох значущих атак: операції Red October (2013), атаки на Офіс управління персоналом США (2015), кібератаки на Міжнародний кримінальний суд (2023) та операції "Star Blizzard" (2023) [8-10]. Цей підхід дозволив виявити спільні риси атак, зокрема використання вразливостей програмного забезпечення, таргетованих фішингових кампаній та шкідливого ПЗ, а також оцінити вплив людського фактора на успішність таких операцій.

Для формулювання рекомендацій щодо запобігання кібершпіонажу було використано системний підхід. Зокрема, вивчення технічних методів атак дозволило запропонувати заходи з удосконалення технологічного захисту, а аналіз соціальних аспектів — підкреслити важливість навчання співробітників та розвитку культури кібербезпеки. Крім того, враховуючи геополітичний контекст атак, особливу увагу було приділено рекомендаціям із посилення міжнародної співпраці у сфері протидії кібершпіонажу.

Таким чином, методологічна основа дослідження забезпечує всебічне розуміння проблеми кібершпіонажу та формує базу для розробки інтегрованих підходів до її вирішення.

Опис кейсів

Операція Red October (2013 рік). Операція Red October, або Rocra, є одним із наймасштабніших і найтриваліших прикладів кібершпіонажу. Вона тривала понад п’ять років і була спрямована на дипломатичні місії, урядові установи та наукові інститути, головним чином у Східній Європі, Центральній Азії та Західній Європі. Основною метою операції було викрадення конфіденційної інформації, такої як дипломатична кореспонденція, технічна документація, а також дані з мобільних пристроїв і USB-накопичувачів (Zetter, 2013) [6, 7].

Кампанія починалася з таргетованих фішингових листів, які містили заражені документи Microsoft Word і Excel. Використовувалися експлойти CVE-2012-0158 та CVE-2010-3333, що дозволяли виконувати шкідливий код після відкриття документа. Інфікування супроводжувалося встановленням модуля "Dropper", який надавав зловмисникам віддалений доступ до системи. Шкідливе ПЗ мало модульну архітектуру: воно могло оновлюватися та адаптуватися до середовища жертви, що забезпечувало довготривалий вплив (Gooding, 2013).

Передача даних на командно-контрольні (C&C) сервери здійснювалася через зашифрований трафік HTTP та FTP. Для ініціалізації з’єднань використовувалися DNS-запити з динамічними доменними іменами. Сервери C&C розташовувалися у різних країнах, що ускладнювало їхнє виявлення. Особливою рисою було використання спеціальних модулів для збору даних із USB-пристроїв, навіть якщо вони не були підключені до мережі (Brewster, 2014) [1].

Кібератака на Офіс управління персоналом США (2015 рік). Кібератака на Офіс управління персоналом США у 2015 році стала однією з наймасштабніших подій у сфері кібершпіонажу. Метою зловмисників було отримання доступу до персональних даних 21 мільйона осіб, які зберігалися у системі, включаючи відбитки пальців та анкети безпеки SF-86. Атака почалася з розсилки таргетованих фішингових листів адміністраторам систем. Після відкриття заражених вкладень встановлювався бекдор Sakula, що забезпечував стійкий доступ до мережі (Сааков, 2015).

Зловмисники використовували викрадені облікові дані для отримання доступу до критичних серверів. Sakula використовував HTTPS для передачі даних на C&C сервери, маскуючи трафік під звичайний вебтрафік. Для горизонтального переміщення мережею застосовувалися вразливості

протоколів SMB і LDAP, а також техніка Pass-the-Hash. Ця операція виявилася можливою через недостатню сегментацію мережі та відсутність захисту від таргетованих атак (Маріц, 2015) [10].

Кібератака на Міжнародний кримінальний суд (2023 рік). Кібератака на Міжнародний кримінальний суд (МКС) у 2023 році мала на меті викрадення конфіденційної інформації, пов'язаної з розслідуваннями воєнних злочинів. Зловмисники використовували вразливості ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) у Microsoft Exchange Server для проникнення у внутрішню мережу МКС. Після зламу серверів зловмисники встановлювали вебшели, які дозволяли їм виконувати віддалений код і керувати інфікованими системами (International Criminal Court, 2023).

Для викрадення облікових даних застосовувався інструмент Mimikatz, який дозволяв отримувати паролі та токени доступу з пам'яті серверів. Трафік передавався через зашифровані TLS-з'єднання, а маршрутизація відбувалася через VPN та проксі-сервери, що ускладнювало ідентифікацію джерела атак [11].

