

**Верголяс Олександр Олександрович**

кандидат юридичних наук,

інженер відділення програмного та інформаційного

забезпечення інформаційно-обчислювального центру

Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна

ORCID: 0000-0002-9780-1298

arnijazov@gmail.com

**ЛЮДСЬКИЙ ВЕКТОР ПРОНИКНЕННЯ В ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ:
ЗІСТАВЛЕННЯ ТРЬОХ НЕЗАЛЕЖНИХ ОБЛІКІВ ПОЧАТКОВОГО ДОСТУПУ**

Анотація. Стаття присвячена одному конкретному механізму ураження об'єктів критичної інфраструктури — тому, у якому проникнення починається з людини, а завершується втручанням у технологічний сегмент. Проблема, з якої виросло дослідження, лежить не в дефіциті публікацій, а в тому, що два наявні масиви літератури не перетинаються: українські роботи про критичну інфраструктуру описують об'єкти, загрози і правові режими, роботи про соціальну інженерію і фішинг описують поведінку користувача поза галузевим контекстом, і працівник, через якого відбувається вхід на енергетичний об'єкт, випадає з обох. У вступі показано, що ця прогалина має не бібліографічну, а практичну ціну: захисні заходи проєктуються або під технологічний периметр, або під офісного користувача, і стик між ними лишається без власника. Теоретичні основи дослідження будують ланцюг ураження як послідовність чотирьох ланок — вплив на працівника, отримання початкового доступу, бічне переміщення до межі технологічного сегмента, втручання в керування — і фіксують, що кожна ланка має власну статистику, власний набір захисних заходів і власну наукову літературу, а перехід між ланками не описано ніде. Методика дослідження полягає в зіставленні трьох незалежних обліків початкового доступу за період, що частково збігається: глобального звіту Verizon про розслідування витоків даних, європейського огляду ландшафту загроз ENISA і північної аналітики Державного центру кіберзахисту. Результати дослідження складаються з чотирьох частин. Перша — зафіксована розбіжність: частка соціальної інженерії в трьох обліках становить від шістнадцяти до шістдесяти відсотків, і ці числа не зводяться прямим порівнянням. Друга — пояснення розбіжності через чотири методологічні відмінності, головна з яких стосується одиниці обліку; наведено перерахунок, який зводить європейські дані до тієї самої одиниці, що й глобальні, і показує, що залишковий розрив припадає не на фішинг, а на експлуатацію вразливостей. Третя — відтворюваність ланцюга на українському матеріалі, де документований епізод 2015 року зіставлено з пізнішими кампаніями, у яких вектор входу був іншим або не розкритим. Четверта — оцінка того, що саме змінив у цьому ланцюгу генеративний штучний інтелект, і чому підвищення обізнаності персоналу за наявними експериментальними даними не закриває вектор. Дослідний текст пропонуваного доповнення до пункту 9 Загальних вимог з кіберзахисту об'єктів критичної інфраструктури наведено в результатах, а висновки містять напрями подальших розвідок, серед яких — перенесення оцінок піддатливості до переконування з загальної популяції на операторів автоматизованих систем керування технологічними процесами.

Ключові слова: критична інфраструктура; соціальна інженерія; початковий доступ; фішинг; АСУ ТП; людський вектор; кіберзахист; генеративний штучний інтелект.

ВСТУП

Постановка проблеми. Двадцять третього грудня 2015 року знеструмлення трьох українських обленерго почалося не з експлуатації вразливості в системі керування, а з документа Microsoft Office, надісланого поштою працівникам адміністративної та інформаційно-технологічної мереж [1]. Ця послідовність — вплив на людину, початковий доступ, рух до технологічного сегмента, втручання в керування — від того часу відтворювалася в різних варіантах, але саме як послідовність вона майже не досліджується. Наявна література розпадається на дві частини, що не мають спільних посилянь. Перша



описує об'єкти критичної інфраструктури (далі – КІ), режими їх захисту і моделі зрілості відповідних систем; друга описує соціальну інженерію, фішинг і поведінку користувача, здебільшого на матеріалі корпоративного офісу. Працівник енергетичного підприємства, через якого відбувається вхід, не належить жодній із них: для першої він зовнішній чинник, для другої — звичайний користувач без галузевої специфіки.

Ціна цього розриву не бібліографічна. Коли захист проєктується окремо під технологічний периметр і окремо під офісного користувача, стик між ними лишається без власника, і саме на цьому стику працює зловмисник. При цьому кількісна картина, на яку спирається вибір пріоритетів, теж не є однозначною: різні незалежні обліки початкового доступу дають для соціальної інженерії частки, що відрізняються в чотири рази, і жоден із них не пояснює, чому його числа не збігаються з іншими, тож керівник, що розподіляє обмежений бюджет між навчанням персоналу і технічними бар'єрами, отримує три різні відповіді на одне питання.

Аналіз останніх досліджень і публікацій. Український доробок із соціальної інженерії і фішингу за останні роки помітно виріс і має власний інструментарій. Класифікацію фішингових атак і методи їх виявлення систематизовано в роботі Штонди Р. та співавторів [2]; ефективність двофакторної автентифікації у зв'язці з людським фактором оцінено Опірським І., Сікорським Р. і Мартинюком Д. [3]. Окрему лінію утворюють дослідження людського фактора в кіберфізичних системах: Кожедуб Ю., Крамська Ю. і Гирда В. аналізують його вплив на кіберфізичну систему як на цілісний об'єкт [4]. Костюк Ю., Складанний П. та співавтори розглядають інтелектуальні системи керування і захисту в середовищах Smart Grid [5]. Перехід від обізнаності до керованого поведіння з людськими ризиками обґрунтовано Козубцовою Л., Ліщиною В. і Козубцовим І. [6]. У той же час слід констатувати, що наразі залишається недостатньо вивченим саме перехід від ураження людини до ураження технологічного процесу: жодна з перелічених робіт не доводить ланцюг до межі автоматизованої системи керування технологічним процесом (далі – АСУ ТП), а роботи про АСУ ТП не повертаються до того, як зловмисник до неї потрапив.

