**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

№ 4 (квітень)

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. Київ, 2026. № 4 (квітень). 152 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

Кібервійна проти України та операції у відповідь

«Хакери, пов'язані з Росією, провели масштабну довгострокову шпигунську кампанію, в результаті якої було зламано щонайменше 284 електронні поштові скриньки прокурорів, слідчих та військових чиновників в Україні, країнах НАТО та на Балканах. Операція, що тривала з вересня 2024 року по березень 2026 року, була викрита дослідницьким колективом Ctrl-Alt-Intel після того, як хакери припустилися серйозної оперативної помилки, ненавмисно залишивши викрадені електронні листи та журнали на загальнодоступному сервері. Хоча незалежні експерти з кібербезпеки підтвердили зв'язки хакерів з Москвою — а деякі дослідники вказали на сумнозвісну військову хакерську групу «Fancy Bear» — це відкриття надало рідкісну, безпрецедентну можливість зазирнути в механізми російської шпигунської кампанії…

В Україні хакери спеціально націлилися на чиновників, які займаються боротьбою з корупцією та викриттям російських колабораціоністів, зокрема на співробітників Спеціалізованої антикорупційної прокуратури та Агентства з повернення та управління активами. Злом також поширився на конфіденційні військові та урядові акаунти в Румунії, Греції, Болгарії та навіть Сербії, що свідчить про те, що шпигунські зусилля Москви не оминають її традиційних союзників. Зрештою, ця кампанія підкреслює, як російські спецслужби використовують кібервійну для стеження за судовими процесами та військовими операціями далеко за межами своїх кордонів». ***(Raphael Satter. Exclusive: Russia-linked hackers compromised scores of Ukrainian prosecutors' email accounts, data shows // Reuters (https://www.reuters.com/world/russia-linked-hackers-compromised-scores-ukrainian-prosecutors-email-accounts-2026-04-15/). 15.04.2026).***

***

Світові тенденції в галузі кібербезпеки

«Згідно з доповіддю Sophos «Cybersecurity Trust Reality 2026», в рамках якої було опитано 5 000 організацій у 17 країнах, довіра до постачальників послуг з кібербезпеки стала нестабільним, але надзвичайно важливим фактором, що безпосередньо впливає на рівень ризиків підприємства та процес прийняття рішень як на оперативному рівні, так і на рівні керівництва. Дослідження виявляє значну кризу довіри: аж 95% організацій визнають, що не мають повної довіри до своїх постачальників послуг з кібербезпеки. Ця невизначеність створює реальні проблеми, оскільки 79% респондентів мають труднощі з оцінкою надійності нових партнерів, а більше половини повідомляють про посилення занепокоєння щодо потенційних кіберінцидентів як безпосереднього наслідку цього…

Як пояснює керівник служби інформаційної безпеки компанії Sophos Росс Маккерчар, довіра більше не є абстрактним поняттям, а є вимірюваним фактором ризику. Дослідження вказує на розбіжність у підходах до оцінки довіри: керівники служб інформаційної безпеки надають пріоритет прозорості постачальника під час інцидентів та стабільній технічній ефективності, тоді як ради директорів приділяють більшу увагу незалежним перевіркам та сертифікаціям. Зрештою, у звіті робиться висновок, що постачальники послуг з кібербезпеки повинні постійно завойовувати довіру завдяки прозорості, підзвітності та незалежним перевіркам, оскільки організації більше не можуть дозволити собі просто розраховувати на неї». ***(Ben Leitch. Report finds only 5% of organisations have full trust in their cybersecurity vendors // Intelligent CISO (https://www.intelligentciso.com/2026/04/01/report-finds-only-5-of-organisations-have-full-trust-in-their-cybersecurity-vendors/). 01.04.2026).***

***

«У сучасній логістичній галузі кібербезпека перетворилася з другорядної IT-проблеми на критично важливе питання забезпечення безперебійної діяльності, яке розглядається на рівні керівництва. Платформи ланцюгів постачання та системи управління складами вже не обмежуються лише обробкою даних; вони безпосередньо керують фізичним потоком товарів за допомогою автоматизації, робототехніки та доставки замовлень клієнтам. Як пояснює технічний директор Consafe Logistics Андреас Анюру, коли ці системи виходять з ладу, робота зупиняється, доходи припиняються, а довіра клієнтів ставиться під загрозу. Основна загроза часто походить не від драматичних, прямих атак, а від тихого використання відомих вразливостей у широко використовуваному, але незахищеному програмному забезпеченні… Хоча компанії можуть відкладати оновлення, щоб уникнути перебоїв у роботі, особливо в пікові сезони, така затримка створює сприятливі умови для зловмисників, які за допомогою автоматизованих сканувань виявляють і використовують саме ці вразливості. Високоінтегрований характер сучасних ланцюгів постачання, що поєднує системи управління складом (WMS), ERP та транспортні системи, значно збільшив площу атаки, проте багато організацій продовжують працювати на застарілих платформах, що не підтримуються, вважаючи їх стабільними та такими, що не потребують оновлення. Це створює значну та зростаючу вразливість, оскільки системи, що не підтримуються, не можуть бути виправлені, що залишає їх постійно незахищеними…

Отже, справжня зрілість у сфері кібербезпеки полягає не в тому, щоб запобігти кожній уразливості, а в тому, щоб мати налагоджену систему управління, відповідні процеси та узгодженість між IT-підрозділом та операційним підрозділом, що дозволить швидко й ефективно реагувати, коли така уразливість неминуче виникне. Це вимагає постійних інвестицій у системи безпеки, такі як ISO 27001, регулярного моделювання загроз і, що найважливіше, чіткого та фінансово забезпеченого плану модернізації систем. Керівництво має перенести акцент з технічних деталей на стратегічну стійкість, ставлячи критичні запитання щодо

підтримки систем, швидкості управління виправленнями та готовності до реагування на інциденти…

Зрештою, кібербезпека в ланцюгу поставок є спільною відповідальністю постачальників технологій та їхніх клієнтів; завдяки спільним зусиллям, спрямованим на забезпечення пріоритетності безпеки та створення надійних і сучасних систем, вони можуть захистити не лише свої платформи, а й загальну цілісність операційної діяльності, репутацію та довгострокову конкурентоспроможність». ***(David Priestman. Cybersecurity in Logistics isn't just IT Responsibility // Logistics Business (https://logisticsbusiness.com/it-in-logistics/cybersecurity-in-logistics-isnt-just-it-responsibility/). 02.04.2026).***

***

«У сучасному фінансовому секторі кібербезпека стала синонімом довіри клієнтів та безперебійності бізнесу, виходячи за межі простого захисту інфраструктури та охоплюючи захист персональних даних, облікових даних та грошових коштів. Це робить фінансові організації основною мішенню для кіберзлочинців: за даними Британського управління з фінансового регулювання та нагляду (FCA), понад 20 % усіх кібератак, спрямованих на бізнес, спрямовані саме на них… Унікальна вразливість цього сектору зумовлена суворим регуляторним середовищем (зокрема DORA та PSD2), можливістю зловмисників миттєво монетизувати порушення безпеки, а також гіперпідключеною екосистемою фінтех-компаній та сторонніх постачальників, що експоненціально збільшує площу атаки…

Отже, кібербезпека у фінансовій сфері базується на кількох основних принципах: надійне управління ідентифікацією та доступом за допомогою моделей «нульової довіри», потужне шифрування та запобігання витоку даних для захисту конфіденційної інформації про клієнтів, а також передові засоби виявлення загроз та реагування на них, такі як центри безпеки (SOC), що працюють у режимі 24/7. До основних загроз належать складні кампанії з використанням програм-вимагачів, що застосовують подвійне або потрійне вимагання, надзвичайно переконливий фішинг та шахрайство з ідентифікацією, а також атаки на ланцюг постачання та API відкритого банкінгу, які зараз дедалі частіше доповнюються фейковими відео, створеними за допомогою штучного інтелекту…

У перспективі галузь рухається в напрямку більш автоматизованої системи безпеки, орієнтованої на ідентифікацію користувачів, яка використовує штучний інтелект для прогнозного виявлення загроз та запобігання шахрайству. У міру посилення регуляторного тиску та розширення цифрової екосистеми основна увага буде зосереджуватися на комплексному операційному стійкості, постквантовій криптографії та інтеграції кібербезпеки як центрального елементу цифрової стратегії, адже у світі фінансів безпека сьогодні нерозривно пов'язана з довірою». ***(Álvaro Lama. Why is cybersecurity important in the financial sector? // Telefónica S.A. (https://www.telefonica.com/en/communication-room/blog/cybersecurity-important-financial-sector/). 07.04.2026).***

***

«Новий звіт за 2026 рік, опублікований Інститутом SANS та GIAC, показує, що проблема кадрового забезпечення у сфері кібербезпеки кардинально змінилася: від дефіциту персоналу вона перетворилася на критичний розрив у компетенціях, причому 60 % організацій зазначають, що їхнім існуючим командам бракує необхідних навичок для захисту від сучасних загроз. Цей дефіцит навичок вже не є теоретичним; він безпосередньо пов'язаний із реальними провалами в системі безпеки, зокрема 27% організацій стикаються з витоками даних, і посилюється швидкою інтеграцією штучного інтелекту, що підриває традиційні шляхи навчання на початковому рівні…

Хоча штучний інтелект сприяє підвищенню ефективності, він не вирішує проблему нестачі кваліфікованих кадрів, особливо в секторах критичної інфраструктури та промисловості, де спеціалізовані знання в галузі безпеки операційних технологій (OT) мають вирішальне значення. Регуляторний тиск, зокрема з боку NIS2 та DORA, також різко посилився: 95 % організацій зараз повідомляють про певний вплив нормативних вимог на їхні практики найму персоналу, що є значним зростанням порівняно з лише 40 % рік тому… Це змушує проводити масштабну реорганізацію кіберкоманд і спричиняє різке зростання попиту на фахівців у сферах управління штучним інтелектом, ризиків та дотримання нормативних вимог, вакансії яких заповнити надзвичайно складно: багато керівних та експертних посад залишаються вакантними від шести місяців до понад року.

Загалом, отримані дані підкреслюють, що ризики у сфері кібербезпеки дедалі частіше зумовлені прогалинами у кваліфікації персоналу, а не суто технологічними вразливостями». ***(Anna Ribeiro. SANS 2026 report flags cybersecurity skills crisis, putting critical infrastructure and OT sectors at measurable breach risk // Industrial Cyber (https://industrialcyber.co/reports/sans-2026-report-flags-cybersecurity-skills-crisis-putting-critical-infrastructure-and-ot-sectors-at-measurable-breach-risk/). 06.04.2026).***

***

«Ринок праці у сфері кібербезпеки у 2026 році переживає бурхливе зростання: прогнозується, що попит на фахівців збільшиться на 10–15 % у порівнянні з попереднім роком. Це зумовлено постійним глобальним дефіцитом кадрів, який становить приблизно 3,5–4,8 мільйона вакансій, а також посиленням загроз, пов’язаних із кібератаками на основі штучного інтелекту з агентною поведінкою та квантовими ризиками. Цей сплеск змушує організації надавати пріоритет точним наймам у таких важливих сферах, як безпека хмарних технологій та штучного інтелекту, що призводить до високої конкуренції на ринку фахівців середнього та вищого рівня…

Як наслідок, знання в сферах Zero Trust та SASE стали обов’язковими для багатьох керівних посад, а фахівці з практичним досвідом у галузі безпеки штучного інтелекту отримують зарплати, що на 60 % перевищують зарплати їхніх колег. Хоча автоматизація на основі штучного інтелекту бере на себе виконання рутинних завдань, що може викликати занепокоєння у фахівців початкового рівня, попит на стратегічних керівників та спеціалістів у вузьких галузях стрімко зростає.

До найбільш затребуваних посад належать фахівці з безпеки ШІ, архітектори хмарної безпеки та інженери DevSecOps, а також зберігається високий попит на керівників служб інформаційної безпеки (CISO), які зараз мають розбиратися у складнощах впровадження «тіньового ШІ» та розширення глобальних нормативних вимог…

Щоб подолати дефіцит кваліфікованих кадрів, компанії все частіше готові наймати досвідчених фахівців з безпеки, які не мають безпосереднього досвіду роботи з ШІ, а потім навчати їх власними силами — ця тенденція, як очікується, стане ще більш поширеною в найближчому майбутньому. Зрештою, у міру того як сфера кібербезпеки еволюціонує в бік ери битв «ШІ проти ШІ», успіх визначатиметься здатністю організації інвестувати в безперервне навчання, передбачати нові загрози та формувати стійку, адаптивну «Skillforce», де співпраця людини та ШІ є наріжним каменем захисту». ***(David Weldon. Cybersecurity roles lead the pack in tech hiring // Spiceworks Inc. (https://www.spiceworks.com/it-careers/cybersecurity-roles-lead-the-pack-in-tech-hiring/). 03.04.2026).***

***

«Хоча кібербезпека на навколоземній орбіті вже є серйозним викликом, розширення людської діяльності в навколомісячний простір та на поверхню Місяця зробить її ще складнішою. Великі відстані та затримки у зв'язку, властиві місіям на Місяць, вимагають значної залежності від автономних, програмно-визначених систем, що різко розширює площину атаки. На відміну від відносно недовговічного обладнання супутникових груп на низькій навколоземній орбіті (LEO), місячна інфраструктура повинна залишатися функціональною протягом 10–15 років, що робить традиційне виправлення програмного забезпечення та заміну обладнання практично неможливими…

Як пояснив Сем Віснер із Space-ISAC, затримка в двосторонньому зв'язку, що становить майже три секунди для Місяця і до 44 хвилин для Марса, унеможливлює пряме керування в режимі реального часу, а це означає, що кожна операція — від переміщення марсоходів до моніторингу систем — є IT-інтенсивною та програмно-орієнтованою. Це створює критичну залежність від цілісності інформаційних систем. Багатонаціональний, державно-приватний характер програми NASA «Артеміда» ще більше ускладнює ситуацію з безпекою, оскільки різні стандарти та розгалужена мережа зацікавлених сторін збільшують ризик вразливостей та внутрішніх загроз…

Загалом, забезпечення безпеки космічних систем вимагає проактивних, скоординованих стратегій, стандартизованих рамок та проектування, орієнтованого на стійкість, оскільки кіберризики в цій сфері безпосередньо впливають на успіх місій, безпеку та майбутнє космічних операцій». ***(Shaun Waterman. Cybersecurity in Space is Hard; In Cislunar Space, it's Really Hard // Via Satellite Magazine (https://interactive.satellitetoday.com/via/april-may-2026/cybersecurity-in-space-is-hard-in-cislunar-space-its-really-hard). 07.04.2026).***

***

«Сьогодні організації стикаються зі складним і мінливим середовищем кібербезпеки, яке характеризується загрозами на основі штучного інтелекту, вразливостями ланцюгів постачання та посиленням регуляторного тиску. Штучний інтелект став двосічним мечем: з одного боку, він допомагає захисникам, а з іншого — зловмисники використовують його для проведення надзвичайно витончених і прихованих кампаній. ШІ покращує фішинг за допомогою діпфейків, персоналізованого контенту та реалістичних синтетичних медіа, як продемонстрували операція RaccoonO365, спрямована проти користувачів Microsoft, та кампанія «Diesel Vortex» проти логістичних компаній на початку 2026 року. Шкідливе програмне забезпечення також еволюціонує: такі загрози, як програмне забезпечення-вимагач PromptSpy, інтегрують GenAI, щоб уникнути виявлення та протистояти видаленню. Зловмисники ще більше експлуатують ШІ за допомогою отруєння даних, джейлбрейкінгу моделей — наприклад, атаки GTG-1002 на Claude Code від Anthropic — та створення самореплікуючих «черв'яків GenAI». Демократизація доступних інструментів ШІ знизила бар'єр для входу, дозволивши менш кваліфікованим учасникам застосовувати ці складні загрози…

