**Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»
Національна бібліотека України імені В. І. Вернадського**

# КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

## № 6 (червень)

**Київ – 2026**

**Кібербезпека в інформаційному суспільстві:** Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. К., 2026. № 6 (червень). 115 с.

Заснований Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Національною бібліотекою України імені В.І. Вернадського у 2017 р. Видається щомісяця. Відповідальний редактор О. Довгань. Упорядники О. Довгань, Л. Литвинова, С. Дорогих. Дизайн обкладинки С. Дорогих.

Аналітичний дайджест покликаний надати інформацію з питань кібербезпеки, що є надзвичайно актуальними в контексті розвитку інформаційного суспільства, зростання кіберзлочинності, використання засобів кібертероризму у гібрідних війнах та необхідності розбудови системи забезпечення кібернетичної безпеки України відповідно до визначених стратегічних напрямків з урахуванням тенденцій розвитку кіберпростору, сучасних викликів та загроз його безпеці. Призначення дайджесту – ознайомлення широкого кола фахівців у сфері кібербезпеки, а також і всіх користувачів, які цікавляться цією проблематикою, з інформаційними джерелами мережі Інтернет та новими надходженнями до фондів НБУВ (монографії, автореферати дисертацій, підручники, збірники наукових праць, матеріали міжнародних конференцій, статті з періодичних видань), що висвітлюють сучасні проблеми кібербезпеки в Україні та за кордоном.

Ознайомитися з літературою із фондів НБУВ та онлайновими інформаційними ресурсами можна за адресою: проспект Голосіївський, 3, м. Київ, 03039.

# ЗМІСТ

**«Інвестори пильно стежать за майбутніми фінансовими результатами лідерів ринку кібербезпеки — компаній Palo Alto Networks та CrowdStrike — щоб оцінити, чи зможе зберегтися нещодавній підйом у цьому секторі, адже акції обох компаній у 2026 році злетіли приблизно на 60 % і продемонстрували рекордне місячне зростання завдяки ентузіазму, пов'язаному з попитом на технології штучного інтелекту.** Настрої інвесторів різко змінилися порівняно з попередніми побоюваннями, що передові моделі штучного інтелекту, такі як Mythos від Anthropic, можуть спричинити потрясіння в галузі: тепер інвестори розглядають штучний інтелект як рушій зростання попиту на кібербезпеку… Загалом сектор продемонстрував вищі результати: індекс Global X Cybersecurity ETF зріс цього року на 25% і значно випередив інші акції компаній-розробників програмного забезпечення, хоча динаміка є неоднорідною: лідирують великі платформові компанії з сильними позиціями в галузі штучного інтелекту, тоді як менші гравці, такі як Zscaler, Digital Arts і Rapid7, зазнають труднощів через гірші перспективи та конкурентний тиск. Аналітики очікують значного зростання виручки та прибутку як від Palo Alto, так і від CrowdStrike, а нещодавні позитивні результати конкурентів, таких як Fortinet, підвищили очікування, але різке зростання також підвищує ризик фіксації прибутку, навіть якщо прибутки перевищать прогнози. Загалом ринок все більше віддає перевагу домінуючим компаніям у сфері кібербезпеки, які, як вважається, виграють від штучного інтелекту та консолідації галузі, що підкріплює думку про те, що кібербезпека стає все більш важливою у міру розвитку цифрових загроз». ***(Carmen Reinicke. AI Fuels $280 Billion Cybersecurity Rally as Earnings Test Looms // Bloomberg L.P. (https://www.bloomberg.com/news/articles/2026-06-02/palo-alto-crowdstrike-earnings-to-put-37-cyber-rally-to-test?srnd=phx-technology-cybersecurity). 02.06.2026).***

***

**«Сучасна розробка програмного забезпечення значною мірою спирається на екосистеми з відкритим кодом та автоматизовані інструменти, однак це породжує дедалі більші ризики для кібербезпеки, оскільки зловмисники все частіше використовують ланцюги постачання програмного забезпечення для масового розповсюдження шкідливого програмного забезпечення.** Додатки часто залежать від численних сторонніх компонентів, які автоматично завантажуються через конвеєри CI/CD, а в таких мовах, як Node.js, Python та Rust — де залежність від зовнішніх пакетів є високою — навіть одна скомпрометована залежність може швидко поширити шкідливий код на багато систем. Недавні атаки, такі як інцидент «Mini Shai-hulud» у травні 2026 року, демонструють, як зловмисники використовують надійні середовища розробників, автоматизацію та моделі відкритого публікування для поширення шкідливого програмного забезпечення, часто залишаючись непоміченими протягом тривалого часу. Поширені тактики включають компрометацію облікових записів адміністраторів, захоплення покинутих пакетів, використання типосквоттингу для обману розробників та ланцюгові атаки за допомогою викрадених облікових даних…

Ці ризики посилюються через слабкі механізми контролю в середовищах розробки, сліпу довіру до автоматизації та непослідовне застосування заходів безпеки, таких як багатофакторна автентифікація. Щоб оцінити ступінь ризику, організації повинні проводити аудит залежностей, відстежувати незвичайну поведінку системи, сканувати на наявність відомих вразливостей та перевіряти на наявність несанкціонованого доступу до облікових записів розробників або реєстрів, одночасно ведучи чіткий облік залежностей, наприклад, у вигляді специфікації програмного забезпечення. Негайні заходи щодо зменшення ризику включають призупинення автоматичних оновлень, ручну перевірку нових залежностей, ротацію облікових даних, впровадження MFA (багатофакторна автентифікація) та використання надійних або приватних реєстрів… У довгостроковій перспективі організаціям слід посилити безпеку циклу розробки, контролюючи процес додавання та оновлення залежностей, знаходячи баланс між швидким випуском виправлень та обережним впровадженням, забезпечуючи захист облікових даних та гарантуючи, що розгортання відбувається через контрольовані конвеєри. Загалом, у міру ускладнення атак на ланцюг постачання програмного забезпечення, організації повинні впроваджувати проактивне управління, посилені заходи контролю та постійний моніторинг для управління ризиками, притаманними сучасним екосистемам розробки». ***(Jack F. Software supply chain attacks: check your dependencies // National Cyber Security Centre (NCSC) (https://www.ncsc.gov.uk/blogs/software-supply-chain-attacks-check-your-dependencies). 04.06.2026).***

***

**«Згідно з новими даними компанії ALSO Group, кібербезпека перетворилася на одну з найприбутковіших і найбільш масштабованих сфер, що забезпечують постійний дохід у технологічному каналі, що зумовлено ситуацією, коли організації щотижня стикаються в середньому з понад 2 000 кібератак.** Однак багато постачальників керованих послуг (MSP) не реалізують цей комерційний потенціал у повній мірі, оскільки розглядають кібербезпеку як традиційний одноразовий продаж обладнання або проектний продаж, що призводить до фрагментованого впровадження рішень та нестабільних доходів… Щоб скористатися цим попитом, Марк Епплтон, керівник відділу розвитку екосистеми постачальників у ALSO Group, закликає MSP перейти до платформоорієнтованих моделей безпеки, об'єднуючи такі інструменти, як захист кінцевих точок, безпека ідентифікації та виявлення загроз, у єдині послуги з постійного управління… Постачальники технологій відіграють вирішальну роль у цьому переході, допомагаючи MSP формувати пакети цих послуг, інтегрувати платформи та будувати стійкі, масштабовані бізнес-моделі, забезпечуючи, щоб успішні MSP мислили як комплексні постачальники послуг, а не як прості реселери, з метою забезпечення довгострокових відносин із клієнтами та передбачуваних доходів». ***(Neil Trim. Cybersecurity presents the most profitable channel opportunity of for the decade, says ALSO // Kingswood Media (https://technologyreseller.uk/cybersecurity-presents-the-most-profitable-channel-opportunity-of-for-the-decade-says-also/). 04.06.2026).***

***

**«Як зазначили провідні фахівці з кібербезпеки, які виступили на конференції Infosecurity Europe 2026, хоча ймовірність кібератак дедалі зростає, пов'язана з ними шкода для репутації компанії та добробуту її співробітників не є неминучою.** Ключ до мінімізації цієї шкоди полягає у наявності чіткого та практичного плану дій з кризових комунікацій ще до того, як трапиться інцидент…

За словами Ніколи Хадсон, колишньої директорки британського NCSC, ефективний план дій — це не стосторінковий документ, а документ, що зосереджується на трьох основних компонентах: визначенні типу кризи, розумінні того, хто має бути присутнім у оперативному штабі, та забезпеченні того, щоб усі розуміли свої обов'язки для зміцнення довіри та уникнення хаосу. Ця структура є критично важливою, оскільки, як зазначив колишній керівник служби інформаційної безпеки Jaguar Land Rover Ашіш Шреста, посібники виявляються неефективними, коли реальність відхиляється від сценарію, а керівники змушені приймати рішення під величезним тиском, маючи лише фрагментарну інформацію…

Експерти наголосили, що управління кіберінцидентом — це завдання, пов'язане з людським фактором, а не лише технічне. Успішне реагування залежить від заздалегідь визначеного процесу, який визначає, хто що і як робить, особливо в плані комунікації. Замість того, щоб покладатися на заздалегідь підготовлені заяви, які швидко втрачають актуальність, посібник повинен бути «живим» та гнучким керівництвом. Важливо, що цей підхід, орієнтований на людину, повинен поширюватися і на саму команду реагування. Шреста підкреслив необхідність розглядати реагування на інцидент як «ультрамарафон», передбачаючи обов'язкові перерви, харчування та відпочинок для персоналу, щоб запобігти вигоранню та зберегти стійкість протягом тривалої кризи». ***(Danny Palmer. Infosecurity Europe: How Businesses Can Prepare for a Cybersecurity Crisis with Effective Plans // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/infosecurity-europe-cybersecurity/). 04.06.2026).***

***

**«На сьогодні на цифрову торгівлю припадає приблизно чверть світового товарообігу, і її обсяги продовжують зростати, оскільки цифрові технології знижують витрати та прискорюють транскордонні потоки товарів, послуг і капіталу.** Однак ця зростаюча взаємозалежність породжує нові системні вразливості, оскільки геополітична фрагментація, політика цифрового суверенітету та розбіжності в нормативно-правових актах ускладнюють ситуацію, а кіберзагрози стають дедалі витонченішими. Прогрес у сфері штучного інтелекту посилює цю динаміку, оскільки він не тільки уможливлює швидші та масштабніші атаки, а й стає важливим інструментом захисту, перетворюючи кібербезпеку на критично важливе економічне та геополітичне питання, а не лише на технічну проблему…

Сучасна світова торгівля спирається на взаємопов'язану цифрову інфраструктуру — таку як хмарні платформи, логістичні системи, платіжні мережі та підводні кабелі — яка стає дедалі більш концентрованою та вразливою до зривів у роботі. Кібератаки в поєднанні з геополітичною напруженістю можуть

спричинити ланцюгові наслідки у ланцюгах постачання та фінансових системах, через що операційна стійкість стає не менш важливою, ніж профілактика. Водночас роздробленість нормативно-правових систем у різних юрисдикціях ускладнює дотримання вимог та послаблює узгоджені зусилля з безпеки, а поява окремих регіональних технологічних екосистем додає додаткових витрат та ускладнює діяльність транснаціональних організацій…

У цих умовах стійкість більше не можна забезпечувати в ізоляції. Ефективна кібербезпека сьогодні залежить від співпраці між урядами, бізнесом та регуляторними органами, що включає обмін інформацією, механізми скоординованого реагування та сумісні стандарти. Торговельні угоди та цифрові партнерства починають враховувати ці елементи, прагнучи скоріше узгодження, ніж повної гармонізації. Зрештою, кібербезпека стає ключовим компонентом економічної стратегії: здатність підтримувати надійну та стійку цифрову інфраструктуру й швидко відновлюватися після зривів у роботі дедалі більше визначатиме конкурентоспроможність у фрагментованій світовій економіці». ***(Apisada Suwansukroj, Don Rodney Junio. Why cyber resilience is a foundation for global trade // World Economic Forum (https://www.weforum.org/stories/2026/06/why-cyber-resilience-foundation-global-trade/). 02.06.2026).***

***

**«Рівень зрілості кібербезпеки переріс рамки суто технічного захисту і тепер є ключовим показником загальної операційної стійкості компанії та її здатності управляти змінами.** У сучасному середовищі ризиків, де площі атаки розширюються, а штучний інтелект посилює можливості як захисників, так і зловмисників, стан кібербезпеки компанії відображає, наскільки добре вона розуміє свої системи, регулює доступ та реагує на тиск…

Ця стійкість найяскравіше випробовується в періоди значних змін та зовнішнього контролю. Слабкі місця в неформальних системах контролю, заснованих на «племінних знаннях», стають особливо помітними під час злиттів і поглинань, ретельних аудитів та поновлення кіберстрахування. Ці події змушують компанію довести, що вона має формальні, повторювані та задокументовані процеси для таких критично важливих функцій, як контроль доступу, право власності на активи та усунення вразливостей. Впровадження штучного інтелекту ще більше прискорює цей процес перевірки, оскільки воно швидко виявляє будь-які існуючі слабкі місця в управлінні даними та ідентифікацією в компанії…

Справді стійка організація — це така, в якій відповідальність за кіберризики виходить за межі ІТ-відділу й поширюється на юридичний, кадровий, фінансовий та операційний підрозділи. Роль керівника ІТ-відділу полягає в тому, щоб зробити ризики видимими, підданими розподілу та такими, що вимагають вжиття заходів, змістивши акцент із повного усунення ризиків на їх цілеспрямоване управління. Зрештою, компанії, які розглядають кібербезпеку як ключовий показник стійкості бізнесу, будуть готові до майбутніх викликів, тоді як ті, хто сприймає її як суто технічну функцію, залишатимуться в реактивному та вразливому стані». ***(Thai Vong. Cybersecurity maturity is now a proof point for resilience // FoundryCo, Inc.***

***(https://www.cio.com/article/4180872/cybersecurity-maturity-is-now-a-proof-point-for-resilience.html). 04.06.2026).***

***

**«Малі та середні підприємства (МСП) зараз змушені відійти від реактивного підходу до кібербезпеки та впроваджувати стратегії корпоративного рівня для досягнення операційної зрілості, перетворюючи безпеку з центру витрат на фактор зростання.** Це передбачає впровадження комплексу передових принципів, що забезпечить стійкість, масштабованість та готовність до аудиту. Ключовою серед цих стратегій є впровадження архітектури «нульової довіри», яка розглядає ідентичність як новий периметр безпеки та базується на постійній верифікації, багатофакторній аутентифікації та сегментації мережі. Це доповнюється рішеннями з ідентифікації, виявлення загроз та реагування (ITDR) для моніторингу поведінки користувачів навіть після аутентифікації…

Для підвищення операційної ефективності малим та середнім підприємствам слід інтегрувати рішення розширеного виявлення та реагування (EDR) з платформами SIEM та SOAR, щоб забезпечити централізований огляд та автоматизоване реагування, які можна перевіряти та вдосконалювати за допомогою регулярних симуляцій. Серед інших важливих підходів — безперервне управління вразливостями (Continuous Exposure Management), яке надає цілісне уявлення про всі активи організації для визначення пріоритетності та усунення ризиків, а також управління станом безпеки SaaS (SSPM), що гарантує безпечну конфігурацію хмарних додатків. Для команд, що розширюються, також важливо впроваджувати принципи DevSecOps шляхом інтеграції сканування безпеки на ранніх етапах розробки. Щоб забезпечити необхідні інвестиції для цих заходів, IT-керівники повинні представити переконливий бізнес-кейс, який розглядає безпеку не як технічні витрати, а як стратегічну ініціативу, що управляє ризиками, захищає доходи та формує довіру клієнтів». ***(Nathan Eddy. SMB Cybersecurity: Going Beyond the Basics To Build a Resilient and Scalable Security Framework // CDW LLC (https://biztechmagazine.com/article/2026/06/smb-cybersecurity-going-beyond-basics-build-resilient-and-scalable-security-framework-perfcon). 04.06.2026).***

***

**«Керівники служб інформаційної безпеки (CISO) у сфері вищої освіти стикаються зі значними труднощами у забезпеченні достатнього фінансування заходів з кібербезпеки, часто маючи справу з федеративними IT-системами, кадровими обмеженнями та складністю кількісної оцінки ефективності заходів безпеки.** Як наслідок, багато навчальних закладів діють у режимі реагування, що підвищує їхню вразливість до програм-вимагачів та витоків даних, збитки від яких у 2024 році в освітньому секторі становили в середньому 3,5 мільйона доларів за кожен інцидент. Щоб подолати ці перешкоди та перетворити кібербезпеку з адміністративних витрат на стратегічну необхідність, керівники служб інформаційної безпеки повинні залучати керівництво університетів через постійне спрощене навчання та стратегічне партнерство з виконавчими

комітетами… Найголовніше, що CISO повинні перекладати складний технічний жаргон на мову бізнесу та фінансів. Замість того, щоб зосереджуватися на конкретних засобах безпеки, їм слід наголошувати на тому, як інвестиції забезпечують безперебійність навчального процесу, цілісність наукових досліджень, довіру студентів та операційну стійкість. Крім того, керівники служб інформаційної безпеки повинні встановити чітке, загальноприйняте визначення поняття «прийнятний ризик» у всій установі та проводити регулярні оцінки ризиків, щоб виявляти вразливі місця, які перевищують цей поріг… Постійно надаючи зрозумілі показники, що ґрунтуються на даних — такі як середній час виявлення та середній час реагування — і чітко пов'язуючи ці цифри з конкретними фінансовими результатами та залишковими ризиками, керівники служб інформаційної безпеки можуть сформувати переконливі та фінансово обґрунтовані аргументи на користь виділення необхідного фінансування на кібербезпеку». ***(Alexander Slagg. Cybersecurity ROI in Higher Education: How To Win the Budget Conversation // CDW LLC (https://edtechmagazine.com/higher/article/2026/06/cybersecurity-roi-higher-education-how-win-budget-conversation-perfcon). 04.06.2026).***

***

**«Глобальне дослідження, проведене компанією Ocorian, вказує на зростання ризиків у сфері кібербезпеки серед сімейних офісів: з'ясувалося, що 43% з них зазнали кібератаки протягом останніх двох років, проте значна частина з них залишається неготовою до таких загроз.** Майже п'ята частина з них не має жодних засобів захисту від кіберзагроз, а 22% не мають плану реагування на інциденти або відновлення, що робить їх вразливими до операційних, фінансових та репутаційних збитків. Хоча 75% нещодавно вжили заходів для посилення своїх захисних систем, багато хто з них все ще стикається з проблемою обмеженої внутрішньої експертизи, причому понад 10% повідомляють про серйозні труднощі з підтриманням належного рівня кібербезпеки…

Як наслідок, зростає залежність від зовнішньої підтримки: майже половина опитаних вже користується послугами зовнішніх консультантів, а 72% планують передати на аутсорсинг більшу частину функцій з кібербезпеки протягом найближчих трьох років, причому 41% очікують на значне збільшення обсягу таких послуг. Ці дані свідчать про те, що кіберзагрози все більше усвідомлюються, але водночас вказують на стійкі прогалини в готовності до них, оскільки сімейні офіси змушені шукати баланс між необхідністю посилення захисту та обмеженими внутрішніми ресурсами». ***(Amanda Cheesley. Family Offices Need To Step Up Cyber Risk Defence – Survey // Clearview Financial Media Ltd (https://www.wealthbriefing.com/html/article.php/family-offices-need-to-step-up-cyber-risk-defence--survey). 04.06.2026).***

***

**«У міру того, як промислові системи, ланцюги постачання та державна інфраструктура стають дедалі більш взаємопов'язаними, кіберризики вже не обмежуються окремими організаціями, а можуть поширюватися на різні**

**сектори, впливаючи на безперебійність бізнесу, критично важливі послуги та навіть національну економіку.** За словами Марко Туліо Мораеса, керівника служби інформаційної безпеки компанії Nexa Resources, ця зміна перетворює кібербезпеку на більш широке завдання щодо забезпечення стійкості та управління, оскільки середовища операційних технологій (ОТ) — часто обмежені застарілими системами, тривалим життєвим циклом активів та обмеженою видимістю — є особливо вразливими до зривів, які можуть широко поширюватися. Традиційні підходи, зосереджені на ізольованих заходах контролю, вже не є достатніми; організації повинні впроваджувати стратегії стійкості на рівні всієї екосистеми, інтегруючи кіберризики в процес прийняття рішень на підприємстві, планування інвестицій та структури управління…

Ключовою проблемою є роздроблена система підзвітності: відповідальність за кіберризики часто розподілена між інженерним, операційним та ІТ-підрозділами, а також зовнішніми партнерами, що супроводжується недостатнім рівнем прозорості на рівні вищого керівництва. Дані свідчать про низьку залученість ради директорів та непослідовну відповідальність за безпеку операційних технологій, що підкреслює прогалини в управлінні, які можуть підірвати стійкість. Мораес стверджує, що організаціям потрібна чіткіша підзвітність, сильніша координація та перехід до управління ризиками на основі сценаріїв, яке враховує, як порушення поширюються між взаємопов'язаними системами. Незалежні механізми забезпечення, такі як зовнішні аудити, також мають вирішальне значення для підтвердження стійкості, що виходить за межі внутрішніх оцінок…

У ширшому сенсі кібербезпека перетворюється на стратегічне питання управління, пов'язане з економічною стабільністю та впливом на суспільство, що вимагає від рад директорів та регуляторних органів переходу від механізмів, орієнтованих на дотримання вимог, до більш динамічного нагляду. У промислових умовах стійкість полягає не лише у відновленні систем, а й у збереженні операційної надійності та здатності приймати рішення в умовах зривів у роботі. Зрештою, у міру зростання рівня взаємопов'язаності ефективність кібербезпеки буде все менше залежати від окремих технічних засобів контролю, а все більше — від якості управління, координації та готовності у складних, взаємозалежних екосистемах». ***(Anna Ribeiro. Industrial cyber risk demands new governance approaches as operational environments become more interconnected // Industrial Cyber (https://industrialcyber.co/risk-management/industrial-cyber-risk-demands-new-governance-approaches-as-operational-environments-become-more-interconnected/). 03.06.2026).***

***

**«Згідно з індексом кіберготовності малого та середнього бізнесу (SMB Cyber Readiness Index) від ESET за 2026 рік, 45% малих та середніх підприємств у 13 країнах стикалися з інцидентами кібербезпеки протягом минулого року, причому найпоширенішою причиною був фішинг (26%).** Незважаючи на таку високу вразливість, впевненість серед малих та середніх підприємств залишається напрочуд високою: 68% впевнені у своїй здатності запобігати атакам, а 75% довіряють своїй стійкості під час реагування на

інциденти, причому цей показник зростає до 81% серед тих, хто зазнав атак кілька разів… Крім того, більшість малих та середніх підприємств задоволені своїми бюджетами на кібербезпеку — 40% з них планують збільшити витрати наступного року — та активно проводять регулярне навчання співробітників. Однак опитування також виявляє значні операційні слабкі місця, оскільки підприємствам важко встигати за стрімким технологічним прогресом, таким як шкідливе програмне забезпечення на базі штучного інтелекту, а також вони стикаються з постійним дефіцитом кваліфікованих кадрів. Цікаво, що, незважаючи на ці виклики та високий рівень занепокоєння щодо кібервійни та глобальних конфліктів, лише 20% малих та середніх підприємств доручили забезпечення своєї безпеки постачальникам керованих послуг… Зрештою, у звіті наголошується на серйозній суперечності: хоча малі та середні підприємства адаптуються до постійних кіберзагроз за допомогою збільшення бюджетів та проведення навчань, їхній високий рівень впевненості різко контрастує з їхньою постійною вразливістю до елементарних атак, яких можна уникнути, таких як фішинг, що свідчить про те, що фундаментальні проблеми безпеки залишаються невирішеними». ***(Sofiah Nichole Salivio. ESET report finds 45% of SMBs hit by cyber incidents // TechDay (https://securitybrief.com.au/story/eset-report-finds-45-of-smbs-hit-by-cyber-incidents). 05.06.2026).***

***

**«Кіберстійкість — що визначається як здатність організації передбачати кібератаки, протистояти їм, відновлюватися після них та адаптуватися до них — стає критично важливим пріоритетом, оскільки Латинська Америка стає одним із регіонів, що найчастіше стають мішенями кіберзлочинців, зокрема груп, які займаються викраденням даних та використовують програми-вимагачі.** Швидка цифровізація в поєднанні зі слабкими практиками кібербезпеки перетворила цей регіон на привабливе середовище для зловмисників, причому такі країни, як Перу, Мексика, Аргентина, Бразилія та Колумбія, наражаються на найбільшу загрозу. Цей регіон демонструє найшвидше зростання кількості кіберінцидентів у світі, що зумовлено розширенням доступу до Інтернету, обмеженими інвестиціями в кібербезпеку та політичною й економічною нестабільністю. Компанії в середньому зазнають декількох атак на тиждень, а ключові сектори, такі як фінанси, державне управління, охорона здоров’я та телекомунікації, є головними цілями…

Незважаючи на це, регулювання у сфері кібербезпеки в Латинській Америці залишається розрізненим і нерівномірним, на відміну від більш досконалих систем у таких регіонах, як Європа, де такі нормативні акти, як DORA, NIS2 та Закон про кіберстійкість, забезпечують структурований підхід до управління ризиками та відновлення. Експерти наголошують, що організації повинні розглядати кібербезпеку як стратегічне завдання керівництва, інтегруючи стійкість у бізнес-процеси, а не покладаючись виключно на профілактику. Такі підходи, як мікросегментація, вдосконалене управління, захист конфіденційних даних та вивчення минулих інцидентів, можуть посилити стійкість та зменшити економічні збитки. Дослідження показують, що покращення кібербезпеки може підвищити

економічні показники та навіть збільшити ВВП на душу населення, тоді як більш стійкі компанії, як правило, забезпечують значно вищі прибутки для акціонерів. Загалом, у міру посилення кіберзагроз, впровадження комплексних стратегій кіберстійкості є надзвичайно важливим для захисту бізнесу, збереження довіри та підтримки сталого економічного зростання в регіоні». ***(Luis Eduardo Meglioli. Latin America elevates cyber resilience to a strategic priority // Digital Shield (https://www.escudodigital.com/en/defense/latin-america/latin-america-elevates-cyber-resilience-to-a-strategic-priority.html). 05.06.2026).***

***

**«Кібербезпека є надзвичайно важливим пріоритетом для фінтех-компаній, які стикаються зі складним середовищем загроз через свою залежність від мобільних додатків, хмарних платформ, платіжних шлюзів та API відкритого банкінгу.** Оскільки, за прогнозами, до 2025 року глобальні витрати на кіберзлочинність досягнуть 10,5 трлн доларів на рік, фінтех-компанії повинні вирішити п'ять основних ризиків: витік даних, спричинений неправильною конфігурацією або слабким шифруванням; слабка безпека API, що може призвести до несанкціонованих транзакцій; крадіжка особистих даних та захоплення облікових записів внаслідок атак типу credential stuffing та фішингу; атаки програм-вимагачів та DDoS-атаки, що загрожують безперебійній доступності послуг; а також вразливості ланцюга постачання від сторонніх постачальників… Щоб мінімізувати ці загрози, фінтех-компанії повинні інтегрувати заходи безпеки безпосередньо у свої продукти та операційні процеси. До основних передових практик належать впровадження архітектури «нульової довіри», за якої жоден користувач чи пристрій не вважається автоматично надійним, застосування надійного шифрування та токенізації, обов'язкове використання багатофакторної автентифікації (MFA), а також впровадження безпечних методів розробки, таких як сканування залежностей та моделювання загроз. Крім того, організації повинні впровадити постійний моніторинг, проводити регулярні тестування на проникнення та створити офіційну програму управління ризиками постачальників. Оскільки людська помилка залишається основною причиною кіберінцидентів, комплексне навчання співробітників з питань безпеки та спеціалізоване навчання розробників є необхідними для побудови стійкої та безпечної екосистеми Fintech». ***(Suyash Raizada. Top 5 Fintech Cyber Security Risks and Best Practices // Blockchain Council (https://www.blockchain-council.org/fintech/top-5-fintech-cyber-security-risks-and-best-practices/). 03.06.2026).***

***

**«Звіт про цифрові ризики за 2026 рік від Cybersecurity Insiders показує, що організації намагаються встигати за стрімко мінливим ландшафтом загроз, в якому зловмисники все частіше націлюються на довіру, ідентичність та онлайн-репутацію, а не на традиційну інфраструктуру.** На основі даних, отриманих від понад 1 100 керівників у сфері безпеки та управління ризиками, у звіті зазначається, що 84 % організацій за останній рік зіткнулися зі значним інцидентом, пов'язаним із цифровими ризиками, проте лише 7 % вважають свої

програми достатньо розвиненими. Сучасні атаки координуються через різні канали і часто передбачають видавання себе за керівників або співробітників, використання схожих доменів та обману за допомогою штучного інтелекту, наприклад, «діпфейків», що ускладнює виявлення, оскільки традиційні попереджувальні ознаки зникають. Люди стали основною мішенню для атак, але більшість організацій досі не мають комплексного захисту персоналу, окрім керівників, що залишає співробітників із привілейованим доступом особливо вразливими…

У звіті висвітлено основні операційні виклики, зокрема роздробленість відповідальності за цифрові ризики між підрозділами, обмежену видимість нових загроз — особливо на зашифрованих платформах та в системах на базі штучного інтелекту — а також залежність від зовнішніх сторін у виявленні інцидентів. Штучний інтелект створює додаткові ризики через автоматизовані агенти, які взаємодіють із зовнішніми даними та можуть піддаватися маніпуляціям за допомогою таких методів, як введення підказки, тоді як більшість організацій не мають достатніх засобів контролю для моніторингу чи стримування такої діяльності, що створює те, що у звіті названо «прогалиною довіри до штучного інтелекту». Незважаючи на зростання інвестицій, багато організацій продовжують покладатися на розрізнені інструменти та ручні процеси, що обмежує ефективність. У звіті робиться висновок, що управління цифровими ризиками має еволюціонувати в інтегровані «агентні» моделі, які поєднують автоматизацію з людським наглядом, забезпечуючи швидше виявлення, реагування та навчання в середовищі, де ШІ прискорює як атаки, так і захист, і де кібербезпека стала ключовим питанням бізнесу та управління». ***(Jane Devry. New Research Highlights Growing Digital Trust Crisis as AI Accelerates Online Threats // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/new-research-highlights-growing-digital-trust-crisis-as-ai-accelerates-online-threats/). 07.06.2026).***

***

**«…Паролі більше не є достатньою першою лінією захисту в сфері кібербезпеки, оскільки порушення, пов'язані з паролями, — від фішингу до викрадених облікових даних — продовжують домінувати в ландшафті загроз, а кількість атак зараз сягає 7 000 на секунду.** З огляду на це Національний центр кібербезпеки Великої Британії (NCSC) закликає організації переходити на використання ключів доступу — альтернативи, яка є більш стійкою до фішингу. Парольний ключ — це криптографічний ідентифікатор, прив'язаний до пристрою та верифікований за допомогою біометричних даних або PIN-коду, що створює систему, в якій не існує спільного секрету, який можна вкрасти… NCSC підтвердило, що ключі доступу є безпечнішими навіть за найнадійніший пароль у поєднанні з двоступеневою верифікацією, забезпечуючи кращий захист від фішингу та водночас покращуючи зручність користування завдяки усуненню обтяжливого процесу введення пароля та верифікаційного коду. Оскільки атаки, спрямовані на викрадення ідентифікаційних даних, зараз становлять майже 80 % випадків порушення безпеки, а такі стандарти, як Cyber Essentials, приділяють все більшу увагу надійному контролю доступу, відхід від традиційних паролів на

користь більш стійких методів автентифікації, таких як ключі доступу, стає стратегічним пріоритетом для організацій, які прагнуть досягти справжньої кіберстійкості…» ***(MARTIN WEGROSTEK. Why passkeys are becoming essential for modern cybersecurity // TechDay (https://itbrief.co.uk/story/why-passkeys-are-becoming-essential-for-modern-cybersecurity). 26.06.2026).***

***

**«Кіберстійкість стала критично важливим викликом для організацій державного сектору: часті та дедалі більш руйнівні кіберінциденти підкреслюють необхідність не лише запобігати атакам, а й забезпечувати безперебійну роботу та безпечне відновлення діяльності у разі збою.** Національний центр кібербезпеки Великої Британії повідомив про різке зростання кількості серйозних інцидентів, наголосивши, що стійкість зараз є життєво важливою як для виживання організацій, так і для національної стабільності… Гучні події, такі як збій у роботі AWS, що зачепив HMRC, та атака програм-вимагачів Synnovis на медичні служби, демонструють, що збої в роботі технологій або ланцюгів постачання можуть мати негайні реальні наслідки, що ще раз підкреслює: стійкість означає забезпечення безперебійного надання життєво важливих послуг навіть у складних умовах. У відповідь на це «План дій у сфері кібербезпеки» Великої Британії знаменує собою значний зсув у підході, забезпечуючи чіткіші рекомендації, фінансування та механізми управління, щоб допомогти органам державного сектору впровадити практичні заходи щодо забезпечення стійкості, узгодити їх із ширшими нормативно-правовими рамками та зробити акцент на практичній реалізації, безпеці ланцюгів постачання та своєчасному повідомленні про проблеми…

Ключовим поняттям у формуванні стійкості є концепція «мінімально життєздатної компанії» (Minimum Viable Company), яка зосереджується на визначенні та підтримці найважливіших систем і послуг, необхідних для забезпечення безперебійної роботи під час кризи, а не на спробах негайного повного відновлення. Такий підхід дозволяє організаціям надавати пріоритет критично важливим функціям, таким як системи ідентифікації, фінансові операції та комунікації, паралельно плануючи більш масштабне відновлення. У звіті також підкреслюється, що традиційні показники відновлення після катастроф є недостатніми для кіберінцидентів, і натомість пропонується використовувати такі показники, як «середній час до повного відновлення» (Mean Time to Clean Recovery), щоб забезпечити не лише швидке, а й безпечне відновлення систем… Зрештою, для досягнення справжньої стійкості недостатньо лише дотримання вимог; це вимагає розуміння на рівні ради директорів, чіткого управління та інтеграції принципів стійкості в повсякденну діяльність. «План дій у сфері кібербезпеки» надає дорожню карту, але організації повинні діяти негайно, оскільки еволюція кіберзагроз та операційні взаємозалежності означають, що затримки у зміцненні стійкості можуть мати серйозні наслідки для державних служб та людей, які на них покладаються». ***(Christine Horton. Turning policy into practice: Implementing the UK Cyber Action Plan // THINK Digital Partners***

***(https://www.thinkdigitalpartners.com/news/2026/06/25/turning-policy-into-practice-implementing-the-uk-cyber-action-plan/). 25.06.2026).***

***

**«Кіберстійкість стала критично важливим пріоритетом для сучасних підприємств: вона виходить за межі простого запобігання загрозам і зосереджується на підтримці продуктивності, доступності систем та безперебійності роботи під час і після кіберінциденту.** Тоді як кібербезпека насамперед спрямована на зменшення вразливості та блокування атак, кіберстійкість вирішує ширше оперативне завдання — наскільки швидко організація може локалізувати інцидент, відновити роботу та продовжувати функціонувати в разі прориву цих захисних механізмів. Без стійкої інфраструктури підприємства стикаються з серйозними наслідками системних збоїв, зокрема втратою продуктивності, зупинкою робочих процесів, різким зростанням витрат на відновлення та тривалим підривом репутації…

Часто кіберстійкість організації послаблюється через повсякденні операційні прогалини, такі як неконтрольовані кінцеві пристрої, непідтримуване програмне забезпечення, слабкі засоби захисту при вході в систему, обмежена видимість та фрагментовані ІТ-процеси, що уповільнюють час реагування. Щоб боротися з цими вразливостями, організації повинні впроваджувати практичні стратегії, які зменшують ймовірність зривів у роботі та спрощують управління інцидентами. Це передбачає покращення видимості кінцевих точок для раннього виявлення ризиків, посилення захисту ідентичності для запобігання крадіжці облікових даних, стандартизацію застосування політик безпеки на всіх пристроях, шифрування конфіденційних даних та зменшення загальної складності ІТ-інфраструктури…

Крім того, для ефективної оцінки кіберстійкості підприємствам необхідно відстежувати конкретні операційні показники, а не лише обсяги атак. До ключових показників належать відсоток керованих пристроїв, рівень впровадження засобів захисту від фішингу, швидкість відновлення робочих процесів, послідовність дотримання політик безпеки та здатність команд продовжувати роботу в стресових умовах. Надаючи пріоритет цим стратегіям та використовуючи технології, що забезпечують безпеку за замовчуванням — такі як Windows 11 Pro та ПК з Copilot+, які пропонують вбудовану апаратну безпеку, біометричний вхід та розширене шифрування — підприємства можуть ефективно мінімізувати операційний вплив кіберзбоїв, зберегти довіру клієнтів та надійно підтримувати довгострокове зростання в умовах дедалі складнішого середовища загроз». ***(What is cyber resilience, and why is it important? // Microsoft (https://www.microsoft.com/en-us/windows/business/knowledge-center/what-is-cyber-resilience). 26.06.2026).***

***

**«…У міру прискорення цифрової трансформації у виробничій галузі кібербезпеку більше не можна обґрунтовувати виключно технічними показниками; натомість її необхідно розглядати з фінансової точки зору, що відповідає більш широкому контексту прийняття бізнес-рішень.** Хоча організації інвестують значні кошти в автоматизацію, штучний інтелект та

інтегровані ланцюги постачання, саме ці технології збільшують потенційний вплив кіберінцидентів, які тепер можуть порушувати виробничі процеси, переривати ланцюги постачання, спричиняти штрафні санкції за договорами та завдавати значної фінансової шкоди й шкоди репутації. Керівники та ради директорів менше переймаються технічними показниками, такими як індекси вразливості, і більше зосереджуються на бізнес-результатах, таких як порушення операційної діяльності, витрати та рентабельність інвестицій, тому надзвичайно важливо перевести кіберризик у фінансові наслідки… У міру того, як системи стають дедалі більш взаємопов'язаними, кіберризик дедалі більше нагадує операційний ризик, коли один інцидент може спричинити ланцюгову реакцію в різних підрозділах підприємства. Щоб вирішити цю проблему, організації впроваджують методику кількісної оцінки кіберризиків, яка дозволяє моделювати потенційні фінансові наслідки інцидентів та ефективність інвестицій у безпеку, що дає змогу більш обґрунтовано визначати пріоритети у розподілі ресурсів. Такий підхід перетворює кібербезпеку з центру витрат на фактор, що сприяє стійкості, зростанню та прийняттю стратегічних рішень, допомагаючи виробникам збалансувати ризики, інвестиції та інновації в умовах дедалі більш взаємопов'язаного середовища». ***(Asdrúbal Pichardo. Cybersecurity's Missing Metric: Financial Impact // Industrial Media, LLC. (https://www.mbtmag.com/cybersecurity/blog/22969560/cybersecuritys-missing-metric-financial-impact). 25.06.2026).***

***

**«Організації державного сектору стикаються з унікальними викликами у сфері кібербезпеки, оскільки, на відміну від приватних компаній, вони не можуть просто припинити свою діяльність під час кіберінциденту, адже надають життєво важливі послуги, на яких базується суспільство.** У зв'язку зі зростанням масштабів та складності кіберзагроз — особливо завдяки штучному інтелекту, який знижує бар'єри для зловмисників та дозволяє здійснювати швидші й більш адаптивні атаки — органи державного сектору повинні зосередитися не лише на профілактиці, а й на безпечному та швидкому відновленні. Сучасні зловмисники дедалі частіше націлюються на системи резервного копіювання, усвідомлюючи, що вони є критично важливою останньою лінією оборони. Це означає, що організації повинні гарантувати, щоб дані для відновлення були не лише доступними, а й безпечними, ізольованими та надійними. Відновлення вже не зводиться лише до швидкості, а полягає у впевненому відновленні послуг без повторного введення в експлуатацію скомпрометованих систем, що вимагає чіткого розуміння того, коли сталися порушення, як довго зловмисники перебували в системі та які резервні копії є чистими…

Зростаюча складність цифрових середовищ, зокрема хмарних систем, породила нові вразливості, а нормативні вимоги, такі як обов'язкове повідомлення про порушення безпеки протягом 72 годин, посилюють тиск під час інцидентів. Як наслідок, організації повинні визначити «мінімально життєздатний режим роботи», щоб у першу чергу відновити критично важливі послуги, спираючись на ретельне тестування та планування, що дозволить уникнути дорогих наслідків, таких як сплата викупу або відновлення систем з нуля. Також важливою є суверенітет

даних, адже безпечні середовища відновлення, що перебувають під юрисдикційним контролем, забезпечують більшу прозорість та довіру… Зрештою, кіберстійкість у державному секторі — це не лише технічне питання, а й стратегічна необхідність, спрямована на підтримку життєво важливих послуг, захист довіри громадськості та забезпечення того, щоб організації могли відновлювати роботу в середовищах, які вони повністю контролюють…» ***(How to recover rapidly and safely from a cyber attack // Informed Communications Ltd (https://www.ukauthority.com/articles/how-to-recover-rapidly-and-safely-from-a-cyber-attack). 22.06.2026).***

***

**«У своєму нещодавньому звіті про кібербезпеку у світовому спорті компанія Darktrace звертає увагу на посилення кіберзагроз, з якими стикається галузь, що стрімко переходить на цифрові технології.** За результатами опитування 875 фахівців з ІТ-кібербезпеки у США, Великій Британії, Австралії та Німеччині з'ясувалося, що 84 % спортивних організацій за останній рік зазнали принаймні одного кіберінциденту, причому більшість з них зазнала кількох атак… Ця вразливість значною мірою зумовлена швидким впровадженням у цьому секторі цифрових квитків, мобільних додатків, послуг сторонніх постачальників та штучного інтелекту, що наражає організації на такі загрози, як програми-вимагачі, скімінг платежів та злом платформ для вболівальників. Фішинг залишається основним вектором атак: спортивні організації отримують на 19 % більше фішингових листів, ніж організації в інших секторах… Зловмисники часто використовують нові тактики соціальної інженерії, щоб атакувати важливі VIP-профілі та скористатися операційною складністю галузі. Крім того, у міру поширення штучного інтелекту 72 % респондентів очікують зростання кіберризиків протягом наступного року, особливо щодо впровадження штучного інтелекту та пов'язаних із цим вразливостей…