В іноземній літературі стан подібний, хоч і з іншим розподілом. Найближче до предмета підходять Nifakos S., Chandramouli K. і Stathakourou N., поєднуючи соціальну інженерію з критичною інформаційною інфраструктурою, проте в межах ширшого огляду поведінкових чинників [7]. Огляд кібератак на енергетичну інфраструктуру Abraham D., Houmb S. H. і Erdodi L. фіксує фішинг як первинний вхід у кейсі 2015 року і зіставляє інциденти з матрицею ATT&CK for ICS, але не розглядає людську ланку як самостійний об'єкт захисту [8]. Chowdhury N. і Gkioulos V. у профільному огляді підготовки персоналу для захисту КІ показують, чого бракує наявним навчальним програмам, і водночас не зіставляють їх результативність із незалежними експериментальними даними [9]. Психологічне підґрунтя піддатливості описано класично: Ferreira A. і Teles S. операціоналізують принципи переконування в фішингових листах [10], Sommestad T. і Karlzén H. узагальнюють польові експерименти з піддатливості метааналізом [11]. Жодна з цих робіт не працює з українським матеріалом і з галузевою специфікою операторів енергетики.

Метою статті є пояснення розбіжності між незалежними обліками початкового доступу стосовно ролі людського вектора і встановлення того, у якій формі цей вектор діє проти об'єктів КІ після появи генеративних моделей. Для досягнення мети зіставлено три незалежні масиви даних за частково збіжний період, запропоновано перерахунок, що зводить їх до спільної одиниці обліку, перевірено відтворюваність ланцюга ураження на українських кампаніях 2015–2025 років і сформульовано норму, яка закриває виявлену прогалину в національному регулюванні.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Поняття, з якого тут усе будується, ширше за фішинг. Початковий доступ (initial access) — це спосіб, у який зловмисник уперше отримує керовану присутність у середовищі жертви; він не збігається ні з подією доставки шкідливого повідомлення, ні з фактом компрометації, і саме ця незбіжність дає більшу частину плутанини в галузевій статистиці. Людський вектор початкового доступу — окремий випадок, у якому керована присутність постає внаслідок дії самого працівника: відкриття вкладення, запуску файла, введення облікових даних на підставленій сторінці, виконання інструкції, отриманої голосом. Ця дія є необхідною ланкою; без неї подальший ланцюг не запускається, і тому захисні заходи, що діють після неї, мають іншу природу, ніж заходи, що діють до.

Ланцюг ураження об'єкта КІ через людину доцільно розкласти на чотири ланки. Перша — вплив на працівника, з використанням принципів переконування, серед яких у фішингових повідомленнях найчастіше задіюють авторитет і дефіцит часу [10]. Друга — отримання початкового доступу в корпоративному сегменті, де опиняється більшість службових робочих місць. Третя — бічне переміщення до межі технологічного сегмента, яке в задокументованих епізодах займало місяці й спиралося на легітимні облікові записи [1]. Четверта — втручання в керування, де зловмисник або оперує робочим



місцем оператора безпосередньо, або застосовує спеціалізоване шкідливе програмне забезпечення (далі – ШПЗ) проти протоколів керування [12].

Ключова для подальшого викладу обставина полягає в тому, що кожна ланка вимірюється окремо і різними інструментами: піддатливість персоналу міряють польовими експериментами з симульованим фішингом, і метааналіз таких експериментів дає базові рівні переходу за посиленням у межах кількох десятків відсотків залежно від контексту [11]. Стійкість технологічного сегмента міряють аудитом сегментації і контролем доступу, для чого існує галузева настанова [13]. Перехід між ланками не міряє ніхто, і саме тому загальні показники «частка фішингу» і «частка вразливостей» не можна безпосередньо накладати на об'єкт КІ: вони відповідають на питання про окремі ланки, а не про ланцюг.

МЕТОДИКА ДОСЛІДЖЕННЯ

Матеріалом слугували три незалежні обліки початкового доступу, відібрані за трьома умовами: первинність (масив зібрано самим укладачем, а не переказано з інших звітів), опублікована методологія обліку і період спостереження, що бодай частково перекривається з рештою.

Перший масив — дев'ятнадцяте видання звіту Verizon про розслідування витоків даних, укладене за понад тридцять одну тисячу інцидентів і понад двадцять дві тисячі підтверджених витоків у ста сорока п'яти країнах, з вікном спостереження від жовтня 2024 до листопада 2025 року [14]. Другий — огляд ландшафту загроз ENISA за 2025 рік, виданий у жовтні того самого року, що охоплює період з 1 липня 2024 до 30 червня 2025 року, ґрунтується на 4 875 відібраних подіях і подає розподіл векторів початкового вторгнення в оглядовому розділі [15]. Третій — піврічна аналітика Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України за перше півріччя 2025 року, що ґрунтується на трьох тисячах вісімнадцяти зареєстрованих інцидентах [16]. Для контролю тенденції залучено наступний випуск тієї самої аналітики за друге півріччя 2025 року, у якому зареєстровано дві тисячі дев'яност дев'ять інцидентів [17].

Опрацювання складалося з чотирьох кроків. Спершу з кожного масиву витягнуто розподіл початкового доступу в тих категоріях, у яких його подає сам укладач, без перейменування. Далі для кожного масиву встановлено одиницю обліку — те, що саме укладач рахує одиницею в знаменнику. Третім кроком показники зведено до спільної одиниці там, де сам масив дає для цього коефіцієнт переходу. Нарешті залишкову розбіжність пояснено відмінностями вибірки й таксономії, а не похибкою.