Окрім прямих атак, значну небезпеку становлять ризики, пов’язані з ланцюгом постачання, оскільки взаємопов’язані мережі постачальників створюють непрямі точки вторгнення. Недостатній рівень безпеки у сторонніх постачальників може призвести до руйнівних зломів, прикладом чого є атака на компанію Jaguar Land Rover, здійснена за допомогою викрадених облікових даних сторонніх постачальників, що спричинила збитки на сотні мільйонів та серйозні економічні збитки. Щоб мінімізувати ці ризики, організації повинні запровадити надійну систему управління ризиками, пов’язаними зі сторонніми постачальниками, чітко визначити договірні зобов’язання щодо безпеки та забезпечити постійний нагляд…

Ці технічні виклики ускладнюються жорсткістю правового та регуляторного середовища. Потерпілі все частіше подають колективні позови, а регуляторні органи запроваджують більш суворі стандарти. Кілька штатів США прийняли комплексні закони щодо штучного інтелекту: Каліфорнія ухвалила низку законопроектів, що вимагають дотримання протоколів безпеки, розкриття даних для навчання та людського нагляду у сфері охорони здоров’я, з штрафами до 1 мільйона доларів за кожне порушення; Колорадо та Іллінойс розглянули питання алгоритмічної дискримінації та ШІ у сфері зайнятості; а закон RAISE у Нью-Йорку вимагає звітування про безпеку для передових моделей ШІ. Зростає також відповідальність керівництва, про що свідчить умовний вирок колишньому головному спеціалісту з безпеки Uber за приховування порушення та укладення угоди про врегулювання справи щодо шахрайства між SEC та SolarWinds і її головним спеціалістом з інформаційної безпеки наприкінці 2025 року… Щоб орієнтуватися в цьому середовищі з високими ризиками, організації повинні прийняти проактивну, цілісну стратегію, що включає постійну оцінку ризиків, засоби захисту на основі штучного інтелекту, архітектуру Zero Trust, надійне планування реагування на інциденти, постійне навчання співробітників та тісну співпрацю з юридичними радниками для забезпечення дотримання вимог та готовності». ***(Jody L. Rudman, Cara Arnold & Henry Aho. Emerging Cybersecurity Threats: Safeguarding Your Organization in a Rapidly Evolving Landscape // Husch***

Blackwell LLP. (https://www.governmentenforcementreport.com/2026/04/emerging-cybersecurity-threats-safeguarding-your-organization-in-a-rapidly-evolving-landscape/). 06.04.2026).

***

«Виявлення кіберзагроз у режимі реального часу стало життєво необхідним для сучасних організацій, які стикаються зі складними, автоматизованими та непередбачуваними кібератаками. Традиційні методи безпеки, що базуються на аналізі з затримкою, вже не здатні забезпечити захист від загроз, які можуть порушити цілісність систем за лічені секунди. Натомість виявлення у режимі реального часу — це процес безперервного моніторингу всіх цифрових середовищ, включаючи хмарні платформи, мережі та кінцеві пристрої, з метою виявлення загроз безпеці та реагування на них у міру їх виникнення. Цей проактивний підхід використовує передові технології, такі як штучний інтелект, машинне навчання та поведінкова аналітика, щоб встановити базовий рівень нормальної активності та миттєво виявляти аномалії, наприклад, незвичайний доступ користувачів або підозрілі передачі даних.

Головне значення виявлення в режимі реального часу полягає в його здатності суттєво скоротити «час перебування» зловмисника в системі, виявляти загрози до їх ескалації та забезпечувати миттєве автоматичне реагування, тим самим мінімізуючи фінансові збитки та шкоду репутації. Сучасні платформи здатні виявляти широкий спектр загроз — від шкідливого програмного забезпечення та програм-вимагачів до внутрішніх загроз і вразливостей «нульового дня» — шляхом кореляції численних слабких сигналів у єдине сповіщення з високим рівнем достовірності. Завдяки інтеграції штучного інтелекту та автоматизації ці системи можуть аналізувати величезні обсяги даних, адаптуватися до нових загроз і запускати заздалегідь визначені дії, такі як ізоляція ураженого пристрою, — і все це без втручання людини. Зрештою, впровадження стратегії виявлення в режимі реального часу дозволяє організаціям перейти від реактивної до проактивної позиції захисту, забезпечуючи безперервний захист, операційну ефективність та безперебійність бізнесу в умовах постійно мінливого ландшафту загроз». ***(Pushpendra Mishra. Real-Time Cyber Threat Detection // Techstrong Group Inc. (https://securityboulevard.com/2026/04/real-time-cyber-threat-detection/). 02.04.2026).***

***

«Голова служби кібербезпеки Сінгапуру Девід Кох попередив на конференції Gitex AI Asia 2026, що в умовах розпаду післявоєнного правового порядку та поширення геополітичної напруженості на цифрову сферу кіберстабільність стала невід'ємною складовою сучасного життя та необхідною передумовою для реалізації переваг штучного інтелекту та цифрової економіки. Посилаючись на дані Check Point, він зазначив, що у першому кварталі 2025 року глобальні кіберзагрози зросли на 47% у порівнянні з аналогічним періодом минулого року, а збитки від програм-вимагачів цього року, за прогнозами, становитимуть 74 млрд доларів і можуть сягнути 276 млрд доларів

до 2031 року; у Сінгапурі з 2021 по 2024 рік кількість атак з використанням складних постійних загроз зросла в чотири рази…

Він зазначив, що у 2025 році Сінгапур пішов на незвичайний крок, назвавши зловмисника з групи APT «UNC3886» після того, як той здійснив атаку на критичну інформаційну інфраструктуру країни, щоб посилити усвідомлення громадськості того, що національні об'єкти критичної інформаційної інфраструктури (CII) зазнають атак. Кох попередив, що країни все частіше обговорюють більш рішучі позиції — активну або випереджувальну оборону і навіть «відповідні хакерські атаки» — але ці підходи несуть ризики ескалації в «тумані війни» Інтернету, де неправильно розтлумачені сигнали можуть призвести до ескалації конфлікту.

Щоб зменшити ймовірність конфліктів і зберегти стабільність, він закликав до стриманості та відкритого діалогу навіть із супротивниками, до поглиблення внутрішньої та міжнародної співпраці через такі механізми, як ASEAN та Ініціатива протидії програм-вимагачів, з метою обміну розвідданими та протидії спільним загрозам, а також до поновлення прихильності існуючим міжнародним рамкам, зокрема Статуту ООН та добровільним нормам відповідальної поведінки держав у кіберпросторі, стверджуючи, що без правил і наполегливості постраждають усі країни». ***(Aaron Tan. Singapore Cyber Security Agency chief: Cyber stability a necessity, not a luxury // TechTarget, Inc. (https://www.computerweekly.com/news/366641228/Singapore-Cyber-Security-Agency-chief-Cyber-stability-a-necessity-not-a-luxury). 09.04.2026).***

***

«Криза з Log4j у грудні 2021 року продемонструвала, як швидко сучасні вразливості перетворюються на зброю і наскільки інструменти та інфраструктура «добросовісних» захисників і злочинців можуть бути схожими між собою, причому ключовою відмінністю часто є не техніка, а наявність відповідних повноважень. Етичне хакерство, яке частіше називають тестуванням на проникнення, використовує методи, які в іншому випадку були б незаконними, але вважаються законними, якщо здійснюються з відома та з дозволу власника системи — це концепція, що лежить в основі таких сертифікацій, як сертифікація EC-Council, де «дозвіл» має основне етичне та юридичне значення…

Однак на практиці межа між «санкціонованим» та «несанкціонованим» доступом часто залишається нечіткою в рамках таких законів, як Закон США про комп'ютерне шахрайство та зловживання (CFAA) 1986 року, який забороняє несанкціонований доступ, не даючи чіткого визначення поняття «санкціонування»; історично суди тлумачили це широко, хоча рішення Верховного суду 2021 року у справі «Ван Бюрен проти Сполучених Штатів» звузило сферу застосування закону, постановивши, що зловживання даними, до яких особа має доступ, не обов'язково є «перевищенням дозволеного доступу». Гучні справи, такі як судове переслідування Аарона Сварца, стали символами потенційного перевищення повноважень, і навіть структуровані програми, такі як винагороди за виявлення помилок, можуть наражати дослідників на юридичний ризик, якщо вони відхиляються від правил

взаємодії, як це було у випадках, коли добросовісне повідомлення все одно призвело до затримання або суперечки…

Ситуація ще більше ускладнюється у випадку хакерських атак з боку національних держав, коли дії, які для цивільних осіб вважалися б злочинними, можуть бути дозволені органами національної безпеки, незважаючи на використання тактик, схожих на ті, що застосовують кіберзлочинці. Хоча кодекси професійної етики (наприклад, EC-Council, SANS), органи стандартизації (наприклад, FIRST) та норми скоординованого розкриття інформації (часто близько 90 днів, популяризовані Google Project Zero) надають рекомендації, їм бракує обов'язкового правового захисту, що означає: дослідники все ще можуть зіткнутися з судовим переслідуванням, якщо власник оскаржить їхні дії. Результатом є тривала правова сіра зона, де ті самі дослідження вразливостей, що зміцнюють безпеку, можуть також нести значний особистий та професійний ризик, доки закони не будуть краще узгоджені з сучасною практикою кібербезпеки». ***(Adi Gaskell. Outdated laws treat whitehats and criminals the same: security researchers at risk // Cybernews (https://cybernews.com/news/outdated-laws-whitehats-criminals-security-researchers-risk/). 03.04.2026).***

***

«Компанії вкладають значні кошти в технології захисту від DDoS-атак, проте перебої в роботі все ще трапляються досить часто, оскільки системи захисту встановлюються, але рідко тестуються в умовах реальних атак, що призводить до серйозних розбіжностей між налаштуваннями та фактичною ефективністю. Дані моделювання Red Button показують, що 68% виявлених несправностей є серйозними або критичними, а середній показник стійкості до DDoS-атак під час першого тесту становить лише 3,0 — що значно нижче рекомендованого базового рівня 4,5–5,0 — що свідчить про те, що стійкість вважається само собою зрозумілою, а не вимірюється…

П'ять основних прогалин постійно підривають ефективність захисту від DDoS-атак. По-перше, поширеним є неправильне налаштування: рішення для захисту від DDoS постачаються із загальними заводськими налаштуваннями за замовчуванням, розробленими для широкої сумісності, а не для конкретних архітектур; обмеження пропускної здатності часто виявляються занадто високими, а правила фільтрації — надто консервативними, і вони залишаються неперевіреними в реальних умовах атаки, доки не трапиться інцидент. По-друге, «сліпі зони» у розподілі відповідальності виникають через хибне припущення, що хмарні або CDN-провайдери забезпечують повний захист «від кінця до кінця», тоді як насправді вони захищають лише периферію, залишаючи інфраструктуру джерела, незахищені кінцеві точки, шлюзи API та логіку на рівні додатків у відповідальності клієнта… По-третє, більшість стеків перевіряються на стійкість до простих, типових типів атак, а не до складних багатовекторних атак, які застосовують реальні зловмисники, одночасно поєднуючи об'ємні флуди, зловживання протоколами та атаки на рівні додатків, щоб скористатися прогалинами між рівнями. По-четверте, атаки на рівні додатків (L7) постійно залишаються недостатньо захищеними, оскільки виглядають легітимними —

надсилають невеликий за обсягом, але потужний трафік, такий як HTTP-флуди, — який проходить перевірки на периферії, але вичерпує ресурси бекенду, не викликаючи реакції систем захисту від об'ємних атак та не подаючи чітких сигналів. По-п'яте, командам бракує практичного досвіду реагування на DDoS-інциденти; не знаючи, як системи поводяться під навантаженням, команди SOC та NOC вагаються діяти рішуче, коли атаки лише частково нейтралізовано, що подовжує перебої в роботі…

Моделювання виявляє всі ці прогалини раніше, ніж це зроблять зловмисники, шляхом проведення контрольованих тестів з використанням численних векторів атак та точок проникнення. Це дозволяє з'ясувати, які запити проходять непоміченими, які порогові значення не спрацьовують, як трафік може обійти засоби захисту та як команди насправді реагують у стресових ситуаціях. Регуляторний тиск з боку DORA та NIS2 вимагає, щоб стійкість була перевірена та доведена, а не припущена, тоді як сучасний ландшафт загроз став менш передбачуваним: розширення хмарних технологій створює несподівані шляхи атак, а зловмисники навмисно використовують тривалі атаки з низьким рівнем впливу, призначені для погіршення якості послуг, а не для спричинення негайних перебоїв у роботі. Основна проблема полягає в тому, що майже всі оцінки DDoS є статичними — оцінка конфігурацій, покриття та можливостей постачальників на папері — і дуже мало що вимірюється в умовах, які насправді мають значення, що робить тестування за допомогою симуляції єдиним надійним способом усунути прогалини, перш ніж вони перетворяться на операційні збої». ***(Israel Solomon. Why DDoS Mitigation Fails: 5 Gaps That Testing Reveals // Techstrong Group Inc. (https://securityboulevard.com/2026/04/why-ddos-mitigation-fails-5-gaps-that-testing-reveals/). 05.04.2026).***

***

«Кіберстійкість зосереджується на тому, що відбувається після кібератаки — наскільки ефективно організація витримує вторгнення, відновлює роботу, а потім адаптує свою діяльність та технології, щоб наступного разу відновитися ще краще — виходячи за межі традиційних функцій кібербезпеки, які наголошують на запобіганні та виявленні. Для керівників служб інформаційної безпеки (CISO) показники кіберстійкості є надзвичайно важливими, оскільки вони перетворюють показники безпеки на бізнес-результати, допомагають оцінювати ефективність порівняно з прийнятними цілями, показують, які бізнес-процеси були порушені та як швидко вони відновилися, виявляють прогалини в системах контролю та процесі прийняття рішень, а також дозволяють порівняти рівень зрілості з відповідними стандартами та рамками…

До основних показників належать середній час виявлення та реагування (MTTD/MTTR), час відновлення системи, періодичність та охоплення оновленнями, індикатори ризиків, пов'язані зі сторонніми постачальниками та ланцюгом постачання, показники впливу на бізнес (наприклад, уникнуті збитки), порівняння цільових показників часу відновлення з фактичним часом відновлення, цільові показники точки відновлення даних, відсоток критичних активів, для яких створено належні резервні копії, а також рівні відповідності таким стандартам, як

ISO 27001 або NIST. Впровадження корисних показників вимагає їх узгодження з бізнес-пріоритетами (час безвідмовної роботи, відповідність вимогам, довіра клієнтів), використання встановлених стандартів (наприклад, NIST CSF, показники стійкості MITRE), вимірювання протягом усього життєвого циклу інциденту (від запобігання до навчання після інциденту), перевірки показників за допомогою тестування та моделювання, збалансування технічних та бізнес-заходів, включаючи зовнішні залежності, моніторинг галузевих тенденцій та забезпечення циклу постійного вдосконалення. Нарешті, показники створюють цінність лише тоді, коли про них ефективно повідомляють керівництву: керівники служб інформаційної безпеки повинні адаптувати звіти до аудиторії, наголошувати на невеликому наборі показників, пов'язаних із результатами, використовуючи бізнес-мову, використовувати інформаційні панелі та тенденції для контексту та надавати чіткі описи, що демонструють, як інвестиції в стійкість зменшили час простою, обмежили збитки або покращили управління ризиками». ***(Paul Kirvan. Meaningful metrics demonstrate the value of cyber-resiliency // TechTarget, Inc. (https://www.techtarget.com/searchsecurity/tip/Meaningful-metrics-demonstrate-the-value-of-cyber-resiliency). 06.04.2026).***