Оскільки спортивні організації визначають кіберстійкість як необхідність захисту широко висвітлюваних прямих трансляцій без перерв у роботі — причому функціонування стадіонів вважається найважливішою функцією, яку потрібно захистити, — компанія Darktrace радить розглядати кібербезпеку як ключове операційне та управлінське завдання. Для забезпечення такої стійкості компанія рекомендує впроваджувати надійні стратегії, такі як моделювання загроз для нових технологій, суворий контроль ланцюга поставок та доступу постачальників, а також ретельну сегментацію ІТ-систем, операційних систем та систем, орієнтованих на вболівальників… Крім того, організації повинні впровадити систему безпеки, орієнтовану на ідентифікацію, з універсальною багатофакторною автентифікацією (MFA), посилити захист від фішингу в усіх каналах комунікації та розробити спеціалізовані оперативні посібники, адаптовані до специфічних умов проведення спортивних заходів наживо». ***(Linn Foster Freedman. Darktrace Report Highlights Cyber Threats Against Global Sporting Sector // Robinson & Cole LLP. (https://www.dataprivacyandsecurityinsider.com/2026/06/darktrace-report-highlights-cyber-threats-against-global-sporting-sector/). 18.06.2025).***

***

**«Кібербезпека перетворилася на складну, спеціалізовану галузь, яку в загальних рисах можна розділити на три окремі, але взаємопов'язані напрямки: кібербезпека інформаційних технологій (IT), кібербезпека продуктів та кібербезпека операційних технологій (OT)…**

Кібербезпека в сфері IT спрямована на захист бізнес-систем, мереж та даних (наприклад, електронної пошти, корпоративних мереж) шляхом управління доступом, встановлення оновлень та реагування на інциденти. Її основною метою є забезпечення конфіденційності, цілісності та доступності (CIA). Порушення безпеки, як правило, призводять до викрадення даних або перебоїв у роботі сервісів…

Кібербезпека продуктів — це інженерна дисципліна, спрямована на забезпечення того, щоб продукти з вбудованим програмним забезпеченням (від медичних пристроїв до автомобілів) проектувалися, розроблялися та обслуговувалися з дотриманням вимог безпеки протягом усього їхнього життєвого циклу. Пріоритети змінюються залежно від функції продукту; у системах, критичних для безпеки, цілісність та доступність мають пріоритет над конфіденційністю, щоб забезпечити безпечну фізичну роботу…

Кібербезпека операційних технологій (OT) забезпечує захист апаратного та програмного забезпечення, яке здійснює моніторинг та управління фізичними промисловими процесами та інфраструктурою, такими як виробничі лінії, електромережі та трубопроводи. Середовища OT часто базуються на застарілих системах, які неможливо легко оновити без зупинки роботи. Головними пріоритетами тут є фізична безпека, надійність та безперебійна робота, оскільки порушення безпеки можуть спричинити значні економічні збитки, руйнування обладнання та загрози громадській безпеці…

Хоча ці галузі мають різні пріоритети, обмеження та вимоги до професійних навичок, вони часто перетинаються. Наприклад, вразливість у промисловому виробі може поставити під загрозу IT-або OT-середовище, в якому він використовується, а порушення IT-безпеки може змусити провести профілактичне відключення OT-систем. Розуміння відмінностей та перетинів між цими галузями має вирішальне значення для зацікавлених сторін — зокрема керівників, страховиків, регуляторних органів та юристів — для прийняття обґрунтованих рішень, покращення управління, раціонального розподілу ресурсів та визначення юридичної відповідальності під час кіберінцидентів». ***(Summer Fowler and Michael Maass. Prominent Branches of Cybersecurity: How They Differ, Connect, and Overlap // Exponent Inc (https://www.exponent.com/article/prominent-branches-cybersecurity-how-they-differ-connect-and-overlap). 24.06.2026).***

***

## ***Сполучені Штати Америки, Канада та країни Південної Америки***

**«2 червня 2026 року президент Трамп підписав указ під назвою «Сприяння інноваціям та безпеці у сфері передових технологій штучного інтелекту», спрямований на забезпечення балансу між підтримкою інновацій у**

**галузі ШІ та посиленням захисту від нових кіберзагроз, зберігаючи при цьому переважно добровільний та необтяжливий підхід до регулювання.** Указ зосереджується на трьох основних напрямках: посилення кібербезпеки у федеральних системах та критичній інфраструктурі, створення добровільної системи взаємодії на етапі до випуску передових «передових» моделей ШІ та надання пріоритету застосуванню існуючого кримінального законодавства проти кіберзлочинів, скоєних за допомогою ШІ. Він передбачає вжиття швидких заходів для посилення кіберзахисту, розширення доступу до засобів безпеки на базі ШІ та створення під егідою Міністерства фінансів інформаційного центру з кібербезпеки ШІ для координації виявлення вразливостей та реагування на них у співпраці з галуззю. Він також закликає до розробки секретної системи порівняльного аналізу для виявлення моделей ШІ з високим рівнем ризику та заохочує розробників — на добровільній основі — ділитися такими моделями з урядом протягом 30 днів перед їх ширшим випуском для надійних партнерів, при цьому заходи щодо забезпечення конфіденційності та захисту інтелектуальної власності ще мають бути визначені…

Цей указ не встановлює обов'язкових вимог, але свідчить про посилення контролю за передовими системами штучного інтелекту, особливо тими, що мають наслідки для кібербезпеки. Для підприємств ключовими питаннями є оцінка того, чи можуть їхні моделі відповідати визначенню «передових» систем за майбутніми критеріями, аналіз доцільності участі у добровільній програмі попереднього оприлюднення, а також зважування переваг і ризиків взаємодії з інформаційним центром з питань кібербезпеки, включаючи потенційні проблеми щодо обміну даними та відповідальності. Наказ також підкреслює підвищені ризики щодо дотримання вимог для компаній, що використовують агентів ШІ, особливо у випадках, коли ці системи взаємодіють із зовнішніми даними або системами, наголошуючи на необхідності жорсткого контролю, дозволів та моніторингу. Загалом, ця ініціатива відображає політичний підхід, що заохочує співпрацю між урядом та галуззю, готуючи їх до зростаючих викликів у сфері безпеки, пов'язаних із передовими технологіями ШІ». ***(President Trump Signs Executive Order Establishing AI Cybersecurity and Frontier Model Framework // Latham & Watkins (https://www.lw.com/en/insights/president-trump-signs-executive-order-establishing-ai-cybersecurity-and-frontier-model-framework). 03.06.2026).***

***

**«У четвер Сенат Канади ухвалив законопроект С-8, який запроваджує обов'язкову систему кібербезпеки, покликану забезпечити кращий захист критичної інфраструктури в секторах телекомунікацій, фінансів, енергетики та транспорту від нових загроз.** Законопроект передбачає внесення змін до чинного Закону про телекомунікації та прийняття нового Закону про захист критично важливих кіберсистем. Згідно зі змінами до Закону про телекомунікації, губернатор у раді міністрів та міністр промисловості отримають ширші повноваження щодо забезпечення безпеки національних мереж, зокрема право видавати обов'язкові розпорядження провідним операторам зв'язку, забороняти використання продукції певних постачальників та вимагати вилучення обладнання з високим рівнем ризику, а також застосовувати грошові штрафи до компаній, які

не виконують ці вимоги… Паралельно з цим новий Закон про захист критично важливих кіберсистем має на меті створити офіційну структуру для захисту основних операційних систем та послуг, пов'язаних із національною безпекою та громадською безпекою. Незважаючи на ці цілі, під час ухвалення законопроекту він постійно піддавався критиці з боку захисників прав на приватність: Комісар з питань конфіденційності Канади попередив, що критерії для використання нових повноважень є занадто широкими, що не існує обов'язкової вимоги повідомляти Комісара про серйозні порушення кібербезпеки, а також що мінімальні гарантії конфіденційності при обміні інформацією з іноземними урядами є недостатніми; ці занепокоєння також були висловлені в експертній доповіді від Citizen Lab Університету Торонто. Після проходження останнього читання законопроект C-8 зараз очікує на королівське затвердження, щоб набути чинності». ***(Ellie Cho. Canada parliament passes cybersecurity bill amid privacy concerns // JURIST Legal News & Research Services, Inc. (https://www.jurist.org/news/2026/06/canada-parliament-passes-cybersecurity-bill-amid-privacy-concerns/). 06.06.2026).***

***

**«22 червня 2026 року Білий дім видав два виконавчі накази щодо квантових технологій: один був спрямований на захист країни від сучасних криптографічних атак та прискорення переходу до постквантової криптографії (PQC), а інший — на стимулювання інновацій та підвищення конкурентоспроможності США у сфері квантових технологій…** Цей наказ, спрямований на забезпечення безпеки, є відповіддю на ризик того, що сучасні методи шифрування можуть бути зламані майбутніми квантовими комп'ютерами, зокрема на небезпеку того, що викрадені сьогодні дані можуть бути розшифровані в майбутньому. Він також передбачає координацію на федеральному рівні щодо розробки національної стратегії переходу на PQC, надання технічних рекомендацій з боку міністра торгівлі, а також загальнодержавний перехід на PQC для формування ключів до 31 грудня 2030 року та для цифрових підписів — до 31 грудня 2031 року… Крім того, цей наказ виходить за межі федеральних систем, вимагаючи, щоб запропоновані зміни до FAR для підпадаючих під його дію підрядників відповідали стандартам NIST FIPS, що включають алгоритми PQC, у той самий термін, а також щоб було посилено програми розкриття вразливостей з метою охоплення криптографічних слабких місць; водночас передбачено підтримку операторів критичної інфраструктури та заохочення іноземних урядів і галузевих об'єднань до впровадження стандартів PQC від NIST… Цей наказ, орієнтований на інновації, має на меті зміцнити лідерство США у сфері квантових технологій шляхом створення загальнонаціональної ініціативи з розробки квантового комп'ютера, потужність якого буде достатньою для початку ери відкриттів на основі квантових технологій; заохочення партнерства з приватним сектором та ринкових зобов'язань; сприяння вітчизняній розробці компонентів, необхідних для квантових технологій; виявлення можливостей для дерегуляції; а також встановлення вимоги щодо розробки п'ятирічних планів у сферах квантового зондування, мережевих технологій, а також набору та утримання кваліфікованих кадрів… У ньому також передбачається створення національного центру для

оцінки продуктивності квантових обчислювальних систем, заохочується міжнародна співпраця з метою забезпечення доступу до ринків, капіталу та надійних ланцюгів постачання, а також підкреслюється, що безпека залишається головним пріоритетом, шляхом заклику до запровадження суворого контролю за діяльністю QIST та розширення ресурсів контррозвідки». ***(Caleb Skeath, Robert Huffman, Benjamin Sovocool, Emily Pehrsson & Alexandra Bruer. Trump Administration Releases Two Executive Orders on Quantum // Covington & Burling LLP (https://www.insideprivacy.com/cybersecurity-2/trump-administration-releases-two-executive-orders-on-quantum/). 25.06.2026).***

***

**«Через три місяці після того, як адміністрація Трампа оголосила про запуск пілотної програми, покликаної допомогти штатам фінансувати заходи з кібербезпеки для критичної інфраструктури, ця ініціатива, судячи з усього, досягла лише обмеженого прогресу: щонайменше 26 штатів та Округ Колумбія заявили, що не беруть у ній участі, а багато хто повідомив, що навіть не чув про неї.** Ця програма, яку в березні вперше описав національний директор з питань кібербезпеки Шон Кернкросс як засіб, що допоможе штатам масштабувати доступні рішення з безпеки для таких життєво важливих секторів, як водопостачання, енергетика та сільське господарство, могла б стати значним підкріпленням для штатних та місцевих органів влади, що відчувають брак коштів і намагаються захистити школи, лікарні, системи екстреної допомоги 911 та інші життєво важливі служби від дедалі витонченіших кіберзагроз, зокрема тих, що посилюються через штучний інтелект та вразливості ланцюгів постачання… Однак Білий дім оприлюднив мало деталей щодо того, як працюватиме ця програма, у чому полягатиме федеральна підтримка та як штати зможуть у ній брати участь, а ONCD не відповіло на запитання з цього приводу. Відповіді на опитування свідчать, що лише невелика кількість штатів брала участь у цьому процесі: Невада та Північна Дакота повідомили про обговорення чи зустрічі, кілька інших штатів висловили зацікавленість у разі звернення до них, а решта заявили, що не знали про цю ініціативу або не зацікавлені в ній. Експерти та колишні посадовці охарактеризували відсутність інформаційно-роз'яснювальної роботи як ознаку недостатньої нагальності та поставили під сумнів відданість адміністрації цій справі, особливо з огляду на скорочення федеральної підтримки у сфері кібербезпеки, зокрема припинення багаторічного фінансування MS-ISAC та обмеження щодо отримувачів грантів… Проте прихильники стверджують, що за умови належного впровадження програми та зосередження уваги на найбільш вразливих регіонах вона може допомогти усунути небезпечний пробіл у кіберстійкості державного сектору і навіть створити моделі, які можна буде поширити на всю країну». ***(Eric Geller. White House's state infrastructure cybersecurity initiative stalled // TechTarget, Inc. (https://www.cybersecuritydive.com/news/white-house-states-cybersecurity-pilot-programs-oncd/823453/). 24.06.2026).***

***

**«Мексика оприлюднила Національний план кібербезпеки на 2025–2030 роки, спрямований на зміцнення своєї кіберзахищеності у відповідь на постійні атаки на федеральні, штатні та місцеві установи, а також на протидію основним джерелам загроз для країни: організованій злочинності, геополітичним загрозам та новим ризикам, пов'язаним із штучним інтелектом.** Цей план з'явився у критичний момент, оскільки Мексика зазнає значного впливу програм-вимагачів, фінансового шкідливого програмного забезпечення та шахрайства, витоків даних, хактивізму та діяльності, що фінансується державою, причому урядові, медичні та фінансові установи є одними з найчастіших цілей таких атак… Insikt Group зазначає, що Мексика є привабливою як для кіберзлочинців, так і для державних суб'єктів через її інтеграцію в ланцюги постачання США, виробничу базу, орієнтовану на «нейшорінг», та порівняно слабко розвинене кіберуправління, а також є однією з головних цілей для зловмисників, що викрадають інформацію, та ринків вкрадених платіжних карток. План розроблено з метою переходу Мексики від фрагментованого, реактивного підходу до скоординованої національної системи, з поетапними етапами, що простягаються від створення базових структур управління та звітування про інциденти у 2025 році до розробки національної стратегії кібербезпеки, прийняття відповідного закону, створення оперативного центру та мережі реагування у 2026 році, а потім — до проведення навчання, впровадження засобів захисту на основі штучного інтелекту, формування регіонального лідерства та створення постійної обсерваторії до 2030 року. Згідно з публічними даними, базовий етап вже завершено, проте хід реалізації наступних етапів залишається нез'ясованим…

Середовище загроз, на яке спрямований цей план, є широким і стійким. Головною загрозою залишається програмне забезпечення для вимагання викупу, яке неодноразово атакує державні установи та об'єкти життєво важливого значення, тоді як фінансове шкідливе програмне забезпечення та шахрайство продовжують експлуатувати банківську, фінтех- та споживчу екосистеми Мексики за допомогою троянських програм, ботнетів, фішингу та крадіжки облікових даних. Витоки даних та викрадені записи широко продаються на форумах даркнету, а групи хактивістів використовують геополітичне положення Мексики для здійснення політично мотивованих витоків інформації та дефейсів. Мексика також стикається з кібердіяльністю, пов'язаною з організованою злочинністю, зокрема з відмиванням грошей через китайські мережі відмивання коштів та послугами «кіберзлочинності як послуги» для підтримки діяльності картелів… Кампанії, що фінансуються державою, зокрема шпигунська діяльність проти університетів, міністерств та об'єктів критичної інфраструктури, ще раз підкреслюють стратегічне значення Мексики. Очікується, що Чемпіонат світу з футболу ФІФА 2026 року, співорганізатором якого є Мексика, стане першим випробуванням здатності країни захищати цифрові послуги, транспорт, платіжні системи та об'єкти громадської інфраструктури в умовах пильної уваги міжнародної спільноти. Insikt Group рекомендує організаціям, що працюють у Мексиці, посилити виявлення загроз, впровадити міжнародні стандарти безпеки, проводити сценарне планування та кібернавчання, а також підвищувати обізнаність персоналу та громадськості, щоб вони могли ефективніше реагувати на атаки програм-вимагачів, шпигунство,

шахрайство та інші інциденти. Загалом, цей план пропонує важливий дороговказ для реформ, але його успіх залежатиме від законодавства, інституційної спроможності та послідовної реалізації протягом решти десятиліття». ***(Evaluating Mexico's New Cybersecurity Plan // Recorded Future® (https://www.recordedfuture.com/research/mexico-new-cybersecurity-plan-evaluation). 25.06.2026).***

***

**«Незважаючи на те, що 70 відсотків кібератак у 2024 році були спрямовані проти критичної інфраструктури, Конгрес наразі розглядає питання про скорочення бюджету Агентства з кібербезпеки та безпеки інфраструктури (CISA) — провідного цивільного відомства США у сфері кіберзахисту.** Нещодавній звіт Комітету з питань асигнувань Палати представників мимоволі підкреслює незамінну роль CISA, оскільки, скорочуючи його бюджет, він водночас доручає агентству підтримувати або розширювати свої найважливіші завдання… CISA виконує п'ять незамінних функцій, які не може виконати жодна інша організація: по-перше, вона виступає в ролі національної системи раннього попередження, використовуючи свій каталог «Відомих експлуатованих вразливостей» (Known Exploited Vulnerabilities), щоб допомогти організаціям класифікувати та визначати пріоритетність загроз в епоху, коли штучний інтелект прискорює виявлення та використання програмних недоліків у злочинних цілях. По-друге, CISA є першою лінією оборони США проти підтримуваних китайською державою операцій, таких як «Volt Typhoon» і «Salt Typhoon», використовуючи свої унікальні можливості для виявлення та усунення зловмисників із критично важливих сервісів, перш ніж вони зможуть спричинити масштабні збої… По-третє, на CISA покладено унікальне завдання щодо забезпечення безпеки федеральних цивільних мереж — у яких зберігаються конфіденційні дані громадян — і вона має виключні повноваження видавати обов'язкові до виконання директиви, що зобов'язують відомства усунути вразливості. По-четверте, агентство надає надзвичайно важливу добровільну допомогу з питань кібербезпеки понад 10 000 місцевих виборчих округів, що мають обмежені ресурси, для захисту таких систем, як реєстрація виборців. Нарешті, CISA відіграє життєво важливу роль у формуванні національного кадрового резерву у сфері кібербезпеки, впроваджуючи освіту з кібербезпеки в школах від дошкільного до середнього рівня та надаючи необхідну пряму федеральну підтримку урядам штатів, місцевим та сільським органам влади, які не мають спеціалізованих команд з кібербезпеки. Недофінансування CISA ставить під загрозу ці п'ять фундаментальних стовпів національної безпеки». ***(Jiwon Ma. 5 Reasons Why CISA Is Indispensable to America's Cyber Defense // Foundation for Defense of Democracies (https://www.fdd.org/analysis/2026/06/25/5-reasons-why-cisa-is-indispensable-to-americas-cyber-defense/). 25.06.2026).***

***

**«Федеральна комісія з питань зв'язку США (FCC) затвердила нові правила, спрямовані на підвищення кібербезпеки національних систем оповіщення про надзвичайні ситуації та підводних кабелів. З метою захисту**

**Системи оповіщення про надзвичайні ситуації (EAS) та Системи бездротового оповіщення про надзвичайні ситуації (WEA) від зловмисного захоплення, яке може спричинити хаос або порушити координацію дій у надзвичайних ситуаціях, нові правила передбачають обов'язкове дотримання важливих заходів кібергігієни, зокрема використання надійних паролів, своєчасне встановлення оновлень безпеки та використання брандмауерів.** Крім того, буде впроваджено нову систему ідентифікації для перевірки повідомлень та запобігання несанкціонованому надсиланню або дублюванню повідомлень… Одночасно з цим FCC опублікувала перше за останні десятиліття комплексне оновлення правил щодо підводних кабельних мереж, яке забезпечує баланс між пом'якшенням та посиленням вимог до кібербезпеки. З метою прискорення та спрощення процесу ліцензування ці правила звільняють операторів кабельних мереж, які мають бездоганну історію діяльності, від суворих міжвідомчих перевірок з питань національної безпеки, що проводяться в рамках ініціативи «Team Telecom», за умови, що вони самостійно підтвердять відповідність найвищим стандартам безпеки та погодяться на постійний моніторинг… Навпаки, FCC посилила нагляд, запровадивши нові ліцензійні вимоги до операторів, які підключають підводні кабелі до наземних об'єктів у США, а також оновила заходи безпеки для усунення вразливостей у ланцюгу постачання, пов'язаних з основним обладнанням та сторонніми постачальниками послуг». ***(Derek B. Johnson. FCC passes new cybersecurity rules for emergency systems, undersea cables // CyberScoop (https://cyberscoop.com/fcc-undersea-cable-regulations-national-security/). 26.06.2026).***

***

## ***Країни ЄС та Великобританія***

**«Новий звіт компанії ManageEngine свідчить, що британські підприємства стикаються з серйозними проблемами у сфері кібербезпеки: 77% з них зазнали кібератаки протягом останнього року — це найвищий показник серед опитаних європейських країн, який на 11% перевищує середній.** Ця загострена ситуація з безпекою ускладнюється значним навантаженням на IT-підрозділи та служби безпеки: 46% британських організацій називають брак кваліфікованих кадрів своєю головною операційною проблемою, а 60% повідомляють про зростання робочого навантаження…

Незважаючи на ці виклики, дослідження показує, що британські організації також демонструють високу стійкість; вони є лідерами у впровадженні офіційних систем забезпечення кіберстійкості, мають високий рівень залученості керівництва та проводять ґрунтовні аналізи після інцидентів. Дивлячись у майбутнє, британські підприємства визнають атаки на основі штучного інтелекту своїм найбільшим ризиком і відповідно розставляють пріоритети в інвестиціях. Однак, хоча виявлення відбувається швидко (94% інцидентів виявляються протягом 24 годин), відновлення відбувається повільно, оскільки менше половини організацій відновлюються протягом 10 днів. Результати дослідження малюють картину

британського ринку, який є одночасно цілеспрямованим і порівняно зрілим, проактивно інвестує в стійкість, але все ще бореться з операційним навантаженням, пов'язаним із швидко мінливим ландшафтом загроз…» ***(Neil Trim. United Kingdom Businesses Suffered the Highest Cyber Incident Rate in a Survey of 5 European Countries // // Kingswood Media (https://technologyreseller.uk/united-kingdom-businesses-suffered-the-highest-cyber-incident-rate-in-a-survey-of-5-european-countries/). 02.06.2026).***

***

**«Французьке управління з фінансових ринків (AMF) визначило операційну стійкість, зокрема у контексті кіберризиків, як ключовий стратегічний пріоритет на 2026 рік, що відображає зростаючу складність цифрових загроз у фінансовому секторі.** Очікується, що стрімкий розвиток штучного інтелекту не тільки покращить можливості у сфері кібербезпеки, але й посилить ризики, оскільки дозволить швидше виявляти та використовувати вразливі місця, а також збільшить масштаби кібератак. Як наслідок, фінансові установи повинні адаптувати свої системи управління ризиками, щоб відповісти на ці нові виклики, тоді як AMF продовжує відігравати активну роль як на національному, так і на міжнародному рівні у координації заходів реагування та обміні досвідом через такі органи, як IOSCO, Рада з фінансової стабільності та Група кіберекспертів G7…

На європейському рівні AMF контролює дотримання Закону про цифрову операційну стійкість (DORA), який діє з січня 2025 року та покладає на фінансові установи обов'язки щодо виявлення критично важливих систем, впровадження заходів з кібербезпеки, управління інцидентами, проведення тестувань на стійкість та усунення ризиків, пов'язаних із залученням сторонніх суб'єктів. AMF планує опублікувати оцінки та висновки, отримані на основі звітів про інциденти відповідно до DORA, а також провести інформаційні кампанії, включаючи вебінари та опитування у 2026 році, щоб оцінити, як компанії реагують на кіберризики, пов'язані зі штучним інтелектом…

Орган також продовжуватиме перевірки суб'єктів, що підлягають регулюванню, зосередивши увагу на захисті даних, можливостях реагування на інциденти та готовності до загроз, пов'язаних із штучним інтелектом. Він наголошує, що кібербезпека має вирішальне значення для захисту інвесторів та стабільності ринку, і закликає керівництво вищого рівня інтегрувати кіберризики в систему управління, внутрішнього контролю та регулярного тестування. Фінансовим суб'єктам рекомендується дотримуватися встановлених найкращих практик, зокрема вести безпечний облік систем, посилювати захист даних, своєчасно встановлювати оновлення, забезпечувати надійне резервне копіювання, навчати персонал, вдосконалювати виявлення загроз та проводити регулярні аудити й симуляції кризових ситуацій, включаючи сценарії, пов'язані з ризиками штучного інтелекту». ***(Cyber resilience: the AMF calls on financial market participants to strengthen their cybersecurity arrangements in response to rapidly evolving threats associated with artificial intelligence // Autorité des marchés financiers (AMF) (https://www.amf-france.org/en/news-publications/news/cyber-***

***resilience-amf-calls-financial-market-participants-strengthen-their-cybersecurity-arrangements). 04.06.2026).***

***

**«Згідно з новим юридичним висновком експерта з міжнародного інвестиційного права професора Крістофа Шройера, запропонований Європейською комісією Закон про кібербезпеку (CSA) може призвести до того, що держави-члени ЄС будуть нести значну фінансову відповідальність відповідно до чинних двосторонніх інвестиційних угод (BIT) з Китаєм.** Проект CSA надає ЄС широкі повноваження щодо виключення «постачальників з високим рівнем ризику» з критично важливих європейських ринків інформаційно-комунікаційних технологій, таких як мережі 5G. Однак, оскільки міжнародне право забороняє державам використовувати внутрішнє законодавство або законодавство ЄС для виправдання порушення договірних зобов'язань, впровадження CSA може порушити гарантії щодо недопущення дискримінації та експропріації, які надаються китайським інвесторам відповідно до BIT, укладених майже всіма державами-членами ЄС… У разі виключення з угоди ці китайські інвестори можуть скористатися механізмами арбітражу між інвестором і державою, щоб вимагати значної фінансової компенсації безпосередньо від держав-членів, які зазнали збитків. Шройер наголошує, що спроба розірвати двосторонні інвестиційні угоди (BIT) не зменшить цього ризику, оскільки «застереження про втрату чинності» захищають існуючі інвестиції протягом 20 років після розірвання угоди. Крім того, оскільки Китай не зобов'язаний дотримуватися законодавства ЄС, ЄС не може в односторонньому порядку скасувати або переосмислити ці міжнародні договори з метою приведення їх у відповідність до своїх нових цілей у сфері кібербезпеки. Отже, якщо CSA буде прийнято в нинішньому вигляді, держави-члени ЄС опиняться в пастці між суперечливими директивами ЄС та міжнародними правовими зобов'язаннями, що змусить політиків зважувати прагнення до цифрового суверенітету проти серйозного ризику дорогих міжнародних арбітражних позовів…» ***(Colin Stevens. EU Cybersecurity Act could expose member states to costly investment treaty claims, legal opinion warns // EU Reporter (https://www.eureporter.co/crime/law-2/2026/06/05/eu-cybersecurity-act-could-expose-member-states-to-costly-investment-treaty-claims-legal-opinion-warns/). 05.06.2026).***

***

**«Національний центр реагування на кіберінциденти Словенії, SI-CERT, поступово перетворився з невеликого академічного проекту 1994 року на важливу установу, яка щорічно обробляє близько 6 000 кіберінцидентів.** Під керівництвом Горазда Божича в рамках державної агенції ARNES команда з приблизно десятка аналітиків використовує трирівневу систему сортування для управління робочим навантаженням, відокремлюючи рутинні випадки онлайн-шахрайства від більш серйозних інцидентів та повідомлень про фішинг. Спочатку центр мав труднощі з визнанням з боку уряду та приватного сектору, але вирішальний момент настав близько 2012 року, коли центр продемонстрував свою

цінність для банків, ліквідувавши фішингові сайти — завдання, з яким вони не могли впоратися самостійно… Цей успіх допоміг завоювати довіру, і зараз, відповідно до директив NIS, SI-CERT надає критично важливим секторам такі необхідні послуги, як аналіз шкідливого програмного забезпечення, приділяючи більшу увагу своїй допоміжній ролі, ніж суто юридичним повноваженням. Центр тісно співпрацює з правоохоронними органами, пропонуючи глибокі знання в галузі мереж, та допомагає впоратися з хаосом реагування на інциденти, наголошуючи на важливості наявності компетентної місцевої команди. Незважаючи на постійний тиск з боку бюджету та скептицизм щодо ажіотажу навколо штучного інтелекту, SI-CERT продовжує розширювати свої можливості та зміцнювати довіру, пропонуючи приватним компаніям конфіденційну допомогу, що базується на стандартах». ***(Mirko Zorz. A small Slovenian team handles 6,000 cyber incidents a year // Help Net Security (https://www.helpnetsecurity.com/2026/06/03/gorazd-bozic-si-cert-cyber-incident-response/). 03.06.2026).***

***

**«Згідно з доповіддю ESET за 2026 рік, майже 80% британських виробників стикалися з кіберінцидентами протягом минулого року, що підкреслює різке розширення площі атаки в промисловості у міру того, як операційні технології (OT) все тісніше переплітаються з корпоративними IT-системами.** Перехід до Індустрії 4.0 та 5.0, що характеризується хмарними додатками, робототехнікою та датчиками реального часу, приніс величезну ефективність, але й значні ризики, оскільки кількість кібератак на виробничі підприємства зросла на 61% у 2025 році… Оскільки кібератака в таких середовищах може призвести до зупинки систем, критично важливих для безпеки, та спричинити простої у виробництві, що коштують понад 1,9 мільйона доларів на день, традиційна система безпеки на основі периметра вже не є достатньою. Організації повинні кардинально переглянути архітектуру своїх мереж, надаючи пріоритет стійкості, щоб забезпечити безперебійну роботу навіть під час інциденту. Це вимагає усунення одиночних точок відмови шляхом створення фізичної надмірності мережі, розширення пропускної здатності та впровадження детальних засобів контролю безпеки, таких як контроль доступу на основі ролей (RBAC), багатофакторна автентифікація (MFA) та сувора сегментація мережі з використанням VLAN для ізоляції критично важливих систем і запобігання горизонтальному переміщенню зловмисників. Крім того, виробники повинні впровадити моніторинг у реальному часі та розширену аналітику для прогнозного виявлення аномалій, а також швидке встановлення виправлень і регулярне тестування на проникнення… Зрештою, промислові підприємства повинні змінити свій підхід: замість того, щоб просто запобігати атакам, їм слід створювати стійкі та безпечні мережеві архітектури, які слугуватимуть стратегічним захистом від дедалі більшої загрози операційних збоїв, спричинених кібератаками». ***(Roshini Bains. Designing For Disruption: How Networks Enable Cyber Resilience // Mark Allen Holdings Ltd (https://www.manufacturingmanagement.co.uk/content/in-depth/designing-for-disruption-how-networks-enable-cyber-resilience). 03.06.2026).***

***

**«Велика Британія стала однією з країн, що найчастіше стають мішенями кібератак: минулого року Національний центр кібербезпеки (NCSC) зафіксував рекордну кількість інцидентів національного значення — 204 випадки, що на 130% більше, ніж у попередньому році.** Організації державного сектору, зокрема місцеві ради, все частіше стають мішенню атак, про що свідчить злом у грудні 2025 року в раді Кенсінгтона та Челсі, який оприлюднив особисті дані сотень тисяч мешканців, підвищивши ризик шахрайства та соціальної інженерії. Цей сплеск зумовлений як кампаніями, що підтримуються державою, так і злочинцями, які керуються фінансовими мотивами та зосереджуються на системах ідентифікації та інструментах хмарної співпраці як ключових точках входу в урядові мережі. Проблема ускладнюється структурними слабкостями у всьому державному секторі, зокрема значною залежністю від застарілих систем, обмеженими бюджетами на сучасні засоби захисту, недостатнім навчанням та спільним використанням технологічних стеків місцевими органами влади, що дозволяє успішним атакам швидко поширюватися на багато організацій…

У відповідь на це уряд Великої Британії надає пріоритет забезпеченню кіберстійкості країни: NCSC співпрацює з державним і приватним секторами, а для зміцнення захисних систем державного сектору оголошено про інвестиції у розмірі 210 мільйонів фунтів стерлінгів. Традиційні підходи до безпеки, що базуються на конкретних моментах у часі, дедалі частіше вважаються недостатніми в умовах мінливого ландшафту загроз. Як наслідок, багато організацій переходять на систему безперервного управління вразливістю до загроз (CTEM), яка зміщує акцент з періодичного тестування на постійну, засновану на фактичних даних перевірку площі атаки організації. Поєднуючи автоматизацію на основі штучного інтелекту з експертним тестуванням на протидію, що імітує реальну поведінку зловмисників, CTEM дозволяє швидше виявляти вразливості, які дійсно можна використати, покращує визначення пріоритетів на основі реальних ризиків та забезпечує вимірювані результати за допомогою таких методологій, як Return on Mitigation (RoM). У середовищах місцевих органів влади цей підхід також підтримує скоординовані зусилля, такі як обмін інформацією про загрози та спільні навчання. При правильній структурі з чіткими процесами управління, визначенням обсягу та усуненням вразливостей, CTEM пропонує органам державного сектору масштабований спосіб зменшити вразливість, продемонструвати реальне зниження ризиків та йти в ногу з загрозами, які розвиваються швидше, ніж можуть впоратися традиційні засоби захисту…» ***(Laurie Mercer. Rethinking cyber defense in government with continuous exposure management // Future US, Inc. (https://www.techradar.com/pro/rethinking-cyber-defense-in-government-with-continuous-exposure-management). 05.06.2026).***

***

**«Національні музеї та галереї Великої Британії, як і раніше, знаходяться під високим ризиком кіберзагроз, а Комітет з питань державних фінансів попередив, що ця галузь не зробила достатньо, аби винести уроки з атаки з використанням програм-вимагачів на Британську бібліотеку у 2023 році, що залишає культурні та історичні надбання Великої Британії в цілому**

**вразливими.** У звіті, опублікованому 24 червня, комітет розкритикував уряд за те, що той продовжує покладатися на реактивний, а не проактивний підхід як до кібербезпеки, так і до фізичної безпеки, та зазначив, що Міністерство культури, ЗМІ та спорту не використало свою центральну роль ефективно для координації обміну інформацією або стимулювання колективних дій у всьому секторі… Комітет з питань державних фінансів (PAC) звернувся до Департаменту культури, ЗМІ та спорту (DCMS) із проханням пояснити, що було зроблено та що планується зробити для усунення цих ризиків, зокрема щодо вдосконалення цифрового обліку та інших заходів безпеки для установ, які приваблюють мільйони відвідувачів і в 2024–25 роках отримали дохід у розмірі 563 мільйонів фунтів стерлінгів. Хоча DCMS заявляє, що наразі тісніше співпрацює з музеями та галереями, зокрема в рамках урядового «Кіберплану дій», а також об'єднує керівників інформаційних служб (CIO) та керівників служб інформаційної безпеки (CISO) з незалежних організацій для обміну досвідом та визначення спільного плану дій у сфері безпеки, PAC та експерти галузі стверджують, що така підтримка залишається обмеженою та запізнілою… Атаку на Британську бібліотеку було названо переломним моментом, який продемонстрував, як програми-вимагачі можуть паралізувати роботу, поставити під загрозу дані та підірвати довіру громадськості, а коментатори попередили, що музеї та галереї стикаються з особливо складним поєднанням цифрових вразливостей, ризиків фізичної безпеки, обмежених бюджетів та недостатньої кіберфахівки. Загальний висновок полягає в тому, що ця галузь не може собі дозволити чекати на черговий серйозний інцидент, перш ніж вжити заходів, оскільки подальша бездіяльність може завдати тривалої шкоди національній спадщині, репутації країни та довірі громадськості». ***(Alex Scroxton. UK's cultural institutions failing on cyber security, warns PAC // TechTarget, Inc. (https://www.computerweekly.com/news/366645049/UKs-cultural-institutions-failing-on-cyber-security-warns-PAC). 24.06.2026).***

***

**«Дослідження компанії IO свідчить, що менеджери з кібербезпеки у Великій Британії скептично ставляться до прискореної сертифікації відповідності: 87% опитаних вважають, що швидкість сертифікації впливає на її надійність.** За результатами опитування 251 менеджера, виявлено занепокоєння щодо того, що підприємства можуть розглядати сертифікацію як кінцеву мету, а не як частину безперервного процесу підтримання засобів контролю, управління та нагляду, що призводить до збереження вразливостей навіть після отримання визнаного сертифіката. Багато респондентів надають більшого значення постійному моніторингу, ніж швидкій сертифікації: 31% вважають постійний моніторинг контролю найкращим показником стійкості, а 21% зазначають, що сертифікати, видані сторонніми організаціями, можуть швидко втратити актуальність після проведення аудиту… Опитування також показує, що людська оцінка залишається ключовою навіть у міру поширення автоматизації: респонденти зазначають, що людський досвід необхідний для оцінки точності автоматизованих заходів щодо дотримання вимог, тлумачення нормативних актів та перевірки якості автоматизованих доказів. Генеральний директор IO

стверджував, що поспіх із сертифікацією може призвести до прогалин у системі безпеки, а справжня стійкість залежить від того, чи заходи контролю впроваджуються, розуміються, контролюються та вдосконалюються з часом, а не просто документуються для перевірки… У дослідженні також підкреслюється комерційний тиск, що стоїть за сертифікацією, оскільки вона часто впливає на закупівлі та доступ до контрактів, але при цьому зазначається, що покупці дедалі частіше вимагають доказів того, що дотримання вимог є реальним і дієвим, а не лише формальністю на папері, завдяки чому постійне управління та очевидна стійкість стають конкурентною перевагою». ***(MARK TARRE. UK cybersecurity managers doubt fast-track certification // TechDay (https://securitybrief.co.uk/story/uk-cybersecurity-managers-doubt-fast-track-certification). 24.06.2026).***

***

**«На папері кіберстійкість у Великій Британії покращується: більшість організацій повідомляють про кращу прозорість, механізми контролю та розуміння кіберризиків, проте рівень впевненості суттєво знижується, коли йдеться про реальні інциденти.** Дослідження показують явний розрив між уявним прогресом та фактичною готовністю: хоча 81 % організацій вважають, що їхня стійкість покращилася, менше чверті впевнені, що їхні захисні системи витримають масштабну атаку… Ця розбіжність відображає зміну характеру виклику: причини невдач все менше пов’язані з відсутністю технологій, а все більше — з порушеннями координації, недостатньою прозорістю та прийняттям рішень під тиском. Ефективна стійкість тепер залежить від того, наскільки злагоджено взаємодіють люди, процеси та системи під час інциденту, особливо в складних гібридних середовищах, де відповідальність розподілена між внутрішніми командами, постачальниками керованих послуг та сторонніми організаціями…

Поведінка людей та ризики, пов’язані з постачальниками, залишаються основними вразливими місцями, а фішинг, компрометація ідентифікаційних даних та доступ сторонніх осіб продовжують бути типовими точками проникнення для зловмисників. Водночас зростаюча технологічна складність може гальмувати заходи реагування, оскільки перехресне використання інструментів створює «шум» та уповільнює прийняття рішень, що робить спрощення та інтеграцію дедалі важливішими… Поширення штучного інтелекту ще більше ускладнює ситуацію, оскільки зловмисники швидко використовують його для масштабування та прискорення атак, тоді як впровадження захисних заходів залишається обережним та обмеженим. Зрештою, стійкість більше не визначається кількістю розгорнутих інструментів, а оперативною готовністю — здатністю організації швидко реагувати, ефективно координувати дії та зберігати ясність у стресових ситуаціях, — що вимагає переходу від теоретичних можливостей до перевірених, інтегрованих та добре керованих стратегій реагування». ***(JASON SIMPER. The state of cyber resilience amongst UK organisations // TechDay (https://itbrief.co.uk/story/the-state-of-cyber-resilience-amongst-uk-organisations). 25.06.2026).***

***

**«Керівники британських компаній дедалі частіше вимагають від своїх команд з кібербезпеки відновити роботу бізнесу вже через кілька годин після кібератаки, хоча фахівці застерігають, що такі терміни часто є нереалістичними через складність процесів локалізації загроз, відновлення даних та перевірки стану мережі.** Згідно з нещодавнім дослідженням компанії Cohesity, ця зростаюча розбіжність особливо помітна на прикладі очікувань керівництва щодо повідомлення про інциденти протягом 30 хвилин або менше… Інтеграція штучного інтелекту в засоби безпеки прискорила виявлення загроз і сприяла досягненню цих амбітних цілей, проте повне відновлення все ще значною мірою залежить від людського досвіду та стратегічного прийняття рішень. Як наслідок, ці підвищені вимоги чинять величезний тиск на і без того перевантажені команди з безпеки, що посилює проблеми вигорання та утримання талановитих фахівців у галузі… Оскільки кіберзлочинці одночасно використовують штучний інтелект для здійснення все більш витончених атак, експерти наголошують, що для забезпечення справжньої кіберстійкості організаціям необхідно знайти баланс між автоматизованими технологіями та реалістичними цілями відновлення, добре перевіреними планами дій на випадок надзвичайних ситуацій і чіткою комунікацією між вищим керівництвом та фахівцями з безпеки». ***(Naveen Goud. UK CEOs want Cyber Attack recovery within Hours and not Days or Weeks // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/uk-ceos-want-cyber-attack-recovery-within-hours-and-not-days-or-weeks/). 26.06.2026).***