Атака угруповання "Star Blizzard" на британських парламентарів (2023 рік). Атака угруповання "Star Blizzard" на британських парламентарів стала прикладом політичного шпигунства. Зловмисники використовували фішингові листи з посиланнями на сайти, що експлуатували вразливість Spring4Shell (CVE-2022-22965). Інфікування серверів дозволяло завантажувати шкідливі JAR-файли, які забезпечували зловмисникам доступ до пристроїв жертв (Digmelashvili, 2023) [12].

Основний інструмент атаки — RAT (Remote Access Trojan) — забезпечував можливість перехоплення повідомлень, запису натискань клавіш і викрадення даних. Використовувалися техніки DNS-тунелювання для передачі команд C&C та SSH для завантаження викрадених даних на віддалені сервери. Завдяки складній маршрутизації зловмисники уникали виявлення, створюючи довготривалу присутність у мережах.

Кожна з цих атак демонструє високу технічну складність і стратегічний підхід, спрямований на викрадення критично важливої інформації. Їхній аналіз дозволяє визначити спільні риси, такі як використання фішингу, шкідливого ПЗ, експлойтів і складної інфраструктури C&C, що забезпечує тривалий вплив [13-15].

Аналіз та обговорення

Кібершпіонаж є багатогранною загрозою, яка поєднує технічні виклики, геополітичний контекст та серйозний вплив на міжнародну безпеку. Аналіз кейсів, таких як операція Red October (2013), атака на Офіс управління персоналом США (2015), кібератака на Міжнародний кримінальний суд (2023) та операція "Star Blizzard" (2023), дозволяє виявити як спільні риси, так і унікальні аспекти таких операцій.

Технічний аналіз цих атак показує, що зловмисники широко використовували експлойти, фішингові кампанії, шкідливе ПЗ і методи шифрування для досягнення своїх цілей. Наприклад, операція Red October була побудована навколо експлуатації вразливостей CVE-2012-0158 і CVE-2010-3333, тоді як у кейсі Міжнародного кримінального суду основною технікою стали ProxyShell-експлойти, які дозволяли проникати в сервери Microsoft Exchange. У всіх випадках фішингові атаки відігравали критичну роль, забезпечуючи початковий доступ до системи через ретельно таргетовані листи.

Використання шкідливого ПЗ також було важливою частиною атак. Наприклад, у кейсі Офісу управління персоналом США використовувався бекдор Sakula, а в операції "Star Blizzard" зловмисники впроваджували Remote Access Trojan (RAT), який надавав їм контроль над інфікованими системами. Ці програми часто маскували свою активність через динамічне шифрування трафіку (HTTPS, TLS) і використовували DNS-тунелювання для приховування переданих даних.

Технічні методи цих атак узагальнено у таблиці 1.

Таблиця 1. Технічні методи атак
Table 1. Technical methods of attacks

Метод	Приклад атаки	Деталі
Експлуатація вразливостей	Red October (CVE-2012-0158), МКС (ProxyShell)	Використання відомих уразливостей для отримання віддаленого доступу до систем.
Таргетований фішинг	Усі кейси	Поширення заражених листів серед ключових осіб у цільових організаціях.
Шкідливе програмне забезпечення	Sakula (OPM), RAT ("Star Blizzard")	Інфікування систем для довготривалого доступу, викрадення даних, моніторингу.
Шифрування трафіку	Усі кейси	HTTPS, TLS і DNS-тунелювання для приховування активності.
Інфраструктура C&C	Red October, МКС, OPM	Мережа проксі-серверів і VPN для приховування місцезнаходження атакуючих.

Однією з важливих характеристик атак є їхня довготривалість. Наприклад, Red October тривав понад п’ять років завдяки модульній архітектурі шкідливого ПЗ, яке могло автоматично оновлюватися. У випадку атаки на МКС зловмисники використовували методи "living-off-the-land", які залучали легітимні інструменти, такі як PowerShell, для приховування своєї активності (Смишляєв, 2023).

Аналіз кейсів також виявляє, що всі атаки мали геополітичну складову. Атака на Офіс управління персоналом США була спрямована на створення бази даних для стратегічного використання викрадених персональних даних, тоді як "Star Blizzard" мала на меті втручання у політичні процеси у Великій Британії. Кібератака на МКС підривала довіру до міжнародних інституцій, що може мати довготривалий вплив на глобальне правосуддя.