***

«Мікко Гіппонен (Mikko Hyppönen), який вже десятиліттями відомий своїми дослідженнями шкідливого програмного забезпечення та реагуванням на інциденти у сфері кібербезпеки, перейшов до сфери захисту від дронів і у 2025 році обійняв посаду директора з досліджень у компанії Sensofusion — гельсінській фірмі, що розробляє системи протидії дронам для правоохоронних органів та військових. Його крок відображає його думку, що ера шкідливого програмного забезпечення для споживачів значною мірою добігла кінця і що сьогодні найнебезпечніші наступальні можливості дедалі більше зосереджуються у руках суб'єктів, яких підтримує держава, тоді як війна в Україні висвітлила дрони як одну з головних причин втрат на полі бою та зробила цю проблему нагальною та особистою для Гіппонену як фіна, що мешкає поблизу Росії та служить у резерві… Ця робота базується на тих самих захисних стратегіях, які він застосовував проти шкідливого програмного забезпечення, такого як черв'як ILOVEYOU, — перехоплення сигналів, ідентифікація протоколів та нейтралізація загроз, — за винятком того, що тепер сигнатурами є радіочастотні сигнали та протоколи керування, які використовують дрони, і які можна заглушити або використати для виведення пристрою з ладу. У Sensofusion його команда ефективно створює базу даних для дронів у стилі «вірусних сигнатур», виявляючи та класифікуючи їх за допомогою радіочастотних сигнатур для використання як у цивільній охороні повітряного простору, так і в зонах активних конфліктів. Гіппонен підкреслює, що головним викликом є швидкість: тоді як сигнатури шкідливого програмного забезпечення можуть оновлюватися протягом декількох днів, захист від дронів часто вимагає прийняття рішень від виявлення до реагування за лічені секунди, що звужує межі похибки та підвищує ставки від запобігання втраті даних до запобігання фізичній шкоді». ***(Christian Kelly. The man who discovered the ILOVEYOU virus is now fighting Russian drones using the same***

playbook // Silicon Canals (https://siliconcanals.com/sc-n-the-man-who-discovered-the-iloveyou-virus-is-now-fighting-russian-drones-using-the-same-playbook/).05.04.2026).

***

«Кібербезпека переходить від багаторічного реактивного циклу — виявлення, виправлення, реагування — до більш проактивних заходів, спрямованих на зривання планів супротивників на ранніх етапах, що зумовлено середовищем загроз, яке стає швидшим, більш скоординованим і дедалі автоматизованішим. Двома останніми ознаками цієї зміни є оновлена кіберстратегія Білого дому, яка підкреслює проактивну/«наступальну» позицію, та оголошення Google на конференції RSA про створення підрозділу з протидії загрозам, який використовуватиме юридичні повноваження та технічні заходи для втручання в діяльність груп, що становлять загрозу, до того, як вони завдадуть шкоди жертвам…

Нагальність ситуації зумовлена скороченням часу на реагування: Сандра Джойс із Google зазначила, що середній час від моменту отримання доступу до передачі даних вторинній групі зловмисників скоротився з восьми годин у 2022 році до всього 22 секунд у 2025 році, що відображає модель екосистеми, в якій брокери доступу, оператори та фахівці з монетизації працюють паралельно, а штучний інтелект прискорює процес експлуатації та переміщення даних. Незважаючи на це, «проактивна кібербезпека» розглядається як спосіб перешкоджання — а не самосуд чи «відповідний злом» — із застосуванням таких заходів, як цивільні судові позови, скоординовані блокування, публічне викриття інструментів та зміцнення продуктів, щоб неодноразово накладати витрати та створювати перешкоди, а не остаточно припиняти вторгнення…

Такий підхід також відображає реальність: приватний сектор управляє значною частиною інфраструктури, якою зловживають зловмисники, і володіє можливостями моніторингу та оперативності, яких бракує уряду, але вжиття заходів на ранніх етапах та поза межами власної мережі порушує невирішені питання щодо повноважень, юрисдикції, координації з союзниками та ризику ескалації, особливо коли ворожа інфраструктура розміщена в третіх країнах. Як результат, реальні можливості з порушення роботи зосереджені у кількох великих постачальників платформ (наприклад, Google та Microsoft), які мають масштаб, юридичний вплив та контроль над своїми середовищами, тоді як більшість підприємств не мають можливості вживати таких заходів…

Для керівників служб інформаційної безпеки (CISO) це на практиці означає не розширення повноважень для «переходу в наступ», а подальшу концентрацію уваги на основних принципах безпеки та стійкості, а також оперативну готовність до співпраці у разі вжиття заходів урядом або великими провайдерами — швидкий обмін телеметричними даними, збереження доказів та реагування в режимі реального часу — оскільки перешкоджання на вищих рівнях може дати додатковий час, але не зупинить поточну діяльність зловмисників». ***(Cynthia Brumfield. The rise of proactive cyber: Why defense is no longer enough // FoundryCo, Inc.***

(https://www.csoonline.com/article/4154228/the-rise-of-proactive-cyber-why-defense-is-no-longer-enough.html). 07.04.2026).

***

«Наразі кібербезпека є однією з найбільш динамічних та затребуваних сфер кар'єри у світі: за прогнозами Бюро статистики праці США, до 2031 року кількість вакансій у цій галузі зросте на 35 %. Ця сфера, що розвивається завдяки прискореному переходу до цифровізації, визначається як мистецтво та наука захисту даних і активів, підключених до Інтернету, за допомогою спеціалізованої підготовки, протоколів та технологій. Кар'єра в цьому секторі є надзвичайно привабливою для тих, хто прагне професійної самореалізації, оскільки вона пропонує конкурентоспроможну заробітну плату (яка зазвичай сягає шестизначних сум за умови наявності досвіду), надзвичайну стабільність зайнятості через глобальний дефіцит фахівців, а також можливість зробити відчутний, реальний внесок у захист усього — від особистої конфіденційності до критично важливих медичних пристроїв.

Професійний ландшафт є різноманітним: від аналітиків початкового рівня до керівників вищої ланки. На керівному рівні головний спеціаліст з інформаційної безпеки (CISO) контролює всю інфраструктуру та політику безпеки організації, отримуючи середню заробітну плату приблизно 256 040 доларів на рік. Аналогічно, архітектори мережевої безпеки заробляють в середньому 175 065 доларів за свою роль у проектуванні складних, безпечних мережевих інфраструктур, тоді як інженери з продажу рішень у сфері безпеки поєднують технічні знання та бізнес-стратегію, часто заробляючи понад 157 509 доларів. Інші високооплачувані технічні посади включають інженерів з мережевої безпеки (125 000 доларів) та інженерів з хмарної безпеки (121 823 долари), які відіграють важливу роль у захисті хмарних систем, що є центральними для сучасного бізнесу…

Ця галузь також охоплює спеціалізовані технічні посади, такі як інженери з безпеки додатків (117 111 доларів), які забезпечують безпеку на всіх етапах циклу розробки програмного забезпечення, та фахівці з тестування на проникнення (97 659 доларів), або «етичні хакери», які імітують реальні атаки з метою виявлення слабких місць у системах. Аналітики з інформаційної безпеки виконують роль цифрових вартових, стежачи за мережами на предмет порушень, при цьому їхня середня зарплата становить близько 90 000 доларів, тоді як аналітики шкідливого програмного забезпечення зосереджуються на нейтралізації шкідливого коду, отримуючи в середньому 87 000 доларів. Нарешті, адміністратори кібербезпеки керують загальними організаційними протоколами за приблизно 81 442 долари, а фахівці з виявлення помилок заробляють в середньому 74 867 доларів, виявляючи вразливості в обмін на винагороду. Незалежно від того, чи цікавить людину стратегія, інженерія чи дослідження, сфера кібербезпеки пропонує різноманітні кар'єрні шляхи, що поєднують високий потенціал заробітку з дедалі важливішою місією захисту підключеного світу…» ***(What is a Cyber Security Job? // Nexford University (https://www.nexford.edu/insights/highest-paying-cyber-security-jobs). 04.04.2026).***

***

«Кіберуразливість — це слабке місце в системі безпеки, яке зловмисники можуть використати для викрадення даних або порушення роботи; у міру того, як цифрові ланцюги постачання стають дедалі більш взаємопов'язаними, ризик, пов'язаний із цими недоліками, різко зріс. З огляду на те, що кількість інцидентів, пов'язаних із сторонніми організаціями та ланцюгами постачання, у 2025 році зросте майже до 20% від усіх випадків, а середня вартість витоку даних підніметься до 4,44 млн доларів, нездатність управляти цими ризиками стала серйозною загрозою для бізнесу. Незважаючи на нагальність проблеми, багато організацій все ще мають труднощі з базовим наглядом; хоча великі компанії починають переглядати ризики, пов'язані з постачальниками, лише кожна десята компанія регулярно оцінює вразливості, пов'язані з її безпосередніми постачальниками. Ця відсутність прозорості посилюється аутсорсингом управління IT, що часто позбавляє компанії внутрішньої експертизи, необхідної для ефективного реагування у разі масштабних атак на ланцюги постачання…

Щоб протидіяти цим загрозам, організації повинні надати пріоритет «кібергігієні» — зокрема, регулярному навчанню персоналу, багатофакторній аутентифікації та плановим перевіркам систем на наявність вразливостей — і поширити ці практики на свої відносини з третіми сторонами шляхом проведення постійних, а не одноразових оцінок ризиків. Ключовим компонентом цієї стратегії є використання бази даних «Загальні вразливості та ризики» (CVE) — стандартизованої системи, яка дозволяє експертам відстежувати, обмінюватися інформацією та усувати відомі слабкі місця. Використовуючи дані CVE, організації та спеціалізовані центри захисту, такі як Gallagher Cyber Defense Center, можуть виявляти загальні для галузі закономірності, що дозволяє їм усувати типові вразливості на спільних технологічних платформах до того, як ними скористаються зловмисники. Зрештою, оскільки кіберзлочинці продовжують націлюватися на найслабші ланки ланцюга створення вартості, перехід до проактивного захисту, заснованого на аналітичних даних, є необхідним для зменшення площі атаки та формування довгострокової операційної стійкості». ***(Identifying Cyber Vulnerabilities Before a Catastrophe Strikes // ProgramBusiness.com (https://programbusiness.com/news/identifying-cyber-vulnerabilities-before-a-catastrophe-strikes/). 07.04.2026).***

***

«Сучасна ситуація у сфері кібербезпеки характеризується асиметричною боротьбою, в якій зловмисники використовують штучний інтелект та тактику, що діє зі швидкістю машини, тоді як керовані людьми центри оперативної безпеки (SOC) здебільшого залишаються реактивними та працюють у ручному режимі. Щоб подолати цей розрив, що постійно збільшується, галузь переходить до моделі «агентного SOC» — операційної моделі, розробленої для передбачення дій зловмисників та їх проактивного блокування, а не лише реагування на події постфактум. Ця модель побудована на двох взаємозалежних рівнях: автономному рівні блокування, який використовує засоби

контролю на основі політик для блокування відомих загроз зі швидкістю роботи машин, забезпечуючи безпечну основу, та оперативному рівні, де агенти штучного інтелекту виконують складний аналіз, кореляцію доказів та координацію дій у разі інцидентів…

Автоматизуючи «шум» пов'язаний із повторюваними процедурами сортування та розслідування, агентський SOC звільняє фахівців з безпеки, даючи їм змогу зосередитися на стратегічній роботі з високим рівнем впливу, такій як системне зміцнення безпеки, управління ризиками та глибоке розслідування. Цей зсув кардинально змінює ролі в SOC: аналітики перетворюються з пожежників, які виконують ручну сортування, на контролерів результатів; інженери з виявлення переходять від написання окремих правил до навчання систем тому, що має значення; мисливці за загрозами переходять від ручних запитів до дослідження на основі гіпотез; а керівництво переходить від управління чергами до координації автономних стратегій безпеки.

Перехід до агентного SOC — це багатоетапний процес розвитку. Організації починають з уніфікації своєї платформи безпеки для забезпечення автономного захисту, потім переходять до використання генеративної штучної інтелекту для синтезу контексту та прискорення розслідувань, і, нарешті, розгортають спеціалізованих агентів для автономної координації заходів з усунення вразливостей та оптимізації стану безпеки. Зрештою, ця архітектурна зміна не замінює людський досвід, а навпаки, підсилює його, перекладаючи виконання завдань з низьким рівнем впливу на автономні системи, що дозволяє кваліфікованим фахівцям застосовувати судження, контекст та стратегічне прийняття рішень, необхідні для орієнтування у все більш складному ландшафті загроз». ***(Rob Lefferts and David Weston. The agentic SOC—Rethinking SecOps for the next decade // Microsoft (https://www.microsoft.com/en-us/security/blog/2026/04/09/the-agentic-soc-rethinking-secops-for-the-next-decade/). 09.04.2026).***

***

«Перехід від військової служби до сфери кібербезпеки є дуже перспективним шляхом для ветеранів, оскільки цю галузь слід розглядати не як вузьку IT-функцію, а як управління ризиками підприємства, що здійснюється в умовах цифрового бойового простору. Військові концепції, такі як захист периметра, оперативна готовність та правила застосування зброї, легко переносяться на сферу мережевої безпеки, виявлення загроз та механізми управління. Організації все більше цінують військових лідерів, оскільки вони звикли діяти в умовах невизначеності, управляти складними ризиками та приймати рішучі рішення під час криз — навички, які безпосередньо відповідають функціям кібербезпеки, таким як реагування на інциденти, моделювання загроз та управління ескалацією.