Обмеження методики мають бути названі прямо. Звітні вікна трьох масивів не тотожні: глобальний звіт охоплює жовтень 2024 — листопад 2025 року, європейський огляд — липень 2024 — червень 2025 року, українська аналітика — перше півріччя 2025 року, і спільним для всіх трьох є лише це півріччя. У вересні 2026 року ENISA оприлюднила наступний огляд, який перейшов на календарний рік, охопив 8 257 інцидентів за 2025 рік і подає фішинг уже як частку серед технік соціальної інженерії (77,8 %), а не серед усіх векторів проникнення, причому вектор проникнення в ньому встановлено лише для 5,2 % випадків несанкціонованого доступу, з яких 60,4 % припадає на експлуатацію вразливостей [18]. Коефіцієнтів переходу від спостереженого випадку до проникнення новий огляд не наводить, тому запропонований нижче перерахунок можливий лише на даних попереднього випуску, а сама зміна знаменника між двома суміжними випусками одного укладача є проявом того самого ефекту одиниці обліку, якому присвячено статтю. Категорії укладачів не є взаємно виключними в один і той самий спосіб. Жоден із трьох масивів не виділяє об'єкти КІ в окрему підвибірку з власним розподілом початкового доступу, тому перенесення висновків на енергетичний сектор лишається аргументованим припущенням, а не виміром.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Розбіжність трьох обліків

Зіставлення в первинних категоріях укладачів подано в таблиці 1. Глобальний звіт називає найпоширенішим вектором початкового доступу експлуатацію програмних вразливостей із часткою тридцять один відсоток, зловживання обліковими даними дає тринадцять відсотків, фішинг — шістнадцять, а претекстинг, уперше виділений в окремий вектор, — шість відсотків [14]. В іншому розрізі того самого масиву, за патернами витоку, соціальна інженерія становить шістнадцять відсотків усіх витоків. Європейський огляд дає протилежну картину: фішинг близько шістдесяти відсотків спостережених випадків, експлуатація вразливостей — двадцять один і три десятих, ботнети — дев'ять і дев'ять десятих, шкідливі застосунки — вісім, інсайтери — вісім десятих відсотка [15]. Українська аналітика подає фішинг із часткою двадцять сім відсотків проти дев'ятнадцяти в попередньому півріччі, а розповсюдження ШПЗ — тридцять три відсотки проти сорока трьох, при частці енергетики в чотири



відсотки інцидентів [16]. У наступному півріччі фішинг зріс до тридцяти одного відсотка, розповсюдження ШПЗ після попереднього спаду знову зросло, до тридцяти шести відсотків, а частка енергетики збільшилася до шести відсотків [17].

Таблиця 1

Початковий доступ за трьома незалежними обліками, у первинних категоріях укладачів

Облік	Одиниця обліку	Соціальна інженерія / фішинг	Експлуатація вразливостей	Інші категорії
Verizon DBIR, 19-те вид. [14]	підтверджений витік (понад 22 000)	фішинг 16 %, претекстинг 6 % (як вектори початкового доступу); патерн «соціальна інженерія» — 16 % витоків	31 %	зловживання обліковими даними 13 %
ENISA Threat Landscape 2025 [15]	спостережений випадок початкового вторгнення	≈60 %	21,3 %	ботнети 9,9 %; шкідливі застосунки 8 %; інсайдери 0,8 %
Держспецв'язку, ДЦКЗ, I півріччя 2025 [16]	зареєстрований інцидент (3 018)	27 % (проти 19 % у попередньому півріччі)	не виділено окремо	розповсюдження ШПЗ 33 % (проти 43 %)

Джерело: складено автором за [14], [15], [16]; категорії подано в тому вигляді, у якому їх уживає укладач, без перейменування.

Різниця між шістнадцятьма і шістдесятьма відсотками для однієї й тієї самої категорії не є розбіжністю оцінок — це ознака того, що знаменники різні.

Чому числа не збігаються

Перша і найвагоміша відмінність стосується одиниці обліку. Глобальний звіт рахує підтверджені витoki, тобто завершені компрометації; європейський огляд рахує спостережені випадки початкового вторгнення, включно з тими, що не дали зловмисникові стійкої присутності; українська аналітика рахує зареєстровані інциденти, тобто події, опрацьовані командою реагування, серед яких багато не завершилися компрометацією взагалі. Фішинг генерує багато подій і порівняно мало завершених компрометацій, експлуатація вразливості — навпаки, і будь-який облік, що рахує події, механічно завищує перший і занижує другий.

Цей висновок не є припущенням, адже сам європейський огляд дає коефіцієнти переходу: двадцять сім відсотків фішингових випадків завершуються проникненням проти близько сімдесяти відсотків для експлуатації вразливостей [15]. Перерахунок наведено в таблиці 2. Якщо частку фішингу в шістдесят відсотків помножити на його ж конверсію 0,27, отримуємо шістнадцять і дві десятіх відсоткового пункту вихідної бази; для вразливостей двадцять один і три десятіх при конверсії 0,70 дають чотирнадцять і дев'ять десятіх. Перше число збігається з часткою фішингу в підтверджених витоків за глобальним звітом із точністю до десятіх, і цей збіг є головним кількісним результатом статті: два незалежні масиви, що на перший погляд суперечать один одному вчетверо, у спільній одиниці обліку дають те саме.

Таблиця 2

Зведення європейського розподілу до одиниці обліку глобального звіту

Вектор	Частка у спостережених випадках, % [15]	Конверсія у проникнення [15]	Частка у завершених проникненнях, в. п.	Для порівняння: частка у підтверджених витоків, % [14]
Фішинг	60,0	0,27	16,2	16
Експлуатація вразливостей	21,3	0,70	14,9	31

Джерело: розрахунок автора за коефіцієнтами переходу, які подає сам огляд ENISA; в. п. — відсоткові пункти вихідної бази спостережених випадків.

Залишкова розбіжність припадає не на фішинг, а на експлуатацію вразливостей: чотирнадцять і дев'ять десятіх проти тридцяти одного відсотка. Пояснення цієї частини лежить у складі вибірок, а не в



методі обліку. Глобальний масив із понад двадцятьма двома тисячами підтверджених витоків охоплює переважно комерційний сектор із великою часткою периметрових пристроїв, і саме вони дали приріст експлуатації; європейський огляд зважений на сектори, де периметр вужчий. Друга відмінність — таксономія: українська аналітика веде «фішинг» і «розповсюдження ШПЗ» як окремі категорії, хоча значна частина ШПЗ доставляється саме поштою, і тому двадцять сім відсотків фішингу в цьому масиві не є повною мірою людського вектора. Третя відмінність — географія і характер загрози: український масив описує середовище, у якому пріоритетною загрозою для енергетики названо державно-спонсорований кластер, тоді як глобальний масив зважений на кримінально мотивовану активність [16].