Підсумовуючи, розглянуті кейси демонструють високий рівень організації та використання сучасних технологій у кібершпіонажі. Ключовим викликом для протидії таким атакам залишається виявлення зашифрованого трафіку, швидке усунення вразливостей та підвищення обізнаності співробітників організацій щодо методів соціальної інженерії.

Рекомендації щодо запобігання кібершпіонажу (Recommendations for Preventing Cyber Espionage)

Запобігання кібершпіонажу потребує багатостороннього підходу, який поєднує технічні, організаційні та стратегічні заходи. Однією з основних причин успіху багатьох атак є експлуатація вразливостей програмного забезпечення. Тому важливо, щоб організації регулярно оновлювали свої системи, проводили тестування на проникнення та своєчасно усували знайдені уразливості. У кейсах, таких як Red October чи атака на МКС, саме недоліки у захисті дозволили зловмисникам отримати доступ до ключових систем (Шлапаченко, 2020). Це підкреслює необхідність використання сучасних рішень, наприклад, багаторівневого захисту та сегментації мереж, що обмежує горизонтальний рух зловмисників у разі компрометації однієї з частин інфраструктури.

Водночас важливу роль відіграє людський фактор. У більшості розглянутих кейсів атаки починалися із соціальної інженерії та таргетованого фішингу. Це вказує на нагальну потребу підвищення обізнаності співробітників. Проведення тренінгів з кібербезпеки, симуляція фішингових атак і створення культури відповідального ставлення до інформації допоможуть значно знизити ризики, пов’язані з людськими помилками. Працівники повинні бути здатні розпізнавати підозрілі електронні листи, уникати переходу за сумнівними посиланнями та повідомляти про підозрілу активність.

Раннє виявлення атак є ще одним ключовим компонентом у протидії кібершпіонажу. Організації повинні впроваджувати сучасні системи моніторингу, наприклад SIEM, які дозволяють виявляти аномалії у трафіку та реагувати на них у реальному часі. Аналіз зашифрованого трафіку, зокрема TLS, є особливо важливим, адже більшість зловмисників використовують шифрування для приховування своєї активності. Крім того, моніторинг DNS-

запитів може стати ефективним інструментом для виявлення використання DNS-тунелювання, що є поширеною технікою передачі команд до командно-контрольних серверів.

Організаційні заходи також відіграють важливу роль у запобіганні атакам. Важливо розробляти плани реагування на інциденти, які визначають послідовність дій у разі компрометації систем. Регулярні аудити безпеки допоможуть виявляти слабкі місця до того, як вони будуть експлуатовані зловмисниками (Чеховська, 2021). Крім того, впровадження принципу найменших привілеїв для доступу до даних дозволяє мінімізувати шкоду у випадку компрометації окремих облікових записів.

Оскільки багато атак мають міжнародний характер, посилення співпраці між державами є необхідним для боротьби з кібершпіонажем. Обмін інформацією про загрози, розробка уніфікованого законодавства та спільні навчання допоможуть швидше виявляти атаки й ефективніше протидіяти їм. Особливу увагу варто приділяти дослідженню новітніх технологій, таких як штучний інтелект, який може бути використаний для прогнозування атак, та квантове шифрування, що забезпечить високий рівень захисту даних у майбутньому.

Загалом, боротьба з кібершпіонажем потребує інтегрованого підходу, що включає сучасні технології, людський фактор і міжнародну співпрацю. Це дозволить не лише знизити ризики атак, але й створити стійку систему безпеки, яка зможе ефективно реагувати на нові виклики у цифровому середовищі.

Висновки

Кібершпіонаж став одним із найпотужніших інструментів впливу в сучасному світі, об’єднавши технологічну складність із геополітичними амбіціями. Аналіз кейсів операції Red October, атаки на Офіс управління персоналом США, кібератаки на Міжнародний кримінальний суд та операції "Star Blizzard" дозволив виявити спільні риси, технічні методи та наслідки таких дій. Ці атаки підкреслюють, що головною метою зловмисників є не лише викрадення конфіденційної інформації, але й тривалий контроль над інфраструктурою жертви для досягнення стратегічних цілей.