У міру того, як кібербезпека стає невід'ємною частиною стратегічного прийняття рішень, військові фахівці мають всі шанси відігравати дедалі важливішу роль у сфері управління, ризиків та дотримання нормативних вимог (GRC). Під впливом розвитку таких технологій, як штучний інтелект та хмарні обчислення, а

також у зв'язку з посиленням глобальних регуляторних вимог, компанії шукають фахівців, здатних перетворити операційні ризики на стійкість бізнесу. Військовослужбовці, особливо ті, що мають допуск до секретної інформації, мають значну перевагу в таких секторах, як оборонні контракти та критична інфраструктура, де чесність, довіра та відповідальне поводження з конфіденційною інформацією мають першочергове значення…

Щоб успішно пройти цей перехід, ветеранам слід відкинути поширені хибні уявлення, такі як переконання, що знання в галузі програмування є обов'язковою вимогою або що відсутність цивільного досвіду є перешкодою; насправді в цій галузі на першому місці стоять зрілість, здатність до аналізу та витримка. Найважливішим кроком для персоналу, що переходить на цивільну роботу, є перетворення військового досвіду на бізнес-результати. Резюме повинні бути «очищені від жаргону», а військові абревіатури та термінологія, пов'язана зі званнями, мають бути замінені простою англійською мовою, що підкреслює вплив, наприклад, дотримання вимог щодо захисту даних та зменшення ризиків. Зрештою, успішна інтеграція у сферу кібербезпеки вимагає зміни мислення з орієнтації на звання на орієнтацію на роль, зосереджуючись на тому, як оперативна дисципліна та стратегічне мислення можуть бути застосовані для вирішення сучасних бізнес-викликів». ***(Chetan Anand. Turning Military Experience Into Cyber Advantage // Information Security Media Group, Corp. (https://www.databreachtoday.co.uk/blogs/turning-military-experience-into-cyber-advantage-p-4087). 10.04.2026).***

***

«У багатьох керівних колах досі існує небезпечний міф: переконання, що серйозні кіберінциденти — це суто технічні збої, які має вирішувати ІТ-відділ. Насправді ж кібератаки становлять бізнес-ризики найвищого рівня — вони порушують ланцюги постачання, породжують юридичну відповідальність, знижують ринкову вартість і загрожують життєздатності організації. Сучасне керівництво має усвідомити, що кібератаки — це вже не сценарії типу «якщо», а сценарії типу «коли», які вимагають такої самої ретельності, підготовки та відповідальності керівництва, як і фінансові чи операційні ризики. Лідери з високими результатами перейшли від сподівань на те, що кібербезпека спрацює, до проактивної підготовки до неминучого…

Першим важливим кроком є подолання культури заперечення шляхом усвідомлення того, що в гіперпідключеному світі поверхня атаки є нескінченною, а 100-відсоткова безпека — неможливою. Замість того, щоб запитувати, чи є їхня система безпечною, прогресивні керівники запитують, як швидко вони можуть виявити зловмисників і наскільки стійким залишається їхній бізнес після компрометації. Підносячи кібербезпеку з рівня другорядного центру витрат до пріоритету на рівні ради директорів, керівники перетворюють її з загрози, що нависає, на керовану бізнес-змінну. По-друге, ефективні лідери проводять змістовні навчальні вправи, що імітують важливі бізнес-рішення, а не лише технічні збої: вони відпрацьовують процедури затвердження виплати викупу, планують комунікаційні стратегії на випадок компрометації внутрішніх систем та

відпрацьовують рішення щодо термінів розкриття інформації для регуляторних органів та громадськості. Ці незручні вправи формують організаційну м'язову пам'ять, завдяки чому команди ефективно функціонують під тиском реальної кризи, а не збираються вперше у кризовому штабі… По-третє, керівники стратегічно переходять від спроб запобігти всьому до активного управління ризиками за допомогою аналітики в режимі реального часу щодо кожного підключеного активу — від інтелектуальних систем опалення, вентиляції та кондиціонування до апаратів МРТ та особистих ноутбуків. Це надає керівникам єдиний огляд, що дозволяє відрізнити вразливості, які можуть бути використані зловмисниками, від нерелевантного шуму, завдяки чому вони можуть пріоритетно розподіляти ресурси на захист найцінніших активів. По-четверте, високоефективні організації розглядають порушення не як привід для звинувачень, а як точні дані, проводячи об'єктивний аналіз для розуміння системних збоїв та використовуючи інциденти як каталізатори цифрової трансформації, в результаті чого з'являються більш сучасні та стійкі технології…

Зрештою, кібербезпека — це командна справа, яка вимагає узгодженості дій президента, фінансового директора, головного юрисконсульта та керівника відділу комунікацій; лідерами, які досягнуть успіху в наступному десятилітті, стануть ті, хто усвідомлює, що кібербезпека — це не перешкода для ІТ-відділу, а фундамент довіри, на якому будується весь їхній бізнес, що вимагає лідерства, заснованого на передбаченні, а не на реагуванні на кризові ситуації». ***(ALEX MOSHER. How the Best Leaders Prepare for Cyber Crises // Mansueto Ventures, LLC (https://www.inc.com/alex-mosher/how-the-best-leaders-prepare-for-cyber-crises/91331996). 16.04.2026).***

***

«Компанія Acora повідомляє про зростання попиту на свою послугу «Базова оцінка кіберінцидентів» (Cyber Incident Baseline Assessment) — сервіс, який оцінює кіберризики та ймовірні наслідки атак у всьому ІТ-середовищі організації шляхом поєднання консультативного аналізу з глибокою технічною оцінкою всіх рівнів ІТ-архітектури з метою виявлення вразливостей та реалістичних шляхів проникнення зловмисників. Зростання попиту пов'язане з масштабами кіберзлочинності у Великобританії, про які повідомляє уряд — близько 8,58 мільйона кіберзлочинів з квітня 2024 року по квітень 2025 року, включаючи приблизно 680 000 атак, не пов'язаних з фішингом, — а також із загальним кліматом регуляторних змін, гучними порушеннями безпеки та зростаючими очікуваннями щодо стійкості. Acora повідомляє, що 25 підприємств скористалися цією оцінкою протягом минулого року, оскільки керівники стикаються з більш складними, пов'язаними із зовнішнім світом ІТ-системами та розширеною, постійно мінливою поверхнею атаки, що спонукає відійти від статичних щорічних тестів на проникнення, які часто дають однакові результати…

Натомість організації переходять до більш комплексних підходів до управління площею атаки та вразливістю, які аналізують, як ризик поширюється в ширшій бізнес-екосистемі, з урахуванням поведінки користувачів, процесів,

конфігурації, рівня зрілості хмарних технологій, практик роботи з даними та нових технологій, таких як штучний інтелект... Компанія Acora стверджує, що в рамках одного проекту було виявлено 15 мільйонів потенційних шляхів порушення безпеки, а цілеспрямоване усунення вразливостей — часто шляхом налаштування існуючих інструментів — дозволило зменшити вразливість більш ніж на 95%, що допомогло керівництву обґрунтувати інвестиції та узгодити спільні пріоритети серед команд. Компанія очікує, що ця зміна прискориться у 2026 році, оскільки зростає регуляторний тиск та операційні перебої внаслідок інцидентів, а також побоювання щодо більш витончених загроз на основі штучного інтелекту та агентів ШІ. Опитування показують, що більшість британських організацій продовжують стикатися з інцидентами, і багато хто з них збільшує бюджети на кібербезпеку, включаючи витрати на більш цілеспрямовані стратегії безперервної оцінки ризиків». ***(Alex Rivers. The Rise in Demand For The Cyber Incident Baseline Assessment // IBTimes LLC (https://www.ibtimes.co.uk/uk-businesses-embrace-cyber-risk-assessments-1792141). 16.04.2026).***

***

«У міру посилення цифрових загроз у мережах урядових, корпоративних та критичних інфраструктурних об'єктів питання кібербезпеки вийшло на перший план у глобальних дискусіях про ризики. 87% респондентів останнього дослідження «Global Cybersecurity Outlook» Світового економічного форуму визначили вразливості, пов'язані зі штучним інтелектом, як кіберризик, що найшвидше зростатиме до 2025 року. Таке загострення загроз змушує інвесторів приділяти все більше уваги компаніям, які мають шанси отримати вигоду від зростаючого попиту на надійні рішення у сфері безпеки. Фондові менеджери визначили декількох ключових гравців у сфері кібербезпеки, кожен з яких має унікальні сильні сторони та стратегічні переваги…

Компанія NCC Group, що спеціалізується на забезпеченні інформаційної безпеки, виділяється завдяки комплексному спектру послуг на всіх етапах життєвого циклу — від консалтингу до повного аутсорсингу послуг з безпеки — і, як очікується, отримає вигоду від зростаючого попиту на експертизу в галузі загроз, пов'язаних зі штучним інтелектом. У секторі оборони шведський оператор зв'язку Invisio та фінська інженерна компанія Bittium мають вигідні позиції завдяки власним технологіям, що відповідають вимогам НАТО, а також зростаючій тенденції Європи до надання пріоритету суверенним постачальникам. Компанія Booz Allen Hamilton, провідний постачальник кіберрішень для федерального уряду США, відома своїми передовими, часто секретними проектами та привабливою вартістю акцій… Для ринку малих та середніх підприємств (МСП) постачальник керованих послуг SysGroup пропонує комплексні рішення з хмарного хостингу та кібербезпеки, спрямовані на усунення критичних вразливостей у ланцюгах постачання. Нарешті, глобальна платіжна мережа Mastercard робить кібербезпеку основою своєї діяльності, інвестуючи значні кошти в системи захисту від шахрайства на базі штучного інтелекту, такі як Safety Net, а також придбавши компанії, наприклад Recorded Future, щоб створити на додаток до свого основного платіжного бізнесу набір високоприбуткових послуг з безпеки з високою доданою

вартістю». ***(Emmy Hawker. The cybersecurity stocks managers are backing as digital threats surge // Trustnet Limited (https://www.trustnet.com/news/13475000/the-cybersecurity-stocks-managers-are-backing-as-digital-threats-surge). 23.04.2026).***

***

«У першому кварталі 2026 року галузь програмного забезпечення зазнала значної корекції цін на акції, спричиненої занепокоєнням інвесторів щодо довгострокової життєздатності бізнес-моделей в епоху штучного інтелекту (ШІ). Однак, на думку аналітика Goldman Sachs Research Габріели Боргес, компанії-розробники програмного забезпечення можуть знайти стійку модель адаптації, звернувши увагу на сектор кібербезпеки. Компанії з кібербезпеки навчилися успішно орієнтуватися у світі революційних технологій, активно використовуючи злиття та поглинання (M&A) для заповнення прогалин у своїх можливостях, а не покладаючись виключно на органічний розвиток. Ця гнучкість, що передбачає придбання та ретельну інтеграцію інноваційних стартапів, дозволила їм випереджати постійно мінливий ландшафт загроз і є основною причиною того, що їхні акції зараз торгуються з премією…

Боргес рекомендує великим компаніям-розробникам програмного забезпечення застосовувати цей «перевірений на практиці» підхід, використовуючи екосистему венчурного капіталу для фінансування інновацій нового покоління, а потім придбання найкращих технологій. Важливою передумовою реалізації цієї стратегії є мінімізація «технічного боргу» — накопичення погано інтегрованого коду, що залишився від минулих поглинань або несинхронізованих досліджень і розробок. Чиста, структурно надійна платформа є необхідною умовою для створення ефективних інструментів штучного інтелекту та захисту від навали нових конкурентів, що працюють виключно на базі штучного інтелекту. Оскільки ШІ підвищує планку диференціації продуктів, інвестори все частіше розрізняють «хороші привабливі» компанії, які впроваджують інновації та користуються популярністю серед своїх клієнтів, та «погані привабливі» компанії-монополісти, чиї захисні бар'єри ґрунтуються на інерції користувачів. Щоб процвітати, усталені компанії-розробники програмного забезпечення повинні тепер довести, що їхній глибокий досвід у галузі дозволяє створювати високоякісні продукти на базі ШІ, які підтверджують їхнє лідерство на ринку та конкурентну перевагу». ***(Cybersecurity Firms Show Software Industry How to Navigate AI // Goldman Sachs (https://www.goldmansachs.com/insights/articles/cybersecurity-firms-show-software-industry-how-to-navigate-ai). 23.04.2026).***

***

«Багато малих та середніх підприємств (МСП) впровадили базові заходи з кібербезпеки, такі як антивірусне програмне забезпечення, фільтрування електронної пошти та брандмауери, що створює враження, ніби ризики перебувають під контролем. Однак ці інструменти часто додаються з часом реактивно, без узгодженої стратегії, що призводить до набору рішень, які можуть не відповідати фактичним ризикам організації або не забезпечувати справжнього захисту. Це створює парадокс кібербезпеки для МСП, які стикаються з тими ж

складними загрозами, що й великі підприємства, але не мають бюджету, часу та ресурсів для побудови захисних систем корпоративного рівня…

Щоб досягти справжньої стійкості, малим та середнім підприємствам (МСП) необхідно вийти за межі простого переліку інструментів і розробити чітку стратегію кібербезпеки, яка ґрунтується на відповідях на чотири основні запитання: Що саме ми захищаємо? Де є прогалини? Чи дізнаємося ми, якщо щось піде не так, і як реагувати? Чи зможемо ми відновити роботу, якщо трапиться найгірше? До типових слабких місць належать непослідовне впровадження багатофакторної автентифікації, обмежена видимість загроз, неналежне планування реагування на інциденти, а також недостатні процеси резервного копіювання та відновлення…

Кібербезпека полягає не в тому, щоб робити все, а в тому, щоб робити правильні речі в правильному порядку з урахуванням конкретних ризиків, з якими стикається бізнес. Організації, які починають з чіткого розуміння своїх критично важливих активів, потоків даних та потенційних наслідків, мають кращі можливості для ефективного розподілу інвестицій, зменшення невизначеності та формування більш стійкої системи безпеки, а не просто накопичення все більшої кількості інструментів». ***(Tim Killick. Why most cybersecurity investment isn't doing what you think it is // Newsco Insider Limited (https://www.insidermedia.com/blogs/south-west/why-most-cybersecurity-investment-isnt-doing-what-you-think-it-is). 20.04.2026).***

***

«Кібербезпека стає дедалі дорожчою та важливішою: за даними IBM, середня вартість витоку даних за останній рік зросла на 10 % і становить 4,88 млн доларів, що зумовлено переходом на хмарну інфраструктуру та поширенням гібридних моделей роботи. Це зростання ризиків стимулює значне зростання в галузі кібербезпеки, однак акції окремих компаній можуть бути нестабільними, що робить біржові фонди (ETF) у сфері кібербезпеки привабливим варіантом для інвесторів, які прагнуть диверсифікувати свої вкладення, не ставлячи на одну компанію…

Серед провідних ETF-фондів, що спеціалізуються виключно на кібербезпеці, — First Trust Nasdaq Cybersecurity ETF (CIBR), найбільший з активами понад 11 млрд доларів та 32 позиціями, зосередженими переважно на великих компаніях у сфері кібербезпеки, що котируються на американських біржах, таких як Broadcom, Palo Alto Networks та Cisco; Amplify Cybersecurity ETF (HACK) з активами у 2 млрд доларів та 23 більш концентрованими позиціями; Global X Cybersecurity ETF (BUG), який з моменту запуску у 2019 році перевершив аналоги завдяки 29 позиціям з переважною часткою великих компаній-розробників програмного забезпечення; iShares Cybersecurity and Tech ETF (IHAK) від BlackRock, що пропонує 38 позицій із нижчим коефіцієнтом витрат у 0,47%; WisdomTree Cybersecurity Fund (WCBR) — найновіший та найбільш концентрований фонд із 25 позиціями; та менший Xtrackers Cybersecurity Select Equity ETF (PSWD), що вирізняється низьким коефіцієнтом витрат у 0,20% та ширшою міжнародною експозицією…

Широкопрофільні технологічні ETF, такі як Vanguard Information Technology ETF (VGT), також забезпечують непряму експозицію до сектору кібербезпеки поряд з іншими технологічними трендами. Ці ETF зазвичай перебалансовуються щоквартально, орієнтовані на зростання, а не на дивіденди, а їхні коефіцієнти витрат становлять від 0,45% до 0,6%. При виборі інвестори повинні враховувати такі фактори, як комісії, концентрація портфеля та співвідношення великих і малих компаній. Прогнозується, що світовий ринок кібербезпеки зросте з приблизно 248 млрд доларів у 2026 році до майже 700 млрд доларів до 2034 року завдяки прогресу в галузі штучного інтелекту, квантових обчислень та зростанню обсягів даних, що робить ETF у сфері кібербезпеки привабливим інструментом довгострокового інвестування для використання цієї довгострокової тенденції зростання при одночасному зниженні ризику, пов'язаного з окремими акціями». ***(Matthew Frankel. Best Cybersecurity ETFs to Buy in 2026 and How to Invest // The Motley Fool (https://www.fool.com/investing/stock-market/market-sectors/information-technology/cybersecurity-stocks/cybersecurity-etf/). 20.04.2026).***

***

«Проєкти з кібербезпеки дають можливість людям будь-якого рівня набути практичних навичок, необхідних для роботи, поповнити своє портфоліо та продемонструвати реальні компетенції у сфері, де практичний досвід цінується надзвичайно високо. За даними Бюро статистики праці США, до 2034 року кількість вакансій аналітиків з інформаційної безпеки зросте на 29%, що становитиме близько 16 000 вакансій на рік, тоді як глобальний ринок кібербезпеки, як очікується, розшириться з 227,6 млрд доларів у 2025 році до 351,9 млрд доларів до 2030 року, що зумовлено зростанням загроз та збільшенням вартості витоків даних…