Практичний наслідок цього розбору один, і він не збігається з жодним із трьох заголовкових чисел. Для планування захисту об'єкта КІ орієнтиром має бути не частка фішингу як патерну, а показник участі людського елемента, який глобальний звіт подає окремо: шістдесят два відсотки витоків проти шістдесяти в попередньому виданні [14]. Цей показник зростає, тоді як частка крадених облікових даних як точки входу падає, і теза про згасання ролі людини спирається на підміну одного показника іншим. Той самий напрям фіксує й національний облік, де частка фішингу серед зареєстрованих інцидентів за три поспіль півріччя зросла з дев'ятнадцяти до двадцяти семи і далі до тридцяти одного відсотка [16], [17].

Відтворюваність ланцюга на українському матеріалі

Епізод 23 грудня 2015 року лишається єдиним повністю задокументованим прикладом, у якому всі чотири ланки простежено від початку до кінця. Звіт SANS ICS і E-ISAC фіксує початковий вектор — шкідливі документи Microsoft Office, надіслані поштою особам в адміністративній та інформаційно-технологічній мережах, застосування BlackEnergy 3 і модифікованого KillDisk, шкідливий код для послідовних Ethernet-конвертерів на підстанціях, ураження трьох обленерго і знеструмлення близько двохсот двадцяти п'яти тисяч споживачів о пів на четверту пополудні за місцевим часом, а також тривалу попередню розвідку і пряме інтерактивне керування робочими місцями операторів [1].

Проте наступні епізоди цю послідовність не повторюють, і чесний виклад мусить це показати. У кампанії проти енергетичного об'єкта у квітні 2022 року, де застосовано Industroyer2 разом із CaddyWiper та групою стирачів, вектор початкового доступу публічно не розкрито ні виробником засобів захисту, ні національною командою реагування — зразок було скопійовано двадцять третього березня, тобто щонайменше за два тижні до запланованого спрацювання, але шлях входу лишився невідомим [12]; національна команда реагування описує ту саму кампанію в термінах застосованого ШПЗ, не вектора [19]. У квітні 2024 року плани кібердиверсії майже на двадцять об'єктах енергетики, водо- і теплопостачання в десяти областях реалізовувалися через компрометацію ланцюгів постачання, а не через пошту працівникам [20]. Зіставлення цих епізодів у ширшому огляді підтверджує ту саму нерівномірність [21], [8].

Отже, ланцюг, з якого починається стаття, документований, але не універсальний, і його не слід подавати як типовий сценарій. Водночас у лютому 2025 року зафіксовано кампанію, у якій людський вектор працює вже не проти самого об'єкта, а проти його постачальника: цільова активність кластера UAC-0212 проти розробників і постачальників рішень АСУ ТП тривала з липня 2024 до лютого 2025 року і починалася з документа з посиланням, що вів до завантаження файла-ярлика і запуску команд інтерпретатора [22]. Це той самий ланцюг, зміщений на один крок назад по ланцюгу постачання, і для оператора об'єкта він небезпечніший, бо приходить із довіреного джерела.

Що змінив генеративний штучний інтелект

Зміна стосується не самої можливості обману, а його собівартості й масштабу. Експериментальні дані показують, що листи, згенеровані великою мовною моделлю, дають показники переходу в межах від тридцяти до сорока чотирьох відсотків проти шістдесяти дев'яти — сімдесяти дев'яти для листів, складених за експертною методикою, тобто поступаються людині-експертові, але досягають цього без її участі [23]. Повністю автоматизовані кампанії, у яких модель самостійно виконує розвідку і складає повідомлення, дали п'ятдесят чотири відсотки переходів проти дванадцяти в контрольній групі, а зібрані моделлю розвідувальні дані виявилися придатними у вісімдесяти восьми відсотках випадків [24]. Можливість генерувати шахрайські повідомлення зберігається і в комерційних моделях із фільтрами [25], а окреме дослідження латерального фішингу з уже скомпрометованого внутрішнього облікового запису описує саме ту фазу, що передує виходу до технологічного сегмента [26]. Європейський огляд додає до цього оцінку поширення, запозичену ним із галузевого джерела: понад вісімдесят відсотків фішингових листів, виявлених з вересня 2024 до лютого 2025 року, тією чи іншою мірою створено із залученням моделей [15].

Український матеріал дає задокументований випадок такого поєднання. У липні 2025 року органам виконавчої влади надійшли листи зі скомпрометованої поштової скриньки нібито від представника профільного міністерства, з вкладенням, що маскувалося під додаток у форматі архіву, а виконуваний файл використовував велику мовну модель для формування команд [27]. Собівартість підготовки такого



листа наближається до нуля, тоді як обізнаність персоналу лишилася на попередньому рівні, і саме ця асиметрія, а не поява нового класу атак, становить зміну. Наслідок для виявлення полягає в тому, що окремий класифікатор перестає бути достатнім: рішення доводиться будувати на накопиченні слабких ознак різної природи з явними вагами і порогом, як це запропоновано в попередній роботі автора щодо підтримки прийняття рішень проти впливів, підсиленних моделями [28].

При цьому глобальний звіт фіксує і зміщення каналу: мобільні вектори дають на сорок відсотків вищу медіанну успішність переходу порівняно з поштою, а медіанний зловмисник застосовував допомогу моделей у п'ятнадцяти задокументованих техніках [14]. Людський вектор не згортається — він переміщується туди, де навчання персоналу традиційно не проводиться взагалі.

Чому навчання не закриває вектор

Це місце в аргументі найнезручніше, бо суперечить усталеній практиці. Найбільше польове дослідження такого роду охопило близько чотирнадцяти тисяч працівників упродовж п'ятнадцяти місяців і показало, що вбудоване навчання в момент помилки не дає покращення, а за окремими показниками погіршує результат [29]. Рандомізоване дослідження на близько дев'ятнадцяти тисячах п'ятистах особах упродовж восьми місяців дало статистично нікчемний ефект навчання [30]. Профільний огляд підготовки персоналу для захисту КІ незалежно фіксує, що наявні програми не враховують галузевої специфіки і будуються на загальнокорпоративних сценаріях [9].