Ключовим фактором успіху атак стала експлуатація вразливостей програмного забезпечення та використання людського фактора. Фішингові кампанії, які передували більшості розглянутих атак, свідчать про необхідність посилення обізнаності співробітників і вдосконалення політик інформаційної безпеки. Водночас використання модульного шкідливого ПЗ та інноваційних методів маскування, таких як шифрування трафіку та DNS-тунелювання, вказує на зростаючу технічну досконалість зловмисників.

Проаналізовані кейси також демонструють значний вплив кібершпіонажу на міжнародну безпеку. Атаки можуть спричиняти політичну дестабілізацію, підривати довіру до міжнародних інституцій та створювати серйозні економічні втрати. Зокрема, компрометація Міжнародного кримінального суду підважує здатність глобальних інституцій захищати конфіденційність даних, що ставить під сумнів їхню легітимність.

Запобігання таким загрозам потребує інтегрованого підходу. Необхідно поєднувати технічні заходи, такі як регулярне оновлення програмного забезпечення, використання сучасних інструментів моніторингу та вдосконалення мережевої безпеки, із організаційними ініціативами, спрямованими на підвищення рівня кіберобізнаності співробітників. Крім того, важливим є розвиток міжнародної співпраці, яка дозволить ефективніше обмінюватися інформацією про загрози та координувати зусилля у сфері кібербезпеки.

Таким чином, у сучасних умовах боротьба з кібершпіонажем повинна стати пріоритетним завданням як для державних структур, так і для міжнародної спільноти. Поглиблення досліджень, впровадження інноваційних технологій і посилення міжнародного співробітництва є необхідними кроками для забезпечення довгострокової стійкості у сфері кібербезпеки. Розуміння механізмів атак та їхнього впливу є ключем до створення більш безпечного цифрового середовища.

Рекомендації

Матеріали статті є цінними для науковців, які досліджують сучасні загрози у сфері інформаційної безпеки, а також для фахівців з кібербезпеки, які займаються практичним захистом інформаційних систем. Зібрані кейси та їх аналіз можуть бути використані для розробки нових підходів до виявлення та запобігання кібершпіонажу, а також для навчання співробітників, відповідальних за безпеку корпоративних і державних мереж.

Результати дослідження становлять особливу практичну цінність для державних органів, які відповідають за національну безпеку, зокрема для підрозділів, що займаються аналізом кіберзагроз та реагуванням на інциденти. Запропоновані рекомендації з посилення технологічного захисту та підвищення рівня кіберобізнаності можуть бути інтегровані в існуючі політики інформаційної безпеки.

Крім того, стаття буде корисною для керівників приватних компаній, які стикаються із загрозами витоку інтелектуальної власності. Наведені у статті приклади атак на корпоративні структури допоможуть зрозуміти, які аспекти захисту є найбільш вразливими, та які кроки необхідно зробити для їхнього посилення.

Результати дослідження також можуть бути корисними для міжнародних організацій, які займаються регулюванням та стандартизацією кібербезпеки. Запропоновані заходи з міжнародної співпраці, обміну інформацією про загрози та гармонізації законодавства можуть сприяти створенню глобальної системи протидії кібершпіонажу.

Таким чином, стаття може слугувати базою для подальших досліджень і впровадження практичних заходів у сфері кібербезпеки, спрямованих на протидію сучасним викликам цифрового середовища.