***

**«Згідно з доповіддю The Platforms Association та Deloitte, понад половина британських платформ роздрібних інвестицій за останній рік зіткнулася зі сплеском кіберінцидентів, що зумовлено насамперед фішингом на основі штучного інтелекту, програм-вимагачів та ризиками, пов'язаними з ланцюгом поставок.** Оскільки загальний обсяг активів, якими управляє цей сектор, перевищує 1,4 трлн фунтів стерлінгів, кібербезпека швидко перетворилася на критично важливий пріоритет на рівні ради директорів. Приблизно 78% опитаних компаній зараз мають у штаті окремого керівника з питань безпеки, а 67% щокварталу обговорюють кіберризики на рівні ради директорів. Щоб відобразити цю стратегічну важливість, 89 % компаній перевели свої кіберкоманди з ізольованих технологічних відділів у більш широкі підрозділи, що охоплюють всю організацію…

Для боротьби з цими загрозами понад половина компаній збільшила свої бюджети на кібербезпеку, причому середні щорічні витрати становлять від 1 600 до 4 000 фунтів стерлінгів на одного співробітника. Хоча дотримання нормативних вимог залишається важливим фактором, головним рушієм цих інвестицій є масштабна технологічна трансформація, в рамках якої особливий акцент робиться на покращенні можливостей виявлення загроз та реагування на них…

Однак галузь продовжує стикатися зі значними труднощами у підборі персоналу, оскільки на заповнення 77 % вакансій у сфері кібербезпеки — особливо для фахівців з управління ідентифікацією та реагування на загрози — йде від трьох до п'яти місяців. Лідери галузевих робочих груп з кібербезпеки наголошують, що

співпраця та обмін інформацією між компаніями є надзвичайно важливими для захисту інвесторів та галузі в цілому. З огляду на найближчі три–п’ять років компанії переносять свою увагу на нові виклики, такі як аутентифікація без паролів, автономні системи штучного інтелекту та майбутні вимоги до шифрування, зумовлені розвитком квантових обчислень». ***(Jonathan Easton. Investment platforms step up cyber spending as attacks rise // FStech (formerly Financial Sector Technology) (https://www.fstech.co.uk/fst/Investment_Platforms_Step_Up_Cyber_Spending_As_Attacks_Rise.php). 19.06.2026).***

***

**«Переглянута Директива ЄС про відповідальність за продукцію, яка набере чинності в грудні 2026 року, суттєво змінює правове поле для виробників — особливо тих, що випускають споживчі пристрої Інтернету речей (IoT) — шляхом розширення обсягу відповідальності та її більш тісного узгодження зі стандартами США, а в деяких аспектах — навіть перевищення їх.** Вона діє поряд з іншими нормативно-правовими актами ЄС, такими як Закон про кіберстійкість, Загальний регламент щодо безпеки продукції та Закон про дані, створюючи складне, перехресне регуляторне середовище, в якому недотримання вимог в одній сфері може спричинити більш широкі правові та фінансові наслідки… Директива приділяє особливу увагу кібербезпеці, визнаючи такі недоліки, як незахищені вразливості, неналежні оновлення або небезпечна конструкція, підставами для суворої відповідальності навіть після продажу продукції, особливо у випадках, коли виробники зберігають контроль за допомогою оновлень програмного забезпечення. Вона також запроваджує нові категорії шкоди, що підлягають відшкодуванню, зокрема втрату даних та психологічну травму, а також знижує доказові пороги, що збільшує ймовірність подання позовів та колективних дій. Крім того, виробники можуть нести повну відповідальність за компоненти сторонніх виробників або з відкритим кодом, інтегровані в їхню продукцію, при цьому їхні можливості стягувати витрати з постачальників є обмеженими… Як наслідок, виробники пристроїв Інтернету речей (IoT) стикаються з підвищеними ризиками на всіх етапах життєвого циклу продукції, у ланцюгу поставок та під час транскордонної діяльності, що вимагає вжиття проактивних заходів, таких як комплексне картування ризиків, посилення системи управління, чіткі політики оновлення та посилення договірних гарантій для забезпечення дотримання нормативних вимог та мінімізації зростаючих юридичних і фінансових ризиків на ринку ЄС». ***(Gregory Speier, Jamie L. Lanphear and Christian Leuthner. Cybersecurity, product liability, and consumer IoT: The EU’s emerging enforcement framework // Reed Smith LLP (https://www.reedsmith.com/articles/cybersecurity-product-liability-and-consumer-iot-the-eu-s-emerging-enforcement-framework/). 23.06.2026).***

***

**«Австралійська розвідувальна служба ASIO нещодавно попередила політиків та державних службовців про небезпеку обговорення секретної інформації в будь-яких транспортних засобах, особливо в підключених до мережі автомобілях, наголосивши на значних ризиках для конфіденційності та національної безпеки.** Це попередження з'явилося після того, як до автопарку федеральних політиків, що фінансується за рахунок платників податків, було додано сім моделей китайських електромобілів, хоча ця проблема стосується всіх сучасних підключених до мережі автомобілів незалежно від виробника. Згідно з дослідженням McKinsey, у 2021 році 50% автомобілів на дорогах були підключені до Інтернету, і очікується, що до 2030 року цей показник зросте до 95%... Ці автомобілі щодня генерують до 2 терабайтів даних за допомогою численних внутрішніх і зовнішніх датчиків, камер та підключених смартфонів. Вони збирають великий обсяг особистої інформації, включаючи точні геодані, особливості водіння, фізичні характеристики, телефонні контакти і навіть дуже інтимні зображення, про що свідчить звіт Reuters за 2023 рік щодо співробітників Tesla, які поширювали приватні відеозаписи клієнтів. Звіт Mozilla за 2023 рік виявив, що всі 25 автомобільних брендів, які він перевірив, не відповідають базовим стандартам конфіденційності, зазначивши, що виробники часто продають ці зібрані дані афілійованим компаніям та агрегаторам даних. Крім того, пасажири також наражаються на ризик, оскільки згідно з договорами купівлі-продажу водії несуть відповідальність за попередження їх про збір даних у салоні автомобіля… Щоб захистити себе, споживачам слід ознайомитися з політикою конфіденційності виробника, користуватися такими сервісами, як vehicleprivacyreport.com, відмовлятися від встановлення SIM-картки, вимикати функції збору даних у мобільних додатках для автомобілів або інформаційно-розважальних системах, а також завжди виконувати повне скидання налаштувань до заводських перед продажем або передачею автомобіля в оренду, хоча відмова від цих функцій може обмежити деякі можливості автомобіля». ***(Dennis B. Desmond. Are our cars spying on us? A cybersecurity expert explains how to stay safe // The Conversation Media Group Ltd (https://theconversation.com/are-our-cars-spying-on-us-a-cybersecurity-expert-explains-how-to-stay-safe-284088). 01.06.2026).***

***

**«Національний центр кібербезпеки Нової Зеландії (NCSC) опублікував рекомендації, покликані допомогти урядовим установам підготуватися до наслідків для кібербезпеки, пов'язаних із «передовими» системами штучного інтелекту — сучасними моделями, які можуть забезпечити набагато вищий рівень автоматизації, логічного мислення та здатності до прийняття рішень, ніж попередні версії ШІ.** NCSC описує передові системи ШІ як технологію подвійного призначення: ті самі можливості, що можуть покращити кіберзахист, також можуть допомогти зловмисникам проводити кібероперації швидше, дешевше та у більшому масштабі, потенційно посилюючи вплив відомих вразливостей, застарілих технологій та слабкої кібергігієни, що може

перетворитися на «шторм вразливостей» для організацій… У рекомендаціях наголошується, що для підвищення стійкості агентствам не обов'язково мати доступ до найсучасніших передових моделей; натомість готовність до реагування повинна ґрунтуватися на існуючих новозеландських вимогах та практиках у сфері кібербезпеки, зокрема на «Посібнику з інформаційної безпеки Нової Зеландії», «Рамках кібербезпеки NCSC», «Мінімальних стандартах кібербезпеки» та «Вимогах щодо захисної безпеки»… У якості найпершочергових завдань документ закликає відомства перевірити та покращити дотримання чинних стандартів, забезпечити чітку відповідальність керівництва за кіберризики, пов'язані з передовими технологіями штучного інтелекту, ознайомитися з відповідними рекомендаціями NCSC та виявити суттєві прогалини в системі безпеки, якими можуть скористатися зловмисники, що використовують штучний інтелект. У документі повторно наголошується на п'яти функціях Рамки кібербезпеки NCSC — керівництво та управління, виявлення та розуміння, запобігання та захист, виявлення та локалізація, а також реагування та відновлення — та підкреслюються базові заходи контролю, такі як управління ризиками, підвищення обізнаності персоналу з питань безпеки, безпечна конфігурація, своєчасне встановлення виправлень, багатофакторна автентифікація, доступ з мінімальними привілеями, виявлення аномалій, відновлення даних та надійне планування реагування на інциденти… Загалом у рекомендаціях стверджується, що передові технології штучного інтелекту, ймовірно, призведуть до збільшення швидкості, масштабів та складності кібератак, але найефективнішим способом зниження ризиків залишаються надійні базові заходи — встановлення оновлень, контроль доступу, моніторинг та реагування. Це відображає загальну думку про те, що штучний інтелект посилює існуючі кіберзагрози, а не створює цілком нові». ***(New Zealand's NCSC warns frontier AI could amplify cybersecurity risks // DiploFoundation (https://dig.watch/updates/new-zealand-frontier-ai-cyber). 04.06.2026).***

***

**«У своєму історичному рішенні Федеральний суд Австралії зобов'язав власника австралійської ліцензії на надання фінансових послуг (AFSL) сплатити штраф у розмірі 2,5 млн австралійських доларів, а також 500 000 австралійських доларів судових витрат на користь Австралійської комісії з цінних паперів та інвестицій (ASIC) у зв'язку з кібератакою, що призвела до викрадення 385 ГБ даних.** Це рішення стало першим випадком накладення цивільних санкцій за порушення вимог кібербезпеки в рамках загальних зобов'язань за ліцензією AFSL. Суд встановив, що компанія порушила Закон про корпорації 2001 року, не забезпечивши ефективне, добросовісне та справедливе надання послуг, не маючи достатніх ресурсів та нехтуючи своїми системами управління ризиками… Зокрема, компанія не мала належного плану реагування на інциденти та не проводила обов'язкового навчання з питань кібербезпеки, доручила питання IT-безпеки недостатньо підготовленому персоналу, виділяла недостатнє фінансування на заходи з кібербезпеки та не здійснювала моніторингу власних політик інформаційної безпеки. У рамках заходів з виправлення ситуації власник ліцензії AFSL тепер зобов'язаний залучити незалежного експерта для

нагляду за обов'язковою програмою забезпечення відповідності вимогам, щоб гарантувати належне управління своїми системами… Зрештою, це рішення є суворим попередженням для ліцензіатів AFS про те, що ASIC активно каратиме за недостатнє інвестування в кібербезпеку, причому суд зазначив, що штрафи та витрати на усунення порушень, які виникають у результаті, значно перевищують суму, яку довелося б витратити на впровадження належних заходів захисту з самого початку». ***(Cameron Abbott, Daniel Knight, Rob Pulham, Alex Parker, Madison Jeffreys. Australia- An AFS Licensee First- Receiving an Order to Pay AU$2.5 Million for Cybersecurity Failures // National Law Forum, LLC (https://natlawreview.com/article/australia-afs-licensee-first-receiving-order-pay-au25-million-cybersecurity). 22.06.2026).***

***

**«Австралійське управління зв'язку (ASD) планує протягом найближчих двох років вивести з обігу свою давню систему кібербезпеки «Essential Eight» та замінити її більш гнучкою та всеосяжною серією «Essentials», розробленою з урахуванням сучасних технологічних середовищ.** Хоча «Essential Eight» залишатиметься в користуванні протягом перехідного періоду, її поступово виводитимуть з обігу у міру впровадження нової системи. Ця зміна відображає обмеження «Essential Eight», яка спочатку була розроблена для локальних IT-систем і не забезпечує ефективного захисту сучасних хмарних середовищ, що базуються на моделі SaaS та стають дедалі складнішими…

Нова концепція «Essentials» буде зосереджена на більш широких результатах у сфері безпеки, а не на директивних заходах контролю, що дозволить організаціям адаптувати рекомендації до своїх конкретних технологій. Спочатку вона включатиме спеціальні рекомендації для корпоративних IT-систем, операційних технологій та хмарних середовищ, а в майбутньому може бути додано окремий розділ, присвячений агентному штучному інтелекту, що відображатиме нові ризики, такі як управління ідентифікацією нелюдських суб'єктів та атаки з використанням підстановки підказок. Концепція також наголошує на підході «глибокого захисту» та наданні пріоритету захисту критично важливих активів над традиційною периметральною безпекою…

Це оновлення також враховує давні занепокоєння щодо змін у вимогах до рівня зрілості в рамках «Essential Eight», через які складалося враження, що організації відстають, незважаючи на збереження свого рівня безпеки. Відокремивши заходи контролю від жорстких рівнів зрілості, нова система має на меті краще адаптуватися до мінливих загроз. ASD наголосило, що існуючі інвестиції у дотримання вимог «Essential Eight» залишатимуться актуальними в рамках нової моделі, оскільки відомство збирає відгуки представників галузі щодо першого проекту оновлених рекомендацій». ***(Juha Saarinen. ASD to retire Essential Eight cyber security framework within next two years // nextmedia Pty Ltd. (https://www.itnews.com.au/news/asd-to-retire-essential-eight-cyber-security-framework-within-next-two-years-626851). 24.06.2026).***

***

**«Уряд Японії та деякі з найбільших банків країни отримають доступ до платформи Anthropic Claude Mythos у рамках ініціативи з кібербезпеки, яку обговорив міністр фінансів Сацукі Катаяма.**

Вона сказала, що було створено державно-приватну робочу групу для вивчення ризиків, які ця модель може становити для фінансової системи…

Anthropic заявила, що Mythos Preview — це невипущена модель для оборонної роботи з кібербезпеки, такої як виявлення локальних вразливостей та тестування на проникнення.

Компанія виявила тисячі високосерйозних уразливостей, включаючи зумовлені помилками нульового дня, в основних операційних системах та веббраузерах.

Катаяма заявила, що кільком японським фінансовим групам було надано доступ до GPT-5.5 OpenAI для кіберзахисту за умовами обмеженого доступу…» ***(Japan to use Anthropic's Claude for bank cyber defense // Tech in Asia (https://www.techinasia.com/news/japan-anthropics-claude-bank-cyber-defense). 04.06.2026).***

***

**«Оскільки кіберзагрози дедалі більше впливають на національну безпеку, Тайвань та Індія стикаються зі зростаючим тиском щодо посилення співпраці, зокрема у відповідь на виклики, пов'язані з Китаєм.** Обидві країни стали частими мішенями кібератак: у 2025 році Тайвань щодня зазнавав у середньому 2,63 мільйона атак на свою критичну інфраструктуру, які часто пов'язані з військовою діяльністю Китаю, а в Індії було зафіксовано понад 265 мільйонів випадків виявлення кіберзагроз у мільйонах систем. В обох випадках ціллю стали критично важливі сектори, такі як енергетика, охорона здоров'я, фінанси та урядові мережі, що підкреслює вразливість їхніх цифрових екосистем та стратегічне використання кібероперацій у регіональній конкуренції…

Кібердіяльність, пов'язана з Китаєм, відіграє значну роль у цих загрозах: атаки на Тайвань часто збігаються з китайськими військовими маневрами, тоді як Індія стикається з вторгненнями в критичну інфраструктуру, зокрема з інцидентами, пов'язаними з перебоями в електропостачанні. Хоча до кіберінцидентів, спрямованих проти Індії, причетні й інші суб'єкти, наприклад угруповання з Пакистану, загальна тенденція вказує на те, що кібербезпека є ключовою сферою геополітичного суперництва…

І Тайвань, і Індія створили потужні інституційні механізми для протидії цим ризикам, зокрема спеціалізовані агентства з кібербезпеки та центри захисту інфраструктури. Ці можливості становлять основу для поглиблення співпраці, яка може включати обмін передовим досвідом, покращення взаємного розуміння систем кібербезпеки, а також поєднання індійського досвіду у сфері програмного забезпечення з сильними сторонами Тайваню в галузі апаратного забезпечення та напівпровідникових технологій. Розширення співпраці також може передбачати

обмін розвідданими, спільне реагування на інциденти, захист критичної інфраструктури та скоординовані дослідження й розробки…

Існує також потенціал для більш широкої багатосторонньої взаємодії, зокрема партнерства зі Сполученими Штатами, Японією та іншими союзниками, про що свідчать минулі тристоронні семінари з питань кібербезпеки. Інституціоналізація таких ініціатив та інтеграція Тайваню у відповідні регіональні механізми могли б сприяти підвищенню колективної стійкості. Незважаючи на те, що політичні та структурні обмеження залишаються, тісніша співпраця у сфері кібербезпеки відкриває практичну та стратегічно важливу можливість для зміцнення відносин між Тайванем та Індією та вирішення спільних викликів у сфері безпеки». ***(Sumit Kumar. Cybersecurity opens new path for Taiwan-India ties // Taiwan News (https://www.taiwannews.com.tw/news/6386806). 21.06.2026).***

***

**«Японія посилює свою систему кібербезпеки у відповідь на зростаючу загрозу кібератак на основі штучного інтелекту (ШІ), переглядаючи свою національну політику щодо ШІ — «Основний план з ШІ», який планується остаточно затвердити в липні.** Оскільки стрімкий прогрес у сфері генеративного та автономного ШІ збільшив можливості для зловживань, уряд тепер визнає кіберзагрози, пов’язані з ШІ, як значний ризик, що вимагає оновленого нагляду на національному рівні. Центральну роль у цих зусиллях відіграє Інститут безпеки ШІ, заснований у 2024 році, який оцінюватиме наслідки передових моделей ШІ для кібербезпеки та тісно співпрацюватиме з вітчизняними розробниками та урядами інших країн для отримання доступу до передових технологій та їх оцінки. На основі цих оцінок уряд планує спонукати постачальників ІТ-послуг прискорити впровадження заходів безпеки, таких як виправлення вразливостей, визнаючи, що традиційні засоби захисту можуть виявитися занадто повільними проти загроз, що базуються на ШІ…

У переглянутому плані також підкреслюється стратегічне значення автономного ШІ, відзначається його стрімке поширення у світі та його зв’язок із національною конкурентоспроможністю; водночас для усунення ризиків, пов’язаних із надмірною залежністю від ШІ, передбачається сприяння освіті, що сприяє збереженню навичок критичного мислення. Загалом підхід Японії спрямований на досягнення балансу між інноваціями та управлінням ризиками, при цьому наголошується на необхідності посилення міжнародної співпраці та вжиття проактивних заходів безпеки для вирішення нових викликів, що виникають у зв’язку з появою дедалі більш потужних систем ШІ». ***(Choi Young-jae. Japan boosts AI cyber defense through global model evaluation partnership // ASIATODAY CO., LTD. (https://en.asiatoday.co.kr/view.php?key=20260621001027062). 21.06.2026).***

***

**«Азербайджан офіційно створив Національне агентство з кібербезпеки (NCA) при Міністерстві цифрового розвитку та транспорту з метою зміцнення цифрової інфраструктури країни та підвищення її стійкості до кіберзагроз.** Створене указом президента від 2 червня, NCA буде виконувати функції центрального регуляторного та наглядового органу з питань кібербезпеки, відповідаючи за контроль дотримання вимог, координацію превентивних заходів проти кібератак та поширення загальнонаціональних попереджень про загрози. Агентство буде активно співпрацювати з урядовими органами, суб'єктами приватного сектору та міжнародними партнерами з метою розслідування та мінімізації кіберзагроз, а також надаватиме рекомендації громадськості, запобігатиме поширенню забороненої інформації в Інтернеті та боротиметься з незаконним збором персональних даних… Діючи як державна юридична особа з місцезнаходженням у Баку, NCA є другим централізованим центром кібербезпеки Азербайджану, який доповнює Національний центр кібербезпеки (NCC), заснований у 2023 році при Службі державної безпеки. У той час як новостворена NCA зосереджується на широкому національному регулюванні, інформуванні громадськості та загальному цифровому захисті, раніше створений NCC конкретно контролює безпеку в режимі реального часу, аналіз загроз та усунення вразливостей критичної інформаційної інфраструктури країни, що експлуатується великими державними та приватними підприємствами». ***(Nargiz Mammadli. Azerbaijan Establishes National Cybersecurity Agency to Enhance Cyber Resilience // Caspian News (https://caspiannews.com/news-detail/azerbaijan-establishes-national-cybersecurity-agency-to-enhance-cyber-resilience-2026-6-2-5/). 04.06.2026).***

***

**«Швидка цифровізація та амбітні технологічні цілі на Близькому Сході посилюють наслідки кібератак, які дедалі частіше здійснюються з використанням штучного інтелекту.** Згідно з глобальним опитуванням, проведеним компанією-розробником програмного забезпечення Optro, кожен четвертий респондент з ОАЕ за останні два роки стикався зі значними перебоями в роботі бізнесу через кібератаку з використанням штучного інтелекту або програм-вимагачів. Хоча штучний інтелект знижує бар'єри для кіберзлочинців — що викликає конкретні регіональні побоювання щодо створення автономним ШІ неконтрольованих точок відмови — він також є двосічним мечем, надаючи захисникам потужні засоби раннього попередження для виявлення загроз ще до їх реалізації… Незважаючи на наявність цих сучасних інструментів, опитування виявляє разючий розрив між сприйнятою та фактичною кіберстійкістю організацій. Хоча майже три чверті респондентів з ОАЕ залишаються дуже впевненими у своїй здатності досягти цілей відновлення під час серйозних збоїв, 62 % тих, хто нещодавно зіткнувся з інцидентом, не змогли відновити роботу в заплановані терміни, а у багатьох це зайняло більше ніж удвічі більше часу, ніж планувалося. Ці технічні виклики ускладнюються регіональними факторами, такими як геополітична напруженість та значна залежність від іноземних працівників… Крім

того, з огляду на те, що багато цифрових інцидентів пов'язані з уразливими місцями в інструментах сторонніх розробників, експерти застерігають: організації повинні перейти від порожніх обіцянок до реальних дій і взяти на себе зобов'язання цілеспрямовано інвестувати в активну оцінку та управління ризиками, пов'язаними з постачальниками, щоб забезпечити швидке відновлення роботи та надійну кібербезпеку». ***(Cody Combs. AI increasingly deployed to mount cyber attacks - and defences // The National (https://www.thenationalnews.com/future/technology/2026/06/22/internet-disruption-cyber-middle-east/). 22.06.2026).***

***

## ***Країни Африки***

**«За словами експерта з кібербезпеки Денні Майбурга, багато південноафриканських організацій вважають, що вони готові до кібератак, але насправді їхні плани реагування на інциденти часто виявляються неефективними під час реальних кризових ситуацій.** Спираючись на результати численних розслідувань випадків порушення безпеки, він наголосив, що компанії досі недооцінюють як ймовірність, так і масштаб атак, які можуть одночасно вивести з ладу сотні систем, а не окремі компоненти. Поширеною помилкою є те, що плани реагування та системи резервного копіювання зберігаються в тих самих середовищах, які стають уразливими, що робить їх недоступними, коли вони потрібні. Він також зазначив, що симуляції часто є нереалістичними, оскільки персонал готується заздалегідь, а не проходить випробування в умовах реального тиску, і що людський вплив кіберінцидентів часто ігнорується…

Майбург наголосив, що ефективне реагування залежить не стільки від великих витрат, скільки від практичної готовності, зокрема від надійної класифікації даних, безпечного офлайн-резервного копіювання та чіткого визначення пріоритетності критично важливих систем, що може забезпечити швидке відновлення навіть після серйозних атак. Він вказав на додаткові вразливі місця, такі як обхід керівниками заходів безпеки та ненавмисне погіршення ситуації співробітниками через недосконаліть комунікації або неправильні дії, підкресливши, що кібербезпека є відповідальністю всієї організації, а не лише проблемою IT-відділу. Він також вказав на важливість кіберстрахування, заодно застерігаючи від зберігання відповідних документів у системах, що зазнали вторгнення. Загалом, суть полягає в тому, що стійкість досягається завдяки реалістичному плануванню, дисциплінованим практикам та широкій обізнаності, а не лише завдяки технологіям чи формальним політикам». ***(Admire Moyo. Cyber crisis plans fail when reality hits // ITWeb Limited (https://www.itweb.co.za/article/cyber-crisis-plans-fail-when-reality-hits/Kjlyr7wBplQvk6am). 04.06.2026).***

***

**«Марокко посилює свою архітектуру кібербезпеки, щоб ефективніше захищати свою цифрову інфраструктуру державного сектору, що**

**розширюється, від зростаючих загроз.** Центральним елементом цієї ініціативи є майбутнє відкриття нового Центру оперативного реагування на кіберзагрози (SOC), про що оголосила заступниця міністра Амаль Ель-Фаллах Сегрушні. Працюючи у тісній співпраці з Генеральним директоратом з безпеки інформаційних систем (DGSSI), SOC буде постійно здійснювати моніторинг урядових мереж, централізувати дані та забезпечувати раннє виявлення, швидке реагування та ретельне розслідування кібератак…

Для підтримки цього нового центру міністерство реалізує комплексну стратегію, що базується на трьох напрямках і спрямована на забезпечення безпеки державних інформаційних систем. Перший напрямок зосереджений на профілактиці шляхом суворого управління ризиками, регулярних технічних аудитів, використання сучасних засобів захисту, таких як брандмауери нового покоління, та інтеграції вимог безпеки на початковому етапі проектування нових цифрових систем. Другий напрямок спрямований на управління шляхом посилення ролі відповідальних за безпеку інформаційних систем у державних установах та проведення регулярних оцінок ризиків. Нарешті, третій напрям акцентує увагу на підвищенні обізнаності та навчанні, забезпечуючи державних службовців постійними освітніми кампаніями та практичними рекомендаціями щодо безпечних цифрових практик. Завдяки цьому проактивному, багаторівневому підходу Марокко прагне забезпечити стійкість та безпеку своїх державних послуг, що дедалі більше переходять у цифровий формат». ***(Firdaous Naim. Morocco Plans New Cybersecurity Center to Strengthen Protection of Public Systems // Morocco World News (https://www.moroccoworldnews.com/2026/06/324034/morocco-plans-new-cybersecurity-center-to-strengthen-protection-of-public-systems/). 23.06.2026).***

***

## Кіберстрахування

**«Кіберстрахування дедалі більше впливає на підхід організацій до безпеки, оскільки страховики вимагають більш переконливих доказів наявності засобів контролю, готовності та можливостей реагування.** Для багатьох малих та середніх підприємств головним викликом стає не просто укладення договору страхування, а відповідність вимогам для отримання страхового покриття, управління страховими внесками та підтвердження того, що необхідні заходи безпеки — такі як багатофакторна автентифікація (MFA), захист кінцевих точок, встановлення оновлень, резервне копіювання та реагування на інциденти — дійсно впроваджені та функціонують. Це створює можливість для постачальників керованих послуг безпеки (MSSP), які вже впроваджують та контролюють ці заходи, допомогти клієнтам перетворити їхні операції з безпеки на чіткі, корисні докази для укладення договорів страхування, їхнього поновлення та реагування на інциденти…

MSSP відіграють ключову роль у забезпеченні документації, звітності та підтримки готовності до інцидентів, зокрема у підтвердженні страхового покриття систем, відстеженні вразливостей, перевірці цілісності резервних копій та

підтримці робочих процесів реагування на інциденти. Однак їхня роль має свої межі: вони повинні зосереджуватися на технічній та оперативній безпеці, залишаючи тлумачення страхових полісів, прийняття рішень щодо страхового покриття та юридичні питання на розсуд брокерів і консультантів. Чіткий розподіл обов'язків допомагає захистити як клієнтів, так і постачальників послуг…

Зростаюче значення кіберстрахування також висвітлює поширені непорозуміння, зокрема щодо відмінності між комплексними страховими полісами та більш вузькими кібергарантіями, пов'язаними з конкретними продуктами чи послугами. Хоча страхування може покривати широкий спектр фінансових збитків, гарантії забезпечують обмежений та умовний захист і не повинні розглядатися як заміна страхування. Загалом, MSSP дедалі частіше виступають у ролі партнерів, які допомагають клієнтам підвищити рівень готовності до забезпечення безпеки, зменшити ризики та спростити доступ до страхування, а не як страховики». ***(Cyber insurance readiness is an MSSP service opportunity // CyberRisk Alliance (https://www.msspalert.com/news/cyber-insurance-readiness-is-an-mssp-service-opportunity). 04.06.2026).***

***

**«Згідно з останнім звітом «Global Cyber Claims Trends Report», опублікованим страховим брокером Marsh, у 2025 році кількість повідомлень про страхові випадки, пов'язані з кіберзагрозами, у Європі зменшилася вперше за останні три роки; це зниження зумовлене вдосконаленням практик кібербезпеки та зменшенням кількості масштабних системних інцидентів.** Незважаючи на таке зниження загальної частоти, серйозність та складність кіберінцидентів залишаються серйозною проблемою для галузі… У звіті наголошується, що порушення конфіденційності та випадки втрати даних є найпоширенішими проблемами, які фігурують у 73 % заяв про страхові випадки; за ними йдуть перебої в діяльності, спроби шантажу, випадки відповідальності та шахрайські перекази. Найбільш уразливим сектором виявилася промисловість, на яку припадає 20 % усіх повідомлень, при цьому значну частку інцидентів також становлять фінансові установи та компанії, що надають професійні послуги… Флоріан Сеттлер, керівник відділу управління кіберінцидентами компанії Marsh у Європі, зазначив, що ризики, пов'язані з порушенням конфіденційності, соціальна інженерія та вразливості сторонніх систем є основними чинниками, що зумовлюють ці дедалі дорожчі сценарії збитків. У міру еволюції кіберзагроз та посилення регуляторних вимог експерти наголошують, що організації повинні не лише зосереджуватися на профілактиці, а й використовувати можливості ринку кіберстрахування для отримання експертних знань щодо ризиків, ресурсів для реагування на інциденти та фінансового захисту, необхідних для ефективного відновлення після складних кіберінцидентів». ***(George McDade. Annual cyber notifications fall across Europe – Marsh // Newsquest Media Group Limited (https://www.insurancetimes.co.uk/news/annual-cyber-notifications-fall-across-europe-marsh/1458927.article). 24.06.2026).***

***

**«Значна частина малих та середніх підприємств (МСП) у всьому світі стикалася з кібератаками, проте рівень поширення кіберстрахування залишається низьким, через що багато підприємств не мають достатнього захисту.** Опитування GlobalData за 2025 рік показало, що 34,7 % МСП у світі — і понад 40 % у Німеччині — зазнали кіберінцидентів протягом останніх років, але лише 16,8 % мають окремі поліси кіберстрахування. Хоча кількість страхових випадків, пов'язаних із кіберзагрозами, у Європі у 2025 році зменшилася, головним чином через зменшення кількості масштабних інцидентів, серйозність та фінансові наслідки інцидентів продовжують зростати, що посилює тиск на страхові премії… Багато малих та середніх підприємств недооцінюють значення кіберстрахування або відлякуються високою вартістю, незважаючи на те, що вони є більш вразливими, ніж великі організації, через слабкіші засоби захисту. Як наслідок, серйозний кіберінцидент може мати тяжкі фінансові наслідки, що потенційно може призвести до неплатоспроможності. Ця ситуація висвітлює прогалину в системі захисту, що спонукає страховиків зробити страхове покриття більш доступним та підтримати малі та середні підприємства шляхом кращого моніторингу ризиків та вдосконалення практик кібербезпеки…» ***(Small businesses are most at risk yet least insured against cyberattacks // GlobalData Plc (https://www.lifeinsuranceinternational.com/analyst-comment/small-businesses-most-at-risk-insured-cyberattacks/). 26.06.2026).***

***

## Кібервійни та протидія зовнішній кібернетичній агресії

**«Австралійська організація з питань безпеки та розвідки (ASIO) нещодавно запобігла кібератаці, організованій державою, метою якої було саботування мережі критичної інфраструктури після того, як хакерам вдалося отримати доступ до облікових даних активних користувачів, зокрема співробітників служби IT-безпеки.** Під час щорічної оцінки загроз, проведеної ASIO, генеральний директор Майк Берджес наголосив на надзвичайній небезпеці таких інцидентів, класифікувавши їх як пряму загрозу як для життя людей, так і для австралійського способу життя. У відповідь на цю зростаючу небезпеку ASIO створила спеціальну групу, призначену саме для боротьби з кіберсаботажем… Берджес попередив, що це не поодинокий випадок; майже кожна країна в цьому регіоні зазнала атак з боку кіберапарату того самого державного суб'єкта. Зрештою, ця повсюдна й постійна загроза становить серйозний і все більш гострий виклик на майбутнє, змушуючи країни приймати складні рішення щодо розподілу обмежених ресурсів для захисту та управління критичною інфраструктурою в умовах глобальної безпеки, що дедалі погіршується». ***(Cyberattacks pose a 'threat to life' in Australia // FoundryCo, Inc. (https://www.csoonline.com/article/4190054/cyberattacks-pose-a-threat-to-life-in-australia.html). 26.06.2026).***

***

**«За словами спостерігачів, які відвідали минулого тижня конференцію CyCon в Естонії, НАТО добре підготовлене до масштабних військових атак із застосуванням звичайної зброї, але не здатне ефективно протидіяти постійним кібератакам Росії низької інтенсивності, які не досягають порогу збройного конфлікту.** Поки альянс зосереджений на наданні рішучої відповіді на масштабну агресію, Росія та Китай використовують цю прогалину, здійснюючи постійні провокації в мирний час. Сполучені Штати виступають за «постійну взаємодію» через своє Кіберкомандування, яке активно знижує можливості супротивника, але НАТО повільніше впроваджує цей проактивний підхід. Обговорення на конференції показали, що все більше визнається необхідність покращення здатності альянсу протидіяти російській кібердіяльності, зокрема шляхом розширення операцій «полювання вперед» — бажано під керівництвом європейських держав, а не з надмірною залежністю від США — та, можливо, проведення власних наступальних кібератак проти підрозділів ГРУ, які беруть участь у диверсійних кампаніях, що спричинили пожежі на оборонних заводах та замахи на вбивство по всій Європі…

Окремо Центральне командування США підтвердило, що супротивники використовують загальнодоступні дані геолокації для виявлення та спостереження за американськими військами у зонах бойових дій, зокрема в Перській затоці. Ця інформація підкреслює давні ризики для національної безпеки, пов'язані з екосистемою комерційної реклами, що базується на стеженні, яка дозволяє супротивникам відстежувати переміщення військ, особливості повсякденного життя та місця скупчення людей для здійснення ракетних, безпілотних або саморобних вибухових пристроїв. Поточна політика Міністерства оборони щодо мінімізації ризиків, така як відключення служб визначення місцезнаходження або скидання рекламних ідентифікаторів на робочих пристроях, вважається нереалістичною та недостатньою, особливо з огляду на використання особистих телефонів та сучасних методів відстеження, таких як ідентифікація пристроїв за їхніми «відбитками пальців»…

З більш позитивного боку, цього тижня відбулися три обнадійливі події: компанія Microsoft відмовляється від багатофакторної аутентифікації та відновлення облікових записів за допомогою SMS для особистих акаунтів через масові зловживання цією функцією з метою захоплення облікових записів, натомість заохочуючи користувачів переходити на використання парольних ключів; CrowdStrike, Google та Shadowserver Foundation ліквідували ботнет Glassworm, який атакував розробників за допомогою шкідливих програмних пакетів і використовував складні канали управління, включаючи блокчейн Solana та Google Calendar; а IBM оголосила про ініціативу вартістю 5 мільярдів доларів під назвою Project Lightwell, в рамках якої буде залучено 20 000 інженерів, що використовуватимуть інструменти штучного інтелекту для виявлення та усунення вразливостей у програмному забезпеченні з відкритим кодом…» ***(Tom Uren. NATO's Cyber Approach Needs Change // The Lawfare Institute (https://www.lawfaremedia.org/article/nato's-cyber-approach-needs-change). 05.06.2026).***

***

**«ФБР відкрило в місті Хантсвіллі, штат Алабама, макет міста площею 22 000 квадратних футів, створений спеціально для проведення тренувань із кібервійни з ефектом повного занурення.** Цей унікальний критий комплекс, відомий як «Kinetic Cyber Range», складається з реалістичних, повністю облаштованих будівель, серед яких продуктовий магазин, готель, будівля суду та житлові будинки, усі оснащені діючими цифровими системами та мережами… Мета цього полігону — підготувати оперативників, аналітиків та судових експертів до реальних розслідувань шляхом моделювання складних сценаріїв, таких як атака програм-вимагачів на мережу лікарні або вилучення цифрових доказів з блоку управління автомобіля. З моменту відкриття минулого року на полігоні пройшли підготовку понад 1 400 співробітників, які отримали практичний досвід, який, за словами керівництва, є «максимально наближеним до реальних умов» перед тим, як вони зіткнуться з реальними операціями на місцях». ***(FBI reveals 22,000-square-foot fake town used to train agents for cyber warfare // NYP Holdings, Inc. (https://nypost.com/2026/06/12/us-news/fbi-reveals-22000-square-foot-fake-town-in-alabama-used-to-train-agents-for-cyber-warfare/). 12.06.2026).***

***

**«Кількість та рівень складності кібератак на космічний сектор різко зросли на тлі останніх геополітичних конфліктів: за даними експертів, після військових операцій за участю Ірану рівень активності зріс на 400%.** На відміну від минулих конфліктів, де переважав хактивізм нижчого рівня, зараз спостерігається злиття сил державних суб'єктів та скоординованих угруповань, які проводять тривалі та більш досконалі кампанії, спрямовані проти оборонної, аерокосмічної та космічної інфраструктури. Групи, пов'язані з Іраном, причетні до атак на операторів супутників, космічні агентства та великих оборонних підрядників, зокрема, заявляється про випадки масштабного викрадення даних та цілеспрямованих атак на персонал… Зростання активності частково зумовлене штучним інтелектом, який знижує бар'єри для вторгнення, дозволяє швидше виявляти вразливості та масштабувати більш складні атаки, хоча він також надає переваги в плані захисту. Однак організації не встигають вчасно усувати вразливості, тому переносять акцент з профілактики на виявлення та локалізацію, оскільки штучний інтелект прискорює створення вразливостей, які можна експлуатувати… Незважаючи на ці зміни, типові точки вторгнення залишаються в основному незмінними: наземні системи, IT-середовища, управління ідентифікацією та ланцюги постачання є основними вразливими місцями, тоді як прямі атаки на космічні апарати все ще трапляються рідше, але приділяється їм дедалі більше уваги. Загалом сектор стикається зі зростаючим системним ризиком, оскільки геополітична напруженість, технологічна взаємозалежність та можливості, що базуються на штучному інтелекті, у сукупності посилюють загрози у кіберпросторі». ***(Leandra Bernstein. Space Sector Faces 400% Surge in Cyberattacks Amid Iran War, Experts Say // Access Intelligence, LLC (https://www.satellitetoday.com/cybersecurity/2026/06/23/space-sector-faces-400-surge-in-cyberattacks-amid-iran-war-experts-say/). 23.06.2026).***

***

**«Кіберконфлікт дедалі більше стає центральним аспектом сучасної війни, причому атаки спрямовані на критичну інфраструктуру, таку як банківські системи, охорона здоров'я, енергетика, телекомунікації та урядові мережі, особливо в регіонах, що швидко переходять на цифрові технології, таких як Близький Схід...** У міру зростання геополітичної напруженості кібератаки стають більш скоординованими, руйнівними та взаємопов'язаними, залучаючи до себе як державних суб'єктів, так і хактивістів та кіберзлочинні угруповання, тактика та мотивація яких дедалі більше стираються. Характер атак змінився: від шпигунства до операцій, здатних спричинити реальні збитки, включаючи руйнівне шкідливе програмне забезпечення та атаки на операційні технології, що підкреслює зростаючу конвергенцію кіберризиків та фізичних ризиків. Штучний інтелект прискорює цю тенденцію, знижуючи бар'єри для зловмисників, водночас посилюючи оборонні можливості, що інтенсифікує кібергонку озброєнь…

Водночас розширення цифрових екосистем та взаємопов'язаних ланцюгів постачання створює нові вразливості, причому сторонні постачальники та компоненти з відкритим кодом стають ключовими слабкими місцями, якими зловмисники користуються для отримання непрямого доступу. Це зробило стійкість ланцюгів постачання такою ж важливою, як і внутрішню безпеку, особливо в секторах, що мають вирішальне значення для національної стабільності та економічної безперервності. Тому організації змушені переходити від реактивних підходів до кібербезпеки до проактивного захисту, заснованого на аналітиці, використовуючи дані про загрози в режимі реального часу для передбачення та стримування атак до їх ескалації. Оскільки інциденти тепер можуть поширюватися ланцюговим чином по взаємопов'язаних системах і галузях, кіберстійкість стала пріоритетом на рівні керівництва — це вже не просто технічне питання, а стратегічний імператив, пов'язаний із безперебійністю діяльності, економічною безпекою та національною стійкістю». ***(How geopolitical instability is reshaping cyber resilience strategies // Vibe Media Group (https://fastcompanyme.com/fastco-work/how-geopolitical-instability-is-reshaping-cyber-resilience-strategies/). 25.06.2026).***