З цього не випливає, що навчання зайве. З цього випливає, що обізнаність не є захисним заходом у тому сенсі, у якому ним є сегментація мережі: вона знижує ймовірність помилки, але не змінює наслідків, які настають після неї. Перехід від обізнаності до керування людськими ризиками, обґрунтований в українській літературі [6], означає на практиці облік категорій персоналу за критичністю функцій, диференційовані права доступу і технічні бар'єри, розраховані на те, що помилка станеться. Настанова з безпеки операційних технологій прямо називає підготовку персоналу критичною частиною запобігання інцидентам саме щодо загроз соціальної інженерії і перелічує ролі, для яких вона має бути диференційованою, серед них — оператори, інженери, персонал технічного обслуговування і сторонні постачальники [13].

Пропонована норма

Національне регулювання цю ланку покриває лише частково. Загальні вимоги з кіберзахисту об'єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19 червня 2019 року № 518 у редакції постанови від 13 листопада 2025 року № 1470, зобов'язують суб'єктів організовувати регулярне навчання співробітників з питань кіберзахисту, диференційоване залежно від функціональних обов'язків і професійної кваліфікації, проте диференціюють його за посадою, а не за тим, чи відкриває робоче місце шлях до технологічного сегмента, не поширюють його на працівників підрядників і постачальників та не вимагають заходів, що обмежують наслідки помилки незалежно від результатів навчання [31]. Європейське законодавство таку вимогу вже містить: директива про стійкість критичних суб'єктів вимагає належного управління безпекою персоналу, зокрема визначення категорій персоналу, що виконує критичні функції, встановлення прав доступу і вимог до підготовки, а також підвищення обізнаності персоналу з обов'язковим урахуванням працівників зовнішніх постачальників послуг [32]; директива про високий спільний рівень кібербезпеки закріплює обов'язкове навчання членів керівних органів і відносить кіберігієну та навчання до заходів управління ризиками [33].

При цьому пряме перенесення європейських формулювань не є достатнім, оскільки жодне з них не прив'язує підготовку до межі технологічного сегмента, а саме на цій межі виникають наслідки, заради яких стаття написана. Пропонується доповнити пункт 9 Загальних вимог з кіберзахисту об'єктів критичної інфраструктури абзацом другим такого змісту:

«Суб'єкти визначають перелік категорій персоналу, службові обов'язки яких передбачають доступ до систем, з яких технічно можливий перехід до сегмента автоматизованих систем керування технологічними процесами, включно з працівниками підрядників та постачальників послуг і обладнання. Для кожної визначеної категорії суб'єкти встановлюють диференційовані вимоги до навчання з протидії соціальній інженерії, порядок перевірки готовності не рідше одного разу на рік та технічні заходи, які обмежують наслідки помилкової дії працівника незалежно від результатів такої перевірки. Результативність навчання оцінюється за показниками, що не зводяться до частки виявлених навчальних повідомлень, і підлягає перегляду у разі зміни каналів доставки повідомлень, зокрема переходу на месенджери та голосові канали».

Норма складена так, щоб її виконання не залежало від результативності навчання: обов'язок встановити технічні заходи, які обмежують наслідки помилки, діє незалежно від того, наскільки добре персонал проходить перевірку. Це і є перенесення висновку попереднього підрозділу в нормативну форму.

**ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ**

Чотирикратна розбіжність між незалежними обліками початкового доступу не є суперечністю даних. Укладачі рахують різні одиниці — завершені компрометації, спостережені спроби вторгнення і зареєстровані інциденти, — а показник, що описує одну з цих одиниць, механічно змінює значення при перенесенні на іншу. Зведення до спільної одиниці за коефіцієнтами переходу, які подає сам європейський огляд, дає для фішингу шістнадцять і дві десяті відсоткового пункту проти шістнадцяти відсотків у глобальному звіті, і цей збіг, отриманий на двох масивах, зібраних різними організаціями за різними методиками, є основним кількісним результатом роботи.

Залишковий розрив припадає не на фішинг, а на експлуатацію вразливостей, і пояснюється він складом вибірок, адже глобальний масив зважений на комерційний сектор із широким периметром мережевих пристроїв. Звідси впливає орієнтир, що не збігається з жодним із трьох заголовкових чисел: оператор об'єкта критичної інфраструктури має планувати захист за показником участі людського елемента, який становить шістдесят два відсотки і зростає, а не за часткою фішингу як окремого патерну.

Ланцюг ураження через людину документований, проте не універсальний. Подавати його як типовий сценарій було б помилкою: з чотирьох розглянутих українських епізодів лише в найранішому він простежений від листа до знеструмлення, у кампанії 2022 року вектор входу публічно не розкрито, у кампанії 2024 року він пролягав через ланцюги постачання, а в найсвіжішій зміщений на розробників і постачальників рішень АСУ ТП. Генеративні моделі змінили тут собівартість першої ланки і канал доставки, не змінивши решти.

Обізнаність персоналу за двома незалежними польовими дослідженнями, що разом охопили понад тридцять три тисячі працівників, не дає вимірюваного захисного ефекту і не може лишатися основним заходом на цій ділянці. Запропоноване доповнення до пункту 9 Загальних вимог з кіберзахисту об'єктів критичної інфраструктури переносить центр ваги з навчання як такого на облік категорій персоналу за критичністю функцій та на технічні заходи, розраховані на те, що помилка станеться попри будь-яку підготовку.

Подальші розвідки доцільно спрямувати передусім на емпіричну оцінку піддатливості операторів АСУ ТП, оскільки всі наявні дані здобуто на загальній популяції користувачів, а перенесення їх на персонал об'єктів критичної інфраструктури лишається аргументованим припущенням. Потрібним є й вимірювання переходу між ланками ланцюга, якого не виконує жоден із трьох розглянутих обліків. Окремій роботі вимагають голосові канали та месенджери як вектор проти чергового персоналу, для яких сьогодні немає ні статистики, ні методики перевірки.