Перелік проєктів з кібербезпеки, які класифіковані за рівнем складності, щоб допомогти як початківцям, так і досвідченим фахівцям продемонструвати свої професійні навички…

Для початківців проєкти зосереджуються на базових поняттях та швидких досягненнях для портфоліо. Сюди входять створення інструменту для моделювання фішингових атак з метою відстеження реакції користувачів, розробка засобу перевірки надійності паролів із практичними рекомендаціями, а також налагодження лабораторії «SIEM Lite» з використанням таких інструментів, як Wazuh і Sysmon, для відпрацювання навичок виявлення аномалій у журналах. Інші проекти, придатні для початківців, стосуються візуальної криптографії, розробки програми безпечного обміну файлами або створення додатка-вікторини з кібербезпеки. Ці проекти призначені для зміцнення впевненості та отримання чітких, наочних результатів, таких як звіти, інформаційні панелі та правила виявлення…

Проєкти середнього рівня спрямовані на відпрацювання робочих процесів, необхідних для таких посад, як аналітик SOC або інженер з безпеки додатків. Ці більш складні проекти включають симулятор реагування на інциденти, що відтворює повний цикл реагування, аналізатор безпеки Wi-Fi та простий інструмент для виявлення вразливостей, який зіставляє перелік програмного

забезпечення з відомими CVE. Інші завдання середнього рівня передбачають створення полегшеного механізму кореляції журналів безпеки, системи виявлення програм-вимагачів на основі поведінкових індикаторів та інструменту аудиту безпеки веб-додатків, що поєднує автоматизоване та ручне тестування…

Для досвідчених фахівців, які прагнуть обійняти керівні посади у сферах аналізу загроз, хмарної безпеки або цифрової криміналістики, пропонуються спеціалізовані проєкти. Серед них — розробка платформи для аналізу загроз, яка збирає, доповнює та експортує індикатори компрометації (IOC); створення динамічного механізму впровадження політик безпеки з використанням підходу «політика як код»; побудова пісочниці для аналізу шкідливого програмного забезпечення, що дозволяє безпечно досліджувати підозрілі файли; а також розробка системи виявлення вторгнень на основі машинного навчання. Ці складні проекти покликані продемонструвати глибоку експертизу в галузі та здатність розробляти складні рішення з безпеки…

Щоб досягти максимального ефекту, важливо обоати проєкт, які відповідають конкретним кар'єрним цілям і дають вагомі результати для портфоліо, такі як упорядковані репозиторії GitHub, детальні звіти або функціональні інформаційні панелі. Систематично просуваючись від навчання до реалізації проектів, фахівці можуть ефективно продемонструвати свої практичні навички та виділитися на висококонкурентному ринку праці у сфері кібербезпеки». ***(Vivek G. Top Cyber Security Projects to Build Skills and Portfolio // Simplilearn Solutions (https://www.simplilearn.com/top-cyber-security-projects-article). 20.04.2026).***

***

«У 2026 році, коли кіберзагрози стають дедалі витонченішими та швидшими, організації повинні розглядати управління виправленнями як фундаментальний і проактивний елемент своєї стратегії кібербезпеки, а не як щось другорядне. Неоновлене програмне забезпечення залишається однією з найпоширеніших точок входу для зловмисників, які швидко використовують нещодавно виявлені вразливості, перш ніж підприємства встигають зреагувати, тому своєчасні оновлення є надзвичайно важливими для захисту цифрових активів та забезпечення безперебійної роботи. Структурований підхід до управління оновленнями Microsoft дозволяє організаціям визначати пріоритетність критичних вразливостей на основі рівнів ризику, що значно зменшує площу атаки та запобігає використанню прогалин у безпеці…

Окрім забезпечення безпеки, ефективне управління виправленнями дозволяє мінімізувати витрати, пов'язані з простоєм обладнання та перебоями в роботі, підтримуючи стабільність і надійність систем, що допомагає компаніям уникнути трудомістких і дорогих заходів з відновлення, які часто супроводжують кіберінциденти. Воно також сприяє дотриманню нормативних вимог у різних галузях, гарантуючи регулярне оновлення систем і систематичне усунення вразливостей, тим самим знижуючи ризик штрафних санкцій, юридичних проблем та шкоди репутації…

Крім того, автоматизовані процеси встановлення оновлень підвищують загальну ефективність IT-роботи, зменшуючи обсяг ручної роботи, усуваючи

розбіжності між пристроями та даючи змогу ІТ-командам зосередитися на стратегічних ініціативах, а не на рутинному обслуговуванні. Зрештою, в умовах дедалі складнішого цифрового середовища організації, які впроваджують систематичний моніторинг, автоматизацію та своєчасні оновлення, можуть створити стійку багаторівневу систему кібербезпеки, здатну протистояти як сучасним, так і майбутнім загрозам». ***(Why Effective Patch Management Is Critical for Cybersecurity in 2026 // The Business Matters Brand Ltd (https://bmmagazine.co.uk/business/why-effective-patch-management-is-critical-for-cybersecurity-in-2026/). 23.04.2026).***

***

«Цифрові двійники стрімко еволюціонують від статичних комп'ютерних моделей до динамічних, керованих даними симуляцій, які відтворюють реальну поведінку в режимі реального часу, надаючи потужні можливості для застосувань у сфері кібербезпеки. Спочатку ці віртуальні моделі фізичних систем, процесів або середовищ використовувалися у виробництві для профілактичного технічного обслуговування, але зараз вони постійно оновлюються даними в режимі реального часу, що надходять від датчиків Інтернету речей (IoT), систем аналітики на основі штучного інтелекту та хмарних обчислень. Це дозволяє здійснювати проактивний моніторинг загроз, моделювати сценарії атак, проводити прогнозний аналіз та забезпечувати автономне реагування без ризику для виробничих систем…

Цифрові двійники можна класифікувати як двійники компонентів (окремі елементи мережі), двійники продуктів (інтегровані вузли), двійники процесів (робочі процеси з безпеки) або двійники систем (комплексні моделі екосистем), і всі вони забезпечують моніторинг у реальному часі, планування сценаріїв та оцінку вразливостей. Інтеграція генеративної ШІ дозволяє взаємодіяти з складними моделями за допомогою природної мови, що робить доступ до них доступним для нетехнічних команд та прискорює прийняття рішень, тоді як прогнозне моделювання на основі ШІ виявляє найменші ознаки порушення безпеки та забезпечує автономне локалізування загроз…

За прогнозами, обсяг ринку цифрових двійників зросте з 35 млрд доларів у 2024 році до 379 млрд доларів до 2034 року, що відображає зростання попиту на оперативні системи безпеки у складних гібридних IT/OT-середовищах. Практичні застосування включають управління мережею для перевірки конфігурацій та аналізу радіусу поширення порушень, вдосконалення центру операцій безпеки для безпечного моделювання загроз та навчання реагуванню на інциденти, оптимізацію фізичної безпеки за допомогою віртуального моделювання розміщення камер та сценаріїв загроз, управління ідентифікацією та доступом для прогнозування ескалації привілеїв, оцінку вразливостей для тестування виправлень та засобів контролю без перебоїв у роботі, а також DevOps/безперервність бізнесу для відпрацювання процедур відновлення.

Найкращі практики передбачають стратегічну інтеграцію за допомогою пілотних програм, ретельне управління якістю даних для уникнення ризиків, пов'язаних із принципом «що вкинеш, те й отримаєш», розробку систем безпеки «знизу вгору» з використанням архітектури «нульової довіри» та технології

блокчейн для відстеження походження, а також розвиток кадрового потенціалу для усунення прогалин у кваліфікації при застосуванні цифрових двійників. У міру того, як цифрові двійники продовжують розвиватися завдяки генеративній штучній інтелекту та автономним можливостям, вони символізують перехід від реактивної до проактивної, керованої інтелектом кібербезпеки, що дозволяє організаціям тестувати інновації, моделювати загрози та підвищувати стійкість у дедалі складніших цифрових середовищах». ***(Sam Bocetta. Digital Twins Could Be the Future of Proactive Cybersecurity // AspenCore, Inc. (https://www.embedded.com/digital-twins-could-be-the-future-of-proactive-cybersecurity/). 22.04.2026).***

***

«Згідно з опитуванням страхової компанії Everywhen, у 2026 році кібератаки стали найбільшим ризиком для професійних фірм: про це зазначили 65 % респондентів, що значно перевищує інші фактори, такі як економічний тиск (18 %), позови про професійну недбалість (9 %) та зміни в законодавстві (8 %). Результати дослідження підкреслюють помітну зміну пріоритетів серед підприємств у таких секторах, як юридичні, фінансові та консалтингові послуги, які обробляють великі обсяги конфіденційної інформації про клієнтів і значною мірою покладаються на цифрові системи, що робить їх головними мішенями для витоків даних, програм-вимагачів та пов’язаних з цим збитків… Результати свідчать про те, що кіберризик дедалі частіше розглядається як ключове питання, пов’язане з бізнесом та управлінням, а не як вузькоспеціалізована технологічна проблема, оскільки успішна атака може одночасно вплинути на обслуговування клієнтів, репутацію, дотримання нормативних вимог та фінансові показники. Представник компанії Everywhen зазначив, що кіберінциденти рідко трапляються ізольовано і часто спричиняють переривання діяльності, розслідування з боку регуляторних органів та позови про відшкодування професійної відповідальності, що підкреслює необхідність для компаній розуміти, як діє їхнє страхування, та виявляти потенційні прогалини у страховому покритті… Результати опитування свідчать про те, що професійні компанії переоцінюють взаємодію різних ризиків, особливо в тих випадках, коли кіберінцидент може спричинити ланцюгові юридичні або операційні наслідки, а також відображають зростаюче усвідомлення того, що цифрові загрози на сьогодні становлять фундаментальний і безпосередній ризик для бізнесу в умовах дедалі більш взаємопов’язаного середовища». ***(Sean Mitchell. Cyber-attacks top risk for professional firms in 2026 // TechDay (https://securitybrief.co.uk/story/cyber-attacks-top-risk-for-professional-firms-in-2026). 24.06.2026).***

***

«Опитування, проведене компанією Kocho серед 501 британського IT-директора, аналітика з питань безпеки та IT-фахівця, показало, що понад чверть (27 %) британських фахівців з кібербезпеки відчували тиск з метою приховати інцидент порушення безпеки або втрати даних, що підкреслює наявність стійких культурних проблем всередині організацій, незважаючи на

широке визнання кіберризиків. Хоча 92% респондентів вважають, що керівництво їхніх компаній розуміє повсякденні реалії кібербезпеки, це сприйняття суттєво змінюється під час фактичного порушення, коли 20% повідомляють про стійку культуру звинувачень, а 14% заявляють, що їх вважали особисто відповідальними…

Майже половина (45 %) вважає, що більш виважена реакція ради директорів полегшила б і пришвидшила реагування на інциденти, особливо з огляду на вимогу GDPR щодо повідомлення про порушення захисту персональних даних протягом 72 годин та потенційні штрафи у розмірі до 8,7 млн фунтів стерлінгів або 2 % від глобального обороту за невиконання вимог. Напруженість у відносинах між командами з безпеки та вищим керівництвом залишається високою: 73% опитуваних описують очікування керівництва як надто високі (у компаніях із 100–250 співробітниками цей показник зростає до 81%), 52% повідомляють, що від них вимагали гарантій, яких вони не могли надати, 39% бажають чіткішої підтримки та визнання, а 28% вважають, що сильніша підтримка з боку керівництва покращила б їхні перспективи…» ***(Elizabeth Greenberg. Cyber Professionals Told to Cover Up Security Incidents // DIGIT (https://www.digit.fyi/cyber-professionals-told-to-cover-up-security-incidents/). 20.04.2026).***

***

«У сучасну цифрову епоху межі між професійним та приватним життям стираються, що породжує складну загрозу, відому як «ланцюг особистих атак», коли кіберзлочинці націлюються на особисте життя керівників, щоб у підсумку проникнути в їхні компанії. Цей багатоетапний процес починається з розвідки, під час якої зловмисники збирають особисті дані з таких джерел, як сайти посередників у торгівлі даними та соціальні мережі, після чого проникають у «слабке місце» життя керівника — його часто незахищену домашню мережу та пристрої Інтернету речей (IoT)… Звідти зловмисники переміщуються з особистих пристроїв до конфіденційних облікових записів і, зрештою, досягають своїх цілей, які можуть варіюватися від фінансового шахрайства та доксингу до повного захоплення корпоративного облікового запису…

Стандартного реактивного програмного забезпечення, такого як антивіруси, вже недостатньо; натомість потрібен проактивний підхід, заснований на аналітичних даних. Це передбачає використання Digital Executive Protection (DEP), що діє як «цифровий охоронець» для керівників та їхніх сімей, зменшуючи їхній цифровий слід, зміцнюючи домашні мережі та постійно відстежуючи загрози. Визнаючи, що особиста кібербезпека тепер є корпоративною необхідністю, та впроваджуючи комплексну систему захисту, яка перевіряє кожного постачальника та захищає кожен пристрій, організації можуть розірвати ланцюг особистих атак ще до того, як він розпочнеться…» ***(Brian Hill. Safeguarding Against the Personal Attack Chain in the Age of "Always On" Connectivity // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/safeguarding-against-the-personal-attack-chain-in-the-age-of-always-on-connectivity/). 21.04.2026).***

***

«У сучасних умовах підвищеної геополітичної та економічної невизначеності кіберризики посилюються, оскільки зловмисники використовують розсіяну увагу керівництва та операційні навантаження, щоб виявляти вразливі місця. Кіберінциденти рідко починаються з очевидних тривожних сигналів, а починаються непомітно з компрометації облікових даних або пропущеного з'єднання, що дозволяє зловмисникам вивчити системи та взаємозалежності організації перед тим, як розпочати руйнівну атаку. Це робить швидкість виявлення, а не лише наявність засобів безпеки, критичним фактором, що відрізняє інцидент, який можна контролювати, від повномасштабної бізнес-кризи…

Проблема ускладнюється сучасними цифровими екосистемами, в яких підприємства взаємопов'язані через хмарні платформи та сторонніх постачальників, а це означає, що атака на єдину слабку ланку в ланцюгу постачання може спричинити ланцюговий ефект. У таких умовах керівництво повинно перейти від простого підтвердження наявності заходів безпеки до вимагання чітких, обґрунтованих доказів їхньої перевіреної ефективності. Воно повинно ставити прямі запитання про те, як часто тестуються реальні сценарії атак, які системи є найважливішими та де саме в організації існують найбільші ризики — не в історичному звіті, а саме зараз — щоб забезпечити справжню операційну стійкість…» ***(Keshvinderjit Singh. Opinion: The quiet beginning of a cyber incident: What leaders should be asking now // The Edge Communications Sdn. Bhd. (https://theedgemalaysia.com/node/801118). 24.06.2026).***

***

«…Школи K-12 стикаються з проблемою кібербезпеки, яка стрімко загострюється через технології хмарної синхронізації на таких платформах, як Google Workspace та Microsoft 365. Хоча ці платформи розроблені для співпраці та підвищення ефективності, вони можуть ненавмисно прискорити поширення шкідливого програмного забезпечення по всій мережі, якщо буде зламано хоча б один обліковий запис. Згідно з доповіддю COS MS-ISAC за 2025 рік, 82% шкіл зазнали кіберінцидентів минулого року, причому навчальні заклади K-12 зазнали втричі більше інцидентів безпеки на одного учня, ніж будь-який інший сектор... Середня вартість порушення безпеки даних в освіті досягла 4,88 млн доларів у 2024 році, що на 15% більше, ніж у попередньому році, в основному через програми-вимагачі та витік даних, які експлуатують довірені середовища.