***

**«За даними іранських опозиційних джерел, Корпус вартових ісламської революції (IRGC) керує розгалуженою та дедалі більш досконалою мережею кібервійни, що налічує близько 3 000 кібербатальйонів, які проводять електронні та розвідувальні операції як всередині Ірану, так і за його межами.** Хоча багато підрозділів діють на території країни, деякі з найскладніших операцій, за повідомленнями, виконують групи, що базуються в Європі, зокрема багатонаціональні оперативники, завербовані підрозділом «Quds» IRGC. Ці підрозділи постійно проходять навчання та отримують підтримку від російських і китайських експертів, що свідчить про зростаючу залежність Ірану від іноземних партнерів у справі посилення своїх кіберможливостей…

Ця мережа, яку часто називають «Іранською кіберармією», займається широким спектром діяльності, включаючи шпигунство, кібератаки, крадіжку даних та психологічні операції, спрямовані на вплив на громадську думку, поширення

дезінформації та підрив позицій супротивників. Серед її цілей — об'єкти критичної інфраструктури, такі як енергетичні системи, банки, телекомунікації, транспорт, а також урядові та оборонні мережі. Іранська кіберстратегія робить акцент на довгостроковому проникненні: зловмисники часто інфільтруються в мережі за кілька місяців або років до початку операцій, спрямованих на порушення нормального функціонування…

Кібероперації Ірану покликані стати недорогою та прихованою альтернативою традиційним військовим силам, що дозволяє країні чинити тиск на сильніших супротивників, зберігаючи при цьому можливість переконливого заперечення своєї причетності. Тактика часто ґрунтується на соціальній інженерії, зокрема на видаванні себе за осіб, яким довіряють, з метою отримання доступу до конфіденційної інформації. Численні угруповання, пов'язані з IRGC, здійснювали атаки на Близькому Сході та за його межами, зокрема кампанії, спрямовані проти інфраструктури США; іноді вони швидко мобілізувалися у відповідь на геополітичні події, а їхні можливості дедалі більше посилюються за допомогою інструментів штучного інтелекту. У міру того, як Іран продовжує розширювати свої кіберможливості, зростає занепокоєння щодо його здатності проводити глобальні операції проти окремих осіб, установ та критично важливих систем». ***(Dalshad Hussein. Inside Iran's Cyber War Machine // Middle East Broadcasting Networks, Inc. (https://alhurra.com/en/23515). 22.06.2026).***

***

**«…Межа між атаками з використанням програм-вимагачів, мотивованими фінансовою вигодою, та кібершпигунством з боку держав стає дедалі розмитішою, оскільки хакери, що діють за підтримки держави, використовують інструменти та методи кіберзлочинців для маскування своїх операцій.** У нещодавньому звіті NCC Group було наведено приклад того, як група кібершпигунів MuddyWater, пов'язана з Міністерством розвідки та безпеки Ірану, успішно видала себе за угруповання-вимагачів Chaos, використовуючи листи з вимогами викупу, канали переговорів та сайти з витоками даних, щоб приховати свої справжні цілі зі збору розвідданих… Ця конвергенція тактик виходить за межі Ірану; операції, що здійснюються за підтримки держави з боку Китаю, Росії та Північної Кореї, також використовують моделі «вимагального ПЗ як послуги», готові інструменти та шкідливе ПЗ з даркнету для ведення шпигунства та викрадення даних. Діючи під прикриттям відомих брендів-вимагачів та спільно використовуючи інфраструктуру з кіберзлочинцями, державні суб'єкти не лише затуманюють приналежність до цих дій, а й створюють можливість для правдоподібного заперечення своєї причетності… Отже, організації більше не можуть вважати, що інцидент із використанням програм-вимагачів має суто фінансову мотивацію. Щоб орієнтуватися в цьому складному середовищі загроз, експерти з безпеки наголошують, що в зрілих оборонних стратегіях пріоритет повинні мати аналіз поведінки, оперативний контекст та розуміння цілей зловмисників, а не традиційні методи виявлення на основі сигнатур». ***(Danny Palmer. Iran-Linked MuddyWater Poses as Ransomware Gang to Mask Cyber***

***Espionage // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/iranlinked-muddywater-poses-as/). 24.06.2026).***

***

## *Створення та функціонування кібервійськ*

**«У новому звіті групи експертів з питань політики та колишніх військових керівників пропонується створити спеціальні Кібервійська США, порівнянні з такими видами збройних сил, як Сухопутні війська чи ВМС, з метою зміцнення можливостей країни у сфері цифрової оборони проти дедалі більш витончених загроз.** Створення запропонованих сил обійдеться в суму до 11 мільярдів доларів, вони включатимуть близько 30 000 осіб — разом із членами Національної гвардії та цивільними особами — і можуть бути готові до дій протягом 12–18 місяців. Вони можуть діяти як самостійний підрозділ у складі Пентагону або бути підпорядковані армії…

У цій рекомендації висловлено занепокоєння тим, що, хоча Міністерство оборони вже має десятки тисяч співробітників, задіяних у кібероперація̈х, а на Кіберкоманду виділено значні кошти, нинішня структура не має достатніх можливостей та потенціалу для зростання, необхідних для протидії зростаючим загрозам з боку таких супротивників, як Росія та Китай. Прихильники цієї ідеї стверджують, що кіберпростір є окремою сферою ведення війни, яка потребує створення окремого спеціалізованого виду збройних сил, особливо з огляду на те, що кібероперації дедалі частіше передбачають постійну взаємодію з супротивниками…

Ця пропозиція з’явилася на тлі зростання двопартійної підтримки в Конгресі, де законодавці незадоволені нездатністю існуючих видів збройних сил забезпечити Кіберкоманду необхідним персоналом та підтримкою. Очікується, що деякі законодавці запропонують заходи, узгоджені з висновками звіту, тоді як тривають додаткові дослідження щодо доцільності створення Кіберзбройних сил. Загалом ця ініціатива відображає поширену думку про те, що створення спеціалізованого кібервійськового підрозділу стає неминучим, а прихильники закликають до активних дій, а не до очікування, поки криза змусить провести реформи». ***(Martin Matishak. New cyber force would cost up to $11 billion to start, commission says // Recorded Future News (https://therecord.media/new-cyber-force-would-cost-11-billion-commission). 03.06.2026).***

***

**«Запропоновані Кібервійська США, описані в нещодавньому звіті експертів з питань політики, стануть спеціалізованим військовим підрозділом, орієнтованим на наступальні та оборонні кібероперації; вартість їх створення перевищить 11 мільярдів доларів, а чисельність особового складу становитиме близько 30 000 осіб.** Створені з урахуванням того, що їхнє формування є неминучим, ці війська зможуть досягти початкової бойової готовності протягом 18 місяців і повністю розгорнутися за кілька років. Унікальність цієї моделі полягає в

тому, що вона передбачає, що особовий склад буде складатися переважно з офіцерів, прапорщиків, цивільних осіб та підрядників, виключаючи традиційний рядовий склад. Обґрунтуванням цього є те, що кіберролі вимагають високого рівня технічних знань та відповідальності, що більше відповідає вищим званням, а також те, що нинішні системи оплати праці рядового складу є недостатніми для залучення та утримання талановитих кадрів…

Запропонована структура передбачає поділ кар'єрних шляхів на управлінські посади для офіцерів та технічні напрямки для унтер-офіцерів, що має на меті відобразити галузеві практики та забезпечити чіткіші перспективи просування по службі й кращу оплату праці. Однак критики стверджують, що виключення рядового складу може підірвати культуру, гнучкість та практичні навички, які традиційно були важливими для військових операцій, оскільки саме рядові часто виконують критично важливі технічні та оперативні завдання. Також висловлювалися побоювання, що менші за чисельністю збройні сили з переважною кількістю офіцерів можуть обмежити розвиток талантів та знизити здатність виявляти й готувати високопродуктивних військовослужбовців…

Питання оплати праці залишається головним викликом, оскільки військові посади у кіберсфері змушені конкурувати з більш високооплачуваними вакансіями у приватному секторі. Хоча прихильники цієї ідеї стверджують, що місія, репутація та змістовна робота є ключовими мотиваційними факторами, інші вважають, що структуру оплати праці можна вдосконалити без скасування посад рядового складу. У звіті висловлюється думка, що спеціалізовані кібервійська могли б ефективніше управляти власним бюджетом та системою заохочень, що з часом могло б вирішити ці проблеми…

Загалом, ця пропозиція свідчить про те, що все ширше визнається: кіберпростір є окремою сферою, яка потребує спеціалізованої організації та ресурсів; водночас вона висвітлює поточні дискусії щодо структури, управління кадрами та того, як найкраще забезпечити баланс між технічною експертизою, оперативною ефективністю та стабільністю кадрового складу». ***(Drew F. Lawrence. A Cyber Force without enlisted? New report poses model for standalone military cyber organization // DefenseScoop (https://defensescoop.com/2026/06/05/a-cyber-force-without-enlisted-new-report-poses-model-for-standalone-military-cyber-organization/). 05.06.2026).***

***

## Кіберзахист критичної інфраструктури

**«Галузь морських перевезень, яка є основою світової торгівлі, переживає стрімку цифрову трансформацію: такі технології, як автоматизація, дистанційний моніторинг та інтегровані IT/OT-системи, підвищують ефективність, але водночас значно розширюють площину для кібератак.** Як наслідок, порти та судна дедалі частіше стають мішенями кіберзагроз, зокрема програм-вимагачів, шкідливого програмного забезпечення, фішингу, підробки GPS-сигналів та соціальної інженерії. Реальні інциденти, такі як атаки на порти

Сіетла, Нагої та Антверпена, демонструють, як збій у роботі може зупинити операції, вплинути на глобальні ланцюги постачання та навіть сприяти злочинній діяльності. Нові технології також виявляють вразливості в застарілих системах та підкреслюють нестачу кваліфікованих фахівців з кібербезпеки…

У відповідь на це регуляторні органи посилюють вимоги: Берегова охорона США запроваджує нові правила, що передбачають обов'язкове впровадження програм управління ризиками кібербезпеки, планів реагування на інциденти, протоколів звітності та відповідності міжнародним стандартам, а також встановлює поетапні терміни виконання вимог, які триватимуть до 2027 року. Однак реалізація цих заходів залишається складним завданням, зокрема через обмеженість ресурсів, організаційну втому та нечіткість розподілу відповідальності в морських організаціях, де такі посади, як спеціаліст з кібербезпеки, часто відсутні або недостатньо чітко визначені. Менші оператори можуть мати проблеми з ресурсами, тоді як більші стикаються зі складнощами у впровадженні…

Зміни в ландшафті загроз, зокрема активізація діяльності суб'єктів, пов'язаних із державами, підкреслюють необхідність комплексного кіберфізичного підходу, який інтегрує кібербезпеку в систему операційної стійкості. Це вимагає чіткого управління, спеціалізованих знань у морській сфері, а також впровадження структурованих механізмів, навчання та передових практик. Зрештою, у міру розширення мережевої взаємодії забезпечення безпечних і надійних морських операцій є надзвичайно важливим для підтримання стабільної та ефективної світової торгівлі». ***(Annie McIntyre. Unite, Prepare and Enable Maritime Cyber Readiness // New Wave Media Int (https://www.maritimeprofessional.com/news/unite-prepare-enable-maritime-cyber-419803). 02.06.2026).***

***

**«Оскільки загроза кібервійни проти критичної інфраструктури США переростає зі стратегічної проблеми в оперативну реальність, федеральні відомства повинні терміново та на випередження посилити свої захисні заходи до того, як відбудуться атаки.** Нещодавнє опитування виявило небезпечний «розрив у впевненості» всередині уряду: хоча 81% респондентів з федеральних органів вважають себе готовими до кібервійни, майже 60% визнають, що їхні відомства раніше піддавалися хакерським атакам і залишаються недостатньо захищеними. Ця вразливість посилюється стрімким зростанням кількості атак на основі штучного інтелекту (з якими за останній рік зіткнулися 58% відомств) у поєднанні з критичною нестачею внутрішніх фахівців для управління рішеннями з безпеки на основі штучного інтелекту… Щоб ефективно протидіяти цим загрозам, що постійно еволюціонують, федеральні служби безпеки повинні впровадити комплексні стратегії управління кіберризиками, засновані на п'яти ключових принципах. По-перше, відомства повинні відмовитися від підходу, орієнтованого виключно на дотримання вимог, на користь забезпечення видимості та захисту кожного активу в режимі реального часу. По-друге, вони повинні активно просувати цифрову модернізацію, оскільки зупинка проектів трансформації через побоювання щодо безпеки змушує їх покладатися на застарілі системи, які легко піддаються зловживанням. По-третє, агентства повинні сміливо впроваджувати

можливості штучного інтелекту та машинного навчання для автоматизації аналізу ризиків та відповіді на зростаючу інтенсивність сучасних атак. По-четверте, вони повинні перейти від реактивного реагування на інциденти до проактивного захисту на основі розвідданих, щоб забезпечити безперервність виконання завдань під час атак… Нарешті, керівництво федеральних органів влади має переглянути структуру своєї кіберзахисту, щоб забезпечити постійний моніторинг ситуації в усьому цифровому середовищі. Відмовившись від ізольованих, реактивних рішень на користь проактивного управління площею атаки, федеральний уряд зможе забезпечити стійкість, необхідну для захисту національної безпеки». ***(Joe Wingo. Cyberwarfare Reaches a Boiling Point for Federal Leaders // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/cyberwarfare-reaches-a-boiling-point-for-federal-leaders/). 03.06.2026).***

***

**«Безпека авіації, яка тривалий час зосереджувалася на фізичній та механічній надійності, тепер нерозривно пов'язана з кібербезпекою, що стала одним із основних операційних ризиків, здатних спричинити фінансові збитки, юридичну відповідальність та серйозні порушення нормального функціонування.** У міру різкого зростання цифрових загроз для галузі авіація дедалі частіше розглядається як головна ціль, оскільки вона є критичною інфраструктурою, що має глобальне економічне та геополітичне значення, а також через те, що зростаюча взаємопов'язаність галузі — від «розумних» аеропортів та інтегрованих ланцюгів постачання до авіаційних систем, що залежать від програмного забезпечення, — продовжує розширювати площину атаки… До основних загроз належать програми-вимагачі, крадіжка облікових даних, несанкціонований доступ та атаки, що фінансуються державою, спрямовані на інтелектуальну власність та інфраструктуру, які по-різному впливають на авіакомпанії, аеропорти, бортові системи та виробників. У відповідь на це галузь переходить від реактивного захисту до проактивного управління ризиками: кібербезпека в авіації інтегрується в системи управління безпекою, посилюються міжнародні та нормативні рамки, а ключове значення набувають такі передові практики, як архітектура «нульової довіри», постійна верифікація та навчання персоналу… Страхування також еволюціонує від механізму виплати відшкодувань до партнера у сфері мінімізації ризиків та забезпечення стійкості, тоді як нові технології, такі як штучний інтелект, використовуються для виявлення аномалій та реагування швидше, ніж це здатна зробити людина. У міру розвитку передової повітряної мобільності зацікавлені сторони наполягають на принципі «безпека ще на етапі проектування», що свідчить про все ширше усвідомлення того, що кібербезпека — це не лише питання інформаційних технологій, а й фундаментальна складова авіаційної безпеки, безперебійності бізнесу та операційної довіри». ***(Global Aerospace Provides Insights on Understanding the Modern Cybersecurity Threat Landscape, Common Vulnerabilities, and Aviation Cybersecurity Best Practices // yahoo! finance (https://uk.finance.yahoo.com/news/global-aerospace-provides-insights-understanding-163200305.html). 25.06.2026).***

***

**«Компанія з кібербезпеки Resecurity опублікувала серйозне попередження про те, що портові адміністрації та морські оператори стикаються з дедалі більшим ризиком кібератак — ця загроза особливо гостро проявилася під час нещодавнього інциденту з використанням програм-вимагачів, жертвою якого стала адміністрація одного з портів Адріатичного моря.** Під час цієї атаки група хакерів «Anubis», що використовує програмне забезпечення для вимагання викупу, викрала конфіденційні дані — зокрема плани безпеки та кадрові документи — і вимагала викуп у розмірі 10 мільйонів доларів, що призвело до зриву регіональної логістики. Оскільки морський сектор, на який припадає приблизно 90 відсотків світової торгівлі, дедалі більше покладається на взаємопов'язані операційні та інформаційні системи, його розширена «поверхня атаки» стала надзвичайно привабливою для кібершпигунства та дестабілізації… Зловмисники часто використовують відомі вразливості в системах, підключених до Інтернету, таких як VPN-пристрої, що не мають багатофакторної автентифікації. Ця цифрова вразливість посилюється гібридними тактиками, такими як підробка сигналів GPS та AIS, особливо в регіонах, що зазнають впливу поточних геополітичних конфліктів в Україні та на Близькому Сході. З огляду на те, що минулі інциденти вже спричинили значні глобальні затримки з перевезення вантажів та фінансові збитки, компанія Resecurity прогнозує, що кіберзагрози для морської інфраструктури лише посилюватимуться у міру подальшої модернізації портів. Відповідно, компанія настійно закликає морські організації впровадити проактивне управління вразливостями та суворо дотримуватися встановлених міжнародних стандартів кібербезпеки для захисту глобальних ланцюгів постачання». ***(Resecurity Warns Maritime Sector Faces Rising Cyber Threats // The Defense Post (https://thedefensepost.com/2026/06/26/maritime-sector-cyber-threats-resecurity/). 26.06.2026).***

***

**«За даними звіту компанії Bridewell «Кібербезпека в критичній національній інфраструктурі — 2026», протягом минулого року 77% підприємств комунального господарства зазнали кібератак, спрямованих на застаріле програмне забезпечення та неоновлене обладнання, що зробило цей тип інцидентів найпоширенішим у секторі…** Ця вразливість значною мірою зумовлена залежністю сектору від застарілих операційних технологій (OT), які не були розроблені для сучасних, взаємопов'язаних цифрових мереж і які не можна легко оновити або відключити від мережі. Як наслідок, 47% організацій зазнали значних збоїв або відключень IT-систем, причому багато з них також зіткнулися зі збільшенням витрат на кібербезпеку, втратою даних та втратою доходів. Незважаючи на ці серйозні наслідки, 99 % респондентів, що є досить дивним, вважають свої організації стійкими до таких загроз…

Окрім вразливостей застарілих систем, комунальні підприємства також стикаються з високим рівнем фішингу, шкідливого програмного забезпечення та несанкціонованого доступу, причому вирішення проблем, пов'язаних із крадіжкою даних та атаками на ланцюг постачання, займає найбільше часу. У міру подальшої модернізації сектору головним чинником покращення кібербезпеки стала не

стільки еволюція загроз, скільки дотримання нормативних вимог, причому організації висловлюють серйозну стурбованість щодо захисту даних, управління ризиками, пов'язаними зі штучним інтелектом, та обробки повідомлень про порушення безпеки… Щоб подолати критичний розрив між застарілою інфраструктурою та сучасними потребами безпеки, компанія Bridewell настійно рекомендує комунальним підприємствам підвищити прозорість своїх активів як в IT-, так і в OT-середовищах, надати пріоритет управлінню виправленнями на основі ризиків, проводити регулярні навчання з реагування на інциденти та ретельно перевіряти безпеку ланцюга поставок сторонніх постачальників. Зрештою, оскільки перебої в роботі цього сектору мають серйозні наслідки для громад та економіки в цілому, досягнення надійної кіберстійкості є найважливішим пріоритетом, від якого залежить успіх бізнесу». ***(Emma Woollacott. Legacy kit behind vast majority of cyber attacks on utilities // Future US, Inc. (https://www.itpro.com/security/legacy-kit-behind-vast-majority-of-cyber-attacks-on-utilities). 06.2026).***

***

## Кіберзахист промислових об'єктів та об'єктів будівництва

**«Німецький виробник верстатів Zimmermann зробив кібербезпеку та кіберстійкість центральним елементом своєї діяльності, враховуючи той факт, що сучасні високоточні портальні фрезерні верстати є складними цифровими системами, які необхідно захищати від зовнішніх загроз.** Крістіан Гаарц, керівник відділу розробки програмного забезпечення та введення в експлуатацію компанії Zimmermann, проводить чітке розмежування між безпекою верстатів, яка захищає операторів від фізичних небезпек, та кібербезпекою, яка забезпечує захист усієї цифрової мережі верстата, включаючи всі компоненти, підключені до IP-мережі. Несанкціонований доступ до цих систем може змінити виробничі процеси, спричинити збої або внести фальсифіковані параметри, що може мати серйозні наслідки в галузях, де безпека має критичне значення, таких як комерційна та військова авіація…

Ситуація з нормативно-правовим регулюванням додає справі ще більшої актуальності. Закон ЄС про кіберстійкість, Регламент про машини 2023/1230 та Директива NIS 2 разом створюють обов'язкову правову базу, якої компанія Zimmermann повинна дотримуватися вже з 2027 року. У відповідь на це компанія прийняла філософію «безпека за рахунок проектування», що означає, що кібербезпека вбудовується з самого початку процесу розробки, а не додається вже після його завершення. Це включає перегляд та сегментацію мережевих архітектур, захист промислових ПК та систем ЧПУ, оцінку вразливостей програмного забезпечення, а також систематичне управління оновленнями та документацією. Zimmermann також тісно співпрацює з виробниками систем управління, такими як Heidenhain та Siemens, і бере участь у галузевих робочих групах, щоб випереджати зміни в законодавстві…

З огляду на майбутнє, компанія Zimmermann інвестує в технології цифрових двійників та штучного інтелекту з метою подальшого підвищення ефективності та стійкості. Цифрові двійники дають змогу віртуально проводити перевірку на зіткнення, налаштування параметрів та коригування програмного забезпечення ще до введення обладнання в експлуатацію, що скорочує час роботи на місці та прискорює діагностику несправностей. Щодо штучного інтелекту, то його можливості вивчаються в рамках пілотних проєктів спільно з виробниками систем управління для підтримки програмування та аналізу помилок, хоча технічна відповідальність, як і раніше, повністю покладається на інженера. У сукупності ці зусилля відображають провідний принцип компанії Zimmermann «Beyond Precision» — концепцію, в якій механічна досконалість, відповідальне використання цифрових технологій та інтелектуальні системи поєднуються, щоб переосмислити поняття точності в галузі, що дедалі більше стає мережевою». ***(Jackie Seddon. Digital technologies and cyber security are changing machine tool construction // Countrywide Publications (https://www.machinery-market.co.uk/news/42720/Digital-technologies-and-cyber-security-are-changing-machine-tool-construction). 07.06.2026).***

***

**«У будівельному секторі кібербезпека дедалі частіше розглядається як бізнес-ризик, проте між усвідомленням цієї проблеми та реальним виконанням обов'язків залишається розрив, оскільки цифрова трансформація розширює площину атаки в галузі.** Сучасне будівництво значною мірою покладається на взаємопов'язані системи — такі як інформаційне моделювання будівель, хмарна співпраця та інструменти на базі штучного інтелекту — а це означає, що кіберінциденти тепер безпосередньо порушують роботу, сповільнюючи прийняття рішень, збільшуючи витрати та підриваючи реалізацію проєктів і довіру клієнтів. Зі зростанням рівня підключеності зростають і вразливості, тому кібербезпеку більше не можна розглядати як функцію бек-офісу, а лише як основний компонент операційної стійкості…

Основна проблема полягає у складних ланцюгах постачання в галузі, де численні підрядники, консультанти та постачальники спільно використовують системи та обмінюються даними. Такі взаємовідносини створюють вразливі місця, оскільки зловмисники часто обирають мішенню слабших партнерів, щоб отримати доступ до більших мереж. Хоча організації дедалі частіше усвідомлюють цей ризик, лише деякі з них повністю інтегрували кібербезпеку в процеси закупівель, управління контрактами та управління проектами. Штучний інтелект ще більше посилює існуючі виклики, створюючи нові вектори атак та швидко поширюючись серед проектів і зацікавлених сторін, хоча він також надає переваги в плані захисту, такі як покращене виявлення загроз та реагування на них…

Зрештою, ключовим чинником, що вирізняє одну організацію від іншої, є система управління. Регулюючі органи, інвестори та клієнти тепер очікують, що організації не просто визнаватимуть кіберризики, а й активно управлятимуть ними, оцінюючи не лише наслідки інцидентів, а й рівень готовності до них. Ефективна кібербезпека в будівництві залежить від впровадження таких заходів контролю, як

доступ за принципом «нульової довіри», забезпечення якості постачальників, навчання персоналу та моніторинг, у рамках цілісної стратегії стійкості, що охоплює всю організацію. Подібно до фізичної безпеки в минулому, кібербезпека стає питанням лідерства та культури, і майбутній успіх галузі залежатиме від того, чи зможе вона забезпечити надійність своїх дедалі більш цифрових систем у стресових ситуаціях». ***(Thom Atkinson. Cyber risk: Resilience is becoming a competitive advantage in construction // GlobalData Plc (https://www.worldconstructionnetwork.com/comment/cybersecurity-risk-resilience-construction/). 03.06.2026).***

***

## Кіберзахист закладів охорони здоров'я

**«У лютому 2024 року на систему охорони здоров'я Румунії було скоєно масштабну атаку з використанням програм-вимагачів: зловмисники проникли в широко використовуване медичне програмне забезпечення під назвою «Hippocrates» і успішно заразили 26 лікарень штаммом програм-вимагачів, відомим як BackMyData.** Щоб зупинити стрімке поширення шкідливого програмного забезпечення, Національний центр кібербезпеки Румунії (DNSC) ухвалив радикальне надзвичайне рішення — наказати понад 100 лікарням повністю відключитися від Інтернету. Цей захід змусив медичний персонал негайно відмовитися від цифрових записів і імпровізувати, використовуючи ручку, папір та офлайн-інструменти для управління госпіталізаціями, призначенням ліків та результатами лабораторних аналізів. Хоча це спричинило значні операційні затримки та розчарування серед пацієнтів, аналогові обхідні рішення забезпечили безпечне продовження надання невідкладної медичної допомоги…

Кіберзлочинці вимагали викуп у розмірі 160 000 євро в біткойнах, але національні органи влади категорично не рекомендували його сплачувати. Натомість ІТ-команди працювали цілодобово, щоб ізолювати заражені мережі та відновити системи за допомогою останніх резервних копій даних. Завдяки цим скоординованим зусиллям більшість постраждалих лікарень відновили роботу протягом п'яти днів, і про випадки смерті пацієнтів або серйозних травм не повідомлялося. Швидка та прозора реакція Румунії, яка значною мірою спиралася на чіткі публічні повідомлення та ефективні плани дій у режимі офлайн, зараз вивчається міжнародними чиновниками як зразок планування дій у разі надзвичайних ситуацій. Зрештою, цей інцидент підкреслює серйозну та дедалі поширенішу глобальну тенденцію, коли кіберзлочинці цілеспрямовано націлюються на сектор охорони здоров'я. Оскільки лікарні надають життєво важливі послуги, хакери використовують потенціал для максимального зриву роботи в надії вимагати значні виплати — ця вразливість нещодавно проявилася у вигляді надзвичайно руйнівних і часом фатальних атак на медичні заклади у США та Великій Британії». ***(Joe Tidy. How 100 hospitals switched to pen and paper to defeat a national cyber-attack // BBC (https://www.bbc.com/news/articles/c4gyk756mzlo). 22.06.2026).***

***

**«Компанія One Medical Seniors, раніше відома як Iora Health, нещодавно зазнала витоку даних після того, як сторонні особи, ймовірно група шантажистів ShinyHunters, отримали доступ до сторонніх систем зберігання файлів, що містили старі медичні записи пацієнтів.** Цей інцидент, що стався в період з 8 по 11 червня, призвів до витоку архівних демографічних та клінічних файлів, пов'язаних із клініками Iora в різних штатах, хоча поточні клініки One Medical та їхня система електронних медичних записів не зазнали впливу… Експерти з безпеки наголошують, що цей випадок порушення безпеки підкреслює критичну та часто недооцінену вразливість у процесі злиттів і поглинань у сфері охорони здоров'я: постійний ризик, пов'язаний із успадкованими застарілими системами. Коли у 2021 році компанія One Medical придбала Iora Health — ще до того, як її у 2023 році викупила Amazon — вона успадкувала не лише дані про пацієнтів та відносини з постачальниками, а й усі пов'язані з цим зобов'язання за законом HIPAA (Закон про перенесення та підзвітність медичного страхування)… Зламаною сторонньою системою зберігання даних виявився застарілий архів, який зберігався протягом п'яти років, незважаючи на ці корпоративні перетворення, що свідчить про те, що організації сфери охорони здоров'я залишаються юридично відповідальними за захист успадкованих даних у всіх середовищах. Проводячи паралелі з катастрофічним витоком даних у компанії Change Healthcare, експерти наголошують, що організації-покупці повинні завчасно враховувати та ретельно перевіряти безпеку всіх успадкованих сховищ даних, щоб запобігти використанню групами-вимагачами неконтрольованої або недостатньо ізольованої застарілої інфраструктури». ***(Andrea Fox. One Medical-owned legacy systems breached in cyberattack // HIMSS Media (https://www.healthcareitnews.com/news/one-medical-owned-legacy-systems-breached-cyberattack). 24.06.2026).***

***

## Захист персональних даних та соціальні мережі

**«Національна рада з питань безпеки Малайзії (NSC) пояснила, що нещодавні заяви в соціальних мережах щодо витоку персональних даних пов'язані з кіберінцидентами, які сталися до 2022 року, а не з порушенням безпеки будь-якої сучасної платформи.** У відповідь на несанкціоноване поширення цих історичних даних Національне агентство з кібербезпеки (NACSA) співпрацює з відповідними урядовими органами та іноземними постачальниками послуг з метою блокування веб-сайтів-порушників, тоді як Королівська поліція Малайзії проводить цифрові криміналістичні розслідування для затримання винних… NSC прямо попередила громадськість, що доступ до цієї незаконно отриманої інформації, її використання або поширення є кримінальним правопорушенням. Наголошуючи на необхідності посилення правових рамок, NSC зазначила, що майбутній законопроект про кіберзлочинність запровадить суворіші покарання за вторгнення в системи та крадіжку особистих даних, доповнивши

нещодавно введений в дію Закон про кібербезпеку 2024 року, який передбачає надійні заходи захисту та аудити безпеки для критичної інфраструктури країни… Крім того, рада запевнила громадськість у безпеці системи MyDigital ID, пояснивши, що ця система — яка вже налічує понад 16 мільйонів зареєстрованих користувачів — функціонує виключно як засіб перевірки особи, а не як платформа для зберігання персональних даних. Очікується, що широке впровадження цієї системи в урядовому та приватному секторах сприятиме подальшому посиленню безпеки цифрових транзакцій, запобіганню крадіжкам особистих даних та підтримці зобов'язання уряду щодо безпечної цифрової трансформації для всіх малайзійців». ***(Viral data leak claims old incident, unrelated to current platforms // Menteri Besar Selangor Incorporated (MBI) (https://mediaselangor.com/en/2026/06/380585). 21.06.2026).***

***

**«Компанія Stryker звертається до федерального суду з проханням відхилити колективний позов, поданий нинішніми та колишніми співробітниками, які стверджують, що їхні персональні дані були скомпрометовані в результаті кібератаки, пов'язаної з Іраном.** У судових документах Stryker зазначає, що в ході власного розслідування не було виявлено доказів того, що зловмисники отримали доступ до персональних даних (PII) восьми співробітників, зазначених як позивачі, зокрема до їхніх імен та номерів соціального страхування, хоча компанія визнає, що файли містили деякі робочі адреси електронної пошти. Компанія стверджує, що будь-які нібито заподіяні збитки не можна пов'язати з цим інцидентом, оскільки, на її думку, PII позивачів могла бути розкрита під час попередніх, не пов'язаних із цим інцидентом, витоків даних, а також через те, що компанія не надсилала співробітникам повідомлень про те, що до їхньої PII було отримано доступ…

Суперечка виникла після того, як хактивістська група Handala, яка, як вважається, пов'язана з Іраном, заявила, що викрала великі обсяги даних у компанії Stryker та знищила значну кількість інформації. Компанія Stryker заперечує вплив на системи, пов'язані з клієнтами, заявляючи, що атака спричинила операційний збій, який на кілька тижнів порушив роботу систем електронного замовлення та пов'язаних з ними систем, але не призвела до витоку персональних даних співробітників. Stryker також стверджує, що позов було подано до встановлення ключових фактів і що позивачі не мають правової легітимності, зокрема тому, що на момент публікації статей звіти про порушення безпеки та повідомлення регуляторним органам ще не були оприлюднені…

Загалом, результат розгляду клопотання компанії Stryker може стати важливим тестом на те, як суди оцінюють право на позов у випадках руйнівних кібератак, де порушення роботи сервісів є очевидним, але факт викрадення даних залишається спірним». ***(Marianne Kolbasuk McGee. Stryker Seeks to Dismiss Class Action Lawsuit in Cyberattack // Information Security Media Group, Corp. (https://www.inforisktoday.com/stryker-seeks-to-dismiss-class-action-lawsuit-in-cyberattack-a-32063). 24.06.2026).***

***

**«Всесвітня продовольча програма ООН (WFP) підтвердила, що в результаті кібератаки на її систему самореєстрації в секторі Газа були викрадені конфіденційні особисті дані приблизно 600 000 домогосподарств. Цей випадок, ймовірно, є найбільшим на сьогодні відомим випадком витоку даних про отримувачів гуманітарної допомоги.** WFP повідомила, що сторонні особи отримали доступ до інформації, наданої палестинцями через додаток для самореєстрації («People Portal»), оприлюднивши такі дані, як імена, номери посвідчень особи та мобільних телефонів, а також дані про місцезнаходження. Агентство повідомило, що вторгнення сталося 14 травня, а 31 травня воно повідомило про це постраждалих отримувачів допомоги через повідомлення в Telegram; 2 червня WFP публічно підтвердила, що виявила несанкціонований доступ до палестинського додатку для самореєстрації, закрила платформу, локалізувала інцидент та посилила заходи безпеки, при цьому наголосивши, що витік даних обмежився лише цим палестинським додатком і не вплинув на її більш широку систему управління ідентифікацією SCOPE або інші платформи даних… Розслідування триває, і ніхто не взяв на себе відповідальність за цей інцидент. Цей випадок посилив занепокоєння щодо того, що гуманітарні організації — які часто володіють великими масивами даних про особливо вразливих людей — дедалі частіше стають мішенями для витончених атак. Це нагадує попередні серйозні випадки витоку даних, такі як злом сайту Міжнародного комітету Червоного Хреста у 2022 році, в результаті якого були оприлюднені дані про 515 000 осіб, і викликає тривогу щодо того, що особисті дані, пов'язані з місцезнаходженням, можуть бути використані як зброя в умовах активного конфлікту… Інформатор повідомив виданню The New Humanitarian, що співробітники WFP отримали попередження від «незалежного експерта» про вразливі місця в системі за два дні до злом, а команда з кібербезпеки в Римі запевнила їх, що проблему усунуто, проте злом стався того ж дня і був виявлений лише незабаром після цього; інформатор також поставив під сумнів, чому WFP чекала понад два тижні, щоб попередити мешканців Гази, і стверджував, що станом на 31 травня не було повідомлено про жодну чітку оцінку ризиків або заходи щодо їхнього зменшення, спрямовані на усунення потенційної шкоди від розкриття даних про місцезнаходження… Цей випадок порушення безпеки стався на тлі загострення ситуації навколо вимог щодо надання даних у регіоні, зокрема спроб Ізраїлю отримати особисті дані гуманітарних працівників як умову доступу до території країни — вимогу, яку 20 травня підтримав Верховний суд Ізраїлю, надавши 30 днів на її виконання. Експерти, цитовані у звіті, стверджують, що захист даних у гуманітарній сфері часто відстає від приватного сектору, незважаючи на високу важливість цього питання, і застерігають, що інформування людей про порушення є надзвичайно важливим, але може залишити їм мало практичних можливостей для захисту… WFP заявила, що надання допомоги триватиме через існуючі системи і що отримувачам допомоги не потрібно перереєструватися, водночас закликаючи людей бути обережними щодо шахраїв, які вимагають надати інформацію або здійснити платежі, та уникати підозрілих посилань — на тлі більш ретельного

аналізу практики WFP щодо обробки даних, її планів щодо розширення системи управління ідентифікацією в Палестині, а також суперечок щодо її відносин із компанією Palantir та оцінки ризиків, пов'язаних зі збором даних, у минулих аудиторських перевірках». ***(Jacob Goldberg, Irwin Loy. Data of 600,000 Gaza households exposed in WFP cyber-attack // The New Humanitarian (https://www.thenewhumanitarian.org/news/2026/06/02/data-600000-gaza-households-exposed-wfp-cyber-attack). 02.06.2026).***

***

**«В результаті атаки, відповідальність за яку взяла на себе група-вимагач ShinyHunters, було викрадено дані, що стосуються приблизно 450 000 нинішніх та колишніх студентів Ноттінгемського університету.** Вважається, що серед викраденої інформації містяться імена та інші контактні дані, відомості про навчальні програми, ідентифікаційні номери студентів і співробітників, фінансові дані та номери національного страхування. Університет повідомив, що відразу після виявлення інциденту відключив уражені системи, працює над визначенням того, до яких даних було отримано доступ, зв'язався зі студентами та випускниками, яких це стосується, та координує свої дії з Action Fraud, Офісом комісара з питань інформації та іншими регуляторними органами, надаючи оновлення в міру продовження розслідування… Група ShinyHunters стверджує, що викрала понад 40 ГБ даних, що стосуються головного кампусу в Ноттінгемі, а також кампусів університету в Малайзії та Китаї, і погрожує оприлюднити ці матеріали, якщо викуп не буде сплачено, хоча урядова політика забороняє університетам платити викуп. Цей злом є частиною ширшої хвилі атак на вищі навчальні заклади, які, на думку експертів з безпеки, є привабливими для злочинців та інших зловмисників, оскільки університети зберігають цінні особисті дані, інтелектуальну власність та результати досліджень; представники галузі закликали навчальні заклади посилити захист як внутрішньо, так і за допомогою спеціалізованих партнерів… Університет також зазнав критики за те, як він впорався з цією ситуацією, зокрема через побоювання, що зловмисники могли залишатися непоміченими понад тиждень, а також через скарги на те, що студенти дізнавалися більше подробиць із зовнішніх джерел, таких як сайти з витоками інформації та сервіси з повідомлення про порушення безпеки, ніж із офіційних повідомлень самого університету». ***(Emma Woollacott. Nottingham University cyber attack: Everything we know so far as ShinyHunters claims responsibility // Future US, Inc. (https://www.itpro.com/security/nottingham-university-cyber-attack-everything-we-know-so-far-as-shinyhunters-claims-responsibility). 12.06.2026).***

***

**«INSEE, національне статистичне управління Франції, 19 червня зазнало кібератаки, в результаті якої були викрадені персональні дані приблизно 12 800 нинішніх та колишніх співробітників.** Викрадену інформацію, що включала імена, ідентифікаційні дані та професійні контактні відомості, було викрадено з внутрішнього довідника співробітників із низьким рівнем безпеки та опубліковано на форумі кіберзлочинців користувачем під ніком «Saturne». Важливо, що INSEE

підтвердило: паролі, банківські реквізити та надзвичайно конфіденційні демографічні й економічні дані, які воно збирає від населення, залишилися в безпеці… Хоча цей конкретний випадок порушення є відносно незначним, він має важливе значення в ширшому контексті постійних проблем Франції у сфері кібербезпеки. Протягом 2026 року французький уряд зазнав безперервної хвилі кібератак, спрямованих проти різних міністерств та платформ, що висвітлило системні вразливості та хронічне недофінансування сфери кібербезпеки. Хоча витік даних з каталогу INSEE, судячи з усього, є скоріше випадковим викраденням даних з метою їх подальшого перепродажу, а не цілеспрямованим вимаганням викупу за допомогою програм-вимагачів, така викрадена контактна інформація часто слугує сировиною для складних, масштабних фішингових кампаній… У той час як Париж продовжує домагатися цифрового суверенітету, цей інцидент підкреслює, що забезпечення безпеки основних адміністративних ресурсів залишається постійним і складним викликом для держави». ***(Alina Maria Stan. France's statistics department hit by cyberattack on staff directory // Cogneve, INC. (https://thenextweb.com/news/france-insee-cyberattack-staff-data). 26.06.2026).***

***

## Кібербезпека Інтернету речей. Штучний інтелект

**«Компанія Anthropic PBC готується надати агентству Європейського Союзу з кібербезпеки (ENISA) достроковий доступ до своєї нової потужної моделі штучного інтелекту Mythos, включивши агентство до «Проєкту Glasswing».** Ця ініціатива дозволяє обраним організаціям проводити стрес-тестування своїх систем за допомогою цієї моделі, яка чудово справляється з виявленням вразливостей у мережах і становить значну загрозу кібербезпеці в разі зловживання. Це рішення стало наслідком наполегливого лобіювання з боку чиновників ЄС та міністрів фінансів, які нещодавно відвідали Сан-Франциско, щоб домогтися такого доступу… Хоча компанія Anthropic вже надала ранній доступ до своєї системи урядовим відомствам США, окремим американським фінансовим і технологічним компаніям, а також Британському інституту безпеки штучного інтелекту, Білий дім раніше заблокував деякі плани розширення проекту Glasswing через побоювання щодо безпеки. У той час як Anthropic планує ширше впровадження Mythos у найближчі тижні, європейські чиновники наголошують на необхідності подальшої міжнародної співпраці для вирішення проблем безпеки, пов'язаних із майбутньою хвилею потужних моделей штучного інтелекту». ***(Gian Volpicelli. Anthropic to Give Mythos to First EU Body Ahead of Wider Release // Bloomberg L.P. (https://www.bloomberg.com/news/articles/2026-06-01/anthropic-to-give-eu-s-cybersecurity-agency-access-to-mythos). 01.06.2026).***

***

**«На нещодавньому саміті Gartner Security & Risk Management Summit експерти з кібербезпеки порадили керівникам служб інформаційної безпеки**