СПИСОК ЛІТЕРАТУРИ

1. Fruhlinger J. The OPM hack explained: Bad security practices meet China's Captain America [Електронний ресурс] // CSO Online. – 2020. – Режим доступу: https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html (Дата звернення: 16.08.2025).
2. Mitchell B. Corporate cyberespionage: Identification and prevention // EDPACS. – 2020. – Vol. 62, No. 6. – P. 1–14. – DOI: https://doi.org/10.1080/07366981.2020.1798595 (Дата звернення: 17.08.2025).
3. Abu Samah I. H., Sarip A., Ishak M. K., Shaari R., Rahim N. S. A., Abd Rashid I. M. Navigating data secrecy challenges: A study on cyberespionage intentions in the WFH era // Journal of the Institution of Engineers (India), Series B. – 2024. – Vol. 105, No. 4. – P. 941–957. – DOI: https://doi.org/10.1007/s40031-024-01022-1 (Дата звернення: 18.08.2025).
4. Діордіца І. В. Поняття та зміст кібершпигунства [Електронний ресурс] // Goal International. – 2017. – Режим доступу: https://goal-int.org/ponyattya-ta-zmist-kibershpigunstva/ (Дата звернення: 19.08.2025).
5. Bellovin S. M. Military cybersomethings // IEEE Security & Privacy. – 2013. – Vol. 11, No. 3. – P. 88–89. – Режим доступу: https://ieeexplore.ieee.org/document/6521321 (Дата звернення: 20.08.2025).
6. Zetter K. Cybersleuths uncover 5-year spy operation targeting governments [Електронний ресурс] // Wired. – 2013. – Режим доступу: https://www.wired.com/2013/01/red-october-spy-campaign/ (Дата звернення: 21.08.2025).
7. Brewster T. When a government is behind a cyberattack [Електронний ресурс] // BBC. – 2014. – Режим доступу: https://www.bbc.com/russian/business/2014/04/140423_vert_cap_when_governments_attack (Дата звернення: 22.08.2025).
8. Goodin D. Red October relied on Java exploit to infect PCs [Електронний ресурс] // Ars Technica. – 2013. – Режим доступу: https://arstechnica.com/information-technology/2013/01/massive-espionage-malware-relied-on-java-exploit-to-infect-pcs/ (Дата звернення: 23.08.2025).
9. Сааков В. У США хакери викрали дані мільйонів осіб [Електронний ресурс] // DW. – 2015. – Режим доступу: https://www.dw.com/uk/хакери-викрали-особисті-дані-близько-215-мільйона-людей-у-сша/a-18576309 (Дата звернення: 24.08.2025).
10. Маріц Д. О. "Кібератака" – війна майбутнього [Електронний ресурс]. – Київ: Інститут проблем сучасної інформації, 2015. – Режим доступу: https://ippi.org.ua/sites/default/files/maric.pdf (Дата звернення: 25.08.2025).

11. International Criminal Court. Measures taken following the unprecedented cyber-attack on the ICC [Електронний ресурс]. – 2023. – Режим доступу: https://www.icc-cpi.int/news/measures-taken-following-unprecedented-cyber-attack-icc (Дата звернення: 26.08.2025).
12. Digmelashvili T. The impact of cyberwarfare on national security [Електронний ресурс] // ResearchGate. – 2023. – Режим доступу: https://www.researchgate.net/publication/373855875_The_Impact_of_Cyberwarfare_on_the_National_Security (Дата звернення: 27.08.2025).
13. Смишляєв С. Лондон викрив спроби кібератак на високопосадовців з боку РФ [Електронний ресурс] // DW. – 2023. – Режим доступу: https://www.dw.com/uk/velikobritania-vikrila-sprobi-kiberatak-na-visokoposadovciv-z-boku-rf/a-67659852 (Дата звернення: 28.08.2025).
14. Шлапаченко В. М. Шпигунство як діяльність зі здобування інформації // Інформаційна безпека людини, суспільства, держави. – 2020. – № 1 (17). – С. 99–109. (Дата звернення: 29.08.2025).
15. Чеховська М. М. Кібершпіонаж як загроза національній безпеці // Актуальні проблеми управління інформаційною безпекою держави. – Київ: Наук.-вид. відділ НА СБ України, 2021. С. 232–234. (Дата звернення: 30.08.2025).