Все більшу стурбованість викликає поширення інструментів «тіньового штучного інтелекту» (Shadow AI), які використовуються викладачами та студентами без нагляду IT-спеціалістів, обробляють конфіденційні академічні, медичні та фінансові дані та розширюють площину атаки через приховані дозволи OAuth і нерегульовані потоки даних. У міру закінчення терміну дії фінансування, виділеного в період пандемії, та збереження обмеженої чисельності IT-команд, пріоритет зміщується з реактивного мінімізування збитків на проактивну профілактику. Постійний моніторинг хмарних середовищ, який здійснюється безпосередньо через API-інтерфейси, дозволяє в режимі реального часу аналізувати шаблони активності, базові показники поведінки та індикатори ризику, щоб

виявляти й зупиняти загрози до їх ескалації… Такий підхід скорочує час реагування, мінімізує перебої в роботі та забезпечує необхідний контроль у середовищах, орієнтованих на хмарні технології, допомагаючи адміністраціям перейти від простого відновлення після атаки до запобігання поширенню шкідливого програмного забезпечення в надійних системах». ***(Charlie Sander. Why Cloud Monitoring Has Become K–12's Most Critical Cyber Defense Tool // HackerNoon (https://hackernoon.com/why-cloud-monitoring-has-become-k-12s-most-critical-cyber-defense-tool). 24.04.2026).***

***

«Звіт «CISO Report 2026», підготовлений Cybersecurity Ventures та Sophos, виявляє разючий глобальний дисбаланс у сфері керівництва кібербезпекою: лише близько 35 000 керівників з інформаційної безпеки (CISO) обслуговують приблизно 359 мільйонів підприємств по всьому світу — це приблизно один CISO на кожні 10 000 компаній. Хоча великі корпорації, зокрема компанії зі списку Fortune 500, зазвичай мають спеціалізовані команди з кібербезпеки під керівництвом CISO, що володіють значними ресурсами, переважна більшість малих та середніх підприємств (МСП) працюють без будь-якого офіційного керівництва у сфері кібербезпеки чи навіть базових систем безпеки, що робить їх вкрай вразливими до атак та погано підготовленими до реагування на інциденти, такі як витік даних або атаки програм-вимагачів…

Цей дефіцит керівних кадрів викликає особливе занепокоєння з огляду на прогнозоване зростання глобальних витрат, пов'язаних із кіберзлочинністю, які, за оцінками Cybersecurity Ventures, до 2031 року можуть сягнути 12,2 трлн доларів на рік, причому лише на викуп за програмне забезпечення-вимагач припадатиме понад 74 млрд доларів. У міру прискорення цифрової трансформації у звіті підкреслюється нагальна потреба у збільшенні інвестицій у таланти у сфері кібербезпеки на керівному рівні, а також у вдосконаленні програм підвищення обізнаності та готовності для малих та середніх підприємств, визнаючи, що ефективна кібербезпека вже не є опцією, а є фундаментальною опорою довгострокової стійкості та успіху організації». ***(Naveen Goud. There is only 1 CEO for over 10K Companies says Survey // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/there-is-only-1-ceo-for-over-10k-companies-says-survey/). 24.04.2026).***

***

«Опитування «Стан безпечних комунікацій у 2026 році», проведене компанією BlackBerry Secure Communications серед 700 осіб, відповідальних за прийняття рішень у сфері безпеки в урядових структурах та на об'єктах критичної інфраструктури у США, Великій Британії, Канаді та Сінгапурі, виявило значний розрив між уявленням про безпеку комунікацій та фактичним рівнем ризику. Хоча 83% респондентів зазначають, що WhatsApp використовується для обговорення конфіденційних питань у їхніх організаціях, багато хто з них демонструє обмежене розуміння меж безпеки цієї платформи. Дослідження виявляє «парадокс суверенітету»: 55% організацій надають пріоритет

суверенному контролю над комунікаціями, проте 98% продовжують покладатися на споживчі платформи, що розміщені за кордоном і не призначені спеціально для використання урядом з високим рівнем безпеки або для конфіденційних цілей. Крім того, 52% висловлюють занепокоєння щодо можливості моніторингу або порушення роботи телекомунікаційних мереж, що відображає реальні загрози, такі як шпигунські кампанії, спрямовані проти інфраструктури…

Незважаючи на ці ризики, 88% керівників служб безпеки висловлюють впевненість у безпеці своїх поточних месенджерів, хоча ця впевненість часто ґрунтується на хибних уявленнях, зокрема на переконанні, що шифрування захищає метадані (52%), запобігає підробці особи або спуфінгу (47%) або залишається ефективним навіть після злому пристрою (41%). Під час серйозних криз 90% впевнені у своїх можливостях реагування, проте лише 49% мають єдину безпечну комунікаційну платформу, а багато хто замість цього покладається на розрізнені інструменти, такі як групові чати (54%), ланцюжки електронних листів (51%), спільні таблиці (29%) та телефонні ланцюжки (19%)… У звіті підкреслюється, що платформи обміну повідомленнями для споживачів ніколи не були розроблені для обробки конфіденційної інформації, захисту конфіденційності або задоволення вимог середовищ з високим рівнем безпеки, і міститься попередження, що в міру еволюції загроз у напрямку компрометації облікових записів та широкомасштабного стеження, поточна залежність від цих платформ може свідчити про недооцінку системного ризику. BlackBerry позиціонує свої рішення для безпечного зв'язку як такі, що усувають ці прогалини, пропонуючи захищені від перехоплення голосові та текстові повідомлення урядового рівня для організацій, що потребують суверенного контролю та операційної стійкості». ***(Jane Devry. New BlackBerry Report Exposes Critical Misunderstanding of Messaging App Security Across Government and Critical Infrastructure // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/new-blackberry-report-exposes-critical-misunderstanding-of-messaging-app-security-across-government-and-critical-infrastructure/). 22.04.2026).***

***

«Світовий ринок кібербезпеки переживає період стрімкого зростання: за прогнозами, його обсяг збільшиться з 219 млрд доларів у 2023 році до 578,2 млрд доларів до 2033 року. Це значне зростання, що характеризується середньорічним темпом зростання на рівні 10,4%, зумовлене швидкою цифровою трансформацією таких ключових секторів, як фінанси, охорона здоров’я та виробництво, а також широким впровадженням хмарних обчислень, Інтернету речей (IoT) та штучного інтелекту. У міру того як організації переходять на хмарні технології та впроваджують дистанційну роботу, їхні поверхні атаки різко розширилися, що призвело до зростання попиту на системи безпеки нового покоління, такі як архітектура «нульової довіри», виявлення та реагування на кінцевих точках (EDR) та аналіз загроз у реальному часі. Цей зростаючий попит ще більше підсилюється через збільшення частоти та складності кібератак, включаючи програми-вимагачі та просунуті постійні загрози (APT), а також через більш суворі глобальні норми захисту даних, такі як GDPR…

Визначальним фактором у сфері кібербезпеки 2026 року є поява «гонки озброєнь у сфері ШІ», в якій як зловмисники, так і захисники використовують генеративний та агентний ШІ для отримання переваги. У той час як кіберзлочинці застосовують ШІ для автоматизації складних кампаній з фішингу та експлуатації API, організації протидіють їм за допомогою рішень на базі ШІ для прогнозної аналітики та автоматизованого реагування на інциденти, зміщуючи фокус галузі з реактивної оборони на постійну стійкість. Ця тенденція особливо помітна у стрімкому зростанні сегмента хмарних розгортань та зростаючій залежності від керованих послуг безпеки… У регіональному розрізі Північна Америка залишається найбільшим ринком завдяки розвиненій інфраструктурі та концентрації провідних постачальників технологій, проте найшвидше зростання очікується в Азіатсько-Тихоокеанському регіоні, що зумовлено прискоренням цифровізації та збільшенням інвестицій у сферу безпеки як з боку урядів, так і підприємств. На цьому висококонкурентному ринку провідні гравці, такі як Palo Alto Networks, CrowdStrike та Cisco, використовують стратегічні поглинання та інноваційні продукти для зміцнення своєї глобальної присутності та задоволення складних потреб у сфері безпеки дедалі більш гіперпідключеної цифрової економіки». ***(Cyber Security Market Expansion Driven by Cloud Adoption and Increasing Cyber Threats // openPR (https://www.openpr.com/news/4482129/cyber-security-market-expansion-driven-by-cloud-adoption). 21.04.2026).***

***

«У рамках глобального порівняльного аналізу кіберкомпетентності Hack The Box 2025 було протестовано 796 корпоративних команд з безпеки на реальних сценаріях атак. Результати показали, що лише 21,1 % змогли успішно виявити та усунути поширені веб-уразливості, 18,7 % впоралися із завданнями з безпечного кодування, а 21,3 % успішно виконали завдання з хмарної безпеки. Результати викривають небезпечний розрив між «театром безпеки» — сертифікаціями, аудитами відповідності та придбанням інструментів — та фактичною обороноздатністю під час тестування в реалістичних умовах. Результати різних галузей значно відрізнялися: у сфері охорони здоров'я показник склав 15,6%, у фінансовій сфері — 19,2% у веб-сфері та 10,1% у сфері блокчейну, у роздрібній торгівлі — 20,3%, у сфері освіти — лише 7,8% у веб-сфері та 0% у безпечному кодуванні, а в енергетиці та комунальному господарстві — найнижчий показник — 6,7%...

Незважаючи на значні інвестиції в безпеку, більшість організацій не можуть сформувати практичні навички, оскільки вони зосереджуються на сертифікатах та дотриманні вимог, а не на практичній здатності виявляти та усувати вразливості. Команди з високою ефективністю вирізняються тим, що оцінюють практичні здібності шляхом постійного управління ризиками, залучають фахівців з безпеки до команд розробників та використовують перевірку на основі результатів, а не покладаються на теоретичні знання… Цей тест показує, що зловмисники не переймаються питаннями дотримання нормативних вимог чи наявністю сертифікатів; вони використовують реальні вразливості, які більшість команд з безпеки не можуть надійно виявити. Організації, які й надалі надаватимуть

перевагу «театральним» заходам безпеки над реальними оборонними можливостями, залишатимуться вразливими, тоді як ті, що інвестують у формування практичних навичок у своїх командах, отримають значну конкурентну перевагу в захисті своїх систем та даних». ***(Jacob Krell. When Elite Cyber Teams Can't Crack Web Security // Techstrong Group Inc. (https://securityboulevard.com/2026/04/when-elite-cyber-teams-cant-crack-web-security/). 23.04.2026).***

***

«Забезпечення надійної кібербезпеки на робочому місці є постійною необхідністю, яка вимагає постійної пильності як від роботодавців, так і від працівників, щоб випереджати дедалі більш витончені загрози. Основоположним кроком у цих зусиллях є суворе розділення систем, особливо для віддалених працівників, що гарантує повне відокремлення професійної діяльності та затвердженого компанією програмного забезпечення від особистих пристроїв та незатверджених завантажень. Під час роботи поза офісом надзвичайно важливо дотримуватися належної обережності щодо мережевої безпеки, зокрема використовувати VPN як критично важливий рівень захисту, коли безпечні хаби недоступні…

У міру розвитку технологій організації також повинні надавати пріоритет «готовності до штучного інтелекту», інтегруючи підвищення кваліфікації у сферах штучного інтелекту, машинного навчання та цифрової грамотності у свою основну культуру, а не розглядаючи це як щорічне адміністративне завдання. Розуміння цих нових загроз є життєво важливим, оскільки прогалини у знаннях роблять організацію вразливою за своєю суттю. Цей людський аспект захисту поширюється на безпеку облікових даних, де прості паролі, які легко вгадати, необхідно замінити на складні комбінації символів та підкріпити засобами багатофакторної автентифікації або біометричної верифікації…

Зрештою, ці заходи з контролю поведінки є ефективними лише за умови, що системи постійно оновлюються та оперативно встановлюються виправлення безпеки. Застаріле програмне забезпечення — це пряме запрошення для зловмисників скористатися відомими вразливостями. Зрештою, оскільки навіть один випадок порушення безпеки може мати руйнівні фінансові наслідки та завдати шкоди репутації всієї організації та її партнерів, підтримання проактивного та послідовного підходу до кібербезпеки є одним із найважливіших обов'язків у сучасному бізнес-середовищі». ***(Laura Varley. 4 easy ways to stay on top of cybersecurity in the workplace // Silicon Republic Knowledge & Events Management Ltd (https://www.siliconrepublic.com/advice/top-4-cybersecurity-measures-workplace-skills-balance). 24.04.2026).***

***

«Двопартійна група американських законодавців з обох палат Конгресу внесла на розгляд законопроект «Cyber Ready Workforce Act», покликаний вирішити проблему постійного дефіциту кадрів у сфері кібербезпеки шляхом доручення Міністерству праці створити грантову програму для підтримки розробки, розширення та впровадження зареєстрованих програм навчання у сфері кібербезпеки. Законопроект, авторами якого в Сенаті є Джекі Розен та Марша Блекберн, а в Палаті представників — Сьюзі Лі та Брайан Фіцпатрік, має на меті розширити шляхи до роботи у сфері кібербезпеки, виходячи за межі традиційних вищих навчальних закладів, та надати цільову підтримку підприємствам, вищим навчальним закладам та некомерційним організаціям, які потребують посилення кіберпотенціалу. Прихильники законопроекту наводять значні цифри дефіциту — близько 4 000 вакансій у штаті Невада та, за оцінками, майже півмільйона по всій країні — і стверджують, що цей дефіцит створює серйозні ризики для національної безпеки та економіки. Згідно з пропозицією, гранти Міністерства праці будуть надаватися посередникам у сфері зайнятості для розбудови потенціалу стажування, фінансування розробки навчальних програм та технічного навчання, а також маркетингу та рекрутингу, кар'єрного консультування та наставництва, а також підтримки учасників, такої як допомога з транспортом, житлом та доглядом за дітьми, одночасно заохочуючи координацію між бізнесом, некомерційними та академічними партнерами, щоб уникнути дублювання федеральних інвестицій». ***(Matt Bracken. Lawmakers renew push for Labor Department-backed cyber apprenticeship grants // CyberScoop (https://cyberscoop.com/labor-department-cybersecurity-workforce-apprenticeships/). 02.04.2026).***

***

«Хоча ради директорів компаній дедалі більше усвідомлюють важливість кібербезпеки, їхня здатність ефективно керувати цією сферою покращилася лише незначно, навіть попри те, що рівень кіберзлочинності продовжує зростати — про що свідчать дані ФБР, згідно з якими збитки від кіберзлочинності у 2024 році зросли на 33%... Водночас ради директорів залишаються в основному недостатньо підготовленими: серед 239 членів комітетів з кібербезпеки у 62 компаніях лише один мав офіційну освіту в галузі кібербезпеки, п'ятеро мали сертифікати, а лише 16 мали відповідний практичний досвід. Основні виклики включають цей брак експертизи, недостатню увагу до ризиків безпеки штучного інтелекту та помилкове переконання, що дотримання нормативних вимог дорівнює надійній безпеці…

Замість того, щоб намагатися стати технічними експертами або просто залучати фахівців з кібербезпеки, радам директорів рекомендується зосередитися на підборі та контролі за діяльністю компетентних керівників у сфері кібербезпеки, оцінювати їхню ефективність на прикладі реальних інцидентів або моделювань, а також забезпечувати регулярне стратегічне обговорення кіберризиків. Крім того, вони повинні розглядати штучний інтелект як можливість і як серйозну загрозу,