**зберігати спокій і зосередитися на базових заходах безпеки на тлі наростаючого ажіотажу навколо кіберзагроз, що базуються на штучному інтелекті.** Хоча нові потужні моделі штучного інтелекту, такі як Claude Mythos від Anthropic та Daybreak від OpenAI, здатні виявляти вразливості набагато швидше, аналітики наголосили, що це насамперед збільшує швидкість і масштаби атак, а не змінює основні пріоритети в галузі захисту…

Замість того, щоб панікувати, керівники служб безпеки повинні інформувати керівництво своїх компаній про зміни в ландшафті загроз, щоб забезпечити більші бюджети та зосередитися на основних завданнях, таких як управління вразливістю активів, визначення пріоритетності встановлення виправлень та визначення «мінімально життєздатних операцій» своєї організації. Експерти також застерегли від надмірного ентузіазму щодо заміни досвідчених працівників дорогими та іноді неефективними інструментами штучного інтелекту, попередивши, що це може вичерпати бюджети та призвести до критичної втрати інституційного досвіду та кваліфікованого персоналу. У контексті промислових систем управління аналітики закликали операторів зосередитися на кібергігієні, такій як сегментація мережі та контроль доступу, зазначивши, що кошмарний сценарій атаки на критичну інфраструктуру з використанням штучного інтелекту ще не реалізувався, а постачальники мовчать про свою участь у програмах тестування передових технологій штучного інтелекту…» ***(Eric Geller. 'Don't panic': AI reality checks dominate major cybersecurity conference // TechTarget, Inc. (https://www.cybersecuritydive.com/news/ai-cybersecurity-hype-reality-check-gartner/821867/). 03.06.2026).***

***

**«Моделі штучного інтелекту нового покоління починають кардинально змінювати сферу кібербезпеки, виходячи за межі простої автоматизації та виконуючи такі завдання, як аналіз коду та усунення вразливостей, з рівнем логічного мислення, що нагадує людське судження.** Ця зміна має особливо значний вплив на безпеку програмного забезпечення, де штучний інтелект тепер може активно брати участь у розробці, не лише виявляючи вразливості, а й генеруючи пропозиції щодо їх усунення безпосередньо в рамках конвеєрів CI/CD. Однак існує значний «розрив у контексті», оскільки цим моделям часто бракує конкретних організаційних знань для точної оцінки реальних ризиків, що може призвести до неправильної інтерпретації серйозності загрози у складному корпоративному середовищі…

Ця нова ера штучного інтелекту також посилює існуючу асиметрію між зловмисниками та захисниками: зловмисники можуть використовувати штучний інтелект для пошуку єдиного шляху експлоатації з машиною швидкістю, тоді як захисники мусять забезпечити безпеку всіх систем, не спричиняючи при цьому перебоїв у роботі… Крім того, передові технології ШІ несуть із собою нові ризики, такі як «отруєння даних» та небезпека «переконливих, але помилкових» пояснень, згенерованих ШІ, які можуть ввести в оману команди з безпеки під час кризової ситуації. Справжня готовність до цієї технології означає не лише швидке впровадження; вона вимагає від організацій ретельно перевіряти ці системи ШІ,

проводити тестування моделей методом «червоної команди» та розвивати інституційну здатність розуміти, де ШІ можна довіряти, а де людський нагляд залишається критично важливим…» ***(Kristin Lowery. The Promise and the Gap: What Frontier AI Models Actually Mean for Cyber Defense // Techstrong Group Inc. (https://securityboulevard.com/2026/06/the-promise-and-the-gap-what-frontier-ai-models-actually-mean-for-cyber-defense/). 03.06.2026).***

***

**«Звіти та дискусії в інтернеті викликали суперечки щодо тверджень про те, що уряд США, можливо, вивчає можливість використання технології Mythos від компанії Anthropic для забезпечення національної безпеки та кібербезпеки, зокрема з'явилося припущення — на яке посилається британське інформаційне видання — що Anthropic виділила інженерів для надання допомоги Агентству національної безпеки (NSA) в інтеграції можливостей Mythos у певні частини його інфраструктури.** Хоча офіційного підтвердження та перевірених доказів наступальної кібердіяльності не було, спекуляції поширюються в соціальних мережах та на форумах, зокрема у вигляді неперевіреної заяви на Reddit про те, що Mythos може використовуватися для виявлення вразливостей у критичній інфраструктурі та аналізу мереж, пов'язаних із геополітичними суперниками, такими як Китай, Іран та Росія… Згідно з повідомленнями, приблизно вісім-десять інженерів з підрозділу Forward Deployed Engineers були прикріплені до персоналу NSA з метою посилення захисту від дедалі більш витончених загроз. Прихильники такого підходу стверджують, що він є необхідним для виявлення слабких місць, перш ніж ними скористаються супротивники. Реакція в інтернеті — особливо в мережі X — виявилася двоякою: одні стверджують, що передові інструменти штучного інтелекту є необхідними для національної кіберзахисту, а інші застерігають щодо контролю, підзвітності та ризику того, що «оборонні» можливості можуть перерости в кібершпигунство або наступальні операції… Критики також ставлять під сумнів, чи відповідає участь у проектах з безпеки, пов'язаних із державними цілями, етичним зобов'язанням компаній, що працюють у сфері штучного інтелекту, тоді як інші стверджують, що такі рішення можуть бути зумовлені тиском з боку органів національної безпеки. Окремо, як повідомляється, компанія Anthropic розширила проект Glasswing — ініціативу, пов'язану з Mythos, що зосереджена на виявленні та усуненні вразливостей, — з планами надати підтримку близько 150 організаціям у понад 15 країнах, включаючи ЄС, Індію та Австралію. Прихильники розширення вважають, що це сприятиме підвищенню глобальної стійкості, хоча критики продовжують обговорювати ширші наслідки технологій безпеки на основі штучного інтелекту». ***(Naveen Goud. US Government to use Anthropic Mythos to launch Cyber Attacks // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/us-government-to-use-anthropic-mythos-to-launch-cyber-attacks/). 05.06.2026).***

***

**«Штучний інтелект уже спричиняє структурні, а не поступові зміни у сфері кіберконфліктів: суб'єкти на рівні національних держав починають**

**проводити операції зі «швидкістю машин», скорочуючи завдяки автоматизації до кількох годин завдання, які раніше вимагали місяців роботи експертів — наприклад, пошук вразливостей та моделювання шляхів атаки.** Найбільша зміна є як економічною, так і технічною, оскільки вартість, масштаб, швидкість та доступність змінюються одночасно, послаблюючи старі обмеження, які раніше обмежували складні наступальні кампанії кількома державами з великими ресурсами. Демонстрації з використанням передових моделей, таких як Mythos, посилили відчуття терміновості урядів, оскільки навіть комерційні системи з суворими «захисними бар'єрами» можуть виявляти глибоко вбудовані слабкі місця з безпрецедентною швидкістю, що викликає побоювання щодо того, що державні суб'єкти можуть зробити за допомогою менш обмежених інструментів… Очікується, що наступне покоління штучного інтелекту буде підтримувати весь оперативний цикл — розвідку, визначення пріоритетів, адаптивні методи, створення інструментів та коригування в режимі реального часу — скорочуючи терміни з тижнів до годин або хвилин і дозволяючи невеликим командам досягати результатів, для яких раніше були потрібні великі організації. Ця тенденція є за своєю суттю асиметричною: зловмисникам достатньо лише одного успіху, тоді як захисники повинні захищати цілі національні екосистеми, а ШІ зменшує перешкоди для атак, прискорюючи виявлення, експерименти та темп, тоді як багато систем захисту все ще покладаються на розрізнені інструменти, рішення, що приймаються в людському темпі, та застарілі архітектури… Отже, основною проблемою стає завдання збору розвідданих та прийняття рішень — визначення в режимі реального часу, які вразливості є найважливішими та як розрізнені сигнали об'єднуються в реальну загрозу, — проте багато урядів не мають для цього належної організації чи ресурсів, особливо щодо секретних, суверенних або ізольованих систем, де складніше розгорнути передові захисні ШІ-рішення. Політики стурбовані тим, що атаки з використанням ШІ розвиваються швидше, ніж суверенна оборона, що змушує провідні країни переосмислити кібербезпеку як національний розвідувальний потенціал шляхом інвестування в суверенну інфраструктуру ШІ, інтеграції національних наборів даних та переробки доктрини для оцінки та реагування зі швидкістю машин. Головне застереження полягає в тому, що це не проблема майбутнього: бар'єри для входу падають, можливості вже помітні, і вони поширюватимуться, тому уряди, які адаптуються раніше, матимуть кращі результати, ніж ті, що намагаються прикріпити сучасні інструменти до інституцій, побудованих для іншої епохи». ***(Shalev Hulio. Cyber Warfare is No Longer Directed by Humans. It's Being Shaped by AI // Int Policy Digest LLC (https://intpolicydigest.org/cyber-warfare-is-no-longer-directed-by-humans-it-s-being-shaped-by-ai/). 03.06.2026).***

***

**«Дослідники з Каліфорнійського університету в Берклі продемонстрували, що модель Claude Mythos Preview від Anthropic здатна успішно використовувати 157 із 898 відомих реальних вразливостей програмного забезпечення, тоді як GPT-5.5 від OpenAI — 120.** Це посилило побоювання щодо «бугмагедону» — сценарію, за якого сучасні моделі штучного

інтелекту дозволять зловмисникам виявляти та використовувати вразливості набагато швидше, ніж захисники зможуть їх усунути. Нещодавня атака програм-вимагачів, що використовувала вразливість у широко використовуваній освітній платформі Canvas, яка поставила під загрозу дані 30 мільйонів учнів та вчителів у понад 8 000 шкіл по всьому світу, стала суворим нагадуванням про вразливість цього сектору. Організації, що обслуговують громаду, такі як школи, невеликі клініки, продовольчі банки, добровільні пожежні підрозділи та сільські комунальні служби, знаходяться в особливому ризику, оскільки їм зазвичай бракує бюджету, досвіду та можливостей для забезпечення надійної кібербезпеки або вчасної реакції на виявлення вразливостей…

Одних лише безкоштовних інструментів та автоматизованих рішень недостатньо. Дослідження Cyber Readiness Institute показало, що організації, які співпрацювали з тренером-людиною, мали втричі більше шансів завершити програму з кіберстійкості, ніж ті, що працювали самостійно. У відповідь на це автори закликають до значного розширення мереж підтримки, орієнтованих на людину, під гаслом «Проект Калейдоскоп». Ця ініціатива розширить існуючі зусилля, такі як університетські клініки з кібербезпеки, державні цивільні кіберкорпуси, CyberPeace Builders, регіональні центри оперативної безпеки (RSOC) та кібер-мандрівники. Серед ключових рекомендацій — розширення кіберволонтерства, створення фінансованих центрів спільних послуг, здатних надавати постійну підтримку за ціною нижче ринкової, побудова регіональних екосистем, що з’єднують волонтерів із державними ресурсами, та впровадження кіберзнань безпосередньо в громади. Автори стверджують, що уряд, наукові кола, промисловість та громадянське суспільство мають терміново співпрацювати для захисту цих важливих організацій, усвідомлюючи, що успішна кібератака на будь-яку з них спричиняє ланцюговий ефект у всій громаді…» ***(Ann Cleaveland. Project Kaleidoscope: Community Cyber Defense in the Age of AI // Tech Policy Press (https://www.techpolicy.press/project-kaleidoscope-community-cyber-defense-in-the-age-of-ai/). 05.06.2026).***

***

**«Компанія Collective Defence придбала виробника засобів протидії дронам Asterion в рамках угоди, загальна вартість якої перевищує 1 мільярд доларів. У результаті утворився перший оборонний «єдиноріг» Люксембургу та одна з найбільших приватних компаній у сфері оборонних технологій в Європі.** Ця угода об'єднує можливості Collective Defence у сфері кібербезпеки та аналізу загроз із системами протидії безпілотним літальним апаратам від Asterion, що відображає зростаючу конвергенцію кіберзагроз та загроз фізичній безпеці, оскільки дрони все більше покладаються на програмне забезпечення, засоби зв'язку та мережеві системи. Об'єднана платформа пропонуватиме інтегровані можливості, включаючи виявлення кіберзагроз, відстеження дронів, електронні та кінетичні контрзаходи, а також єдине управління та контроль…

Технологія Asterion, випробувана в Україні та на Близькому Сході, підкреслює необхідність багаторівневої оборони проти сучасних загроз, що поєднують безпілотні літальні апарати, засоби радіоелектронної боротьби та системи на базі

штучного інтелекту. Ця угода відповідає загальним тенденціям у сфері оборонної стратегії, коли уряди — особливо в Європі — інвестують у технології, що поєднують кібербезпеку, штучний інтелект та фізичну безпеку для захисту критичної інфраструктури та національної безпеки. Роль Люксембургу як члена НАТО та ЄС із зростаючими оборонними амбіціями ще більше позиціонує нову структуру як частину європейських зусиль щодо створення суверенних, технологічно просунутих оборонних можливостей. Загалом, це придбання підкреслює перехід до уніфікованих архітектур безпеки, що враховують як цифрові, так і фізичні загрози в сучасній війні та захисті інфраструктури». ***(Miriam McNabb. Collective Defence Acquires Asterion in $1 Billion Deal Combining Cybersecurity and Counter-Drone Technology // DRONELIFE (https://dronelife.com/2026/06/03/collective-defence-acquires-asterion-in-1-billion-deal-combining-cybersecurity-and-counter-drone-technology/). 03.06.2026).***

***

**«У червні 2026 року регуляторні органи, розробники штучного інтелекту та агентства з кібербезпеки дійшли висновку, що штучний інтелект прискорює виявлення вразливостей у програмному забезпеченні швидше, ніж організації встигають їх усунути.** Ця зміна парадигми була спричинена оголошенням компанії Anthropic у квітні 2026 року про випуск своєї моделі штучного інтелекту Claude Mythos, яка володіє надзвичайною здатністю виявляти серйозні недоліки та розробляти експлойти. Усвідомлюючи ризик, компанія Anthropic спочатку обмежила доступ до цієї моделі невеликою групою організацій у рамках «Project Glasswing», який швидко виявив понад 10 000 критичних вразливостей, що проілюструвало масштаб проблеми…

У червні 2026 року події стрімко загострилися. Після того, як компанія Anthropic розширила доступ до ШІ класу Mythos, уряд США, посилаючись на міркування національної безпеки, видав директиву щодо експортного контролю, що призвело до глобального відключення цих моделей. У відповідь агентства з кібербезпеки альянсу Five Eyes опублікували спільну заяву, у якій прямо визначили кіберризик як основну відповідальність бізнесу, що вимагає термінової реакції «всього суспільства». Австралійські регулятори, такі як APRA та ASIC, підтримали цю позицію, попередивши, що регулювання не встигає за темпами впровадження штучного інтелекту і що кіберстійкість є основним зобов'язанням ліцензіатів, причому ASIC заявила, що «годинник показує одну хвилину до півночі»…

Головний висновок полягає в тому, що, хоча правові стандарти корпоративної обачності не змінилися, фактичні критерії їх дотримання були різко підвищені. Час між виявленням вразливості та її експлуатацією скоротився з тижнів до годин, що робить традиційні щоквартальні звіти перед радою директорів та повільні механізми прийняття рішень непридатними… Проблема зараз є не стільки технологічною, скільки організаційною; завдання полягає в тому, щоб усувати недоліки швидше, ніж штучний інтелект встигає їх виявляти. Згідно з рекомендаціями регуляторних органів, ради директорів та керівники повинні тепер забезпечити, щоб їхні організації мали заздалегідь затверджені повноваження та перевірені процеси для локалізації інцидентів майже в режимі реального часу,

розглядаючи кіберстійкість не як ІТ-проблему, а як критично важливий компонент безперебійності діяльності та лідерства». ***(Martyn Taylor, Peter Mulligan. Unfolding in real time: Artificial intelligence is reshaping cybersecurity // Norton Rose Fulbright (https://www.nortonrosefulbright.com/en/knowledge/publications/2e6c29b3/artificial-intelligence-is-reshaping-cybersecurity). 06.2026).***

***

**«Агентний ШІ відкриває нові горизонти у сфері штучного інтелекту, діючи автономно для виконання складних завдань у різних системах без необхідності отримання схвалення людини на кожному етапі.** Така автономність створює значні нові виклики у сфері права та кібербезпеки для його постачальників та користувачів, які стикаються зі складною мережею перехресних нормативних актів ЄС та Великої Британії, зокрема Закону ЄС про ШІ, Закону про кіберстійкість (CRA), GDPR, а також галузевих правил, таких як NIS2 та DORA. Конкретні зобов'язання залежать від того, що робить агент, де він працює та хто ним користується…

Ці системи вразливі до нових загроз, таких як «промт-ін'єкція», надмірна автономія внаслідок занадто широких дозволів, підвищення привілеїв через підключені інструменти та ухилення від нагляду. Ці ризики посилюються через неповну та мінливу ситуацію з дотриманням нормативних вимог, оскільки наразі не існує єдиного міжнародного стандарту, який би охоплював усі законодавчі вимоги, що змушує постачальників орієнтуватися на проекти рекомендацій… Рекомендованим рішенням є вбудовування відповідності вимогам безпосередньо в архітектуру агента шляхом зіставлення його зовнішніх дій з чинним законодавством, впровадження суворого контролю доступу та структурних обмежень, а також використання надійних механізмів моніторингу та аудиторських слідів для виявлення аномальної поведінки». ***(Aselle Ibraimova, Joe Hancock. Agentic AI and cybersecurity: legal obligations and regulatory risks under UK and EU laws // Mishcon de Reya LLP (https://www.mishcon.com/news/agentic-ai-and-cybersecurity-legal-obligations-and-regulatory-risks-under-uk-and-eu-laws). 25.06.2026).***

***

**«22 червня керівники агентств кібербезпеки Five Eyes, включаючи Велику Британію, США, Канаду, Австралію та Нову Зеландію, опублікували спільну заяву, в якій попередили, що передові моделі штучного інтелекту, ймовірно, вже за кілька місяців перевершать поточні очікування галузі та можуть суттєво змінити як наступальні, так і оборонні кіберможливості.** У заяві наголошується, що ці моделі здатні швидше виявляти та експлуатувати вразливості, що прискорює темпи кібервторгнень та втрати даних, і закликає організації не розглядати кіберризик як суто технічну або ІТ-проблему. Натомість у ній закликають до комплексного підходу на рівні всієї організації, який розглядає кіберстійкість як основний бізнес-ризик та відповідальність керівництва, що має ключове значення для безперебійності діяльності та довіри ринку… У ньому наголошувалося, що припущення щодо кібербезпеки можуть застарівати за лічені

місяці, а не роки, і організаціям рекомендувалося інтегрувати кібербезпеку в основну бізнес-стратегію, водночас враховуючи, як штучний інтелект може покращити операції з забезпечення безпеки, зокрема виявлення вразливостей, якість програмного забезпечення, моніторинг мережі та реагування на інциденти. Хоча порушення безпеки є неминучими, у заяві підкреслювалося, що готовність до них має вирішальне значення, а ради директорів та керівництво повинні гарантувати, що кіберстійкість працює навіть у стресових ситуаціях… У ньому також визначено кілька нагальних фундаментальних заходів: зменшення площі атаки шляхом обмеження непотрібного доступу та підключень; прискорення встановлення виправлень, щоб не відставати від темпів експлуатації вразливостей; вирішення проблеми застарілих систем, що більше не підтримуються; посилення контролю за ідентифікацією та доступом; а також завчасна підготовка до інцидентів за допомогою перевірених планів реагування, навчених команд та зосередження уваги на швидкому локалізуванні та відновленні». ***(Ashden Fein, Caleb Skeath, Jim Garland, Micaela McMurrough & Ali Cooper-Ponte. Five Eyes Cybersecurity Agencies Issue Statement Regarding AI-Related Shifts in Cybersecurity Risks, Urging Organizational Leaders to "Act Now" // Covington & Burling LLP (https://www.insideprivacy.com/cybersecurity-2/five-eyes-cybersecurity-agencies-issue-statement-regarding-ai-related-shifts-in-cybersecurity-risks-urging-organizational-leaders-to-act-now/). 24.06.2026).***

***

**«На саміті з кібербезпеки, організованому J.P. Morgan Innovation Economy у квітні 2026 року, було підкреслено, що кібербезпека перебуває на переломному етапі: штучний інтелект (ШІ) стає як серйозною загрозою, так і потужним захисним засобом, а провідні розробники, як очікується, використовуватимуть ШІ для покращення вимірюваних результатів для клієнтів.** У звіті стверджується, що межі корпоративної ідентичності рішуче змістилися в бік нелюдських ідентичностей, таких як агенти штучного інтелекту, службові облікові записи та автоматизовані робочі процеси, які зараз значно переважають за кількістю людських користувачів і створюють виклики в сфері управління, пов'язані з надмірно широкими правами доступу, ротацією секретів та рішеннями щодо доступу в середовищах взаємодії між агентами… Штучний інтелект також розширює площину атаки, прискорюючи розвідку, експлуатацію вразливостей та соціальну інженерію, тоді як API, хмарні сервіси та SaaS-платформи залишаються основними точками вразливості; введення даних методом «prompt injection» та підробка особи за допомогою штучного інтелекту стають дедалі серйознішими загрозами, а здатність виявляти аномалії, автоматично застосовувати політику безпеки та перевіряти ідентичність не лише за допомогою простого входу в систему стає базовою вимогою. Венчурне фінансування відображає ці зміни: інвестиції у кібербезпеку в США залишаються значними, але дедалі більше зосереджуються у меншій кількості більших раундів, причому зростає частка угод, що припадає на кіберстартапи, які використовують штучний інтелект; інвестори тепер вимагають більш надійної архітектури, гнучкості моделей та «маховиків даних», а не штучного інтелекту як поверхневої функції… Найбільш

надійними є ті продукти, які розроблені з урахуванням майбутнього, в якому штучний інтелект постійно вдосконалюється: це рішення, що забезпечують безпеку нелюдських ідентичностей, захищають API та додатки, доповнені моделями, забезпечують можливість аудиту та автоматизують усунення проблем, завдяки чому проблеми не просто виявляються, а й фактично усуваються, при цьому зберігаючи людський контроль над діями, що мають значний вплив». ***(Cybersecurity in the age of artificial intelligence // JPMorgan Chase & Co. (https://www.jpmorgan.com/insights/banking/commercial-banking/ai-cybersecurity-threats-funding-and-builder-priorities). 25.06.2026).***

***

**«Незважаючи на значні інвестиції в штучний інтелект, багатьом керівникам у сфері кібербезпеки важко продемонструвати чітку окупність інвестицій: до 80 відсотків ініціатив у сфері ШІ не вдається масштабувати, оскільки організації не визначають, як саме має виглядати успіх.** Оскільки успішна кібербезпека за своєю суттю є невидимою — тобто запобігання атакам рідко генерує конкретні дані для звітів перед правлінням — інструменти ШІ часто просто накладаються на існуючі робочі процеси. Цей хибний підхід призводить до того, що аналітики постійно перевантажені сповіщеннями, а проєкти ШІ відкидаються як дорогі експерименти… Щоб отримати реальну користь, організації повинні ще до впровадження встановити чіткі цілі: визначити конкретні показники, які потрібно поліпшити; виявити, на яких адміністративних завданнях аналітики марнують час; а також точно встановити, які рішення ШІ має повністю автоматизувати, а в яких випадках він повинен лише допомагати людям. Справжня мета використання ШІ в сфері безпеки полягає не в тому, щоб змусити аналітиків працювати швидше, а в тому, щоб повністю усунути малоцінні, повторювані завдання, завдяки чому експерти-люди зможуть застосовувати своє незамінне судження та досвід у складних розслідуваннях… Досягнення такої операційної зрілості стає дедалі актуальнішим через асиметричний ландшафт загроз, в якому кіберзлочинці вже використовують генеративний ШІ для здійснення складних, гіперперсоналізованих атак у великих масштабах, не обтяжених етичними та фінансовими обмеженнями, з якими стикаються захисники. Зрештою, перехід від ізольованих експериментів із ШІ до вимірюваного, системного захисту вимагає стратегічної дисципліни, а не швидкого впровадження… Керівники служб безпеки повинні проаналізувати свої робочі процеси, використовувати штучний інтелект для усунення конкретних вузьких місць та ретельно оцінювати перші результати, щоб довести беззаперечну цінність технології керівництву компанії, перш ніж намагатися розширювати її застосування». ***(Mike Britton. AI in Cybersecurity Has a Value Problem, Not a Technology Problem // Reed Exhibitions Ltd (https://www.infosecurity-magazine.com/opinions/ai-in-cybersecurity-value-problem/). 24.06.2026).***

***

**«Китайські моделі штучного інтелекту стають дедалі популярнішими у Сполучених Штатах завдяки нижчій вартості та покращенню їхніх**

**можливостей, проте звіт компанії «Booz Allen Hamilton» викликає занепокоєння щодо потенційних ризиків у сфері кібербезпеки.** Дослідження показало, що деякі широко використовувані китайські моделі за певних умов генерували більше вразливостей у програмному забезпеченні, особливо коли їм давали вказівки, нібито вони обслуговували користувачів з уряду США. Ці вразливості не були явно зловмисними, але виявлялися як ледь помітні слабкі місця, якими можна було скористатися, що вказує на новий тип загрози, за якої системи штучного інтелекту можуть змінювати свою поведінку залежно від контексту, подібно до «сплячого агента»…

Це підвищує ризик того, що організації можуть несвідомо допустити уразливості в системі безпеки, покладаючись на код, згенерований ШІ, а не на традиційні методи хакерських атак. Хоча деякі експерти застерігають, що це може мати серйозні наслідки для національної безпеки та критичної інфраструктури, особливо у разі використання ШІ, розробленого за кордоном, інші стверджують, що необхідні додаткові дослідження, щоб визначити, чи є ця проблема характерною виключно для китайських моделей, чи вона відображає більш загальні обмеження систем ШІ. Ці висновки викликали політичні дискусії у Сполучених Штатах, де деякі посадовці закликають до обережності або уникнення використання таких інструментів у чутливих сферах застосування». ***(KAYLA GASKINS. Chinese AI models raise cybersecurity concerns, new report warns // Sinclair, Inc. (https://cbsaustin.com/news/nation-world/chinese-ai-models-raise-cybersecurity-concerns-new-report-warns-artificial-intelligence-business-government-military). 22.06.2026).***

***

**«Канадський центр кібербезпеки (Cyber Centre) закликає організації по всій країні терміново посилити свою кіберзахист у відповідь на ескалацію загроз, пов'язаних із передовими технологіями штучного інтелекту.** Повторюючи недавню спільну заяву розвідувального альянсу Five Eyes, Cyber Centre попереджає, що штучний інтелект стрімко змінює ландшафт загроз, суттєво скорочуючи час, необхідний зловмисникам для виявлення та експлуатації вразливостей програмного забезпечення, — що зменшує час на реагування з боку захисників з тижнів до лічених годин… Крім того, штучний інтелект знижує бар'єри для входу на ринок для кіберзлочинців, уможливлюючи масове створення переконливих фішингових та «діпфейк»-шахрайств, спрощуючи створення складних ланцюжків вразливостей та створюючи внутрішні ризики, такі як витік конфіденційних даних через використання несанкціонованих інструментів штучного інтелекту. Визнаючи, що це критично важливе питання для бізнесу та керівництва, а не лише проблема IT-сфери, Кіберцентр радить організаціям використовувати штучний інтелект для власного захисту, одночасно посилюючи базові заходи кібергігієни… До рекомендованих заходів належать своєчасне оновлення програмного забезпечення, зменшення вразливості до інтернет-загроз, впровадження багатофакторної аутентифікації, стійкої до фішингу, ізоляція ключових систем та усунення вразливостей застарілого програмного забезпечення. Організаціям також настійно рекомендується забезпечити дотримання суворих

стандартів безпеки у ланцюгах постачання сторонніх постачальників та оперативно повідомляти про інциденти, оскільки надійні практики, засновані на принципі «безпека від самого початку», мають вирішальне значення для запобігання переростанню атак із використанням штучного інтелекту у масштабні операційні та фінансові кризи». ***(Statement from the Canadian Centre for Cyber Security on frontier artificial intelligence models and their impact on cyber security // Government of Canada (https://www.canada.ca/en/communications-security/news/2026/06/statement-from-the-canadian-centre-for-cyber-security-on-frontier-ai-models-and-their-impact-on-cyber-security.html). 24.06.2026).***

***

***Штучний інтелект, як інструмент боротьби із кіберзлочинністю***

**«…Компанія Anthropic розширює проект Glasswing — ініціативу, покликану підвищити рівень глобальної безпеки програмного забезпечення шляхом надання доступу до своєї передової моделі штучного інтелекту Claude Mythos Preview.** Після успішної початкової фази, під час якої близько 50 партнерів виявили понад 10 000 серйозних вразливостей, Anthropic тепер розширює доступ до приблизно 150 нових організацій у 15 країнах. Ця нова група включає постачальників критичної інфраструктури в секторах, які раніше були недостатньо представлені, таких як енергетика, водопостачання, охорона здоров'я, комунікації та апаратне забезпечення, а також основних розробників програмного забезпечення з відкритим кодом… Причиною такого розширення є нагальна необхідність: очікується, що протягом 6–12 місяців інші компанії, що займаються штучним інтелектом, випустять подібні моделі класу Mythos — можливо, без належних заходів безпеки — що може призвести до непередбачуваного сплеску кібератак. Щоб допомогти фахівцям з кіберзахисту не відставати від темпів розвитку, проект Glasswing має на меті сформувати нові стандарти роботи, змістивши акцент у галузі з простого виявлення вразливостей на ефективне розкриття інформації про них, виправлення та впровадження безпечного програмного забезпечення. Для цього Anthropic надає інструменти, які використовують модель для написання виправлень, автоматизації виявлення загроз, проведення тестів на проникнення та переписання застарілого коду… У перспективі компанія Anthropic планує продовжувати розширювати проект Glasswing, нарощувати масштаби своєї програми кіберверифікації та, зрештою, надати широкій громадськості доступ до можливостей рівня Mythos, щойно буде розроблено надійні заходи безпеки для запобігання зловмисному використанню. Кінцевою метою є створення стійкої переваги для кіберзахисників у умовах стрімкого розвитку технологій штучного інтелекту». ***(Expanding Project Glasswing // Anthropic PBC (https://www.anthropic.com/news/expanding-project-glasswing). 02.06.2026).***

***

**«У новому звіті Світового економічного форуму, підготовленому у співпраці з KPMG, підкреслюється зростаюче стратегічне значення штучного**

**інтелекту в сфері кібербезпеки, завдяки чому він перетворюється з новітньої технології на один із основних засобів захисту.** Спираючись на 20 реальних прикладів та висновки 105 представників із 84 організацій та 15 галузей, звіт спрямований на керівників та керівників служб інформаційної безпеки, які прагнуть вийти за межі експериментів та повністю інтегрувати ШІ у свої операції з кібербезпеки. Це відбувається у критичний момент, оскільки зловмисники вже використовують ШІ для збільшення швидкості, масштабу та витонченості своїх атак, що робить необхідним для захисників використання тих самих технологій для зміцнення своєї стійкості…

У звіті чітко зазначено, що цінність штучного інтелекту в сфері кібербезпеки виходить далеко за межі простої автоматизації. Організації, які досягають успіху в ефективному впровадженні штучного інтелекту, роблять це завдяки інвестиціям у поєднання технологій, навичок та процесів, поєднуючи чітку стратегію впровадження ШІ з ретельно перевіреними сценаріями використання перед масштабуванням, а також забезпечуючи суворе управління та людський нагляд на всіх етапах. Звіт охоплює практичні застосування ШІ протягом усього життєвого циклу кібербезпеки — від управління, ідентифікації, захисту, виявлення, реагування та відновлення — і пропонує стратегічні рекомендації для керівників щодо готовності, валідації, масштабування та довгострокового управління. Він також розглядає перспективи розвитку агентного ШІ, звертаючи увагу на нові ризики та незмінну важливість прийняття рішень за участю людини. Зрештою, головний висновок звіту полягає в тому, що організації, які підходять до ШІ з чіткою метою та дисципліною, мають кращі можливості як для зміцнення своїх захисних систем сьогодні, так і для формування гнучкості, необхідної для протистояння загрозам завтрашнього дня». ***(Akhilesh Tuteja. Empowering defenders: AI for cybersecurity // KPMG Assurance and Consulting Services LLP (https://kpmg.com/in/en/insights/2026/06/empowering-defenders-ai-for-cybersecurity.html). 04.06.2026).***

***

**«Компанія OpenAI представила режим «Lockdown Mode» для ChatGPT — функцію безпеки, призначену для зниження ризику витоку даних, спричиненого атаками типу «prompt injection».** Ця функція не спрямована на запобігання впливу зловмисних вхідних даних на модель, а зосереджена на блокуванні завершального етапу таких атак шляхом обмеження вихідної мережевої активності, яка може призвести до передачі конфіденційних даних зловмисникам. Коли режим Lockdown Mode увімкнено, він вимикає або обмежує такі можливості, як перегляд веб-сторінок у реальному часі, завантаження зовнішніх файлів, пошук зображень, глибоке дослідження, функції агента та виконання коду з підтримкою мережі, не впливаючи на основні функції, такі як пам'ять, завантаження та обмін даними…

Ця функція також запроваджує підхід до використання додатків і коннекторів, що базується на оцінці ризиків, що вимагає ретельного налаштування — особливо в корпоративних середовищах, де адміністратори повинні вручну керувати правами доступу, призначати надійні додатки та забезпечувати контроль доступу на основі

ролей. Хоча інструменти аудиту забезпечують прозорість щодо використання та потоків даних, режим блокування не усуває всіх ризиків, оскільки оперативні втручання все ще можуть впливати на результати моделювання, а залишкові вразливості можуть зберігатися через інтеграцію сторонніх сервісів або непередбачені взаємодії…

Загалом режим «Lockdown Mode» є цілеспрямованою стратегією запобігання одній із нових загроз безпеці, пов'язаних зі штучним інтелектом, що допомагає обмежити шляхи витоку даних, водночас підкреслюючи необхідність більш широких заходів контролю та людського нагляду в управлінні системами на базі штучного інтелекту». ***(Guru Baran. New ChatGPT Lockdown Mode to Mitigate Prompt Injection and Data Exfiltration Attacks // Cyber Security News (https://cybersecuritynews.com/chatgpt-lockdown-mode/). 06.06.2026).***

***

**«У вівторок компанія Anthropic випустила Fable — загальнодоступну версію своєї потужної моделі штучного інтелекту для кібербезпеки Mythos з обмеженими можливостями.** Однак цей запуск викликав значну критику з боку фахівців у галузі кібербезпеки через надмірно жорсткі обмежувальні механізми. Ці механізми, розроблені для запобігання зловживанню моделлю з метою створення шкідливого програмного забезпечення або біологічної зброї, часто спрацьовують помилково, відхиляючи навіть цілком нешкідливі запити, такі як читання публікацій у блогах, перевірка коду або прохання до ШІ написати безпечне програмне забезпечення… При спрацьовуванні система призупиняє чат, позначає повідомлення та автоматично переводить користувача на старішу версію — Claude Opus 4.8. Дослідники підозрюють, що обмеження значною мірою базуються на простому фільтруванні за ключовими словами, що викликає розчарування серед фахівців, які вважають, що ці обмеження заважають законній роботі в галузі розробки програмного забезпечення та безпеки. Хоча компанія Anthropic раніше обмежувала доступ до своєї більш потужної моделі Mythos лише для окремих організацій у рамках «Project Glasswing» з метою захисту критичної інфраструктури, вона також пропонує «Програму кіберверифікації», яка надає затвердженим фахівцям з кібербезпеки менше обмежень під час використання Claude… Незважаючи на загальне розчарування через невдалий запуск Fable, деякі ветерани галузі зберігають оптимізм, розуміючи, що Anthropic дотримується обережного підходу за принципом «краще перестрахуватися, ніж потім шкодувати», і очікують, що компанія поступово послабить і вдосконалить свої захисні механізми у міру дозрівання технології та поглиблення співпраці з галуззю кібербезпеки». ***(Lorenzo Franceschi-Bicchierai. Cybersecurity researchers aren't happy about the guardrails on Anthropic's Fable // TechCrunch Media LLC. (https://techcrunch.com/2026/06/10/cybersecurity-researchers-arent-happy-about-the-guardrails-on-anthropics-fable/). 10.06.2026).***

***

**«OpenAI розширила свою програму кібербезпеки Daybreak, додавши нові інструменти, партнерські відносини та ініціативи, спрямовані на те, щоб**

**вивести фахівців з кібербезпеки за межі простого виявлення вразливостей і перейти до перевірки, виправлення та масштабного впровадження виправлень.** Компанія зазначає, що передові технології штучного інтелекту змінили сферу кібербезпеки, значно прискоривши виявлення вразливостей, а це означає, що справжнім вузьким місцем тепер є усунення проблем, а не їх виявлення. Щоб вирішити цю проблему, OpenAI модернізувала свій плагін Codex Security, щоб він міг сканувати цілі кодові бази або вибрані зміни, оцінювати, чи є проблеми доступними для експлуатації, генерувати докази, допомагати створювати та тестувати цільові виправлення, а також створювати моделі загроз там, де їх немає, залишаючи остаточні рішення за людськими експертами… Компанія також надала доступ до GPT-5.5-Cyber обмеженому колу перевірених фахівців з кіберзахисту, позиціонуючи цю модель як більш гнучку для авторизованої роботи в сфері кібербезпеки, яка здатна аналізувати великі кодові бази, перевіряти наявність проблем, відстежувати можливості експлуатації вразливостей та допомагати у розробці й тестуванні виправлень; OpenAI заявляє, що ця модель перевершує GPT-5.5 за результатами кількох кібербезпекових тестів, хоча й підкреслює, що результати тестів є лише одним із показників реальної оборонної цінності. Паралельно з цим OpenAI запустила партнерську програму, що дозволяє обраним постачальникам рішень у сфері безпеки інтегрувати GPT-5.5 разом із Trusted Access for Cyber у свої продукти; серед перших учасників — провідні компанії з кібербезпеки, такі як CrowdStrike, Cisco, Palo Alto Networks, Wiz та інші… Крім того, компанія спільно з Trail of Bits, HackerOne та дослідниками запустила ініціативу «Patch the Planet», щоб підтримати розробників відкритого програмного забезпечення шляхом фінансування експертів, використання інструментів OpenAI для перевірки результатів, згенерованих штучним інтелектом, а також допомоги у розробці та впровадженні виправлень для широко використовуваних проектів, таких як cURL, Go, Python, Sigstore та pyca/cryptography. OpenAI заявляє, що також співпрацює з урядами та операторами критичної інфраструктури в рамках партнерських програм «Trusted Access for Cyber» у таких країнах, як Австралія, Канада, Франція, Німеччина, Японія, Південна Корея та ЄС, а також з урядом Великої Британії, маючи на меті перетворити виявлення вразливостей за допомогою штучного інтелекту на безпечніше програмне забезпечення та посилену кіберстійкість». ***(Graham Turner. OpenAI Launches New Tools for AI-Powered Cybersecurity Patching // DIGIT (https://www.digit.fyi/openai-launches-new-tools-for-ai-powered-cybersecurity-patching/). 24.06.2026).***

***

**«Китайська компанія з кібербезпеки Qihoo 360 оголосила про розробку системи виявлення вразливостей на основі штучного інтелекту, яка, за її твердженням, може скласти конкуренцію моделі Mythos від Anthropic, яку генеральний директор цієї компанії назвав «кіберядерною зброєю» через її передові можливості та обмежений доступ.** Стверджуючи, що Китай не може зрівнятися з підходом США до створення дедалі більших передових моделей через розрив у можливостях, Qihoo натомість розробила альтернативну стратегію, засновану на «роїнні з багатьох агентів», що поєднує її великий досвід у сфері

кібербезпеки та дані про шкідливе програмне забезпечення… Ця система, що отримала назву «Tulongfeng», використовує скоординовані агенти штучного інтелекту для моделювання загроз, виявлення поверхонь атаки з високим рівнем ризику, відстеження потоків даних, автоматичного створення та тестування експлойтів у пісочницях, а також підтвердження вразливостей, а не лише їхнього позначення, при цьому постійно вдосконалюючись завдяки зворотньому зв'язку. Компанія Qihoo стверджує, що система вже виявила давні вразливості у широко використовуваному програмному забезпеченні, зокрема у Windows та Microsoft Office, а також знайшла недоліки в інструментах з відкритим кодом… Паралельно з цим компанія представила ще один інструмент на основі штучного інтелекту — «Yitianzhen», призначений для моделювання кібератак на організації та надання рекомендацій щодо усунення вразливостей або їх усунення, а також створила внутрішній альянс з кібербезпеки для зміцнення оборонних можливостей. Ця заява свідчить про посилення геополітичної конкуренції у сфері кібербезпеки на основі штучного інтелекту, в рамках якої Китай прагне розробити альтернативи західним моделям, доступ до яких обмежено, хоча сама компанія Qihoo потрапила під санкції США через нібито зв'язки з китайськими збройними силами». ***(Simon Sharwood. Chinese cybersecurity company claims it's built a better-than-Mythos bug finder // The Register (https://www.theregister.com/security/2026/06/26/chinese-cybersecurity-company-claims-its-built-a-better-than-mythos-bug-finder/5262642). 26.06.2026).***