REFERENCES

1. J. Fruhlinger, “The OPM hack explained: Bad security practices meet China’s Captain America,” CSO Online, Aug. 5, 2020. [Online]. Available: https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html
2. B. Mitchell, “Corporate cyberespionage: Identification and prevention part 2,” EDPACS, vol. 62, no. 6, pp. 1–14, 2020, doi: 10.1080/07366981.2020.1798595.
3. I. H. Abu Samah, A. Sarip, M. K. Ishak, R. Shaari, N. S. A. Rahim, and I. M. Abd Rashid, “Navigating data secrecy challenges: A study on cyberespionage intentions in the WFH era,” Journal of the Institution of Engineers (India): Series B, vol. 105, no. 4, pp. 941–957, 2024, doi: 10.1007/s40031-024-01022-1.
4. I. V. Diorditsa, “The concept and content of cyberespionage,” Goal International, 2017. [Online]. Available: https://goal-int.org/ponyattya-ta-zmist-kibershpigunstva/ [in Ukrainian].
5. S. M. Bellovin, “Military cybersomethings,” IEEE Security & Privacy, vol. 11, no. 3, pp. 88–89, 2013, doi: 10.1109/MSP.2013.68.
6. K. Zetter, “Cybersleuths uncover 5-year spy operation targeting governments,” WIRED, Jan. 14, 2013. [Online]. Available: https://www.wired.com/2013/01/red-october-spy-campaign/
7. T. Brewster, “What can you do when governments attack?,” BBC, Apr. 23, 2014. [Online]. Available: https://www.bbc.com/russian/business/2014/04/140423_vert_cap_when_governments_attack [in Russian].
8. D. Goodin, “Red October relied on Java exploit to infect PCs,” Ars Technica, Jan. 15, 2013. [Online]. Available: https://arstechnica.com/information-technology/2013/01/massive-espionage-malware-relied-on-java-exploit-to-infect-pcs/
9. V. Saakov, “Hackers stole the data of millions of people in the USA,” Deutsche Welle, Jul. 10, 2015. [Online]. Available: https://www.dw.com/uk/хакери-викрали-особисті-дані-близько-215-мільйона-людей-у-сша/a-18576309 [in Ukrainian].
10. D. O. Marits, “Cyberattack – The war of the future,” Institute of Modern Information Problems, 2015. [Online]. Available: https://ippi.org.ua/sites/default/files/maric.pdf [in Ukrainian].
11. International Criminal Court, “Measures taken following the unprecedented cyber-attack on the ICC,” ICC, Sep. 22, 2023. [Online]. Available: https://www.icc-cpi.int/news/measures-taken-following-unprecedented-cyber-attack-icc
12. T. Digmelashvili, “The impact of cyberwarfare on national security,” ResearchGate, 2023. [Online]. Available: https://www.researchgate.net/publication/373855875_The_Impact_of_Cyberwarfare_on_the_National_Security

13. C. Smishlyayev, “London exposed cyberattacks on high-ranking officials by the Russian Federation,” Deutsche Welle, Dec. 7, 2023. [Online]. Available: https://www.dw.com/uk/velikobritania-vikrila-sprobi-kiberatak-na-visokoposadovciv-z-boku-rf/a-67659852 [in Ukrainian].
14. V. M. Shlapachenko, “Espionage as an activity of information retrieval,” Human, Society, and State Information Security, vol. 1, no. 17, pp. 99–109, 2020. [in Ukrainian].
15. M. M. Chekhovska, “Cyberespionage as a threat to national security,” in Current Issues in State Information Security Management, Kyiv, Ukraine: Scientific Publishing Department of the Security Service of Ukraine, 2021, pp. 232–234. [in Ukrainian].

Tovkun Yuliia *PhD student*
Kharkiv National University of Radio Electronics
Nauky Ave, 14, Kharkiv, Kharkiv Oblast, 61166
e-mail: ytovkun@gmail.com
https://orcid.org/0009-0000-5916-2897

Methods of Cyber Espionage and Their Impact on International Security

The relevance of this research is determined by the increasing role of cyber espionage as a geopolitical tool and a means of obtaining confidential information. In the context of digitalization, government institutions, international organizations, and corporate entities are becoming key targets of cyberattacks, posing significant threats to national security and global stability.
This article aims to analyze the phenomenon of cyber espionage, particularly its technical, organizational, and social aspects, based on real-world cases. The study focuses on the use of modern attack methods, such as targeted phishing, software vulnerability exploitation, and modular malware deployment. The article seeks to identify common characteristics of cyber espionage campaigns and develop recommendations to counter such threats.
A theoretical methodological approach was used in the study, combining literature review, case analysis of attacks (Red October operation, the attack on the U.S. Office of Personnel Management, the cyberattack on the International Criminal Court, the "Star Blizzard" operation), and a systematic analysis of factors contributing to the success of cyber espionage campaigns.
The study identified key technical methods of attacks, their impact on information security, and the role of the human factor in the success of cyber espionage. Recommendations for strengthening cybersecurity were formulated, encompassing technical, organizational, and international measures.
The findings of this article are of interest to researchers, cybersecurity professionals, and governmental bodies dealing with information protection issues and can be used for developing policies to counteract cyber espionage.

Keywords: *cyber threats, espionage software, targeted phishing, information security, cyber espionage.*

Надійшла у першій редакції 29.03.2025, в останній - 11.05.2025.
The first version has been received on 29.03.2025, the final version - on 11.05.2025.