ДЕКЛАРАЦІЯ ПРО ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Під час підготовки рукопису автор використовував систему генеративного штучного інтелекту Claude (Anthropic; моделі сімейства Claude Opus, вересень 2026 року) для пошуку джерел і перевірки їхніх реквізитів, зв'язання числових даних із першоджерелами, підготовки й редагування чернетки тексту та оформлення рукопису за шаблоном журналу. Кожне джерело, числове значення, розрахунок і формулювання пропонованої норми автор перевіряв за першоджерелами й затвердив особисто, а задум дослідження та остаточні наукові висновки належать авторові. Система штучного інтелекту не цитується як джерело і не є співавтором, відповідальність за зміст статті повністю несе автор.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lee, R. M., Assante, M. J., & Conway, T. (2016). *Analysis of the cyber attack on the Ukrainian power grid: Defense use case*. Electricity Information Sharing and Analysis Center; SANS ICS. <https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf>
2. Штонда, Р., Черниш, Ю., Терещенко, Т., Терещенко, К., Цикало, Ю., & Поліщук, С. (2024). Класифікація та методи виявлення фішингових атак. *Кібербезпека: освіта, наука, техніка*, 4(24), 69–80. <https://doi.org/10.28925/2663-4023.2024.24.6980>
3. Опірський, І., Сікорський, Р., & Мартинюк, Д. (2025). Аналіз ефективності двофакторної автентифікації та людського фактора у кібербезпеці. *Кібербезпека: освіта, наука, техніка*, 4(28), 413–434. <https://doi.org/10.28925/2663-4023.2025.28.853>



4. Кожедуб, Ю., Крамська, Ю., & Гирда, В. (2020). Аналіз впливу людського фактору на кіберфізичну систему. *Information Technology and Security*, 8(1), 102–115. <https://doi.org/10.20535/2411-1031.2020.8.1.218013>
5. Костюк, Ю., Складанний, П., Рзаєва, С., Самойленко, Ю., & Коршун, Н. (2025). Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid. *Кібербезпека: освіта, наука, техніка*, 2(30), 125–156. <https://doi.org/10.28925/2663-4023.2025.30.956>
6. Козубцова, Л., Ліщина, В., & Козубцов, І. (2025). Від обізнаності до управління: концепція людських ризиків в системі кіберзахисту. *Кібербезпека: освіта, наука, техніка*, 2(30), 360–373. <https://doi.org/10.28925/2663-4023.2025.30.895>
7. Nifakos, S., Chandramouli, K., & Stathakarou, N. (2025). Social engineering: The human behavior impact in cyber security within critical information infrastructures. In N. Pitropakis & S. Katsikas (Eds.), *Security and privacy in smart environments* (pp. 173–184). Springer. https://doi.org/10.1007/978-3-031-66708-4_8
8. Abraham, D., Houmb, S. H., & Erdodi, L. (2025). Cyber-attacks on energy infrastructure — A literature overview and perspectives on the current situation. *Applied Sciences*, 15(17), Article 9233. <https://doi.org/10.3390/app15179233>
9. Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, 40, Article 100361. <https://doi.org/10.1016/j.cosrev.2021.100361>
10. Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human-Computer Studies*, 125, 19–31. <https://doi.org/10.1016/j.ijhcs.2018.12.004>
11. Sommestad, T., & Karlzén, H. (2019). A meta-analysis of field experiments on phishing susceptibility. In *2019 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1–14). IEEE. <https://doi.org/10.1109/eCrime47957.2019.9037502>
12. ESET Research. (2022, April 12). Industroyer2: Industroyer reloaded. *WeLiveSecurity*. <https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/>
13. Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). *Guide to operational technology (OT) security* (NIST Special Publication 800-82 Rev. 3). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-82r3>
14. Verizon. (2026). *2026 data breach investigations report* (19th ed.). Verizon Business. <https://www.verizon.com/business/resources/T1f0/reports/2026-dbir-data-breach-investigations-report.pdf>
15. European Union Agency for Cybersecurity. (2025). *ENISA threat landscape 2025*. https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf
16. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. (2025). *Російські кібероперації: аналітика за I півріччя 2025*. Держспецзв'язку. <https://cip.gov.ua/services/cm/api/attachment/download?id=71278>
17. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. (2026). *Кіберзагрози: Україна. Аналітика за II півріччя 2025*. Держспецзв'язку. <https://cip.gov.ua/services/cm/api/attachment/download?id=74645>
18. European Union Agency for Cybersecurity. (2026). *ENISA threat landscape 2026*. https://www.enisa.europa.eu/sites/default/files/2026-09/ENISA%20Threat%20Landscape%202026_Final.pdf
19. CERT-UA. (2022, 12 квітня). *Кібератака групи Sandworm (UAC-0082) на об'єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435)*. <https://cert.gov.ua/article/39518>
20. CERT-UA. (2024, 19 квітня). *Плани UAC-0133 (Sandworm) щодо кібердиверсії на майже 20 об'єктах критичної інфраструктури України*. <https://cert.gov.ua/article/6278706>
21. Kozak, P., Klaban, I., & Šlajs, T. (2023). Industroyer cyber-attacks on Ukraine's critical infrastructure. In *2023 International Conference on Military Technologies (ICMT)* (pp. 1–6). IEEE. <https://doi.org/10.1109/ICMT58149.2023.10171308>
22. CERT-UA. (2025, 23 лютого). *Цільова активність UAC-0212 у відношенні розробників та постачальників рішень АСУТП з метою здійснення кібератак на об'єкти критичної інфраструктури України (CERT-UA#13702)*. <https://cert.gov.ua/article/6282517>