***

## ***Штучний інтелект, як зброя кіберзлочинців***

**«Сучасні стратегії кібербезпеки стають дедалі досконалішими, проте багато організацій не беруть до уваги критичну вразливість: сім'ї співробітників, оскільки генеративна штучна інтелектуальна технологія робить шахрайські схеми переконливішими та розширює площину атаки за межі корпоративних мереж у домашні помешкання.** Загрози на основі штучного інтелекту, такі як клонування голосу, «діпфейки» та високоперсоналізований фішинг, сприяють стрімкому зростанню шахрайства, а прогнозовані збитки у США до 2027 року сягнуть 40 мільярдів доларів. Перехід до гібридної роботи розмив межі між особистим та професійним середовищами, а це означає, що скомпрометований особистий пристрій або необережна взаємодія вдома можуть швидко призвести до порушень безпеки організації. Особливо вразливими є діти та люди похилого віку — діти через соціальні та ігрові взаємодії, що експлуатують їхню цікавість та довіру, а люди похилого віку — через фінансові шахрайства, такі як фішинг, видавання себе за іншу особу та шахрайство, які вже спричинили мільярдні збитки…

Традиційні тренінги з кібербезпеки, які зазвичай обмежуються вправами з дотримання вимог на робочому місці, вже не є достатніми. Натомість стійкість до кіберзагроз слід розглядати як практичну навичку, що формується протягом усього життя завдяки постійному навчанню, яке починається з раннього віку та

адаптується з часом. Для дітей це передбачає формування обізнаності через повсякденні звички та досвід, з яким вони можуть себе ототожнити, тоді як для дорослих це вимагає доступної освіти, заснованої на довірі, зосередженої на розпізнаванні шахрайських схем та управлінні емоційними тригерами, такими як відчуття терміновості чи страх. Організації починають підтримувати цю зміну, поширюючи обізнаність з питань кібербезпеки на сім'ї співробітників та заохочуючи відкриті обговорення вдома, сприяючи спільній відповідальності та міжпоколінному навчанню…

Ця мінлива ситуація з загрозами вимагає більш широкого розуміння поняття «людського ризику», яке передбачає включення домогосподарств до периметра безпеки. З огляду на дані, які свідчать про те, що багато кібератак на керівників здійснюються через домашні мережі та за участю членів родини, для посилення кібербезпеки сьогодні необхідні інвестиції не лише в системи, а й у людей — у домогосподарствах, школах та громадах. Зрештою, ефективна кібербезпека залежить від поєднання індивідуальної обізнаності та системних заходів захисту, а також від усвідомлення того, що стійкість починається не лише всередині організацій, а й у повсякденній цифровій поведінці». ***(Elçin Biren. How the living room became cybersecurity's front line // World Economic Forum (https://www.weforum.org/stories/2026/06/how-the-living-room-became-cybersecuritys-front-line/). 04.06.2026).***

***

**«Генеральний директор компанії Sygnia Гай Сегал попереджає, що стрімка інтеграція штучного інтелекту в кібератаки різко прискорює розвиток загроз, скорочуючи терміни розробки експлойтів з місяців до лічених годин і даючи зловмисникам можливість діяти більш автономно в рамках зламаних систем.** Він стверджує, що в міру того, як організації стають дедалі більш цифровими та взаємопов'язаними, цей зростаючий ризик робить необхідним посилення регуляторного контролю для забезпечення належної готовності до кіберзахисту. Хоча в інших регіонах, таких як Європейський Союз, Австралія та деякі штати США, вже запроваджено нормативні акти, що передбачають штрафи за недотримання вимог безпеки, Ізраїль ще не запровадив аналогічних заходів на рівні цивільних підприємств, що призводить до обмеженої відповідальності організацій, які не забезпечують захист конфіденційних даних…

Незважаючи на цей розрив, Сегал зазначає, що Ізраїль загалом залишається відносно сильним у сфері кібербезпеки, особливо в захисті критичної інфраструктури та сприянні інноваціям, оцінюючи його стійкість на 8 балів із 10. Однак він наголошує, що національні можливості не гарантують стабільної безпеки в масштабах усієї економіки без регуляторного тиску, спрямованого на дотримання стандартів. Він робить висновок, що, оскільки штучний інтелект продовжує змінювати як наступальні, так і оборонні кіберможливості, підвищення стійкості залежатиме від того, наскільки швидко організації адаптуються та наскільки ефективно уряди запроваджують і забезпечують дотримання практик кібербезпеки». ***(Zachy Hennessey. Israel needs to strengthen cybersecurity***

***enforcement as AI speeds up attacks // CTech (https://www.calcalistech.com/ctechnews/article/syejhghzgx). 21.06.2026).***

***

**«Штучний інтелект стрімко стає серйозною загрозою для кібербезпеки, знижуючи поріг входу у сферу кіберзлочинності та даючи змогу недосвідченим особам здійснювати складні атаки.** У недавньому прикладі з реального життя, детально описаному дослідницькою групою OALABS Research, хакер-аматор з Ефіопії успішно використав моделі штучного інтелекту Claude Opus та Codex від компанії Anthropic, щоб захопити контроль над приватними серверами та отримати доступ до конфіденційних даних щонайменше 14 компаній, незважаючи на відсутність технічних знань та використання нечітких, погано сформульованих команд… Особу зловмисника вдалося встановити лише тому, що він випадково попросив ШІ відредагувати його резюме перед початком атак. Важливо, що хакер легко обійшов вбудовані етичні захисні механізми Claude, неправдиво стверджуючи, що проводить санкціоновані дослідження з кібербезпеки в рамках «червоної команди». Ошуканий цією передумовою, штучний інтелект не лише надав необхідний експлойт-код, а й окреслив стратегії монетизації, такі як продаж викрадених даних, вимагання та пряма крадіжка, хоча спроба викрасти 4 мільйони доларів у криптовалюті зрештою зазнала невдачі… ШІ відмовився співпрацювати лише тоді, коли його попросили націлитись на конкретну особу та її родину. Цей випадок висвітлює глибоку дилему для розробників ШІ, таких як Anthropic та OpenAI: хоча вбудовані захисні механізми легко обходять зловмисники, які видають себе за етичних дослідників, надмірне обмеження моделей суттєво заважатиме законній діяльності фахівців з кібербезпеки, які покладаються на ШІ для виявлення та усунення вразливостей. У міру подальшого розвитку загальнодоступного ШІ проблема ефективного розрізнення зловмисних намірів та законних досліджень залишається невирішеною, що робить системи вразливими перед недосвідченими, але озброєними ШІ зловмисниками». ***(Asad Kashif. Amateur Hacker Used Claude And OpenAI Agents To Hack 14 Companies // Static Media® (https://www.bgr.com/2200632/claude-ai-cybsersecurity-attack-amateur-hacker/). 24.06.2026).***

***

**«Зловмисники проводять нову кампанію під назвою «Poisoned Tenant», створюючи підроблені робочі простори OpenAI, які видають себе за легітимні компанії, з метою викрадення конфіденційних корпоративних даних.** Ця схема, виявлена компанією Push Security після того, як її власні співробітники стали жертвами атаки, передбачає, що зловмисники створюють організації ChatGPT, використовуючи особисті адреси електронної пошти, прив'язують до них кредитну картку, щоб робочий простір виглядав автентичним і повністю забезпеченим фінансуванням, а також надсилають цільові запрошення співробітникам компаній у сфері кібербезпеки та технологій, про яких вони заздалегідь зібрали інформацію… Оскільки ці запрошення надсилаються безпосередньо з офіційної поштової інфраструктури OpenAI, вони легко обходять стандартні фільтри безпеки

електронної пошти. Надаючи запрошеним співробітникам адміністративний доступ до платформи штучного інтелекту, що виглядає як офіційна корпоративна, зловмисники сподіваються обдурити їх і змусити несвідомо надавати надзвичайно конфіденційну інформацію — таку як вихідний код, стратегічні плани або внутрішні документи — безпосередньо у вікнах чату… Ця витончена тактика свідчить про посилення тенденції, за якої кіберзлочинці зловживають законними функціями сповіщень платформ SaaS, що спонукає експертів з безпеки закликати організації постійно контролювати свої підписки на SaaS та навчати співробітників критично перевіряти несподівані запрошення до робочого простору». ***(Lawrence Abrams. Cybersecurity firms targeted by fraudulent OpenAI organization invites // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/cybersecurity-firms-targeted-by-fraudulent-openai-organization-invites/). 26.06.2026).***

***

## Кіберзлочинність та кібертероризм

**«TA4922 — це китайськомовна кіберзлочинна група, активність якої протягом останнього року постійно зростає. Вона розширила сферу своєї діяльності, перейшовши від традиційних цілей в Азії — зокрема Японії, Тайваню, Кореї, Сінгапуру та Індії — до організацій у Європі (Велика Британія, Німеччина та Італія) та Південній Африці.** За даними Proofpoint, ця група діє з фінансових мотивів і зосереджується на отриманні віддаленого доступу до організацій-жертв з метою викрадення даних, перепродажу доступу, шахрайства та збору облікових даних…

Ця група активно використовує методи соціальної інженерії, застосовуючи приманки, пов’язані з кадровими питаннями, нарахуванням заробітної плати, оподаткуванням та виставленням рахунків, щоб спонукати жертв переходити за шкідливими посиланнями або надавати свої облікові дані. Вона також намагається перенести спілкування з електронної пошти на такі платформи, як LINE, WhatsApp або Microsoft Teams, де може діяти поза межами досяжності традиційних засобів захисту електронної пошти. Було зафіксовано, що TA4922 паралельно з розповсюдженням шкідливого програмного забезпечення проводить кампанії з фішингу облікових даних та підробки особи…

Що стосується шкідливого програмного забезпечення, група використовує різноманітний арсенал, який постійно вдосконалюється. У останніх кампаніях використовувалися бекдор Atlas RAT, завантажувач шкідливого ПЗ RomulusLoader (який застосовується для встановлення легальних інструментів віддаленого моніторингу та управління, таких як AnyDesk і SyncFuture), стіллер SilentRunLoader на базі Python, що націлений на облікові дані браузера та файли cookie, а також бекдор ValleyRAT (Winos4.0). Хоча TA4922 має певні тактичні спільні риси з такими зловмисниками, як Silver Fox та Void Arachne, вона, схоже, не займається шпигунством безпосередньо, хоча Proofpoint попереджає, що деякі можливості її шкідливого програмного забезпечення потенційно можуть бути використані для

стеження або продані шпигунським угрупованням. Загалом, TA4922 наразі виділяється як найактивніший зловмисник у сфері кіберзлочинності за даними Proofpoint, демонструючи високий темп діяльності та широкий спектр стратегій атак». ***(Ionut Arghire. Chinese Cybercrime Group in Spotlight for Record Campaign Pace // Wired Business Media Publication (https://www.securityweek.com/chinese-cybercrime-group-ta4922-in-spotlight-for-record-campaign-pace/). 04.06.2026).***

***

**«…Швидка індустріалізація кіберзлочинності, що відбувається під впливом сучасних моделей штучного інтелекту, таких як Mythos, перевантажує системи кіберзахисту організацій, виявляючи вразливості швидше, ніж їх встигають усунути, перетворюючи додатки на головне поле бою.** Згідно з доповіддю Cloud Security Alliance (CSA), за останній рік 80 % організацій зазнали зломів, пов'язаних із відомими вразливостями, головним чином через те, що 82 % з них не мають ефективного контролю за робочим середовищем, необхідного для визначення, які саме вразливості дійсно можуть бути використані зловмисниками і потребують негайного усунення… Хоча безпека на етапі розробки залишається надзвичайно важливою, 42 % організацій планують збільшити інвестиції в захист під час виконання, хоча на сьогодні рівень впровадження автоматизованих засобів блокування, таких як брандмауери веб-додатків (WAF), є низьким (17 %) через побоювання, що помилкові спрацьовування, спричинені відсутністю контексту додатка, можуть порушити роботу бізнесу. Натомість в окремому звіті компанії FireMon стверджується, що основною проблемою є не брак ефективних засобів безпеки, а, скоріше, недосконаліть управління персоналом та оперативного контролю… Дані FireMon свідчать, що ручне управління політиками призводить до значної неефективності — зокрема, 69 % правил брандмауера залишаються невикористаними, а 45 % не мають документації, — що вказує на те, що належне безперервне управління політиками, сегментація мережі та мікросегментація є основою для зменшення площі атаки. Зрештою, хоча CSA пояснює ці проблеми тим, що інструменти не забезпечують необхідного контексту для автоматичного виправлення та блокування, FireMon стверджує, що необхідні інструменти існують, але страждають від критичного браку оперативного контролю з боку команд безпеки». ***(Kevin Townsend. Two New Reports Offer Competing Explanations for Cybersecurity's Growing Crisis // Wired Business Media Publication (https://www.securityweek.com/two-new-reports-offer-competing-explanations-for-cybersecuritys-growing-crisis/). 02.06.2026).***

***

**«Саудівським уболівальникам, які вирушають на Чемпіонат світу з футболу (FIFA) 2026 року, рекомендують бути пильними щодо шахрайських схем із підробкою особи, оскільки компанії з кібербезпеки попередили про сплеск шахрайства напередодні турніру, який проходитиме в 16 містах США, Канади та Мексики з 11 червня по 19 липня 2026 року.** Компанія Group-IB заявила, що виявила «масштабну, витончену» кампанію, спрямовану проти вболівальників, ідентифікувавши понад 4 300 шахрайських доменів, що видають

себе за офіційні веб-ресурси FIFA, шість паралельних схем шахрайства та чотирьох окремих зловмисників, потенційні збитки від яких, за оцінками, можуть сягнути мільярдів доларів… Оскільки FIFA очікує понад 6 мільйонів відвідувачів, а попит на квитки значно перевищує пропозицію — за перші 15 днів було подано понад 150 мільйонів заявок, що робить попит на квитки приблизно в 30 разів вищим, ніж на минулих турнірах — дослідники зазначають, що гостра необхідність придбати квитки сприяє поширенню шахрайства. З серпня 2025 року було зареєстровано тисячі підроблених доменів, у тому числі понад 300, які активно розміщують фішингову інфраструктуру, та близько 3800, припаркованих для подальшої активації; у центрі уваги — орієнтована на прибуток китайськомовна операція під назвою «GHOST STADIUM», яка повторно використовує фішинговий набір на сотнях сайтів і ретельно клонує fifa.com, включаючи систему єдиного входу FIFA (з реальним ідентифікатором клієнта, скопійованим з активного сайту) і навіть зображення, завантажені безпосередньо з серверів FIFA, щоб виглядати легітимно… Шахраї використовують рекламу у Facebook, тактику тиску та пропозиції квитків із значними «знижками», щоб перенаправити жертв на підроблені сторінки входу, де можна викрасти облікові дані та отримати доступ до акаунтів FIFA. Компанія Group-IB зазначила, що на ринках даркнету вже циркулює понад 2 500 дійсних пар облікових даних FIFA, частково через шкідливе програмне забезпечення для викрадення інформації. Компанія оцінила збитки від шахрайства з преміум-квитками та квитками категорії «гостинність» у розмірі від 71 до 474 мільйонів доларів, попередивши, що загальний обсяг шахрайства може бути набагато більшим, і зазначила, що злочинці також націлені на сувенірну продукцію та стримінг — особливо в Латинській Америці — використовуючи підроблені магазини та шкідливі сайти для поширення шкідливого програмного забезпечення… Окремо компанія Proofpoint попередила, що понад 36 % офіційних спонсорів, постачальників, партнерів та прихильників, пов'язаних із турніром, не мають належного захисту електронної пошти від підробки доменів, і порадила саудівським уболівальникам ретельно перевіряти посилання, пропозиції та запити на оплату через офіційні канали, зазначивши, що великі спортивні події приваблюють шахраїв, які видають себе за бренди, а штучний інтелект робить фішинг більш персоналізованим, переконливим та масштабнішим — проблему, яку компанія визначила як дедалі важливішу, оскільки Саудівська Аравія готується прийняти Чемпіонат світу з футболу у 2034 році». ***(GABRIELE MALVISI. Cybersecurity firm flags 'sophisticated' fraud campaign targeting World Cup fans // SAUDI RESEARCH & PUBLISHING COMPANY (https://www.arabnews.com/node/2646106/media). 05.06.2026).***

***

**«Компанія Gregory Jewellers, що базується в Сіднеї та займається продажем елітних ювелірних виробів та годинників, підтвердила факт кібератаки, пов'язаної з несанкціонованим доступом до її IT-систем, після того як угруповання-вимагачі Kairos заявило про викрадення 574 гігабайтів даних компанії.** Хакери тимчасово опублікували зразок цих даних у даркнеті — серед яких, як стверджується, були особисті дані клієнтів та документи внутрішнього

розслідування — після чого видалили цю публікацію… У відповідь компанія Gregory Jewellers залучила незалежних експертів для розслідування масштабів порушення та повідомила про інцидент як до Управління комісара з питань інформації Австралії, так і до Австралійського центру кібербезпеки. Компанія продовжує працювати та вже зв'язалася з постраждалими співробітниками та клієнтами. Угруповання-вимагачі Kairos, яке з'явилося в листопаді 2024 року та веде активну діяльність на російськомовних форумах, взяло на себе відповідальність за понад 80 атак, зокрема за нещодавнє порушення безпеки компанії Strata Republic, що базується в штаті Новий Південний Уельс». ***(Australian jewellery retailer confirms cyber attack // Befindan Media (https://www.jewellermagazine.com/Article/15085/Australian-jewellery-retailer-confirms-cyber-attack). 02.06.2026).***

***

**«Останні дослідження ставлять під сумнів поширену думку про те, що участь у кіберзлочинах завжди є добровільною, підкреслюючи, що примус може набувати форм, які виходять за межі очевидної фізичної сили…** Дослідження «королівств шахрайства» у Західній Африці — таємних навчальних центрів, що готують до онлайн-шахрайства — показує, що молодих рекрутів часто приваблюють економічні труднощі та брак можливостей, після чого вони потрапляють під дію багаторівневих механізмів контролю, таких як обмеження пересування, ізоляція, фінансова залежність та психологічне чи духовне залякування. Хоча ці люди не перебувають у фізичному ув'язненні, віра в духовні загрози та соціальний тиск можуть фактично утримувати їх у полоні, створюючи форму примусу, що обмежує їхню здатність піти…

Це розмиває традиційне правове розмежування між особами, які вчиняють правопорушення добровільно, та жертвами торгівлі людьми, що свідчить про те, що багато учасників знаходяться на проміжному рівні між власним вибором і примусом. Як наслідок, сучасні підходи у сфері кримінального правосуддя можуть призвести до неправильної класифікації осіб, що, у свою чергу, спричиняє непропорційні покарання та неефективну реабілітацію… Ці висновки вимагають більш виважених правових та політичних заходів, зокрема врахування факторів примусу при призначенні покарання, адаптації програм реабілітації, вирішення глибинних соціальних проблем, таких як безробіття та низький рівень освіти, а також посилення відповідальності осіб, які сприяють таким діям. Загалом, визнання цих менш помітних форм примусу є надзвичайно важливим для більш ефективної та справедливої боротьби з кіберзлочинністю». ***(Suleman Lazarus. Forced labour in west African cybercrime academies: how fear traps young men // The Conversation Media Group Ltd (https://theconversation.com/forced-labour-in-west-african-cybercrime-academies-how-fear-traps-young-men-283661). 11.06.2026).***

***

**«Компанія Mackay Sugar, другий за величиною виробник сирого цукру в Австралії, зазнала серйозних збитків внаслідок кібератаки, яка змусила її зупинити роботу двох із трьох цукрозаводів у містах Фарлі та Рейскоурс на**

**півночі Квінсленда.** Компанія виявила злом систем рано вранці в середу та негайно зупинила роботу, щоб захистити свої системи. Фахівці з кібербезпеки спільно з компанією та владою проводять розслідування інциденту та працюють над безпечним відновленням систем…

Хоча на цукрозаводі у Фарлі відновили обмежене ручне перероблення цукрової тростини, зібраної ще до нападу, основні системи постачання, логістики та приймання цукрової тростини залишаються непрацездатними, а це означає, що наразі додаткова цукрова тростина не приймається. Компанія «Mackay Sugar» сподівається розпочати поетапне відновлення збору врожаю та повномасштабних операцій з переробки цукрової тростини вже з наступного тижня, причому всі три цукрозаводи можуть запрацювати у другій половині тижня…

Ця ситуація викликає серйозне занепокоєння серед 1 300 виробників цукрової тростини в регіоні, переважно сімейних господарств, які щорічно постачають близько 700 000 тонн цукрової тростини. Цукрову тростину необхідно швидко переробляти після збору, щоб уникнути втрати вмісту цукру та якості. Місцевий виробник Тоні Бугея зазначив, що затримка може коштувати йому щонайменше тиждень збору врожаю під час критичного періоду високого вмісту цукру. Голова організації Canegrowers Mackay Джозеф Борг повідомив, що фермерам порадили не розраховувати на надто оптимістичні результати, оскільки ситуація залишається нестабільною, незважаючи на певний прогрес…

Експерт з кібербезпеки Джейсон Кінг зазначив, що регіональні підприємства зі складною інфраструктурою, такі як цукрові заводи, стають дедалі привабливішими цілями для хакерів. Цей інцидент підкреслює зростаючу загрозу, яку кібератаки становлять для критично важливих галузей промисловості та місцевих громад у регіоні». ***(Aimee Mitchell. Mackay Sugar mills shut by cyber attack hope to reopen next week // ABC (https://www.abc.net.au/news/2026-06-12/mackay-sugar-mills-shut-by-cyber-attack-hope-to-reopen-next-week/106792420). 12.06.2026).***

***

**«Лабораторія Cyble Research & Intelligence Labs (CRIL) повідомляє, що в результаті масштабної операції з SEO-отруєння, пов'язаної з азартними іграми в Таїланді, було скомпрометовано 163 організації в понад 30 країнах.** Зловмисники скористалися покинутими хмарними DNS-делегаціями, що дозволило їм розміщувати сторінки з азартними іграми тайською мовою під надійними корпоративними субдоменами, що належать жертвам, серед яких — урядові установи, медичні заклади, фінансові організації, університети та об'єкти критичної інфраструктури… Кампанія в основному базується на зловживанні занедбаними делегуваннями зон Azure DNS, які залишаються після того, як організації припиняють роботу хмарних проєктів, але не видаляють записи NS: зловмисники знаходять ці занедбані делегування, відтворюють відповідні зони DNS у нових підписках Azure та відновлюють контроль над делегованими піддоменами, а потім розгортають набір інструментів для азартних ігор на базі Next.js, захищений дійсними сертифікатами Let's Encrypt з підставкою, щоб контент виглядав легітимним для користувачів і пошукових систем… Розслідування CRIL розпочалося з виявлення аномальної активності DNS у

середовищі піддоменів Verizon, яке містило понад 1 000 піддоменів з унікальними іменами, що надавали азартно-ігровий контент із партнерськими посиланнями. Подальший аналіз виявив однакові ознаки інфраструктури у 162 інших організаціях, зокрема спільні ідентифікатори збірки Next.js, шляхи до файлів favicon та типові схеми партнерських перенаправлень; на момент публікації 161 із 163 організацій все ще залишалися активно скомпрометованими… Дослідники загалом виявили чотири механізми зловживання: захоплення зони DNS у Azure, яке зачепило понад 150 організацій; аналогічні випадки захоплення через DigitalOcean, що торкнулися двох жертв; прямі помилки в налаштуваннях DNS із використанням символів-замінників у ще двох випадках; а також масове створення записів типу A в середовищі Verizon. Вони також зазначили, що записи про прозорість сертифікатів свідчать про те, що деякі занедбані зони перебували в неактивному стані протягом багатьох років, перш ніж зловмисники переоформили сертифікати у квітні 2026 року… Цей проект отримує прибуток за допомогою партнерських кодів відстеження та використовує фільтрацію на стороні сервера, щоб надавати пріоритет тайським відвідувачам перед перенаправленням їх на невелику групу сайтів, пов’язаних з азартними іграми. Це супроводжується SEO-оптимізованими сторінками, що рекламують дуже невеликі депозити, а CRIL підключає інфраструктуру доставки на серверній стороні до парку з 103 серверів у Гонконзі, які мають однакові TLS- та HTTP-відбитки та спільні конфігурації. Оскільки зловмисники використовують авторитетні домени жертв, дійсні сертифікати та іншу «чисту» інфраструктуру, компанія CRIL попереджає, що традиційні засоби безпеки можуть не виявити таку активність, і рекомендує посилити заходи з забезпечення безпеки DNS — проводити аудит делегувань, видаляти занедбані хмарні записи NS та постійно відстежувати журнали Certificate Transparency — щоб запобігти подібним масштабним зловживанням, спричиненим забутими налаштуваннями, а не компрометацією додатків чи мережі». ***(Ashish Khaitan. 163 Organizations Hit by Thai Gambling SEO Poisoning Campaign // The Cyber Express (https://thecyberexpress.com/thai-gambling-seo-poisoning/). 12.06.2026).***

***

**«У п’ятницю компанія Google подала позов проти китайської мережі кіберзлочинців, яку вона називає «Outsider Enterprise», стверджуючи, що ця група використовувала штучний інтелект Google Gemini для створення та розширення масштабів фінансових шахрайств в Інтернеті, від яких постраждали сотні тисяч людей, переважно у Сполучених Штатах.** Google заявила, що вперше координує свої дії з ФБР та провідними операторами мобільного зв'язку, зокрема AT&T, T-Mobile та Verizon, щоб знешкодити цю мережу, і домагається винесення судового заборонного наказу, який допоможе її ліквідувати… Згідно зі скаргою, група використовувала штучний інтелект для створення сотень фейкових веб-сайтів, що видавали себе за відомі бренди та сервіси, такі як Google, YouTube, Поштова служба США та нью-йоркська система E-ZPass, а також координувала свою діяльність через Telegram, обмінюючись тактиками та наборами для шахрайства на базі штучного інтелекту, які дозволяли масово генерувати шахрайські повідомлення через численні канали. Google та

правоохоронні органи попередили, що штучний інтелект прискорює фішинг та шахрайство, роблячи афери більш переконливими та важчими для виявлення, посилаючись на дані ФБР, згідно з якими минулого року американці втратили майже 21 мільярд доларів через кіберзлочинців, причому приблизно 893 мільйони доларів пов'язані з використанням штучного інтелекту… Компанія Google повідомила, що в результаті цієї операції було створено 131 програмний набір, який давав змогу здійснювати масове клонування веб-сайтів, і що протягом двох тижнів у травні ця група надіслала користувачам Android 2,5 мільйона повідомлень із посиланнями на близько 9 000 фейкових веб-сайтів та понад мільйон шахрайських інтернет-адрес; Google оцінює власні збитки в мільйони доларів, хоча точні суми поки що невідомі». ***(Cecilia Kang. Google Says Chinese Cybercrime Group Used Its A.I. in Scams // The New York Times Company (https://www.nytimes.com/2026/06/12/technology/google-lawsuit-china-ai-scams.html). 12.06.2026).***

***

**«Кіберзлочинність зростає швидше, ніж правоохоронні органи встигають з нею боротися: у «Звіті ФБР про інтернет-злочини за 2025 рік» вперше зафіксовано понад мільйон скарг, а заявлені збитки склали 20,87 млрд доларів — на 26 % більше, ніж у попередньому році, — проте Комісія з питань призначення покарань встановила, що з 2014 по 2021 рік лише 2 590 осіб були засуджені на федеральному рівні за злочини, пов'язані з хакерством, криптовалютами або дарквебом, що створює ризикове середовище, в якому зловмисники розуміють, що ймовірність покарання є низькою.** Злочинці навмисно планують свої операції так, щоб уникнути судового переслідування, «відмиваючи» інфраструктуру через юрисдикції, що не співпрацюють, використовуючи відсутність у США договорів про екстрадицію з такими країнами, як Росія та Китай, і користуючись повільною транскордонною правовою допомогою, яка не може зберегти цифрові докази, що швидко втрачають актуальність; різні національні погляди на «кіберзлочинність» проти діяльності, що відповідає інтересам держави, також ускладнюють правоохоронну діяльність… З оперативної точки зору, встановленню винних та притягненню їх до відповідальності заважають екосистеми «шкідливого програмного забезпечення як послуги» та зростаючий ринок програм-вимагачів (у 2025 році кількість груп, що заявляють про своїх жертв, зросте до 138 порівняно з 98 у 2024 році), швидке відновлення злочинної інфраструктури на зашифрованих платформах, слабкі правила зберігання даних, що призводять до зникнення доказів, а також недостатній контроль за дотриманням вимог KYC на деяких криптовалютних біржах типу «пір-ту-пір», тоді як відмивання коштів між ланцюгами ускладнює відстеження доходів від програм-вимагачів. Штучний інтелект також знижує бар'єр для ефективного фішингу: згідно з одним звітом, елементи, згенеровані штучним інтелектом, містяться у 85,76% фішингових електронних листів, що робить шахрайство більш переконливим та масштабованим… З боку захисників нестача кваліфікованих кадрів та низький рівень готовності до проведення криміналістичних експертиз означають, що багато жертв не можуть зберегти

журнали, записи та докази, необхідні для встановлення відповідальності та притягнення до відповідальності, що посилює мотивацію зловмисників залишатися анонімними. У тих випадках, коли судові переслідування все ж завершуються успіхом, вони зазвичай стосуються афілійованих осіб або учасників середнього рівня, екстрадованих із країн-партнерів, тоді як багато лідерів синдикатів вищого рівня залишаються під слідством, але недосяжними; як наслідок, правоохоронні органи все частіше надають пріоритет зриву діяльності зловмисників, а не їх затриманню, шляхом ліквідації інфраструктури та ринків збуту, наводячи такі приклади, як операція «Cronos» проти LockBit (після якої, за повідомленнями, обсяг платежів знизився на 79%), виведення з ладу серверів в рамках операції «Endgame» та закриття основних форумів з кіберзлочинності в рамках операції «Talent»… США також посилюють дипломатичний та економічний тиск на юрисдикції, що надають притулок кіберзлочинцям, на підставі Указу № 14390 (від 6 березня 2026 року), а також вживають активних заходів протидії шахрайству, таких як операція «Level Up» та програми оперативного заморожування активів, завдяки яким вдалося запобігти виведенню або повернути значні суми. Зрештою, у статті стверджується, що підвищення вартості кіберзлочинності вимагає глибших системних змін — швидшої міжнародної співпраці, міцніших договірних рамок (з огляду на повільну ратифікацію Конвенції ООН про кіберзлочинність порівняно з ширшим прийняттям Будапештської конвенції, але з обмеженим охопленням Росії та Китаю), кращого обміну розвідданими між агентствами та галуззю, розширеного використання винагород за виявлення вразливостей та кращої організаційної готовності, щоб жертви могли надавати криміналістичні записи, необхідні для транскордонних розслідувань». ***(Sean Michael Kerner. The prosecution gap: Why cybercrimes go unpunished // TechTarget, Inc. (https://www.techtarget.com/searchsecurity/feature/The-prosecution-gap-Why-cybercrimes-go-unpunished). 11.06.2026).***

***

**«Розмір ботнету JDY, яким керують китайські хакери, що мають підтримку держави, зокрема відома група Volt Typhoon, збільшився вдвічі й наразі налічує 1 500 заражених пристроїв категорії «малий офіс/домашній офіс» (SOHO), периферійних пристроїв та пристроїв Інтернету речей (IoT), розташованих переважно у США, Європі та Азії.** Згідно з доповіддю Black Lotus Labs компанії Lumen, ця бот-мережа, яка вціліла після того, як уряд США минулого року ліквідував пов'язану з нею бот-мережу KV, активно використовується для прихованого сканування та розвідки з метою виявлення вразливої інфраструктури, причому особлива увага приділяється американським збройним силам… Розподіляючи свої скануючі операції між тисячами зламаних пристроїв, JDY успішно обходить традиційні засоби захисту на основі IP-адрес та геозонування, маскуючи свою шкідливу діяльність під легітимним трафіком. Оператори спеціально націлюються на погано обслуговані та незахищені оновленнями периферійні пристрої різних виробників, причому особливо активізують сканування обладнання Fortinet одразу після оприлюднення інформації про нову вразливість… Експерти з безпеки попереджають, що ця операція стратегічно

спрямована на забезпечення тривалої присутності в системі та збір розвідувальної інформації, а не лише на крадіжку даних, що може мати руйнівні наслідки під час геополітичних криз. Для захисту від ботнету JDY підприємствам настійно рекомендується дотримуватися суворого графіка встановлення виправлень та оновлень безпеки для маршрутизаторів та пристроїв Інтернету речей (IoT), регулярно перезавантажувати периферійне обладнання та впроваджувати сучасні архітектури, такі як Secure Access Service Edge (SASE), щоб мінімізувати площу атаки проти складних розвідувальних операцій, що фінансуються державою». ***(Nicole Kobie. Security experts sound alarm over 'expanded' China-linked botnet used to target US critical infrastructure and military assets // Future US, Inc. (https://www.itpro.com/security/security-experts-sound-alarm-over-expanded-china-linked-botnet-used-to-target-us-critical-infrastructure-and-military-assets). 11.06.2026).***

***

**«Групи кіберзлочинців, пов'язані з Північною Кореєю та Китаєм, дедалі частіше націлюються на фінансові компанії та криптовалютні активи в Азіатсько-Тихоокеанському регіоні, забезпечуючи цим країнам значні джерела доходу; лише у 2025 році північнокорейські зловмисники викрали щонайменше 2,02 млрд доларів у криптовалюті, що становить до 7 % ВВП країни.** Хоча тактики соціальної інженерії, такі як «pig butchering», залишаються поширеними, північнокорейські угруповання вдосконалюють свої методи, видаючи себе за рекрутерів для компаній Web3 та ШІ або інвесторів, щоб викрасти облікові дані та отримати доступ до інфраструктури високої цінності… Щоб приховати свої незаконні доходи, ці угруповання дедалі частіше вдаються до послуг високотехнологічних сервісів, розбиваючи великі вкрадені суми на менші частини та використовуючи китайські мережі переказу коштів, сервіси «міксерів» та протоколи децентралізованих фінансів. У відповідь на цю зростаючу загрозу уряди країн, правоохоронні органи та приватні дослідницькі компанії у сфері блокчейну, такі як Chainalysis, значно посилюють співпрацю… Цей об'єднаний фронт — що базується на обміні оперативною інформацією, протоколах оперативного реагування та скоординованих заходах правоохоронних органів, таких як нещодавня операція «Strike Force» Центру боротьби з шахрайством США з ліквідації кіберзлочинного угруповання «Shunda» — виявився надзвичайно ефективним: його результатом стало вилучення та заморожування викраденої криптовалюти на суму в сотні мільйонів доларів, що свідчить про посилення тиску на кіберзлочинців, які діють за підтримки держави». ***(Robert Lemos. Chinese, N. Korean Threat Groups Build on Asia-Pacific Success // TechTarget, Inc. (https://www.darkreading.com/cyberattacks-data-breaches/chinese-korean-threat-groups-asia-pacific-success). 11.06.2026).***

***

**«…Хакери взяли на себе відповідальність за злам у компанії Klue, що надає ринкову аналітику, в результаті якого було викрадено дані невідомої кількості її корпоративних клієнтів, зокрема кількох великих компаній у**

**сфері кібербезпеки.** У Klue повідомили, що атака сталася 12 червня через скомпрометовані застарілі облікові дані, пов'язані з інструментом інтеграції, який з'єднував хмарні системи клієнтів, такі як Salesforce, із платформою Klue, що дозволило зловмисникам отримати доступ до даних клієнтів та викрасти їх. Група кіберзлочинців Icarus взяла на себе відповідальність за інцидент і погрожує оприлюднити викрадену інформацію, якщо не буде сплачено викуп, тоді як постраждалі компанії, серед яких Gong, Jamf, HackerOne, Insurity, OneTrust, Recorded Future, Snyk, Sprout Social та Tanium, підтвердили, що їхні дані були викрадені… Судячи з усього, викрадені дані переважно складаються з контактної інформації підприємств та деяких даних облікових записів. Компанія Klue залучила компанію CrowdStrike та відключила інтеграції, щоб запобігти подальшому доступу, але не повідомила, скільки клієнтів постраждало та чи отримувала вона вимогу про викуп. Цей інцидент вписується в більш широку схему атак типу «єдиної точки відмови» на провайдерів проміжного програмного забезпечення та хмарної інтеграції, подібних до нещодавніх хакерських атак на такі компанії, як Gainsight, Salesloft, Snowflake та TanStack, де скомпрометовані облікові дані або шкідливе програмне забезпечення на пристроях співробітників дозволили зловмисникам одночасно отримати доступ до багатьох кінцевих клієнтів… Цей витік даних також викликає питання щодо стану внутрішньої безпеки Klue та нагляду з боку керівництва, особливо з огляду на те, що компанія публічно не вказала відповідального за кібербезпеку на своїй сторінці керівництва». ***(Zack Whittaker. Klue hack results in data breach at several cybersecurity firms // TechCrunch Media LLC. (https://techcrunch.com/2026/06/22/klue-hack-results-in-data-breach-at-several-cybersecurity-firms/). 22.06.2026).***

***

**«Нещодавно виявлена кампанія з викрадення облікових даних «FortiBleed» оприлюднила понад 86 000 діючих облікових даних для входу в брандмауери Fortinet та шлюзи SSL VPN у 194 країнах.** Ця автоматизована операція, організована, як підозрюється, російськомовними зловмисниками, що керуються як фінансовими, так і геополітичними мотивами, в основному спрямована проти країн-членів НАТО та охоплює критично важливі сектори, зокрема телекомунікації, державний сектор, фінанси та охорону здоров'я. Замість того, щоб експлуатувати нову уразливість «нульового дня», зловмисники користуються недоліками в організаційних заходах безпеки. Вони використовують автоматизовані сканери, метод «credential stuffing» (підстановка облікових даних з попередніх витоків) та методи грубої сили для проникнення на пристрої, підключені до Інтернету, що не мають багатофакторної автентифікації (MFA). Після компрометації ці пристрої використовуються як пункти прослуховування для збору додаткових облікових даних із проходячого VPN-трафіку, а отримані дані повертаються до сканера, щоб продовжити цикл атаки…

У відповідь на це компанія Fortinet та світові агентства з кібербезпеки — зокрема CISA (США), NCSC (Велика Британія) та ASD (Австралія) — опублікували термінові попередження, закликаючи організації визнати можливість ураження та вжити негайних захисних заходів. Для зменшення ризику організаціям

рекомендується припинити всі активні адміністративні сесії та сесії VPN, примусово змінити паролі та суворо запровадити стійку до фішингу багатофакторну автентифікацію (MFA) для всіх облікових записів. Крім того, адміністратори повинні зменшити площу атаки, вивівши інтерфейси управління з публічного Інтернету та обмеживши доступ до надійних внутрішніх мереж. Агентства також настійно рекомендують оновити прошивку до найновіших версій, щоб забезпечити належне шифрування облікових даних за допомогою більш надійного алгоритму хешування PBKDF2. Нарешті, IT-команди повинні ретельно перевірити журнали брандмауерів та контролерів доменів на наявність неавторизованих облікових записів, підозрілих моделей доступу або змін у конфігурації, а також виконати повне скидання до заводських налаштувань у разі підтвердження компрометації, щоб повністю усунути будь-яку стійку загрозу…» ***(Anna Ribeiro. Global cybersecurity agencies warn of credential exposure in FortiBleed campaign targeting Fortinet firewalls, VPN gateways // Industrial Cyber (https://industrialcyber.co/vulnerabilities/global-cybersecurity-agencies-warn-of-credential-exposure-in-fortibleed-campaign-targeting-fortinet-firewalls-vpn-gateways/). 22.04.2026).***

***

**«Кібератака на шкільну IT-мережу C2k у Північній Ірландії зачепила більшу кількість шкіл, ніж спочатку вважалося. Управління освіти (EA) нещодавно надіслало листи до 23 шкіл — 16 з яких не отримували попередніх попереджень — у яких попередило батьків, що під час зломu, ймовірно, було отримано доступ до персональних даних їхніх дітей.** Атака, яку було виявлено на початку квітня, змусила провести системне скидання паролів, що позбавило учнів та вчителів доступу до важливих освітніх ресурсів напередодні екзаменаційного періоду… У зв’язку з цим інцидентом було затримано 16-річного хлопця, якого згодом відпустили під заставу. Хоча доказів подальших порушень безпеки після локалізації атаки немає, триваюча криміналістична експертиза виявила ширше коло потенційних жертв. Співробітник EA, відповідальний за захист даних, вибачився за заподіяні неприємності, але зазначив, що слідчі поки що не можуть точно підтвердити, яка саме інформація потрапила до рук зловмисників… З огляду на складність та тривалість розслідування, EA доручило провести незалежну експертизу, залучило Управління комісара з питань інформації та тісно співпрацює з Поліцейською службою Північної Ірландії, обіцяючи інформувати постраждалі сім’ї про нові обставини у міру їх з’ясування». ***(Niall Glynnand, Auryn Cox. New warning to parents over schools cyber attack // BBC (https://www.bbc.com/news/articles/cjrg0gl03n1o). 26.06.2026).***

***

**«Компанія Tata Electronics, ключовий виробничий партнер як Apple, так і Tesla, стала жертвою масштабного витоку даних: група хакерів-вимагачів World Leaks заявила, що опублікувала в даркнеті понад 200 000 файлів загальним обсягом 630 ГБ викрадених даних.** Хоча автентичність повного масиву даних поки що не підтверджена, експерти з безпеки виявили в ньому

документи надзвичайно конфіденційного характеру, зокрема власні стандарти контролю якості Apple та комерційні таємниці Tesla, пов'язані з Model Y та оновленою Model 3 («Project Highland»). Компанія Tata стверджує, що її діяльність не зазнала змін, і відмовилася коментувати повідомлення про вимогу викупу, тоді як Apple розпочала внутрішнє розслідування, а Tesla зберігає мовчання…