інтегруючи контроль безпеки у процес впровадження штучного інтелекту. Виходячи за межі простого дотримання вимог, ради директорів повинні надавати пріоритет кібербезпеці як ключовому елементу операційної стійкості та конкурентної переваги, включаючи управління ризиками у взаємопов'язаних партнерських мережах та ланцюгах постачання. Зрештою, ефективне управління кібербезпекою залежить від сильного лідерства, відповідальності керівництва та проактивного, орієнтованого на бізнес підходу, а не від покладання на технічні знання чи переліки вимог регуляторних органів». ***(Jeffrey Proudfoot, Stuart Madnick. Boards Are Falling Short on Cybersecurity // Harvard Business School Publishing (https://hbr.org/2026/04/boards-are-falling-short-on-cybersecurity). 02.04.2026).***

***

«Дослідники у сфері кібербезпеки, які проаналізували код та поведінку в мережі нещодавно випущеного мобільного додатка Білого дому, попереджають, що він регулярно надсилає дані користувачів, такі як IP-адреси, часові пояси та ідентифікатори пристроїв/сеансів, стороннім сервісам, не повідомляючи про це відкрито, як це зазвичай роблять більшість додатків. Додаток, який швидко став одним із найпопулярніших новинних додатків в App Store від Apple і який президент Трамп рекламував як пряме джерело новин адміністрації, покладається на зовнішніх постачальників для виконання ключових функцій, зокрема на OneSignal для push-повідомлень та Elfsight, російського постачальника віджетів; дослідники зазначили, що інтеграція Elfsight також оприлюднила особисту інформацію деяких співробітників Білого дому через додаток. Експерти повідомили NOTUS, що хоча збір даних сторонніми SDK є поширеною практикою, додаток Білого дому повинен відповідати вищим стандартам безпеки та прозорості, особливо в умовах підвищеної геополітичної напруженості, і вони розкритикували використання нефедеральних, несертифікованих стеків послуг замість урядових середовищ, таких як FedRAMP або GovCloud…

Головне занепокоєння викликає те, що «маніфест» конфіденційності додатка в App Store залишився порожнім — що натякає на відсутність збору даних — хоча дослідники стверджують, що дані насправді передаються третім сторонам, що, на їхню думку, вводить користувачів в оману і зазвичай загрожує видаленням додатка з магазинів додатків; Білий дім відповів, що інформація користувачів є «безпечною та захищеною», що використання третіми сторонами є стандартною практикою і що дані користувачів не зберігаються, при цьому поклавши відповідальність за конкретну проблему на Elfsight та заявивши, що додаток пройшов перевірку безпеки IT-відділом Білого дому. Дослідники також висловили занепокоєння щодо основних аспектів безпечного розроблення, зокрема щодо відсутності таких засобів захисту, як обфускація коду та прив'язка сертифікатів, і зазначили, що внутрішні файли додатка вказують на те, що розробником є 45Press — веб-компанія з Огайо, що спеціалізується на WordPress, яка, за повідомленнями, отримала контракт на 1,4 мільйона доларів на надання онлайн-послуг для Білого дому, що викликає сумніви щодо того, чи відображає ця версія достатній рівень експертизи в галузі мобільної

безпеки, навіть якщо вона не виглядає явно шкідливою». ***(Emily Kennard and Samuel Larreal. The White House App Is Riddled With Cybersecurity Vulnerabilities // NOTUS (https://www.notus.org/technology/trump-white-house-app-cybersecurity). 03.04.2026).***

***

«Агентство з кібербезпеки та безпеки інфраструктури (CISA) за останні 14 місяців зазнало різкого скорочення штату, втративши майже третину своїх співробітників — їхня кількість зменшилася з приблизно 3 300 до 2 400 — внаслідок низки звільнень за результатами випробувального терміну, припинення контрактів та добровільних звільнень. Це скорочення включає повне розформування «червоної команди» агентства та значні кадрові втрати у підрозділах з безпеки виборів та реагування на інциденти. На додаток до цього скорочення, у бюджетному запиті адміністрації Трампа на 2027 фінансовий рік, опублікованому 7 квітня 2026 року, пропонується додаткове скорочення на 707 мільйонів доларів. У разі прийняття цих скорочень операційний бюджет CISA знизиться приблизно до 2 млрд доларів, а ще 860 посад буде ліквідовано. Адміністрація характеризує цей крок як необхідну переорієнтацію на «основні завдання», такі як безпека федеральних мереж, тоді як критики засуджують його як навмисний розпуск агентства…

Пропонований бюджет спрямований саме на зовнішні операції CISA, що передбачають тісну співпрацю з партнерами. Серед ключових програм, які планується ліквідувати, — апарат з безпеки виборів, зокрема Центр обміну та аналізу інформації про виборчу інфраструктуру (EI-ISAC) та спеціалізовані радники з безпеки виборів, а також партнерства у сфері міжнародних відносин та офіси, відповідальні за координацію з операторами інфраструктури приватного сектору. Адміністрація обґрунтовує ці скорочення звинуваченням CISA у тому, що раніше вона зосереджувалася на «цензурі» через свої зусилля з протидії дезінформації, які відтоді було припинено. Хоча очікується, що основні функції, такі як федеральні системи виявлення вторгнень, збережуться, скорочення консультативної інфраструктури неминуче обмежить безкоштовну інформацію про загрози та підтримку, які CISA історично надавала меншим організаціям та місцевим органам влади, що не мають ресурсів безпеки корпоративного рівня. Хоча пропозиція стикається з двопартійним опором у Конгресі, значної шкоди можливостям та чисельності персоналу агентства вже завдано, що створює передумови для суперечливої бюджетної дискусії щодо того, чи буде агентство, що залишилося, скорочуватися ще більше». ***(Allison Steffens Herrera. Trump's FY27 budget would cut $700M from CISA and kill election security // Cogneve, INC (https://thenextweb.com/news/cisa-budget-cut-700-million-trump-fy27). 07.04.2026).***

***

«Згідно зі звітом ФБР про інтернет-злочини за 2025 рік, збитки від кіберзлочинності у Сполучених Штатах зросли до 20,877 млрд доларів, що на майже 26% більше, ніж у попередньому році. Майже 85% цих збитків припадає на шахрайство з використанням кібертехнологій, причому фішинг та спуфінг

залишаються найпоширенішими способами атак, на які надійшло понад 192 000 скарг. Хоча ці види шахрайства є найпоширенішими, інвестиційні афери, особливо ті, що пов'язані з криптовалютою, спричинили найбільші загальні збитки в доларовому еквіваленті, які сягнули 8,65 млрд доларів, що на 25% більше, ніж у 2024 році. Криптовалюта стала основним механізмом як для обману жертв, так і для відмивання незаконних коштів, фігуруючи у двох третинах п'ятірки категорій шахрайства з найбільшими збитками в доларовому еквіваленті…

Особливе занепокоєння у цих статистичних даних викликає зростання кількості випадків шахрайства щодо людей похилого віку, збитки від якого зросли до 7,748 млрд доларів, що на 59% більше, ніж у попередньому році. Люди похилого віку дедалі частіше стають жертвами фішингу, шахрайства під виглядом технічної підтримки та інвестиційних афер; при цьому варто відзначити, що кількість романтичних афер, спрямованих на цю демографічну групу, зросла на 30%, а кількість випадків видавання себе за представників державних органів майже подвоїлася. Таке зростання ефективності шахрайських схем зумовлене визначальною тенденцією 2025 року: розширеною інтеграцією генеративної штучної інтелекту та криптовалюти. Шахраї використовують складні, легкодоступні інструменти штучного інтелекту для клонування голосу, створення відео з використанням технології «діпфейк» та синтезу надзвичайно реалістичних зображень, що дозволяє їм масштабувати та персоналізувати свої атаки з безпрецедентною складністю…

Окрім збитків, яких зазнають окремі споживачі, ФБР наголошує на зростаючій системній загрозі для критичної інфраструктури. Сектор фінансових послуг наразі посідає третє місце серед секторів критичної інфраструктури, що найчастіше стають мішенями атак, а в усіх 16 визначених секторах інциденти, пов'язані з програмним забезпеченням-вимагачем та витоком даних, призвели до сукупних збитків на суму понад 261 мільярд доларів. Ці загрози стають дедалі витонченішими та пов'язані з суб'єктами, пов'язаними з державою, а глобальні конфлікти ще більше посилюють ситуацію. Оскільки технології продовжують випереджати законодавчі зусилля щодо запобігання шахрайству, ФБР наголошує, що освіта та інформування залишаються найефективнішими засобами захисту. Дослідження показують, що ймовірність того, що споживачі стануть жертвами шахрайства, знижується на 80%, якщо вони вже знають про нього, що підкреслює важливість проактивного інформування клієнтів — особливо людей похилого віку та вразливих верств населення — для стримування зростаючої хвилі витончених кіберзлочинів». ***(Taylor J. Bandy, Roxanne Rehm, Elizabeth C. Wheeler. FBI Releases Its 2025 Internet Crime Report and Highlights Significant Cyber Threats to Financial Institutions and Their Customers // Bressler, Amery & Ross, P.C. (https://www.bressler.com/news-fbi-releases-its-2025-internet-crime-report-and-highlights-significant-cyber-threats-to-financial-institutions-and-their-customers). 16.04.2026).***

***

«Кіберзахист еволюціонує від абстрактної, централізованої інституційної функції до більш конкретного, мобільного та оперативно інтегрованого

потенціалу. Поставка перших стандартизованих, мобільних наборів засобів кіберзахисту Кіберкомандуванням США до мереж партнерів є відчутним кроком у цьому напрямку, що дає змогу спеціалізованим командам виявляти, аналізувати та реагувати на загрози безпосередньо в передових районах, а не з віддалених центрів. Цей розвиток подій відповідає більш широкому визнанню того, що космічні системи зараз є критичною інфраструктурою, яка піддається кіберзагрозам, підкреслюючи, наскільки цифрові операції залежать від розподілених фізичних архітектур. У глобальному масштабі перехід відбувається нерівномірно: тоді як деякі країни зберігають централізовані моделі, інші — зокрема Сполучені Штати — рухаються в напрямку тіснішої інтеграції з військовими операціями через місії передової присутності в мережах союзників, де кіберкоманди активно вистежують загрози у місцях їхнього виникнення… На практиці ці мобільні «кібернабори» поєднують в собі захищене обладнання (захищені ноутбуки, портативні сервери, мережеве обладнання) зі спеціалізованим програмним забезпеченням для аналізу трафіку, виявлення аномалій та цифрової криміналістики, що дозволяє швидко розгортати їх у неоднорідних або незнайомих середовищах без переривання оперативної діяльності. Це відображає зміну доктрини, згідно з якою кіберпростір розглядається як активний експедиційний потенціал — який планується, підтримується та забезпечується так само, як і інші оперативні функції, — водночас створюючи нові вимоги до логістики та забезпечення. Однак така мобільність також збільшує залежність від складних гібридних інфраструктур, що поєднують наземні та космічні сегменти, зокрема супутникові групи на низькій навколоземній орбіті, які слугують як критично важливими факторами, так і новими джерелами вразливості через слабкі місця в наземних станціях, ланцюгах постачання та каналах зв'язку… Як наслідок, кіберзахист більше не обмежується лише захистом інформаційних систем; тепер він вимагає забезпечення безпеки всієї взаємопов'язаної екосистеми фізичних та цифрових активів, що робить здатність розгортати, підтримувати та захищати ці можливості центральним стратегічним питанням». ***(Cyber defense is moving into the field: from United States deployable kits to satellite constellations // Defense Innovation Review (DIR) (https://defenseinnovationreview.com/cyber-defense-is-moving-into-the-field-from-united-states-deployable-kits-to-satellite-constellations/). 20.04.2026).***

***

«Шон Планкі, кандидат президента Дональда Трампа на посаду глави Агентства з кібербезпеки та безпеки інфраструктури (CISA), відкликав свою кандидатуру через 13 місяців, завдавши чергового серйозного удару по агентству, яке й так переживає складні часи, та зусиллям адміністрації Трампа щодо впровадження сміливої нової програми у сфері кібербезпеки… У листі до Білого дому та Міністерства внутрішньої безпеки Планкі заявив, що стало очевидно, що Сенат не затвердить його кандидатуру, водночас висловивши підтримку майбутньому кандидату на заміну, якого запропонує Трамп. Його призначення затягнулося через заперечення сенаторів з обох партій, зокрема сенатора Рона Вайдена (демократ від штату Орегон), який висловив незгоду з відмовою CISA оприлюднити звіт про вразливості в системі безпеки

телекомунікацій, та сенатора Ріка Скотта (республіканець від штату Флорида), який виступив проти рішення щодо контракту з Береговою охороною у своєму штаті… Попереднє безцеремонне звільнення Планкі з його високої посади в DHS у березні ще більше погіршило його перспективи. В результаті CISA продовжує працювати без постійного директора, а обов'язки виконує заступник директора Нік Андерсен. До своєї номінації Планкі обіймав високі посади в галузі технологій та кібербезпеки як у приватному секторі, так і під час першого терміну Трампа, зокрема в Раді національної безпеки та Міністерстві енергетики». ***(Eric Geller. Trump's CISA director pick withdraws after tumultuous nomination // TechTarget, Inc. (https://www.cybersecuritydive.com/news/cisa-sean-plankey-withdraw-nomination/818266/). 22.04.2026).***

***

«Канадський центр кібербезпеки запустив ініціативу «Стійкість критичної інфраструктури та реагування на ескалацію загроз» (CIREN), щоб допомогти організаціям, відповідальним за надання життєво важливих послуг, підготуватися до серйозних кіберзбоїв та забезпечити безперебійну роботу під час них. Центр зазначив, що кіберінциденти стали частішими, руйнівнішими та витонченішими через активніше використання штучного інтелекту та автоматизації для поширення зловмисної діяльності, а також через геополітичну нестабільність, яка підвищує ризик державних кібероперацій, спрямованих проти секторів критичної інфраструктури, таких як енергетика, телекомунікації, транспорт та водопостачання. Такі зриви можуть призвести до тривалих перебоїв у наданні послуг, значних економічних втрат, ризиків для здоров'я та безпеки населення, а в крайніх випадках навіть до людських жертв, одночасно підриваючи національний суверенітет…

З метою протидії цим загрозам CIREN окреслює основні заходи з підготовки, зокрема підготовку критично важливих систем до автономної роботи протягом періоду до трьох місяців, розробку та тестування планів реагування на випадок автономної роботи, а також створення планів відновлення систем після серйозних кіберінцидентів…

Ця ініціатива є частиною більш широкого комплексу консультацій та рекомендацій центру щодо критичної інфраструктури, який супроводжується регулярними брифінгами, спільними форумами, бюлетенями про загрози, брифінгами з оцінки кіберризиків, а також обміном показниками компрометації для сприяння виявленню вторгнень. У 2024 році центр надіслав понад 300 попереджувальних повідомлень про загрозу зараження програмним забезпеченням-вимагачем та опублікував численні рекомендації, попередження та оперативні повідомлення про кіберзагрози, виходячи з їхньої терміновості та важливості». ***(Jacqueline So. Canadian Centre for Cyber Security rolls out initiative focused on cyber incident response // KM Business Information (https://www.lexpert.ca/news/infrastructure-law/canadian-centre-for-cyber-security-rolls-out-initiative-focused-on-cyber-incident-response/394147). 21.04.2026).***