23. Heiding, F., Schneier, B., Vishwanath, A., Bernstein, J., & Park, P. S. (2024). Devising and detecting phishing emails using large language models. *IEEE Access*, 12, 42131–42146. <https://doi.org/10.1109/ACCESS.2024.3375882>
24. Heiding, F., Lermen, S., Kao, A., Schneier, B., & Vishwanath, A. (2024). *Evaluating large language models' capability to launch fully automated spear phishing campaigns: Validated on human subjects* (arXiv:2412.00586) [Препринт]. arXiv. <https://doi.org/10.48550/arXiv.2412.00586>
25. Roy, S. S., Thota, P., Naragam, K. V., & Nilizadeh, S. (2024). From chatbots to phishbots?: Phishing scam generation in commercial large language models. In *2024 IEEE Symposium on Security and Privacy (SP)* (pp. 36–54). IEEE. <https://doi.org/10.1109/SP54263.2024.00182>
26. Bethany, M., Galiopoulos, A., Bethany, E., Bahrami Karkevandi, M., Beebe, N., Vishwamitra, N., & Najafirad, P. (2025). Lateral phishing with large language models: A large organization comparative study. *IEEE Access*, 13, 60684–60701. <https://doi.org/10.1109/ACCESS.2025.3555500>
27. CERT-UA. (2025, 17 липня). *Кібератаки UAC-0001 на сектор безпеки та оборони із застосуванням програмного засобу LAMENUG, що використовує LLM (велику мовну модель)* (CERT-UA#16039). <https://cert.gov.ua/article/6284730>
28. Verholias, O. (у друці). Decision support for AI-powered protection against AI-enhanced influence operations targeting safety-critical domains. In *2026 16th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. IEEE.
29. Lain, D., Kostiaenen, K., & Čapkun, S. (2022). Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 842–859). IEEE. <https://doi.org/10.1109/SP46214.2022.9833766>
30. Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., Liu, L., Longhurst, C. A., Dameff, C., Savage, S., & Voelker, G. M. (2025). Understanding the efficacy of phishing training in practice. In *2025 IEEE Symposium on Security and Privacy (SP)* (pp. 37–54). IEEE. <https://doi.org/10.1109/SP61157.2025.00076>
31. Кабінет Міністрів України. (2019). *Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури* (Постанова № 518; у ред. постанови від 13.11.2025 № 1470). <https://zakon.rada.gov.ua/laws/show/518-2019-п>
32. European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. *Official Journal of the European Union*, L 333, 164. <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>
33. European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148. *Official Journal of the European Union*, L 333, 80. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

**Oleksandr O. Verholias**

PhD in Law, Engineer of the Software and Information

Support Division, Information and Computing Centre

Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine

ORCID: 0000-0002-9780-1298

arnijazov@gmail.com

**THE HUMAN VECTOR OF INTRUSION INTO CRITICAL INFRASTRUCTURE FACILITIES:
RECONCILING THREE INDEPENDENT ACCOUNTS OF INITIAL ACCESS**

Abstract. The paper addresses one specific mechanism by which critical infrastructure facilities are damaged: the one in which intrusion starts with a member of staff and ends with interference in the technological segment. The problem behind the study is not a shortage of publications but the absence of any overlap between two existing bodies of literature. Ukrainian work on critical infrastructure describes facilities, threats and legal regimes, while work on social engineering and phishing describes user behaviour outside any sectoral context, and the employee through whom entry into an energy facility actually occurs falls out of both. The introduction shows that this gap carries a practical rather than a bibliographic cost: protective measures are designed either for the technological perimeter or for the office user, and the seam between them is left without an owner. The theoretical basis of the study reconstructs the damage chain as a sequence of four links — influence on the employee, acquisition of initial access, lateral movement to the boundary of the technological segment, and interference in control — and records that each link has its own statistics, its own set of protective measures and its own research literature, while the transition between links is described nowhere. The research methodology consists in reconciling three independent accounts of initial access over partially overlapping observation windows: the global Verizon Data Breach Investigations Report, the European ENISA Threat Landscape, and the semi-annual analytics of the State Cyber Protection Centre of Ukraine. The results comprise four parts. The first records the divergence: the share attributed to social engineering ranges across the three accounts from sixteen to sixty per cent, and these figures do not reconcile by direct comparison. The second explains the divergence through four methodological differences, the principal one concerning the unit of account, and presents a recalculation that converts the European distribution into the same unit as the global one and shows that the residual gap falls not on phishing but on the exploitation of vulnerabilities. The third examines the reproducibility of the chain on Ukrainian material, where the documented episode of 2015 is set against later campaigns in which the entry vector was different or was never disclosed. The fourth assesses what generative artificial intelligence has actually changed in this chain, and why raising staff awareness does not close the vector according to the available experimental evidence. The verbatim text of a proposed addition to paragraph 9 of the General Requirements for Cyber Protection of Critical Infrastructure Facilities is given in the results, and the conclusions set out directions for further research, among them the transfer of susceptibility-to-persuasion estimates from the general population to operators of industrial control systems.

Keywords: critical infrastructure; social engineering; initial access; phishing; industrial control systems; human vector; cyber protection; generative artificial intelligence.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Lee, R. M., Assante, M. J., & Conway, T. (2016). *Analysis of the cyber attack on the Ukrainian power grid: Defense use case*. Electricity Information Sharing and Analysis Center; SANS ICS. <https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf>
2. Shtonda, R., Chernish, Yu., Tereshchenko, T., Tereshchenko, K., Tsykalo, Yu., & Polishchuk, S. (2024). Classification and methods of detection of phishing attacks. *Cybersecurity: Education, Science, Technique*, 4(24), 69–80. <https://doi.org/10.28925/2663-4023.2024.24.6980>
3. Opirskyy, I., Sikorskyi, R., & Martyniuk, D. (2025). Analysis of the effectiveness of two-factor authentication and the human factor in cybersecurity. *Cybersecurity: Education, Science, Technique*, 4(28), 413–434. <https://doi.org/10.28925/2663-4023.2025.28.853>