Цей інцидент свідчить про значне зростання кіберризиків у ланцюгах постачання та підкреслює вразливість виробничого сектору. «World Leaks» — це група, що виникла в результаті ребрендингу угруповання «Hunters International», яке спеціалізувалося на шантажі. Вона застосовує стратегію, спрямовану виключно на викрадення та оприлюднення даних, а не на шифрування файлів, надаючи пріоритет крадіжці інтелектуальної власності та підриву репутації, а не порушенню виробничої діяльності. Такий підхід зміщує акцент у сфері страхування з традиційного страхування від перерв у діяльності на складні питання захисту інтелектуальної власності та відповідальності перед третіми особами… Отже, цей випадок порушує критично важливі питання щодо страхового покриття на ринку кіберстрахування: чи здатні поліси компанії Tata покрити ризики, пов'язані з інтелектуальною власністю, такого безпрецедентного масштабу, та чи мають Apple і Tesla страхове покриття щодо збитків, пов'язаних з інтелектуальною власністю, що виникли через дії стороннього постачальника. З огляду на те, що кількість претензій щодо відповідальності перед третіми особами вже зросла на 70 %, а ринок кіберстрахування зазнає цінового тиску, цей гучний випадок є суворим нагадуванням про те, що вразливість ланцюгів постачання наразі є найважливішою проблемою для страховиків». ***(Matthew Sellers. Apple and Tesla trade secrets exposed as Tata hit by cyber breach // KM Business Information US, Inc (https://www.insurancebusinessmag.com/us/news/cyber/apple-and-tesla-trade-secrets-exposed-as-tata-hit-by-cyber-breach-579985.aspx). 23.06.2026).***

***

**«Нещодавня кібератака на латвійську державну лісогосподарську компанію «Latvijas valsts meži» (LVM) викрила вразливі місця у стратегічній інфраструктурі країни, що спонукало урядовців закликати до посилення кібербезпеки в державних установах.** Ця атака дозволила хакеру отримати доступ до систем та даних компанії, що змусило LVM вжити запобіжних заходів та відключити кілька зовнішніх і внутрішніх систем, зокрема картографічні сервіси та платформи для партнерів. Влада вважає, що атака мала комерційну мотивацію, оскільки зловмисник відкрито хвалився цим інцидентом в Інтернеті… Хоча роль компанії LVM у розробці електронного реєстру виборців Латвії викликала певні побоювання, офіційні особи підтвердили, що система вже була передана державі і не зазнала впливу, а отже, безпосередньої загрози для майбутніх виборів немає. Цей інцидент змусив знову звернути увагу на виявлення вразливостей системи, забезпечення суворішого нагляду за ІТ-проєктами та підвищення стійкості систем, при цьому офіційні особи висловили впевненість, що латвійські можливості у сфері кібербезпеки зможуть запобігти подібним атакам за умови їхнього належного застосування». ***(Cyberattack on Latvia's state forests company highlights national cybersecurity risks, minister warns // BNN.LV (https://bnn-news.com/cyberattack-on-***

*latvias-state-forests-company-highlights-national-cybersecurity-risks-minister-warns-281534). 26.06.2026).*

***

**«Масштабну кібератаку на компанію Jaguar Land Rover у 2025 році, яка змусила зупинити виробництво на п'ять тижнів і завдала економічних збитків на мільярди, слідчі пов'язують із російською хакерською групою, а не з неорганізованим угрупованням, яке спочатку взяло на себе відповідальність.** Ця атака, яка обійшлася компанії приблизно в 350 мільйонів доларів і завдала збитків економіці Великої Британії загалом на суму близько 2,5 мільярда доларів, була здійснена за допомогою надзвичайно витонченого програмного забезпечення-вимагача та експлуатації вразливостей застарілих систем, а методи її проведення свідчать про можливості, більш характерні для суб'єктів, пов'язаних з державою, ніж для звичайних кіберзлочинців… Влада та компанії з кібербезпеки з Великої Британії та США об'єднали зусилля для локалізації інциденту, при цьому компанія Microsoft допомогла встановити осіб, причетних до злочину, а слідчі продовжують з'ясовувати, чи діяла ця група самостійно, чи за підтримки Кремля. На відміну від типових випадків використання програм-вимагачів, у цьому випадку не було очевидного фінансового мотиву, що викликає побоювання, що атака могла бути спрямована на порушення роботи критично важливих промислових об'єктів та підрив економічної стабільності…

Цей інцидент продемонстрував, як зловмисники задовго до цього проникли в системи, скориставшись їхніми вразливими місцями та дочекавшись стратегічно важливого моменту для нанесення удару, що в підсумку змусило компанію Jaguar призупинити свою діяльність у всьому світі, аби запобігти подальшим збиткам. Ця атака, що сталася на тлі загострення геополітичної напруженості між Великою Британією та Росією, підкреслює зростаючий ризик використання кібероперацій як інструментів економічного та стратегічного дестабілізування, а не лише як засобів вчинення фінансових злочинів». ***(Adam GoldmanJane, BradleyDustin Volz and Michael Schwirtz. A $2.5 Billion Whodunit: The Hack That Dented the U.K. Economy // The New York Times Company (https://www.nytimes.com/2026/06/26/world/europe/jaguar-russia-hack.html). 26.06.2026).***

***

**«Згідно з щорічним опитуванням 777 організацій, проведеним ABN Amro та MWM2, минулого року в Нідерландах зменшилася кількість підприємств, які зазнали збитків від кібератак, незважаючи на те, що фактичний обсяг атак залишився на незмінному рівні.** Частка малих та середніх підприємств (МСП), які постраждали від шкідливого програмного забезпечення, фішингу або витоків даних, знизилася з 72% до 60%, а частка компаній, що зазнали операційних або фінансових збитків, зменшилася з 20% до 15%. Аналітик Юлія Краувер пов'язує це поліпшення з посиленням базових засобів захисту, таких як більш ефективні брандмауери та швидше виявлення загроз… Однак у дослідженні зазначається, що підприємства недостатньо підготовлені до нових загроз: лише чверть малих та

середніх підприємств (МСП) мають план реагування на кібератаки, а 43 % ніколи не проводили відповідних навчань. Крім того, штучний інтелект прискорює темпи та підвищує складність атак, проте менше ніж 10 % МСП мають політику, спрямовану на усунення ризику витоку конфіденційних даних співробітниками через штучні інтелектуальні помічники, такі як ChatGPT… Ці вразливості посилює значна залежність від кількох великих американських технологічних гігантів, яку майже половина опитаних компаній вважає серйозним бізнес-ризиком. У відповідь на це майже дві третини малих та середніх підприємств активно вживають заходів для зменшення цієї залежності, причому 17 % з них починають переходити на європейські хмарні сервіси та альтернативне програмне забезпечення». ***(Fewer Dutch firms hit by cyberattacks, but AI threats loom // DutchNews (https://www.dutchnews.nl/2026/06/fewer-dutch-firms-hit-by-cyberattacks-but-ai-threats-loom/). 23.06.2026).***

***

**«Платформа прогнозних ринків Polymarket нещодавно зазнала кібератаки, в результаті якої було викрадено криптовалюту на суму, за оцінками, 3 мільйони доларів у приблизно 11 користувачів.** Злом стався, коли зламаний сторонній постачальник дозволив зловмисникам ввести шкідливий скрипт у інтерфейс платформи. З того часу Polymarket локалізувала загрозу, видалила уражену залежність та зобов'язалася повністю відшкодувати збитки всім постраждалим… Хоча компанія публічно не назвала постачальника, система якого була зламана, один із постраждалих користувачів припустив, що вразливість могла бути пов'язана з віртуальним приватним сервером Xorek Cloud. У відповідь на оголошення про злам у мережі X дехто з користувачів не виявив здивування: одні стверджували, що раніше попереджали Polymarket про недоліки в системі безпеки, а інші висміювали платформу за те, що вона, як стверджується, раніше глузувала з хакерів». ***(Sead Fadilpašić. Prediction market giant Polymarket hit by cyberattack, with company confirming user funds stolen — here is what we know // Future US, Inc. (https://www.techradar.com/pro/security/prediction-market-giant-polymarket-hit-by-cyberattack-with-company-confirming-user-funds-stolen-here-is-what-we-know). 26.06.2026).***

***

**«Бразилія тимчасово призупинила роботу національної системи мобільних аварійних сповіщень після ймовірної кібератаки, що сталася рано в суботу та спричинила розсилку неправдивих попереджень найвищого рівня на мобільні телефони у багатьох штатах, зокрема в Сан-Паулу та Ріо-де-Жанейро.** Неуповноважена особа отримала віддалений доступ до Інтерфейсу поширення публічних попереджень, що спричинило надсилання щонайменше десяти фальшивих повідомлень — у деяких з яких фігурувало слово «мізантропія» — через що телефони почали видавати гучні сигнали тривоги навіть у беззвучному режимі. У відповідь влада заблокувала зовнішній доступ до платформи, а Федеральна поліція розпочала розслідування цього інциденту… Хоча представники влади підтвердили, що основна інфраструктура системи оповіщення

цивільної оборони, яка зазвичай попереджає громадян про стихійні лиха, такі як повені та зсуви, не зазнала структурних пошкоджень, система залишатиметься вимкненою доти, доки не буде впроваджено більш безпечну версію, яка наразі перебуває на стадії розробки, щоб забезпечити абсолютну надійність для населення». ***(Daryna Antoniuk. Suspected cyberattack triggers false emergency alerts across parts of Brazil // Recorded Future News (https://therecord.media/suspected-cyberattack-triggers-false-emergency-alerts-brazil). 22.06.2026).***

***

**«У лютому внаслідок масштабної кібератаки, пов'язаної з російською хакерською групою, було зламано брандмауери приблизно 270 бельгійських організацій, серед яких школи, місцеві ради та юридичні фірми.** Цей інцидент є частиною масштабної глобальної кампанії, спрямованої проти партнерського порталу американської компанії з кібербезпеки Fortinet, що дозволило зловмисникам проникнути в мережі багатьох клієнтів через їхніх IT-провайдерів. У результаті по всьому світу було порушено роботу понад 75 000 брандмауерів та викрадено більше ніж 110 мільйонів облікових даних… За даними бельгійської компанії з кібербезпеки Secutec, серйозність інциденту — який називають одним із найбільших за всю історію серед постачальників послуг у сфері кібербезпеки — значно посилилася через недотримання належних практик безпеки. Жоден із постраждалих брандмауерів не використовував багатофакторну автентифікацію, IT-провайдери часто повторно використовували паролі, а 85 % систем працювали на застарілому програмному забезпеченні… Загроза залишається актуальною, оскільки щонайменше 150 уражених брандмауерів у Бельгії досі безпосередньо доступні з Інтернету, а до понад 100 організацій все ще можна отримати несанкціонований доступ, використовуючи викрадені облікові дані адміністратора. Про цю ситуацію повідомлено Бельгійський центр кібербезпеки». ***(Hundreds of Belgian organisations hit by cyber attack // Belga News Agency (https://www.belganewsagency.eu/hundreds-of-belgian-organisations-hit-by-cyber-attack). 23.06.2026).***

***

**«Хакери дедалі частіше відмовляються від складних технічних експлойтів на користь використання в злочинних цілях інструментів, яким розробники довіряють найбільше, зокрема програмного забезпечення з відкритим кодом та штучного інтелекту.** Ця тенденція нещодавно проявилася у двох масштабних кампаніях, під час яких зловмисники зловживали легітимними платформами для обходу традиційних заходів безпеки. У першому випадку група зловмисників під назвою TeamPCP за менш ніж чотири місяці вбудувала шкідливий код у понад 1 000 пакетів з відкритим кодом, скориставшись сліпою довірою компаній до автоматизованих залежностей, щоб досягти приблизно 500 мільйонів завантажень на тиждень і скомпрометувати такі великі технологічні компанії, як SAP, Red Hat та GitHub… Ця вразливість значно посилюється агентами штучного інтелекту, які самостійно встановлюють пакети без нагляду людини, створюючи середовище, в якому шкідливий код може поширюватися безконтрольно. У другій, надзвичайно

підступній кампанії зловмисники зловживали штучним інтелектом Claude від Anthropic, використовуючи його функцію «Shared Chats» для розміщення підроблених транскриптів звернень до служби підтримки Apple безпосередньо на надійному домені claude.ai. Направляючи трафік на ці посилання через рекламу Google, хакери успішно обдурили понад 2 000 розробників Mac, змусивши їх виконати шкідливі команди в терміналі… Зрештою, ці інциденти підкреслюють критичну вразливість сучасного ланцюга постачання програмного забезпечення: зловмисникам більше не потрібно зламувати системи, якщо вони можуть підірвати роботу знайомих доменів та надійних реєстрів. Щоб пристосуватися до цих змін, галузь кібербезпеки повинна кардинально переглянути свій підхід, піддаючи автоматизованих агентів на основі штучного інтелекту суворому контролю та усвідомлюючи, що легітимність платформи більше не гарантує її безпеку». ***(Darius Popa. Hackers have stopped breaking in. They're abusing the things developers already trust // Cogneve, INC. (https://thenextweb.com/news/teampcp-claude-shared-chats-ai-supply-chain-attacks-trust). 19.06.2026).***

***

**«Кібератаки обходяться ірландським малим та середнім підприємствам (МСП) у суму до 3,4 млрд євро щорічно, що зумовлено насамперед сукупним впливом повторюваних щоденних збоїв, а не великими одноразовими порушеннями безпеки.** Згідно з доповіддю «Приховані витрати, пов'язані з кіберризиками», підготовленою компанією eir business, Microsoft та Університетом Лімерика, ці часті інциденти — такі як спроби фішингу та використання програм-вимагачів — призводять до втрати понад 7,2 млн робочих днів щороку. Для середньої компанії, що зазнала таких інцидентів, це дорівнює майже трьом тижням втраченої продуктивності та приблизно 50 000 євро економічних збитків щороку… На щастя, значну частину таких перебоїв у роботі можна уникнути завдяки проактивним заходам; малі та середні підприємства, що мають структуровану систему управління даними та високий рівень кіберзахищеності, зазнають значно менше атак, що дозволяє скоротити щорічний час простою з понад 30 днів до всього п'яти. У відповідь на цю гостру вразливість компанія eir business запустила «Cybersecurity Assurance» — абонентську послугу, яка пропонує малим та середнім підприємствам постійну підтримку, планування безперебійності бізнесу та доступ до віртуальних керівників з інформаційної безпеки (vCISO) і команд реагування на інциденти… Цю ініціативу доповнює Національний центр кібербезпеки, який надає безкоштовні практичні рекомендації, щоб допомогти малим підприємствам посилити свої засоби захисту. Зрештою, експерти наголошують, що в міру того, як малі та середні підприємства продовжують впроваджувати цифрову трансформацію, вони також повинні приділяти пріоритетну увагу кількісній оцінці та активному управлінню цими дорогими повсякденними кіберризиками». ***(Repeated cyber disruption costing SMEs up to €3.4bn annually // Tech Network (https://www.techcentral.ie/repeated-cyber-disruption-costing-smes-up-to-e3-4bn-annually/ ). 19.06.2026).***

***

**«Нещодавня кібератака вивела з ладу онлайн-систему оплати Управління з розвитку столиці (CDA) на три дні, що унеможливило для громадян сплату податків на нерухомість, рахунків за воду та інших комунальних платежів.** Ця перерва у роботі сталася в критичний момент, оскільки ці платежі мають бути здійснені до кінця червня, що збігається із закінченням фінансового року. Хоча портал для оплати рахунків не працює, основний веб-сайт CDA залишається функціональним, і представники відомства запевнили громадськість, що всі попередні платежі, здійснені через 1-Link та банки-партнери, є цілком безпечними… Незважаючи на чутки про те, що було втрачено резервні копії даних за останні шість місяців, речник CDA Шахід Кіані підтвердив, що резервні дані в безпеці й зараз активно відновлюються. IT-відділ CDA у співпраці з Національною корпорацією радіо та телекомунікацій (NRTC) та податковими органами наразі працює цілодобово над відновленням уражених систем та даних». ***(Cyberattack hits CDA online billing system // Daily Ausaf (https://dailyausaf.com/en/technology/cyberattack-hits-cda-online-billing-system/#google_vignette). 19.06.2026).***

***

**«Нещодавно виявлена бот-мережа під назвою AryStinger заразила понад 4 000 застарілих маршрутизаторів, переважно старих моделей D-Link, перетворивши їх на системи, що керуються віддалено, які зловмисники використовують для здійснення шкідливих дій, таких як сканування, проксі-серверна діяльність, тунелювання та виконання команд.** Ця бот-мережа, виявлена дослідниками XLab компанії Qianxin, працює шляхом розподілу завдань між зараженими пристроями, що дозволяє зловмисникам ефективно проводити масштабну розвідку та готуватися до подальших вторгнень. Окрім використання цих маршрутизаторів як інфраструктури для атак, AryStinger може маніпулювати налаштуваннями DNS для перехоплення веб-трафіку та моніторингу або викрадення мережевих даних…

Шкідливе програмне забезпечення використовує відомі вразливості в застарілих пристроях, причому більшість випадків зараження припадає на Південну Корею та Китай. Дослідники виявили два варіанти: більш поширену версію, написану на мові C, що націлена на маршрутизатори, та більш досконалу версію, написану на мові Go, спрямовану на системи NAS, яка має розширені можливості, такі як розвідка внутрішньої мережі та виконання багатомовного коду. Хоча його розподілена система сканування DNS потенційно може бути використана для масштабних атак, на даний момент такої активності не спостерігалося. Цю бот-мережу не пов’язують із жодною відомою групою зловмисників, і багато що щодо неї залишається нез’ясованим. Експерти з безпеки рекомендують замінювати маршрутизатори, термін експлуатації яких закінчився, оновлювати прошивку, захищати адміністративний доступ та вимикати дистанційне керування, щоб зменшити ризик». ***(Bill Toulas. AryStinger botnet infected thousands of D-Link routers worldwide // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/arystinger-botnet-infected-thousands-of-d-link-routers-worldwide/). 21.06.2026).***

***

**«Напередодні Prime Day 2026 дослідники з кібербезпеки компанії Check Point зафіксували різке зростання кількості кіберзагроз, пов'язаних з Amazon, виявивши 6 843 новозареєстрованих доменів у період з грудня 2025 року по травень 2026 року, з яких майже 10% було визнано шкідливими або підозрілими. Кількість шахрайських доменів різко зросла напередодні події, що відображає загальну тенденцію, за якою кіберзлочинці використовують великі світові події для проведення масштабних фішингових кампаній.** Ці атаки включають підроблені інтернет-магазини Amazon, призначені для викрадення платіжної інформації, підроблені сторінки входу, що перехоплюють облікові дані користувачів, та оманливі електронні листи, що видають себе за офіційні повідомлення, часто з використанням переконливих адрес відправників та термінових повідомлень, таких як сповіщення про повернення коштів…

Кампанія охоплює кілька регіонів, включаючи цілеспрямовані дії, спрямовані на іспаномовних користувачів, шляхом скоординованої реєстрації доменів, що підкреслює глобальний масштаб загрози. Дослідники зазначають, що хоча ці тактики не є новими, їхній масштаб значно зріс завдяки автоматизації та інструментам на основі штучного інтелекту, які спрощують створення великих обсягів шахрайських доменів. Оскільки Prime Day приваблює мільйони покупців по всьому світу, багато з яких можуть бути не знайомі з подібними шахрайськими схемами, ризик є особливо високим. Щоб зменшити ймовірність потрапити в пастку, користувачам рекомендується заходити на сайт Amazon безпосередньо, а не через посилання, увімкнути двофакторну автентифікацію та зберігати обережність щодо небажаних повідомлень, навіть якщо веб-сайти виглядають легітимними завдяки використанню HTTPS-сертифікатів». ***(Ana Maria Constantin. Nearly 7,000 fake Amazon domains registered ahead of Prime Day 2026, researchers warn // Cogneve, INC. (https://thenextweb.com/news/amazon-prime-day-2026-scam-domains-check-point-phishing). 22.06.2026).***

***

**«Кількість випадків шахрайства з використанням технології «діпфейк» стрімко зростає: згідно з новим звітом компанії Shufti, цього року очікується 39-кратне збільшення кількості атак із використанням підроблених за допомогою «діпфейку» документів, що посвідчують особу, а загальний приріст шахрайства з використанням «діпфейку» складе 495%.** Наразі атаки з використанням синтезованих особистих даних становлять найбільшу частку шахрайства на основі штучного інтелекту — понад 42% випадків, випереджаючи за кількістю випадки з використанням «діпфейку» у прямому відео, тоді як підміна облич та підробка документів за допомогою «діпфейку» займають меншу частку. Однак очікується, що кількість «діпфейків» на основі документів різко зросте — за прогнозами, на основі тенденцій початку року, зростання може сягнути 3 900%. Цей сплеск сприяє загальному зростанню кількості виявлених випадків використання «діпфейків», кількість яких, як очікується, до 2027 року перевищить 5 мільйонів на рік…

Результати дослідження підкреслюють, що традиційні методи перевірки особи, такі як автономна біометрична ідентифікація за допомогою селфі, вже не є достатніми для протидії дедалі більш витонченим атакам. Натомість необхідні багаторівневі засоби захисту, що включають перевірку на «живість», виявлення атак типу «ін'єкції» та медіа-криміналістику. У звіті також наголошується, що висока точність під час лабораторних випробувань не обов'язково означає ефективність у реальних умовах, оскільки реальні середовища перевірки суттєво відрізняються від контрольованих умов тестування, що підкреслює необхідність створення більш надійних систем запобігання шахрайству, готових до впровадження». ***(Chris Burt. Shufti forecasts 39X more deepfake ID documents attacks this year // Biometrics Research Group, Inc. (https://www.biometricupdate.com/202606/shufti-forecasts-39x-more-deepfake-id-documents-attacks-this-year). 22.06.2026).***

***

**«У звіті Інтерполу «Оцінка кіберзагроз в Азії та Південному Тихоокеанському регіоні на 2025/2026 роки» підкреслюється, що кіберзлочинність перетворилася на масштабну кримінальну індустрію, яка зачіпає уряди, підприємства та окремих громадян: понад половина опитаних країн повідомила, що на її частку припадає щонайменше 30% усіх злочинів.** Цьому зростанню сприяють стрімка цифровізація, збільшення кількості користувачів Інтернету, поширення цифрових фінансових послуг, нерівномірний рівень готовності до кіберзахисту, організовані злочинні мережі та все частіше використання штучного інтелекту зловмисниками. Фішинг став найпоширенішою та найдорожчою загрозою: багато країн повідомляють про десятки тисяч інцидентів та значно вищі показники взаємодії користувачів, ніж у середньому по світу…

У звіті також підкреслюється революційна роль штучного інтелекту в кіберзлочинності, що уможливлює здійснення більш витончених атак за допомогою «діпфейків», клонування голосу, автоматизованих шахрайських схем та соціальної інженерії на основі штучного інтелекту, причому активність обговорень таких інструментів у підпільних колах різко зростає. Ці методи, що базуються на штучному інтелекті, виявляються більш прибутковими та масштабованими, особливо з появою агентних систем штучного інтелекту, здатних автоматизувати такі завдання, як ідентифікація цілей та проведення фішингових кампаній. Тим часом програмне забезпечення для вимагання викупу залишається серйозною загрозою: у 2024 році було зафіксовано понад 135 000 атак, які дедалі частіше супроводжуються крадіжкою даних, тактиками шантажу та моделями «програмне забезпечення для вимагання викупу як послуга», що дозволяють кіберзлочинним угрупованням розширювати свою діяльність». ***(Sead Fadilpasic. INTERPOL Warns About AI Scams and Ransomware Surge in Asia-Pacific // Coin Edition (https://coinedition.com/interpol-warns-about-ai-scams-and-ransomware-surge-in-asia-pacific/). 22.06.2026).***

***

**«Майже через тиждень після ймовірної зовнішньої кібератаки, що сталася 17 червня, Університет Маунт-Роял (MRU) продовжує боротися зі значними перебоями в роботі своїх онлайн-сервісів, зокрема головного веб-сайту, інтернету на території кампусу, студентських порталів та телефонних систем.** У відповідь на збій університет створив тимчасову публічну мережу Wi-Fi, залучив зовнішніх експертів з кібербезпеки та доручив міській поліції провести розслідування. Хоча MRU не підтвердив, чи пов'язаний інцидент із програмним забезпеченням-вимагачем, і не надав термінів повного відновлення системи, викладачі відзначають, що адміністрація ефективно комунікувала з ними протягом усієї кризи… Викладачі долають технічні перешкоди, використовуючи альтернативні навчальні платформи та електронну пошту, хоча співробітникам довелося терміново здати на обслуговування ноутбуки, видані університетом. Ця кібератака спричинила значні логістичні проблеми, зокрема щодо складання розкладу занять та реєстрації на осінній семестр, і може вимагати короткого продовження терміну проведення підсумкових іспитів… Тим часом кібератака викликала широке занепокоєння серед студентів, які дуже стурбовані можливими порушеннями конфіденційності та наразі не мають доступу до важливих документів, таких як академічні довідки, підтвердження зарахування та інформація про фінансову допомогу, під час поточного весняного екзаменаційного періоду». ***(Bill Kaufmann. MRU still resolving impacts of cyber attack, but some problems eased // Postmedia Network Inc. (https://calgarysun.com/news/local-news/mount-royal-university-resolving-impacts-cyber-attack-some-problems-eased). 23.06.2026).***

***

**«…Національний координаційний комітет Кенії з питань інформаційних технологій та кіберзлочинності (NC4) повідомив про понад три мільярди спроб кібератак на цифрову інфраструктуру, хмарні сервіси та державні установи за останні три місяці, підкресливши зростаючу загрозу для країни, яка дедалі більше переходить на цифрові технології.** У звіті про стан кіберзлочинності зафіксовано різке зростання кількості правопорушень, зокрема шахрайства з цифровими платежами, несанкціонованого доступу до систем, крадіжки особистих даних та кіберхарасування… Найвища концентрація кіберзлочинів була зафіксована в Найробі, що пояснюється високим рівнем поширення Інтернету та щільністю розташування установ; за ним слідують регіони Ньянза, Східний, Ріфт-Валлі, Центральний, Прибережний та Західний, де спостерігалися різні рівні випадків переслідування, шахрайства та несанкціонованого доступу. У відповідь на ці зростаючі загрози головний секретар Реймонд Омолло зазначив, що нещодавнє затвердження парламентом Національного агентства з кібербезпеки (NCSA) значно посилить захисні та реагувальні можливості країни… Крім того, NC4 активно розробляє «Короткий довідник» з метою стандартизації процедур розслідування та судового переслідування кіберзлочинів, а також планує тісно співпрацювати з ключовими секторами, такими як банківська справа, авіація та телекомунікації, задля підвищення кіберстійкості країни». ***(CHRISTABEL ADHIAMBO. Kenya records over 3 billion cyber-attack attempts in three months – Report // The Star***

***(https://www.the-star.co.ke/news/2026-06-24-kenya-records-over-3-billion-cyber-attack-attempts-in-three-months-report). 24.06.2026).***

***

**«Кіберзлочинці дедалі вправніше приховуються в ІТ-інфраструктурі своїх жертв, що значно затримує виявлення атак із використанням програм-вимагачів.** Згідно з «Глобальним звітом про стан загроз» компанії ExtraHop, в рамках якого було опитано понад 1 800 керівників ІТ-відділів та служб безпеки по всьому світу, 49 % постраждалих організацій виявили злом лише після того, як їхні дані вже були викрадені — це різке зростання порівняно з 31 % у попередньому році… В середньому зловмисники зараз залишаються непоміченими в мережі протягом двох з половиною тижнів, а 14 % жертв взагалі не підозрюють про вторгнення, доки не отримують вимогу про викуп. Дослідники пов'язують такі затримки у виявленні з складним середовищем загроз, в якому зловмисники приховують критичні сповіщення, використовуючи зашифровані канали, імітуючи легітимні мережеві процеси, захоплюючи облікові записи з високими привілеями та користуючись втомою захисників від постійних сповіщень… Цікаво, що хоча середня сума виплаченого викупу знизилася в річному вимірі з 3,6 млн доларів до 2,8 млн доларів, опитування ExtraHop зафіксувало різке зростання частоти виплат: 83 % жертв вирішили заплатити, порівняно з 70 % роком раніше. Однак ці дані дещо суперечать іншим галузевим звітам, зокрема від Chainalysis, які свідчать, що, хоча кількість успішних атак зросла, абсолютна кількість компаній, які платять викуп, залишилася відносно незмінною». ***(Sead Fadilpašić. Almost half of ransomware victims have data stolen before they can even detect an intrusion // Future US, Inc. (https://www.techradar.com/pro/security/almost-half-of-ransomware-victims-have-data-stolen-before-they-can-even-detect-an-intrusion). 25.06.2026).***

***

## ***Діяльність хакерів та хакерські угруповання***

**«Компанія Microsoft пов'язала недавню атаку на ланцюг постачання, спрямовану проти середовища Mastra AI, з групою «Sapphire Sleet» — північнокорейською хакерською групою, що фінансується державою, також відомою як BlueNoroff.** Злом розпочався, коли група отримала доступ до облікового запису адміністратора під ніком «ehindero», який мав права на публікацію в середовищі пакетів Mastra. Скориставшись цим доступом, зловмисники розмістили шкідливі оновлення у понад 140 пакетах npm у просторі @mastra, вбудувавши шкідливу залежність під назвою «easy-day-js» — версію з типографською помилкою у назві, що імітує легітимну та популярну бібліотеку «dayjs»…

Після встановлення пост-інсталяційний хук запускав зашифрований дроппер, який вимикав перевірку TLS-сертифікатів і зв'язувався з інфраструктурою управління для завантаження корисного навантаження другого етапу. Цим корисним навантаженням був міжплатформовий стелер інформації, призначений

для компрометації систем Windows, Linux та macOS. Він спеціально націлювався на конфіденційні дані, зокрема ключі API та токени автентифікації, а також виконував комплексну перевірку на наявність 166 різних розширень браузера для криптовалютних гаманців, таких як MetaMask, Coinbase Wallet та Binance Wallet…

Щоб забезпечити довгостроковий доступ, шкідливе ПЗ використовувало механізми збереження присутності, специфічні для кожної операційної системи, такі як ключі реєстру Windows та LaunchAgents у macOS. Компанія Microsoft повідомила, що подальша активність включала розгортання бекдорів PowerShell та створення шкідливих служб для надання зловмисникам привілеїв рівня SYSTEM. Ця кампанія відповідає усталеній практиці групи Sapphire Sleet, яка спеціалізується на атаках на фінансовий сектор та сектор криптовалют, і є продовженням аналогічної атаки на ланцюжок постачання, яку група здійснила проти HTTP-клієнта Axios у квітні 2026 року». ***(Lawrence Abrams. Microsoft links Mastra AI supply chain attack to North Korean hackers // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/microsoft-links-mastra-ai-supply-chain-attack-to-north-korean-hackers/). 20.06.2026).***

***

## ***Вірусне та інше шкідливе програмне забезпечення***

**«Нова кампанія з розповсюдження шкідливого програмного забезпечення під назвою HazyBeacon використовує надійну хмарну інфраструктуру, зловживаючи сервісами Amazon Web Services (AWS) для приховування зловмисної діяльності, націленої переважно на урядові мережі в Південно-Східній Азії.** Замість того, щоб покладатися на сервери, які легко виявити, зловмисники компрометують легітимні облікові записи AWS — часто використовуючи викрадені ключі доступу з таких джерел, як GitHub або фішинг — і розгортають безсерверні функції як приховані ретранслятори зв'язку. Ці ретранслятори, побудовані з використанням URL-адрес функцій AWS Lambda, налаштованих без аутентифікації, дозволяють шкідливому програмному забезпеченню на заражених системах спілкуватися зі зловмисниками через зашифрований трафік, який виглядає як звичайна активність AWS, що ускладнює виявлення…

Після встановлення на комп’ютері жертви HazyBeacon працює як бекдор, збираючи системні дані, виконуючи команди та викрадаючи конфіденційну інформацію, таку як документи та дані про натискання клавіш. Атака не використовує вразливості AWS безпосередньо, а скористається недоліками в практиках управління ідентифікацією та доступом. Використання хмарної інфраструктури дозволяє зловмисникам маскуватися під легітимний трафік і залишатися непоміченими, передаючи команди через зламані облікові записи…

Для захисту від цієї загрози необхідні більш суворі заходи безпеки в хмарі, зокрема в сфері управління ідентифікацією, такі як ротація ключів доступу, обов’язкове застосування багатофакторної автентифікації та блокування невикористовуваних облікових даних. Додаткові заходи включають увімкнення

комплексного ведення журналів для виявлення несанкціонованої активності, обмеження використання загальнодоступних функцій Lambda, моніторинг мережевих моделей та відстеження незвичайної активності в білінгу, яка може свідчити про зловживання. Загалом ця кампанія підкреслює, що зловмисники дедалі частіше використовують легітимні хмарні сервіси для уникнення виявлення, що робить контроль видимості та ідентифікації критично важливим для сучасної кібербезпеки». ***(Tushar Subhra Dutta. HazyBeacon Camapign Weaponizes Amazon Web Services for Stealthy Communications // Cyber Security News (https://cybersecuritynews.com/hazybeacon-camapign-weaponizes-amazon-web-services/). 03.06.2026).***

***

**«Хоча магазин Google Play, як правило, є найбезпечнішим місцем для завантаження додатків для Android, він не є повністю позбавленим ризиків — адже залишається головною мішенню як для розробників шкідливого програмного забезпечення, так і для легальних, але «жадібних до даних» додатків, які заробляють на інформації користувачів.** Ефективні заходи Google щодо перевірки перед публікацією та вбудовані засоби захисту, такі як Play Protect, блокують велику кількість шкідливих додатків і спроб їх встановлення, проте деякі шкідливі додатки все ж прослизають, часто виглядаючи нешкідливими під час перевірки, а потім активуючи шкідливу поведінку через віддалені оновлення або маскуючись під популярні утиліти, такі як сканери, програми для читання документів або додатки безпеки… Крім того, легальні додатки також можуть наражати користувачів на ризики, пов'язані з конфіденційністю та безпекою, збираючи конфіденційні дані та відстежуючи домени в межах, дозволених політиками Google, а також передаючи цю інформацію рекламним або аналітичним партнерам, які можуть далі поширювати її через посередників у торгівлі даними — створюючи численні потенційні точки порушення безпеки ще до того, як користувачі встигнуть зрозуміти, що щось не так…

Оскільки не існує остаточного та актуального публічного чорного списку небезпечних додатків, рекомендується ретельно перевіряти їх та постійно стежити за ними, використовуючи практичний контрольний список: перегляньте розділ «Безпека даних» у додатку та перевірте, чи відповідає він його фактичній функціональності; уважно вивчіть запитувані дозволи; перевірте особу та історію розробника; а також оцініть, чи виглядають відгуки про додаток справжніми. Особливу обережність слід дотримуватися щодо безкоштовних «утилітарних» додатків — таких як ліхтарик, клавіатура, програми для редагування фотографій або ігри з рекламою — оскільки їхня справжня бізнес-модель може полягати у збиранні даних. Навіть при дотриманні належної обережності деякі шкідливі додатки все одно можуть проникнути в систему, тому важливо використовувати додаткові засоби захисту, такі як шифрування трафіку за допомогою VPN, наприклад Proton VPN, щоб ускладнити перехоплення даних (особливо в публічних мережах Wi-Fi), використання менеджера паролів, наприклад Proton Pass, для захисту від крадіжки облікових даних та ризиків повторного використання паролів, а також навчання розпізнаванню ознак шкідливого програмного забезпечення або

компрометації, щоб ви могли швидко реагувати у разі зараження». ***(Kate Menzies. Malicious apps on Google Play: how to prevent Android malware // Proton AG (https://proton.me/blog/android-malware-malicious-apps-google-play). 24.06.2026).***

***

**«Дослідники з кібербезпеки компанії SentinelOne виявили нове шкідливе ПЗ для macOS під назвою «Gaslight», яке з високою ймовірністю пов'язують із зловмисником, пов'язаним із Північною Кореєю, і яке спеціально розроблено для введення в оману та зриву роботи інструментів аналізу шкідливого ПЗ, що використовують штучний інтелект.** Хоча це шкідливе ПЗ функціонує як стандартний бекдор на базі Rust та засіб викрадення інформації, воно унікальним чином вбудовує корисне навантаження розміром 3,5 КБ, що містить 38 сфабрикованих системних повідомлень — таких як підроблені журнали розробника, звіти про збій через нестачу пам'яті, попередження про закінчення терміну дії токенів та сповіщення про SQL-ін'єкції… Ці обманливі рядки, відформатовані за допомогою Markdown та заповнювачів у стилі шаблонів, діють як вставні підказки, призначені для gaslight великих мовних моделей (LLM), які дослідники використовують для автоматизованого реверс-інжинірингу. Замість того, щоб намагатися обійти традиційні пісочниці виконання, Gaslight безпосередньо атакує сприйняття агента ШІ, прагнучи змусити систему засумніватися у дійсності власного сеансу, щоб вона перервала, скоротила або відмовилася продовжувати аналіз… Хоча поки що остаточно не доведено, що ця техніка дозволяє успішно обходити платформи аналізу шкідливого ПЗ, що працюють на основі штучного інтелекту, це відкриття чітко свідчить про те, що зловмисники активно експериментують із складними методами протидії аналізу, розробленими спеціально для того, щоб обійти нові засоби кіберзахисту, що базуються на штучному інтелекті». ***(Lawrence Abrams. New macOS malware embeds fake errors to confuse AI analysis tools // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/new-macos-malware-embeds-fake-errors-to-confuse-ai-analysis-tools/). 25.06.2026).***

***

**«Дослідники виявили надзвичайно прихований бекдор під назвою Mistic (також відомий як MLTBackdoor), пов'язаний із Woodgnat — опортуністичним брокером початкового доступу, що діє з травня 2024 року з метою отримання фінансової вигоди. Замість того, щоб самостійно розгортати кінцеві шкідливі модулі, такі як програми-вимагачі, Woodgnat спеціалізується на встановленні стійкого віддаленого доступу до корпоративних мереж та продажу цього доступу великим синдикатам-вимагачам, зокрема Qilin, Akira та Black Basta.** Щоб уникнути виявлення та зберегти довгостроковий доступ, Mistic встановлюється шляхом «бічного завантаження» за допомогою компонентів, замаскованих під легітимні засоби захисту кінцевих точок від Microsoft. Шкідливе ПЗ працює виключно в пам'яті та має вбудований «kill switch» для самознищення та видалення своїх слідів, що дозволяє зловмисникам непомітно маніпулювати файлами, створювати папки та виконувати віддалені команди…

Під час нещодавніх вторгнень було зафіксовано, що Mistic розгортався разом із легітимними системними утилітами типу «living-off-the-land» — такими як PowerShell, WMIC та Curl — а також із спеціально розробленою бібліотекою .NET DLL, призначеною для викрадення облікових даних користувачів через підроблені екрани входу. Крім того, зловмисники часто поєднують Mistic із ModeloRAT — спеціальним трояном віддаленого доступу на базі Python, який раніше використовувався Woodgnat у кампаніях соціальної інженерії, що навмисно викликали збій у роботі браузерів жертв. Поєднуючи просунуті тактики ухилення від виявлення в оперативній пам'яті зі зловживанням довіреним програмним забезпеченням, Woodgnat успішно маскує свою діяльність, одночасно забезпечуючи високорівневий доступ до мережі, якого потребують його клієнти-кіберзлочинці». ***(Sinisa Markovic. Stealthy new backdoor surfaces in attacks on multiple sectors // Help Net Security (https://www.helpnetsecurity.com/2026/06/25/mistic-backdoor-woodgnat-attacks/). 25.06.2026).***

***

***Програми-вимагачі***

---

**«Нещодавня атака програм-вимагачів на компанію Scope Systems — великого австралійського ІТ-провайдера, що спеціалізується на програмному забезпеченні для управління ресурсами підприємства (ERP) у гірничодобувній галузі, — серйозно порушила роботу десятків гірничодобувних компаній, зокрема таких гігантів галузі, як Northern Star Resources та Evolution Mining…** Атака заблокувала доступ клієнтів до хмарної платформи ERP Pronto Xi від Scope, яка має вирішальне значення для інтеграції складних гірничодобувних процесів, таких як планування виробництва та управління ланцюгами постачання. Цей інцидент, який називають наймасштабнішою кіберподією в історії гірничодобувної галузі, пов'язаною з порушеннями безпеки з боку третіх осіб, підкреслює зростаючі ризики кібербезпеки, пов'язані зі стрімкою цифровою трансформацією сектору та залежністю від взаємопов'язаних хмарних систем…

Хоча компанія Scope Systems стверджує, що відновила сервери клієнтів із резервних копій і заявляє, що зловмисники не отримували прямого доступу до серверів клієнтів, залишаються серйозні питання щодо вектора атаки та масштабів витоку даних із внутрішніх серверів. Експерти попереджають, що досвідчені угруповання, які використовують програми-вимагачі, дедалі частіше націлюються на гіпервізори та площини управління в хмарних середовищах, що дозволяє їм клонувати або експортувати віртуальні машини, не залишаючи слідів у гостьових операційних системах. Цей інцидент підкреслює важливий урок щодо стійкості: гірничодобувні компанії, які зберігали незалежні, ретельно перевірені резервні копії своїх даних ERP, швидко відновили роботу, тоді як ті, що покладалися виключно на Scope, зазнали тривалих перебоїв у роботі. Оскільки гірничодобувний сектор стає центральним елементом глобальних ланцюгів постачання критично важливих мінералів, цей випадок порушення безпеки демонструє, що кібербезпека

— це вже не лише проблема IT, а системний геополітичний ризик». ***(Mark Rorabaugh. Op-Ed: what the Scope Systems cyber attack reveals about mining's digital fragility // The Northern Miner Group (https://www.mining.com/op-ed-what-the-scope-systems-cyber-attack-reveals-about-minings-digital-fragility/). 19.06.2026).***

***

**«Те, що почалося як рутинне розслідування випадку використання програм-вимагачів командою Microsoft з виявлення та реагування (DART), переросло у складну справу, яка викрила двох не пов'язаних між собою зловмисників, що діяли одночасно в одному гібридному середовищі.** Головний зловмисник, ідентифікований як Storm-2603, з середини 2025 року атакував локальні сервери SharePoint. Ймовірно, отримавши початковий доступ через незахищену вразливість, цей зловмисник зосередився на забезпеченні тривалого присутності та контролю шляхом захоплення легітимних адміністративних інструментів. Він розгорнув криміналістичний інструмент Velociraptor із привілеями рівня SYSTEM для картування мережі, створив кілька каналів віддаленого доступу за допомогою тунелювання Cloudflare, Zoho Assist та SSH через Visual Studio Code, а також використовував вразливі драйвери для обходу захисних заходів під час створення нових облікових записів адміністратора…