4. Kozhedub, Yu., Kramka, Yu., & Hyrda, V. (2020). Analysis of the human factor influence on the cyber-physical system. *Information Technology and Security*, 8(1), 102–115. <https://doi.org/10.20535/2411-1031.2020.8.1.218013>
5. Kostiuk, Yu., Skladannyi, P., Rzaieva, S., Samoilenko, Yu., & Korshun, N. (2025). Intelligent control and security systems in cyber-physical and cloud environments of Smart Grid. *Cybersecurity: Education, Science, Technique*, 2(30), 125–156. <https://doi.org/10.28925/2663-4023.2025.30.956>
6. Kozubtsova, L., Lishchyna, V., & Kozubtsov, I. (2025). From awareness to management: The concept of human risks in cyber security systems. *Cybersecurity: Education, Science, Technique*, 2(30), 360–373. <https://doi.org/10.28925/2663-4023.2025.30.895>
7. Nifakos, S., Chandramouli, K., & Stathakarou, N. (2025). Social engineering: The human behavior impact in cyber security within critical information infrastructures. In N. Pitropakis & S. Katsikas (Eds.), *Security and privacy in smart environments* (pp. 173–184). Springer. https://doi.org/10.1007/978-3-031-66708-4_8
8. Abraham, D., Houmb, S. H., & Erdodi, L. (2025). Cyber-attacks on energy infrastructure — A literature overview and perspectives on the current situation. *Applied Sciences*, 15(17), Article 9233. <https://doi.org/10.3390/app15179233>
9. Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, 40, Article 100361. <https://doi.org/10.1016/j.cosrev.2021.100361>
10. Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human-Computer Studies*, 125, 19–31. <https://doi.org/10.1016/j.ijhcs.2018.12.004>
11. Sommestad, T., & Karlzén, H. (2019). A meta-analysis of field experiments on phishing susceptibility. In *2019 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1–14). IEEE. <https://doi.org/10.1109/eCrime47957.2019.9037502>
12. ESET Research. (2022, April 12). Industroyer2: Industroyer reloaded. *WeLiveSecurity*. <https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/>
13. Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). *Guide to operational technology (OT) security* (NIST Special Publication 800-82 Rev. 3). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-82r3>
14. Verizon. (2026). *2026 data breach investigations report* (19th ed.). Verizon Business. <https://www.verizon.com/business/resources/T1f0/reports/2026-dbir-data-breach-investigations-report.pdf>
15. European Union Agency for Cybersecurity. (2025). *ENISA threat landscape 2025*. https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf
16. State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine. (2025). *Russian cyber operations: Analytics for the first half of 2025*. SSSCIP. <https://cip.gov.ua/services/cm/api/attachment/download?id=71278>
17. State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine. (2026). *Cyber threats: Ukraine. Analytics for the H2 2025*. SSSCIP. <https://cip.gov.ua/services/cm/api/attachment/download?id=74646>
18. European Union Agency for Cybersecurity. (2026). *ENISA threat landscape 2026*. https://www.enisa.europa.eu/sites/default/files/2026-09/ENISA%20Threat%20Landscape%202026_Final.pdf
19. CERT-UA. (2022, April 12). *Sandworm (UAC-0082) cyberattack on Ukrainian energy facilities using INDUSTROYER2 and CADDYWIPER malware (CERT-UA#4435)*. <https://cert.gov.ua/article/39518>
20. CERT-UA. (2024, April 19). *UAC-0133 (Sandworm) plans for cyber sabotage at almost 20 critical infrastructure facilities of Ukraine*. <https://cert.gov.ua/article/6278706>
21. Kozak, P., Klaban, I., & Šlajs, T. (2023). Industroyer cyber-attacks on Ukraine's critical infrastructure. In *2023 International Conference on Military Technologies (ICMT)* (pp. 1–6). IEEE. <https://doi.org/10.1109/ICMT58149.2023.10171308>
22. CERT-UA. (2025, February 23). *Targeted activity of UAC-0212 against developers and suppliers of ICS solutions aimed at cyberattacks on critical infrastructure facilities of Ukraine (CERT-UA#13702)*. <https://cert.gov.ua/article/6282517>
23. Heiding, F., Schneier, B., Vishwanath, A., Bernstein, J., & Park, P. S. (2024). Devising and detecting phishing emails using large language models. *IEEE Access*, 12, 42131–42146. <https://doi.org/10.1109/ACCESS.2024.3375882>



24. Heiding, F., Lermen, S., Kao, A., Schneier, B., & Vishwanath, A. (2024). *Evaluating large language models' capability to launch fully automated spear phishing campaigns: Validated on human subjects* (arXiv:2412.00586) [Preprint]. arXiv. <https://doi.org/10.48550/arXiv.2412.00586>
25. Roy, S. S., Thota, P., Naragam, K. V., & Nilizadeh, S. (2024). From chatbots to phishbots?: Phishing scam generation in commercial large language models. In *2024 IEEE Symposium on Security and Privacy (SP)* (pp. 36–54). IEEE. <https://doi.org/10.1109/SP54263.2024.00182>
26. Bethany, M., Galiopoulos, A., Bethany, E., Bahrami Karkevandi, M., Beebe, N., Vishwamitra, N., & Najafirad, P. (2025). Lateral phishing with large language models: A large organization comparative study. *IEEE Access*, 13, 60684–60701. <https://doi.org/10.1109/ACCESS.2025.3555500>
27. CERT-UA. (2025, July 17). *UAC-0001 cyberattacks on the security and defence sector using the LAMEHUG software that employs an LLM (large language model) (CERT-UA#16039)*. <https://cert.gov.ua/article/6284730>
28. Verholias, O. (in press). Decision support for AI-powered protection against AI-enhanced influence operations targeting safety-critical domains. In *2026 16th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. IEEE.
29. Lain, D., Kostiaainen, K., & Čapkun, S. (2022). Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 842–859). IEEE. <https://doi.org/10.1109/SP46214.2022.9833766>
30. Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., Liu, L., Longhurst, C. A., Dameff, C., Savage, S., & Voelker, G. M. (2025). Understanding the efficacy of phishing training in practice. In *2025 IEEE Symposium on Security and Privacy (SP)* (pp. 37–54). IEEE. <https://doi.org/10.1109/SP61157.2025.00076>
31. Cabinet of Ministers of Ukraine. (2019). *On approval of the General requirements for cyber protection of critical infrastructure facilities* (Resolution No. 518, as amended by Resolution No. 1470 of 13 November 2025). <https://zakon.rada.gov.ua/laws/show/518-2019-п>
32. European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. *Official Journal of the European Union*, L 333, 164. <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>
33. European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148. *Official Journal of the European Union*, L 333, 80. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

Отримано редакцією журналу / Received: 07.06.26

Прорецензовано / Revised: 22.07.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.