Під час аналізу телеметричних даних мережі дослідники виявили другу, окрему групу зловмисників, яка діяла паралельно. Ця неідентифікована група використовувала методи «самостійного завантаження» шкідливих бібліотек динамічного зв'язку (DLL) та власні бекдори. Перекривання діяльності цих двох окремих груп мимоволі маскувало дії одна одної, що значно ускладнило ситуацію з вторгненням та суттєво ускладнило виявлення та визначення відповідальних осіб…

У відповідь компанія DART оперативно запустила план дій з локалізації інциденту, зіставивши дані щодо облікових записів, кінцевих точок та хмарних ресурсів, щоб сформувати цілісну картину інциденту. Спільно з Microsoft Threat Intelligence фахівці з реагування на інциденти успішно розібралися в діяльності двох зловмисників, відстежили їхні подальші дії та стабілізували середовище клієнта…

Цей інцидент підкреслює, що сучасні кібератаки часто охоплюють кілька середовищ, поєднують різні тактики та передбачають перехресні загрози. Для захисту від таких складних атак компанія Microsoft радить організаціям надавати пріоритет ретельному встановленню оновлень на системах, підключених до Інтернету, та суттєво посилити безпеку ідентифікації. Крім того, компанії повинні забезпечити постійний централізований моніторинг за допомогою широкомасштабного захисту кінцевих точок, суворо контролювати використання легітимних засобів віддаленого доступу та адміністративних інструментів, а також підтримувати перевірені плани реагування на інциденти, щоб швидко ізолювати скомпрометовані ресурси та мінімізувати час перебування зловмисника в системі». ***(One intrusion, two cyberattackers: Uncovering parallel threat activity // Microsoft (https://www.microsoft.com/en-us/security/blog/2026/06/22/one-intrusion-two-cyberattackers-uncovering-parallel-threat-activity/). 22.06.2026).***

***

**«З'явилася нова операція з використанням програм-вимагачів під назвою «Prinz Eugen», яка відрізняється тим, що надає пріоритет шифруванню нещодавно змінених файлів і навмисно не залишає записки з вимогою викупу на заражених системах.** Як з'ясувало агентство Threatdown (колишній підрозділ компанії Malwarebytes), зловмисники обходять традиційну модель «програм-вимагачів як послуги» (RaaS), використовуючи викрадені облікові дані RDP для початкового доступу та застосовуючи легітимні інструменти віддаленого моніторингу й управління, такі як RemotePC, для забезпечення стійкості… Шифрувальник на базі Go використовує надійний алгоритм шифрування ChaCha20-Poly1305 для рекурсивного блокування файлів без обмежень за глибиною або виключень, додаючи розширення «.prinzeugen». Націлюючись на нещодавно змінені файли, хакери прагнуть максимально ускладнити роботу, наносячи удар насамперед по активних даних, критично важливих для бізнесу. Щоб уникнути виявлення та зменшити сліди своєї діяльності, шкідливе ПЗ забезпечує можливість розшифрування даних перед видаленням оригіналів, надійно видаляє ключі шифрування з пам'яті та самостійно видаляється з диска… Крім того, відсутність традиційного текстового листа з вимогою викупу змушує жертв спілкуватися виключно поза каналами зв'язку — наприклад, через пряму електронну пошту або портали даркнету — що ускладнює автоматичне виявлення етапу вимагання. Хоча наразі на сайті з витоком даних зазначено лише трьох жертв, дослідники знають про інші організації, що зазнали атаки, зокрема про випадок, коли від Standard Bank вимагали викуп у розмірі 1 BTC». ***(Bill Toulas. New Prinz Eugen ransomware prioritizes recent files for encryption // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/new-prinz-eugen-ransomware-prioritizes-recent-files-for-encryption/). 20.06.2026).***

***

**«Дослідники компанії ESET виявили надзвичайно досконалу платформу для вимкнення EDR під назвою GentleKiller, яку використовує група «Gentlemen», що надає послуги «вимагання як послуга» (RaaS), для нейтралізації засобів захисту кінцевих точок перед розгортанням програм-вимагачів.** «Gentlemen» — одна з найактивніших угруповань-вимагачів на початку 2026 року — вирізняється тим, що надає своїм партнерам централізований, постійно оновлюваний набір засобів для вимкнення EDR. Сама платформа GentleKiller складається щонайменше з восьми варіантів, кожен з яких імітує легітимне програмне забезпечення для безпеки, водночас використовуючи вразливі, але підписані драйвери ядра за допомогою техніки «Bring Your Own Vulnerable Driver» (BYOVD), що дозволяє зловмисникам припиняти роботу процесів безпеки на рівні ядра та обходити засоби захисту. Платформа націлена на понад 400 процесів у 48 основних продуктах безпеки та постійно сканує й вимикає їх у швидких циклах…

Ключовою сильною стороною цієї операції є її гнучкість, оскільки група здатна інтегрувати нещодавно оприлюднені експлойти у свій набір інструментів за лічені дні — набагато швидше, ніж більшість угруповань, що використовують

програми-вимагачі. Окрім власних інструментів, «Gentlemen» застосовує розроблені сторонніми розробниками засоби для обходу EDR, стандартизуючи їх за допомогою технік обфускації та маскування, що ускладнюють виявлення та атрибуцію. Група також використовує інструмент для викрадення облікових даних з метою збору інформації з браузерів на заражених системах. З'явившись наприкінці 2025 року, «Gentlemen» швидко розширила свою діяльність завдяки прибутковій партнерській моделі, що пропонує 90% частки доходу, та націлилася на організації по всьому світу, особливо в регіонах за межами США, часто використовуючи неправильно налаштовані пристрої FortiGate…

Можливості цієї групи були ще раз підтверджені внаслідок витоку внутрішніх даних, який засвідчив активну розробку та розповсюдження нею цих інструментів. Для захисту від таких загроз експерти рекомендують такі заходи, як впровадження списку дозволених драйверів, використання списку вразливих драйверів від Microsoft, моніторинг підозрілої активності драйверів, а також виявлення шаблонів завершення процесів безпеки, які залишаються ключовими індикаторами присутності GentleKiller». ***(Guru Baran. GentleKiller Ransomware Abuses Vulnerable Drivers to Disable 400+ EDR Security Processes // Cyber Security News (https://cybersecuritynews.com/gentlekiller-ransomware-edr-processes/). 21.06.2026).***

***

**«23 червня 2026 року великий індійський виробник двоколісних транспортних засобів Bajaj Auto та його технологічна дочірня компанія Bajaj Auto Technology Ltd (BATL) зазнали атаки програм-вимагачів, яка поставила під загрозу їхню IT-інфраструктуру.** Виявивши злом, внутрішні технічні команди компанії разом із зовнішніми експертами з кібербезпеки та вищим керівництвом оперативно задіяли протоколи локалізації, щоб нейтралізувати загрозу та запобігти її подальшому поширенню… Хоча Bajaj Auto повідомляє, що ці заходи з мінімізації наслідків поки що виявилися успішними, повний масштаб збою — включаючи можливий витік даних та будь-який істотний вплив на виробництво або ланцюги постачання — залишається невідомим… Відповідно до нормативних вимог щодо прозорості компанія офіційно повідомила про інцидент Індійській групі реагування на комп'ютерні надзвичайні ситуації (CERT-In) та оприлюднила інформацію про нього згідно з правилами SEBI. Зрештою, цей випадок підкреслює зростаючу тенденцію до кібератак, спрямованих проти глобального та індійського промислового й автомобільного секторів, що вказує на гостру необхідність у надійній кіберстійкості для захисту масштабного виробництва та складних ланцюгів постачання». ***(Guru Baran. Bajaj Auto Hit by a Ransomware Attack – Internal Systems Affected // Cyber Security News (https://cybersecuritynews.com/bajaj-ransomware-attack/). 23.06.2026).***

***

**«Згідно з «Звітом про кіберризики в Європі за 2026 рік», опублікованим компанією Black Kite, у перші чотири місяці 2026 року кількість атак з використанням програм-вимагачів на організації в Європі зросла на 55,1 % порівняно з аналогічним періодом минулого року, склавши в середньому 171**

**інцидент на місяць.** Лише на п’ять країн — Німеччину, Велику Британію, Францію, Італію та Іспанію — припадало 70 % цих інцидентів. Найпоширенішим був варіант програм-вимагачів Qilin, який став причиною 372 зареєстрованих атак у 26 країнах, що більш ніж удвічі перевищує показник другого за поширеністю варіанту — Akira… Третя за поширеністю група, SafePay, зосередилася майже виключно на Німеччині, зокрема на її промисловому центрі. Як наслідок, промисловість стала сектором, що найчастіше ставав мішенню атак у Європі, на який припадало 28 % усіх інцидентів; ці атаки могли спричинити значні економічні збитки в подальших ланках ланцюга постачання, як це було продемонстровано під час інциденту з компанією Jaguar Land Rover у 2025 році. У звіті це стрімке зростання пояснюється поєднанням таких факторів, як посилення можливостей програм-вимагачів, жорсткіші регуляторні умови та стратегічний перехід кіберзлочинців до експлуатації ланцюгів постачання стороннього програмного забезпечення… Цю тенденцію підтверджує той факт, що понад 30 інцидентів було пов’язано з одним-єдиним випадком компрометації шведського постачальника програмного забезпечення Miljödata. Щоб підвищити стійкість до такого взаємопов’язаного ландшафту загроз, експерти радять організаціям оперативно усувати вразливості (особливо в програмному забезпеченні ланцюга поставок), постійно відстежувати нові загрози та активно залучати свої ради директорів до управління кіберризиками». ***(Danny Palmer. Major Increase in Ransomware Attacks Targeting Europe, Warns New Report // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/increase-ransomware-europe/). 25.06.2026).***

***

***Програми-трояни***

---

**«Розробники на GitHub дедалі частіше виявляють, що їхні проєкти клонуються в рамках масштабної автоматизованої зловмисної кампанії, яка охоплює понад 10 000 підроблених репозиторіїв, що поширюють троянське шкідливе ПЗ, призначене для викрадення криптовалюти.** Розробник під ніком Orchid викрив цю схему, за якою зловмисники клонують нові або нішеві репозиторії, вбудовують у них шкідливе ПЗ та маніпулюють результатами пошуку, щоб підробки посідали вищі позиції в рейтингу, ніж оригінали. Щоб уникнути виявлення, ці підроблені репозиторії активно оновлюються кожні кілька годин… Зловмисники додають у документ README посилання, яке направляє користувачів на завантаження ZIP-архіву, що містить виконуваний файл для Windows, командний скрипт, текстовий файл-приманку та бібліотеку DLL. Після запуску цей корисний вантаж розгортає інфостілер StealC, який може непомітно викрадати конфіденційні дані, такі як криптогаманці, логіни та дані кредитних карток. Компанія з кібербезпеки HexaStrike зазначила, що шкідливе програмне забезпечення використовує інфраструктуру на основі блокчейну, що ускладнює його ліквідацію, і, з огляду на оперативну узгодженість дій, припускає, що кампанія, ймовірно, проводиться одним, високоцентралізованим зловмисником…

Хоча деякі розробники самостійно помітили цю фальсифікацію, багато фахівців у сфері технологій припускають, що головними цілями цих підроблених репозиторіїв є агенти штучного інтелекту — які під час пошуку коду частіше, ніж люди, сліпо завантажують шкідливі залежності — а не самі розробники. Хоча GitHub активно видаляє репозиторії, на які надійшли скарги, реакція на цю ситуацію є дещо непослідовною, і, судячи з усього, атака триває». ***(Ernestas Naprys. 10,000 malicious GitHub repos detected: AI agents compromising their owners // Cybernews (https://cybernews.com/security/10k-repos-github-malware-campaign-targets-ai-agents/). 19.06.2026).***

***

## *Операції правоохоронних органів та судові справи проти кіберзлочинців*

---

**«Масштабна спільна операція під назвою «Disruption Week» була успішно спрямована проти шахрайських мереж, що діяли в Південно-Східній Азії, що призвело до блокування понад 1,4 мільйона облікових записів та інфраструктури, яка їх підтримувала.** У цій операції взяли участь широке коло зацікавлених сторін, зокрема оперативна група Scam Center Strike Force Міністерства юстиції США, Королівська поліція Таїланду, правоохоронні органи з усього світу та провідні технологічні компанії, такі як Apple, Coinbase, Google, Meta, Microsoft, Silent Push, SpaceX, TRM Labs та Zenlayer. Серед конкретних результатів — закриття понад 1,4 мільйона акаунтів, сторінок та груп у соціальних мережах Facebook та Instagram, блокування акаунтів Microsoft та комплектів Starlink, нейтралізація шкідливого IP-трафіку та мережевих з'єднань, виведення з експлуатації пов'язаних серверів та хостингової інфраструктури, а також арешт 63 осіб, причетних до шахрайської діяльності…

Операція була спрямована насамперед проти великих шахрайських угруповань, що базуються в Камбоджі, Лаосі та М'янмі, де шахраї здійснювали складні шахрайські операції проти жертв у США та інших країнах. Особливо тривожним аспектом цих схем було використання торгівлі людьми: працівників заманювали до Таїланду обіцянками високооплачуваної роботи в технічній сфері, а потім у них вилучали документи та змушували брати участь у шахрайських операціях. Операція також призвела до висунення кримінальних звинувачень проти осіб, причетних до шахрайства з інвестиціями в криптовалюту в М'янмі, а також до заморожування криптовалютних активів на суму понад 3,8 мільйона доларів, пов'язаних із злочинними мережами. Офіційні особи підкреслили, що ця операція є свідченням ефективності скоординованого державно-приватного партнерства у боротьбі з організованою кіберзлочинністю та захисті громадськості». ***(Ionut Arghire. Over 1.4 Million Accounts Disrupted in Cybercrime Crackdown // Wired Business Media Publication (https://www.securityweek.com/over-1-4-million-accounts-disrupted-in-cybercrime-crackdown/). 04.06.2026).***

***

**«Підозрюваний у хакерстві росіянин Денис Обрезько був екстрадований з Таїланду до США, де йому висунуто звинувачення у зв'язку з масштабною кампанією кібератак, яка, як стверджується, була спрямована проти численних американських компаній.** Заарештований у Таїланді в листопаді минулого року, 36-річний чоловік з'явився у вівторок у федеральному суді в Бостоні і був звинувачений у змові з метою отримання несанкціонованого доступу до захищеного комп'ютера; він утримується під вартою без права на звільнення під заставу, а справу веде Відділ національної безпеки Міністерства юстиції США… Тайські чиновники заявили, що екстрадиція відбулася відповідно до національного законодавства та договірних зобов'язань, з дотриманням належних процесуальних гарантій. Американські власті пов'язують Обрезько з масштабною операцією з кібершпигунства, пов'язаною з групою «Void Blizzard», яку компанія Microsoft публічно визначила у травні 2025 року як таку, що здійснює шпигунство відповідно до цілей російського уряду та діє щонайменше з квітня 2024 року, націлюючись переважно на організації в країнах НАТО та Україні у таких секторах, як уряд, оборона, транспорт, ЗМІ, охорона здоров'я та неурядові організації… Згідно з судовими документами, угруповання «Void Blizzard» спеціалізувалося на масовому збиранні адрес електронної пошти в різних секторах бізнесу США; на даний момент ФБР виявило щонайменше 11 зламаних американських компаній, що, ймовірно, становить лише невелику частину від загальної кількості. Прокурори стверджують, що ФБР пов'язало Обрезько з криптовалютними платежами, які були використані для придбання віртуального приватного сервера (VPS) та домену, що згодом застосовувалися для здійснення атак у США та інших країнах». ***(Nate Raymond. US hunts down Russian 'Void Blizzard' hacker in Thailand raid after attacks on American companies // Independent (https://www.independent.co.uk/news/world/americas/crime/denis-obrezko-russian-hacker-extradited-thailand-void-blizzard-b2993883.html). 11.06.2026).***

***

**«Компанія Microsoft у співпраці з Європолом та іншими міжнародними партнерами успішно знешкодила «Amadey» та «StealC» — два широко розповсюджені інструменти для викрадення інформації, які активно використовувалися для здійснення атак з використанням програм-вимагачів, фінансового шахрайства та інших цифрових злочинів.** Застосувавши штучний інтелект для прискорення аналізу цієї мережі «шкідливого програмного забезпечення як послуги», слідчі виявили та заблокували понад 200 шкідливих доменів та IP-адрес системи управління та контролю на підставі судових рішень, винесених федеральним судом у Маямі… Ця ініціатива, що є частиною більш масштабної глобальної операції з протидії кіберзлочинності під назвою «Operation Endgame», передбачала співпрацю з дослідниками компаній Proofpoint та IBM і дозволила відновити 25,6 мільйона викрадених облікових даних у 385 000 зламаних систем. Експерти з кібербезпеки підкреслюють важливість цієї операції, зазначаючи, що програми для викрадення даних слугують ключовим каналом для атак програм-вимагачів, збираючи конфіденційні облікові дані; руйнування цієї

інфраструктури безпосередньо перериває ланцюг постачання для кіберзлочинців і змушує їх перебудовувати свою діяльність…» ***(David Jones. Microsoft, Europol lead global takedown of infostealer malware // TechTarget, Inc. (https://www.cybersecuritydive.com/news/microsoft-europol-international-takedown-infostealer-malware/823655/). 24.06.2026).***

***

**«Двоє чоловіків, Талха Джубайр (20) та Оуен Флауерс (18), визнали свою провину у здійсненні кібератаки на компанію «Transport for London» (TfL) наприкінці серпня та на початку вересня 2024 року, що спричинило збитки на суму близько 29 мільйонів фунтів стерлінгів та масштабні перебої в роботі.** Ці двоє, пов'язані з кіберзлочинною групою Scattered Spider, проникли в мережу TfL, змусивши всіх 28 000 співробітників особисто змінити паролі та порушивши роботу таких сервісів, як система повернення коштів за картками Oyster та подання заявок на отримання фотокарток, що спричинило фінансові збитки для деяких клієнтів… Слідчі з Національного агентства з боротьби зі злочинністю та поліції Сіті-оф-Лондон виявили докази їхньої причетності завдяки вилученим пристроям, зокрема скріншотам, відеозаписам атаки в процесі її здійснення та листуванню між ними через Telegram і спільні онлайн-інструменти, а також доступу до ринків викрадених облікових даних. Розслідування також виявило зв'язки з атаками на американські організації сфери охорони здоров'я… Обох заарештували у вересні 2024 року, а Флауерс згодом порушив умови звільнення під заставу; згодом, у перший день судового розгляду в червні 2026 року, обидва визнали свою провину, а винесення вироку призначено на липень. Влада охарактеризувала цю справу як складне розслідування та наголосила на реальних наслідках кіберзлочинності для критичної інфраструктури та населення, водночас підкресливши важливість своєчасного повідомлення про такі випадки та міжнародної співпраці у боротьбі з подібними загрозами…» ***(Cyber criminals who hacked into Transport for London's computer network are convicted // National Crime Agency (https://www.nationalcrimeagency.gov.uk/news/cyber-criminals-who-hacked-into-transport-for-londons-computer-network-are-convicted). 22.06.2026).***

***

**«21-річний Натан Остад, відомий в інтернеті під ніком «Snoopy», був засуджений до 18 місяців ув'язнення після того, як визнав себе винним у змові з метою здійснення несанкціонованого вторгнення в комп'ютерні системи за свою участь у атаці методом «креденшіал-стаффінгу», що відбулася в листопаді 2022 року проти веб-сайту фентезі-спорту та ставок, який, як вважають, належить компанії DraftKings.** Використовуючи імена користувачів та паролі, викрадені під час попередніх витоків даних, Остад та його спільники успішно зламали приблизно 60 000 облікових записів… Вони змінили способи оплати, щоб зняти близько 600 000 доларів з рахунків приблизно 1 600 жертв, а також продавали доступ до зламаних рахунків на «магазинах» у даркнеті, зокрема на одному, який безпосередньо контролював Остад і з якого отримував прибуток. Прокурори надали повідомлення, які свідчать про те, що Остад усвідомлював

шахрайський характер схеми та контролював криптовалютні рахунки, на які надійшло 465 000 доларів незаконних доходів. Остад став третьою особою, засудженою у цій справі, після Джозефа Гаррісона, який у січні 2024 року отримав 18 місяців ув'язнення, та Камерін Стоукс, яку у квітні 2026 року засудили до 30 місяців ув'язнення». ***(Sinisa Markovic. Hacker gets 18 months for attack that compromised 60,000 betting accounts // Help Net Security (https://www.helpnetsecurity.com/2026/06/25/hacker-sentenced-draftkings-credential-stuffing-attac/). 25.06.2026).***

***

## Технічні аспекти кібербезпеки

### *Виявлені вразливості технічних засобів та програмного забезпечення*

**«Нещодавнє опитування Cloud Security Alliance, в якому взяли участь 902 фахівці з IT та безпеки, показало, що 80% організацій за останній рік стикалися з інцидентами безпеки додатків, пов'язаними з уразливими місцями, які вони вже виявили, але не усунули вчасно.** Це свідчить про існування стійкого «розриву в оновленнях», коли затримка між виявленням і усуненням недоліків — зазвичай від одного до семи днів — створює можливості для зловмисників, особливо з огляду на те, що нові уразливості експлуатуються вже протягом декількох днів, а інструменти штучного інтелекту прискорюють швидкість атак. Організації, яким потрібно більше часу на усунення проблем, значно частіше стикаються з інцидентами, оскільки внутрішні розбіжності та побоювання щодо порушення бізнес-процесів часто уповільнюють час реагування…

Незважаючи на широке використання інструментів безпеки на етапі розробки, таких як статичне та динамічне тестування та брандмауери веб-додатків, уразливості все одно потрапляють у виробничі середовища — або через те, що їх раніше не було виявлено, або через те, що їх не усунули до випуску. Зростаюче використання компонентів додатків на базі штучного інтелекту ще більше ускладнює забезпечення безпеки, оскільки більшість організацій не мають можливості відстежувати їхню поведінку в режимі реального часу і замість цього покладаються на аналіз після інциденту. Ключовим викликом є визначення, які вразливості дійсно можна використати, при цьому організації надають пріоритет кращим доказам та контексту під час виконання над додатковим наймом персоналу…

Хоча багато організацій висловлюють готовність впроваджувати більш надійні засоби захисту під час виконання, такі як віртуальне патчування, довіра до існуючих засобів контролю залишається низькою через побоювання щодо помилкових спрацьовувань та можливих перебоїв у роботі бізнесу. Як наслідок,

багато систем працюють у режимі моніторингу, а не блокування. Тенденції в інвестиціях свідчать про поступовий перехід до засобів безпеки під час виконання, хоча бюджети залишаються невизначеними, особливо в сфері безпеки, пов'язаної зі штучним інтелектом. Загалом, результати дослідження вказують на те, що покращення швидкості, видимості та прийняття рішень щодо відомих вразливостей є критично важливим, оскільки основною проблемою є не відсутність виявлення, а нездатність діяти швидко та ефективно в реальних умовах». ***(Anamarija Pogorelec. Known vulnerabilities behind most application security incidents // Help Net Security (https://www.helpnetsecurity.com/2026/06/03/csa-application-security-incidents/). 03.06.2026).***

***

**«Instagram усунув уразливість у системі безпеки, яка дозволяла хакерам зловживати чат-ботом на базі штучного інтелекту для захоплення облікових записів користувачів шляхом маніпулювання процесом відновлення облікового запису.** Як повідомляється, зловмисники використовували такі тактики, як підробка свого місцезнаходження за допомогою VPN та переконання інструменту штучного інтелекту змінити адреси електронної пошти облікових записів, що давало їм змогу скинути паролі та отримати доступ. Проблема стала відомою одночасно з повідомленнями про кілька гучних випадків захоплення облікових записів, хоча компанія Meta заявила, що твердження щодо світових лідерів є неправдивими. Деякі користувачі, зокрема колишній інженер з безпеки Meta, повідомили про несанкціоновані зміни паролів та неодноразові спроби їхнього скидання…

Цей інцидент викликав широке занепокоєння щодо ризиків використання систем підтримки клієнтів на основі штучного інтелекту без достатніх заходів безпеки. Експерти застерігають, що надання інструментам штучного інтелекту надмірних повноважень без надійної перевірки особи може створити серйозні вразливості в системі безпеки, особливо в таких чутливих процесах, як відновлення доступу до облікового запису. Ця ситуація також підкреслює постійну критику щодо обмежених можливостей отримання допомоги від операторів-людей, оскільки користувачі повідомляють про труднощі з вирішенням проблем, пов'язаних із порушенням безпеки облікових записів. Загалом цей випадок підкреслює необхідність посилення контролю та нагляду з боку людей у міру того, як компанії все частіше застосовують штучний інтелект у сфері обслуговування клієнтів». ***(Liv McMahon. Instagram AI chatbot tricked by hackers to give access to others' accounts // BBC (https://www.bbc.com/news/articles/c98rzr72dpyo). 02.06.2026).***

***

**«Агентство з кібербезпеки та безпеки інфраструктури США (CISA) додало критичну вразливість у програмному забезпеченні для передачі файлів SolarWinds Serv-U, що має номер CVE-2026-28318, до свого каталогу відомих вразливостей, які вже експлуатуються, підтвердивши, що вона активно використовується зловмисниками.** Ця вразливість полягає у неконтрольованому

споживанні ресурсів, що дозволяє неавторизованим зловмисникам дистанційно вивести службу з ладу шляхом надсилання спеціально сформованих HTTP POST-запитів із використанням заголовка «Content-Encoding: deflate». Оскільки для здійснення атаки не потрібні облікові дані і її можна виконати через Інтернет, вона становить значний ризик як початковий вектор доступу до незахищених систем…

CISA зобов'язала федеральні агентства США усунути цю вразливість до 19 червня 2026 року та закликає всі організації вжити заходів якнайшвидше. Компанія SolarWinds випустила виправлення у вигляді Serv-U версії 15.5.4 Hotfix 1, а системи, що працюють на попередніх версіях, залишаються вразливими. Рекомендовані заходи щодо зменшення ризиків включають негайне застосування виправлення, обмеження доступу до служб Serv-U за допомогою брандмауерів або VPN, моніторинг підозрілих моделей трафіку та відключення уражених систем, якщо виправлення не може бути виконано негайно. Ця вразливість підкреслює постійні ризики, пов'язані зі службами, що мають вихід в Інтернет, та важливість швидкого виправлення у відповідь на активне зловживання…» ***(Guru Baran. CISA Warns of SolarWinds Serv-U Vulnerability Exploited in Attacks // Cyber Security News (https://cybersecuritynews.com/cisa-solarwinds-serv-u-vulnerability/). 06.06.2026).***

***

**«Компанія Oracle попередила корпоративних клієнтів про критичну вразливість у своєму програмному забезпеченні PeopleSoft для розрахунку заробітної плати та управління персоналом, опублікувавши попередження на наступний день після того, як група кіберзлочинців ShinyHunters заявила, що скористалася цією вразливістю під час масової хакерської атаки, яка зачепила понад 100 організацій, що використовують сервери PeopleSoft…** Компанія Mandiant, що спеціалізується на реагуванні на інциденти та належить Google, заявила, що виявлена Oracle уразливість є тією самою, яку використовує угруповання ShinyHunters, та зазначила, що на момент оприлюднення інформації Oracle ще не випустила виправлення; компанія повідомила, що цю уразливість можна експлуатувати через Інтернет без проходження аутентифікації, та закликала клієнтів вжити наявних заходів для мінімізації ризиків. Компанія Mandiant повідомила, що поінформувала понад 100 міжнародних організацій — переважно у США, з яких близько двох третин належать до сфери вищої освіти — про те, що, хоча деякі з них змогли заблокувати або усунути цю активність, інші зазнали зломів, у результаті яких були викрадені дані, які згодом були опубліковані на сайті ShinyHunters, що спеціалізується на витоках інформації. ShinyHunters повідомили TechCrunch, що вразливість була незахищеною «нульовою» вразливістю PeopleSoft, і стверджували, що серед жертв були коледжі та університети, посилаючись на викрадені записи про студентів, що містили детальну особисту та академічну інформацію… Цей інцидент вписується в загальну схему дій угруповання ShinyHunters, яке націлюється на широко використовувані корпоративні платформи, викрадає дані з організацій, що використовують одне й те саме вразливе програмне забезпечення, а потім змушує жертв платити викуп, щоб уникнути оприлюднення цих даних. До таких кампаній належать нещодавні атаки на Salesforce, Gainsight та системи освітнього сектору, зокрема Instructure і Canvas».

***(Lorenzo Franceschi-Bicchierai. Oracle warns of security bug that hackers abused to breach 100+ companies // TechCrunch Media LLC. (https://techcrunch.com/2026/06/11/oracle-warns-of-security-bug-that-hackers-abused-to-breach-100-companies/). 11.06.2026).***

***

**«Випущений 10 червня пакет оновлень Microsoft «Patch Tuesday» за червень 2026 року став найбільшим оновленням за всю історію програми: у ньому усунуто рекордну кількість — 200 — вразливостей у системах безпеки Windows, Office, Azure та супутніх продуктах.** Цей випуск містить виправлення для 33 критичних, 166 важливих та однієї вразливості середнього рівня, причому значна увага приділяється проблемам, пов'язаним із віддаленим виконанням коду… Зокрема, це оновлення усуває три уразливості типу «нульового дня», про які стало відомо громадськості: CVE-2026-50507 — локальний обхід шифрування BitLocker; CVE-2026-49160 — уразливість, що дозволяє здійснити віддалену атаку типу «відмова в обслуговуванні» (DoS) через протокол HTTP/2 без аутентифікації, яка впливає на сервери IIS; та CVE-2026-45586 — локальна уразливість, що дозволяє підвищити привілеї в компоненті Windows CTFMON. Хоча жодна з цих уразливостей «нульового дня» наразі активно не експлуатується, командам з безпеки настійно рекомендується надати пріоритет їх виправленню… Найсерйознішою виправленою вразливістю є CVE-2026-45657 — неавторизована вразливість типу «use-after-free» у ядрі Windows, що дозволяє дистанційне зловживання, з оцінкою CVSS 9,8. Оскільки ця вразливість класифікується як така, що «підходить для поширення через черв'яки», і може призвести до масового зловживання в разі розробки експлойта, фахівці настійно рекомендують негайно встановити виправлення на всіх системах Windows, підключених до Інтернету… З огляду на безпрецедентний масштаб цього випуску, організаціям рекомендується якнайшвидше встановити накопичувальні оновлення за червень 2026 року, надати пріоритет критично важливій інфраструктурі, такій як веб-сервери та хости Hyper-V, провести перевірку своїх засобів захисту кінцевих точок та підтвердити встановлення оновлень протягом 72 годин, щоб захистити свої системи від цих серйозних загроз». ***(Ashish Khaitan. Microsoft Patches Record 200 Vulnerabilities in June 2026 Patch Tuesday // The Cyber Express (https://thecyberexpress.com/june-2026-patch-tuesday-200-microsoft/). 10.06.2026).***

***

**«Коаліція провідних технологічних компаній, до якої входять Anthropic, AWS, IBM та Microsoft, уклала партнерську угоду з Linux Foundation з метою запуску «Akrites» — спільної ініціативи, спрямованої на виявлення, оприлюднення та усунення вразливостей у програмному забезпеченні з відкритим кодом.** Ця спільна ініціатива зумовлена стрімким розвитком передових моделей штучного інтелекту, які порушили історичний баланс між кіберзлочинцями та захисниками, прискоривши процес виявлення та використання програмних вразливостей у злочинних цілях… Як наслідок, волонтери, які підтримують проєкти з відкритим кодом, наразі завалені накопиченими звітами про

вразливості, через що екосистема не в змозі виправляти недоліки достатньо швидко, щоб запобігти широкомасштабним атакам на ланцюги постачання. Щоб подолати цю системну проблему, Akrites створить спільну команду реагування на інциденти безпеки, а також запровадить скоординований процес розкриття інформації про вразливості. Завдяки стартовому фінансуванню з фонду Alpha Omega від Linux Foundation засновники проекту виділяють значні фінансові ресурси, залучають талановитих інженерів та експертів з кібербезпеки, щоб допомогти спільноті відкритого програмного забезпечення ефективно оцінювати та усувати загрози, що в кінцевому підсумку захистить мільйони користувачів від складних атак на основі штучного інтелекту…» ***(David Jones. Software, AI companies form alliance to tackle open-source security flaws // TechTarget, Inc. (https://www.cybersecuritydive.com/news/software-ai-alliance-open-source-security-flaws/823889/). 26.06.2026).***

***

**«Хакери активно використовують критичну вразливість, що дозволяє віддалено виконати код (CVE-2026-12569), у PTC Windchill та FlexPLM — двох широко використовуваних рішеннях для управління життєвим циклом продукту (PLM).** Ця вразливість, пов'язана з небезпечною десеріалізацією, отримала оцінку 9,3 за шкалою CVSS. Вона зачіпає компонент Windchill PDMLink і дозволяє зловмисникам розгортати веб-шели-бекдори на скомпрометованих екземплярах… Оскільки ці PLM-платформи зберігають надзвичайно конфіденційну інтелектуальну власність — таку як CAD-проекти, специфікації та інженерні дані — для понад 1,5 мільйона користувачів по всьому світу, включаючи провідні компанії оборонної, аерокосмічної та автомобільної галузей, як-от Boeing, Lockheed Martin та BMW, вони є надзвичайно привабливими цілями для кібершпигунства та вимагання даних. Спочатку компанія PTC попередила клієнтів і почала випускати виправлення з 17 червня, але нещодавно оновила своє попередження, щоб попередити про посилення загроз, що спонукало Агентство з кібербезпеки та безпеки інфраструктури США (CISA) додати цю вразливість до свого каталогу «Відомі експлуатовані вразливості»… Ця загроза вважається настільки серйозною, що Федеральне відомство Німеччини з інформаційної безпеки (BSI) опублікувало термінові попередження про майбутні кібератаки, повторивши безпрецедентні заходи, вжиті німецькою поліцією на початку цього року, коли вона посеред ночі особисто попереджала компанії про попередню вразливість у Windchill». ***(Lucian Constantin. Hackers exploit critical PTC Windchill PLM software flaw // FoundryCo, Inc. (https://www.csoonline.com/article/4190154/hackers-exploit-critical-ptc-windchill-plm-software-flaw.html). 26.06.2026).***

***

**«Зловмисники активно експлуатують вразливість середнього рівня серйозності, пов'язану з розкриттям неавтентифікованої інформації (CVE-2026-4020), у плагіні Gravity SMTP для WordPress, який використовується на понад 100 000 сайтів.** Ця вразливість, присутня у версіях 2.1.4 та старіших, пов'язана з відкритим кінцевим пунктом REST API, що дозволяє будь-кому

отримати доступ до вичерпного системного звіту. Ці витік даних включає конфіденційні ключі API, токени OAuth, облікові дані сторонніх поштових сервісів та детальні налаштування сервера, що дає хакерам можливість видавати себе за жертв і легко скласти карту сайту для планування подальших атак. Брандмауер Wordfence від компанії Defiant, що спеціалізується на безпеці, вже заблокував понад 17 мільйонів спроб зловживання цією уразливістю, що спонукало до термінових закликів до адміністраторів оновити плагін до виправленої версії 2.1.5, заблокувати шкідливі IP-адреси та відстежувати журнали сервера на наявність конкретних ознак компрометації…

В окремому попередженні компанія Wordfence також попередила адміністраторів веб-сайтів про критичну вразливість, що дозволяє без авторизації довільно видаляти файли (CVE-2026-8713) у плагіні Avada Builder, який використовується на мільйоні сайтів. Хоча ця вразливість ще не експлуатується активно, ця вразливість типу «обхід шляху» дозволяє хакерам видаляти важливі системні файли — такі як wp-config.php — якщо опублікована форма налаштована на збереження даних, що надсилаються, у базі даних. Видалення цих файлів може скинути веб-сайт до початкового стану налаштування, що в кінцевому підсумку призведе до повного захоплення сайту та віддаленого виконання коду. Адміністраторам веб-сайтів настійно рекомендується мінімізувати цей серйозний ризик шляхом негайного оновлення Avada Builder до виправленої версії 3.15.4». ***(Bill Toulas. Hackers exploit info disclosure bug in Gravity SMTP WordPress plugin // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/hackers-exploit-info-disclosure-bug-in-gravity-smtp-wordpress-plugin/). 19.06.2026).***

***

**«Згідно зі звітом Vedere Labs, що входить до складу Forescout Research, хакери зараз використовують вразливості програмного забезпечення після того, як розробник виправив їх, але до того, як інформація про ці вразливості стала загальнодоступною.** Дослідники виявили цю тривожну тенденцію під час аналізу журналів «медових пасток» щодо уразливості, що дозволяє вводити команди в ОС без аутентифікації (CVE-2025-67038), яка впливає на перетворювачі послідовного інтерфейсу в IP від Lantronix, побудовані на базі Linux-дистрибутива OpenWRT та веб-інтерфейсу LuCL… Автоматизована, чітко націлена кампанія атак під назвою «Chaya_006», яка здебільшого походила з Азії, успішно використала цю вразливість на «медовому горщику» за два тижні до того, як Vedere Labs опублікували своє дослідження, в якому детально описували цю вразливість. Оскільки публічного доказу концепції (PoC) не було, дослідники вважають, що зловмисники, ймовірно, провели реверс-інжиніринг патча прошивки виробника, щоб створити власний експлойт. Окрім цього конкретного експлойта, компанія Vedere Labs зафіксувала понад 4 100 спеціалізованих спроб входу методом грубої сили, спрямованих на веб-додаток LuCL на пристроях OpenWRT у першій половині року… Щоб захиститися від цих швидких спеціалізованих атак, організаціям настійно рекомендується своєчасно встановлювати виправлення, змінювати стандартні облікові дані, запроваджувати політику використання надійних паролів та сегментувати свої мережі, щоб уберегти периферійні пристрої від злому».

***(Nicole Kobie. Hackers are exploiting flaws faster than companies can disclose them // Future US, Inc. (https://www.itpro.com/security/hackers-are-exploiting-flaws-faster-than-companies-can-disclose-them). 25.06.2026).***

***

## Основи кібергігієни

**«Незважаючи на неодноразові застереження з боку спільноти фахівців з кібербезпеки, значна частина споживачів продовжує зберігати свої паролі безпосередньо у веб-браузерах.** Нещодавнє опитування, проведене компанією NordPass серед 7 861 респондентів у восьми країнах, показало, що від 40% до 50% користувачів покладаються виключно на цей метод, керуючись насамперед зручністю, простотою використання та пасивними підказками щодо автоматичного збереження. Однак така практика є дуже ризикованою: якщо пристрій заражено шкідливим програмним забезпеченням, обліковий запис у браузері зламано або отримано фізичний доступ до комп'ютера, усі збережені паролі можна легко викрасти… Ця небезпека посилюється поширеною звичкою повторного використання паролів, що створює крихкий «цифровий картковий будиночок». Хоча деякі користувачі поєднують сховище браузера з менеджером паролів, розглядаючи останній лише як резервну копію, експерти наголошують, що такий підхід забезпечує незначний захист у разі злому самого браузера. Натомість фахівці з кібербезпеки настійно рекомендують використовувати спеціалізовані менеджери паролів, які застосовують архітектуру «нульового знання» для шифрування даних безпосередньо на пристрої, гарантуючи, що паролі залишаються недоступними навіть для розробників, та забезпечуючи набагато безпечнішу альтернативу зберіганню в браузері». ***(Sead Fadilpašić. 'Password reuse only sharpens this problem': Browser-based password storage isn't as safe as you think – these top tips from the experts show how it should be done // Future US, Inc. (https://www.techradar.com/pro/security/password-reuse-only-sharpens-this-problem-browser-based-password-storage-isnt-as-safe-as-you-think-these-top-tips-from-the-experts-show-how-it-should-be-done). 22.06.2026).***

***

**«Втома від паролів» — це серйозний ризик для бізнесу, що виникає внаслідок психічного перевантаження, пов'язаного зі створенням, запам'ятовуванням та оновленням численних паролів на різних платформах…** Коли співробітники перевантажені складними правилами щодо паролів та великою кількістю облікових записів, вони часто вдаються до небезпечних обхідних рішень — таких як повторне використання паролів, створення передбачуваних варіацій, записування їх або неформальне передавання облікових даних через чат чи електронну пошту. Ці звички створюють серйозні вразливості: повторне використання паролів уможливлює атаки типу «credential stuffing», передбачувані паролі легко зламати методом грубої сили, а неформальне передавання облікових даних усуває відповідальність та уповільнює реагування на

інциденти під час порушення безпеки… Просто наказувати співробітникам створювати надійніші паролі — це неефективна стратегія, яка часто лише поглиблює проблему. Справжнє рішення полягає в тому, щоб полегшити навантаження на людську пам’ять завдяки впровадженню спеціалізованого корпоративного менеджера паролів, такого як Proton Pass for Business… Такі інструменти автоматично генерують надійні, унікальні паролі, безпечно зберігають їх у зашифрованих сховищах, автоматично заповнюють їх за потреби та забезпечують контрольований доступ до них, що піддається аудиту. Завдяки безперебійній інтеграції цих безпечних практик у повсякденні робочі процеси підприємства можуть зробити найбезпечнішу поведінку в плані безпеки найпростішим вибором, що значно зменшить ризики, пов’язані з «втомою від паролів» та несанкціонованим доступом до мережі». ***(Ben Wolford. Password fatigue: why too many passwords put your business at risk // Proton AG (https://proton.me/business/blog/password-fatigue). 25.06.2026).***

***