***

«Згідно з Індексом кіберготовності малого та середнього бізнесу (SMB Cyber Readiness Index) від ESET за 2026 рік для Північної Америки, складеним на основі опитування 700 осіб, відповідальних за прийняття рішень у сфері кібербезпеки в організаціях із кількістю кінцевих точок від 25 до 1000 у США та Канаді, малі та середні підприємства виявляють вищу впевненість у своїй кіберстійкості, ніж будь-коли раніше, навіть попри те, що атаки залишаються поширеним явищем і значною мірою зумовлені базовими проблемами, яких можна уникнути. У США 87% малих та середніх підприємств відчувають принаймні «деяку» впевненість у своїй кіберстійкості, тоді як у Канаді так вважають 83%. При цьому рівень впевненості ще вищий серед компаній, які вже зазнавали атак більше ніж один раз протягом минулого року (91% у США та 88% у Канаді)…

Рівень поширення кіберстрахування також є високим: 86 % малих та середніх підприємств (МСП) у США та 78 % канадських МСП мають відповідний страховий захист, а страхові компанії дедалі сильніше впливають на заходи безпеки — 55 % застрахованих МСП у США та 41 % застрахованих канадських МСП зобов'язані впроваджувати конкретні заходи як умову надання страхового покриття. Незважаючи на це, основними причинами інцидентів залишаються традиційні слабкі місця: фішинг (27% у США, 21% у Канаді), відсутність моніторингу безпеки (27% у США, 20% у Канаді), незахищені вразливості (25% у США) та слабкі паролі (20% у Канаді)…

Шкідливе ПЗ на базі штучного інтелекту очолює список майбутніх проблем (32 % у США, 34 % у Канаді), але фактичні порушення безпеки все ще зумовлені людськими помилками та базовими прогалинами. Навчання залишається головним пріоритетом для інвестицій: понад 90 % малих та середніх підприємств оцінюють його як «критично важливе» або «дуже важливе», а майже половина з них зараз впроваджує симуляції фішингових атак... Загалом, результати дослідження свідчать про те, що, хоча рівень впевненості зростає, організації повинні й надалі зосереджуватися на таких фундаментальних аспектах, як запобігання фішингу, моніторинг та встановлення виправлень, щоб вирішити ті проблеми, які можна запобігти і які все ще є причиною більшості інцидентів». ***(Josh Recamara. SMB cyber attacks now 'new normal' as confidence climbs: Report // KM Business Information Canada Ltd. (https://www.insurancebusinessmag.com/ca/news/cyber/smb-cyber-attacks-now-new-normal-as-confidence-climbs-report-572252.aspx). 20.04.2026).***

***

«Нова кіберстратегія Білого дому містить фундаментальний парадокс, поєднуючи чітке бачення стратегічної конкуренції та національної стійкості з політичними рішеннями, які активно підривають державний потенціал, необхідний для їх реалізації. У загальному плані стратегія правильно визначає кіберпростір як сферу тривалої конфронтації, а не як просте питання дотримання вимог. Наголошуючи на стійкості — здатності поглинати удари та швидко відновлювати основні послуги — адміністрація визнає, що здатність до відновлення є життєво важливою формою стримування. Крім того, прийняття

стратегією наступальної кіберпотужності як інструменту формування поведінки супротивника знаменує необхідний перехід від пасивної оборони до активної боротьби політичної волі…

Однак ця стратегічна логіка суперечить реальності, що характеризується значним інституційним занепадом. Адміністрація нещодавно скоротила штат Агентства з кібербезпеки та безпеки інфраструктури (CISA) приблизно на третину та припинила фінансування важливих державних і місцевих ініціатив з обміну інформацією, таких як Міждержавний центр обміну та аналізу інформації (MS-ISAC). Ці скорочення завдають удару по тій самій «сполучній тканині», від якої залежить національна стійкість. Знищення федеральної інфраструктури для планування, аналізу та координації при одночасному вихвалянні стійкості є стратегічно непослідовним, оскільки національне відновлення не може бути досягнуте лише за допомогою риторики; для цього потрібні планувальники, навчання та надійні канали зв'язку з промисловістю.

Особливо суперечливим елементом стратегії є пропозиція «розв'язати руки приватному сектору» шляхом створення стимулів для приватних компаній з метою виявлення та зриву діяльності ворожих мереж. Хоча приватний сектор володіє кращими телеметричними можливостями та швидкістю, такий підхід несе ризик створення сучасної форми «кіберпіратства». Без суворих обмежень приватні суб'єкти можуть ставити комерційні інтереси вище за національну безпеку, помилково ідентифікувати інфраструктуру або спричинити ненавмисні побічні збитки та ескалацію конфлікту. Щоб відповідально мобілізувати приватні кіберресурси, уряд повинен відійти від моделі загального заохочення на користь формальної системи делегування повноважень, що характеризується чіткими категоріями місій, стандартами перевірки цілей та обов'язковим наглядом з боку Конгресу…

Зрештою, успіх стратегії залежить від того, чи залишиться вона лише «глянцевою брошурою», чи перетвориться на стійку доктрину. Щоб досягти успіху, адміністрація повинна розглядати забезпечення стійкості, а не вжиття заходів у відповідь, як своє головне завдання та припинити скорочувати фінансування федеральних відомств, які координують заходи реагування на національному рівні. Резилієнтна кіберпозиція вимагає структурованої державно-приватної допоміжної системи, орієнтованої на безперервність функціонування державних органів, підкріпленої стратегічним керівництвом та фінансовими грантами. Хоча приватний сектор є незамінним партнером, він не може замінити компетентний федеральний уряд. Головним викликом для адміністрації буде збереження інституційного механізму, необхідного для втілення її амбітної кібервізії у функціональну реальність». ***(Jesse Humpal, Alexander Noyes, Emily Valentine. Resilience Without Capacity: The Fatal Flaw in America's New Cyber Strategy // Metamorphic Media (https://warontherocks.com/resilience-without-capacity-the-fatal-flaw-in-americas-new-cyber-strategy/). 22.04.2026).***

***

«Велика Британія проводить наймасштабнішу за останні майже десять років реформу законодавства у сфері кібербезпеки, запроваджуючи законопроект про кібербезпеку та стійкість (CSRB) — законодавче оновлення, яке кардинально розширює та посилює рамки Закону про мережеві та інформаційні системи (NIS) 2018 року. Зараз законопроект CSRB проходить розгляд у парламенті. Він підвищує регуляторні вимоги до операторів критичної інфраструктури, роблячи сильний акцент на національній стійкості та включаючи майже всі системи операційних технологій (OT) у сферу свого застосування…

Основні положення законопроекту передбачають значне розширення сфери регуляторного нагляду з метою охоплення більшої кількості середовищ операційних технологій (OT) — таких як центри обробки даних та постачальники керованих послуг — запровадження обов'язкового повідомлення про кіберінциденти, а також встановлення більш суворих і ефективних санкцій, зокрема заходів, що дозволяють регуляторним органам стягувати витрати на нагляд безпосередньо з операторів, діяльність яких вони контролюють. Для орієнтування в цих посилених вимогах Рамка кібероцінки (CAF) Національного центру кібербезпеки (NCSC) слугує безцінним посібником для власників активів OT. CAF визначає основні принципи управління ризиками безпеки, такі як ведення повного та постійно оновлюваного реєстру активів операційних технологій (OT), а також захисту від кібератак за допомогою надійної системи управління вразливостями, адаптованої до специфічних особливостей промислових середовищ. Крім того, у документі наголошується на важливості виявлення інцидентів у сфері кібербезпеки за допомогою спеціалізованого моніторингу безпеки OT та проактивного пошуку загроз на основі аналітичних даних у конвергентних мережах IT/OT…

Оскільки впровадження CSRB є питанням не «чи», а «коли», власникам операційних активів настійно рекомендується вже зараз розпочати підготовку, привівши свої системи у відповідність до NCSC CAF, підвищивши прозорість активів та розширивши свої можливості з моніторингу та звітності. Таким чином вони зможуть перетворити те, що може сприйматися як обтяжливий процес забезпечення відповідності вимогам, на реальну конкурентну та операційну перевагу». ***(Tom Westenberg. The UK Cyber Security and Resilience Bill: What OT Asset Owners Need to Know Now // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/opinions/uk-cyber-bill-what-ot-it-needs-now/). 03.04.2026).***

***

«Грецькі судноплавні компанії терміново переглядають рівень кіберстійкості своїх IT-систем після отримання рекомендацій від Національного агентства з кібербезпеки Греції, що спонукало їх провести профілактичне сканування на наявність хакерських атак, шкідливого програмного забезпечення та вразливостей. Це пов'язано з побоюваннями, що загострення геополітичної напруженості та нещодавня кіберактивність, пов'язана з Іраном, поширюються на цифрові системи, якими користуються оператори, менеджери та власники. Лідери галузі заявляють, що кіберризик став

повсякденною операційною проблемою, оскільки вразливість судноплавства зростає через збільшення потоків даних між суднами та берегом, хмарні послуги та супутниковий зв'язок, що збільшує кількість точок входу для зловмисників; як наслідок, компанії зосереджуються на виявленні слабких місць, посиленні засобів контролю, таких як брандмауери, покращенні моніторингу та внутрішнього обміну інформацією, а також на навчанні як берегового персоналу, так і екіпажів, які залишаються першою лінією оборони…

Це попередження узгоджується з більш загальними висновками, викладеними в посібнику Cytur з реагування на кіберзагрози в морській галузі на 2026 рік, який містить перелік заходів для конкретного сектору та послідовні протоколи дій у разі інцидентів (зокрема щодо глушіння/підробки сигналів GPS, крадіжки даних та програм-вимагачів), а також повідомляє про 103-відсотковий річний сплеск загроз, спрямованих на інтерфейс IT/операційних технологій у період з 2024 по 2025 рік, поряд із зростанням кількості атак на ланцюги постачання та підробкою активів, що може спричинити збій у роботі багатьох суден. Оскільки починають поставлятися нові судна, замовлені відповідно до кібервимог UR E26/E27 Міжнародної асоціації класифікаційних товариств, дотримання вимог під час морських випробувань може стати умовою поставки, тоді як інші експерти попереджають, що без кращої видимості та контролю над тим, що працює на борту, галузь, ймовірно, зіткнеться з більшою кількістю кіберобману — шахрайських інструкцій, маніпуляцій у комунікаціях та критичних для безпеки операційних помилок — та все більш імовірним серйозним інцидентом». ***(Martyn Wingrove. Iran-backed cyber incidents drive shipping to rescan onboard systems // Riviera Maritime Media Ltd. (https://www.rivieramm.com/news-content-hub/iran-backed-cyber-incidents-drive-shipping-to-rescan-onboard-systems-88405). 09.04.2026).***

***

«Європейська комісія розслідує кібератаку, виявлену 24 березня, яка зачепила хмарну інфраструктуру, на якій розміщена платформа Europa.eu, де знаходяться веб-сайти Комісії та інших інституцій ЄС; Комісія заявила, що швидко локалізувала інцидент, не порушивши доступність сайту, і що її внутрішні системи не зазнали впливу, проте попередні висновки вказують на викрадення певних даних, і про це повідомляються потенційно постраждалі організації Союзу. Група хакерів ShinyHunters публічно взяла на себе відповідальність і додала Комісію до свого сайту з витоками, стверджуючи, що злом був набагато масштабнішим, хоча Комісія не підтвердила повний обсяг цих тверджень…

У повідомленні про прозорість, опублікованому 2 квітня, CERT-EU з високим ступенем впевненості дійшов висновку, що злом був пов’язаний із компрометацією ланцюга постачання, причому початковий доступ було отримано через інцидент у ланцюзі постачання Trivy, який приписують TeamPCP, що призвело до витоку близько 91,7 ГБ (у стисненому вигляді) даних із зламаного облікового запису AWS; викрадені дані містять особисту інформацію, таку як імена, адреси електронної пошти та вміст електронних листів, були опубліковані ShinyHunters 28 березня і можуть стосуватися даних щонайменше 29 інших суб’єктів Союзу. CERT-EU

попередив, що зростання кількості компрометацій ланцюга постачання становить значну загрозу, та закликав організації впровадити рекомендовані заходи щодо її мінімізації». ***(European Commission investigates cyber attack on its websites; CERT-EU publishes recommendations // DataBreaches LLC (https://databreaches.net/2026/04/03/european-commission-investigates-cyber-attack-on-its-websites-cert-eu-publishes-recommendations/). 03.04.2026).***

***

«Закон ЄС про кіберстійкість (CRA) — це не просто норма, що регулює дотримання вимог, а кардинальна зміна підходу до проектування цифрових продуктів, особливо систем біометричного контролю доступу. Він робить кібербезпеку невід'ємною частиною архітектури продукту, процесу оновлення та управління вразливостями протягом усього його життєвого циклу, а це означає, що рішення щодо використання хмарних технологій, віддаленого управління та підключення тепер мають прямі регуляторні наслідки. Закон ставить під сумнів давні звички галузі щодо максимізації видимості, централізованого контролю, реєстрації та віддаленого налаштування, оскільки кожен доданий інтерфейс або зовнішня залежність збільшує площу атаки та може суперечити цілям стійкості…

Що стосується біометричних систем, які базуються на ліцензуванні, базах даних та рівнях віддаленого обслуговування, CRA спонукає виробників до створення конструкцій, що є більш автономними, передбачуваними та обмеженими щодо зовнішнього доступу, з меншою кількістю підключень і більш жорстким контролем оновлень. Хоча офіційний юридичний обов'язок покладається переважно на виробників, які випускають продукцію на ринок ЄС, вплив поширюється на інтеграторів, дистриб'юторів та кінцевих користувачів, які також починають переоцінювати кіберризики та зрілість постачальників у рамках більш широких систем, таких як NIS2. Зрештою, CRA змушує змінити філософію проектування: замість створення систем, які завжди доступні та керовані ззовні, виробники повинні створювати системи, які навмисно обмежені та безпечні за своєю конструкцією». ***(Eduard de Knegt. EU Cyber Resilience Act reshapes biometric access systems // Biometrics Research Group, Inc. (https://www.biometricupdate.com/202604/eu-cyber-resilience-act-reshapes-biometric-access-systems). 06.04.2026).***

***

«Наразі парламент Нідерландів завершує роботу над Законом про кібербезпеку (Cbw), який імплементує Директиву ЄС NIS2 і має на меті встановити обов'язкові стандарти кібербезпеки для критично важливих та важливих суб'єктів господарювання. З огляду на зростання кількості гучних випадків витоку даних, Cbw встановлює суворий «обов'язок дбайливості» (стаття 21), що вимагає від організацій впровадження та документування відповідних технічних та організаційних заходів. До них належать комплексне управління ризиками, реагування на інциденти, безпека ланцюга постачання, кібергігієна та регулярні оцінки ефективності заходів безпеки. Хоча організації можуть використовувати міжнародні стандарти, такі як ISO 27001, для забезпечення

відповідності вимогам, уряд наголошує, що сама лише сертифікація є недостатньою для повного виконання вимог Cbw…

Окрім технічних заходів, цей закон значно підвищує відповідальність керівництва компаній. Згідно зі статтею 24, остаточну відповідальність за дотримання вимог несе керівництво, яке здійснює повсякденне управління, а саме виконавчі директори, а не наглядові ради. Крім того, законодавство поширює потенційну відповідальність не лише на офіційних директорів, а й на «фактичних» керівників — осіб, які фактично здійснюють контроль над прийняттям рішень та дотриманням вимог у організації. Оскільки наглядові органи, такі як Національна інспекція цифрової інфраструктури (RDI), готуються до забезпечення дотримання цих правил, уряд настійно рекомендує організаціям негайно розпочати впровадження рамок Cbw, враховуючи, що ризики кіберінцидентів вже є реальною та нагальною проблемою». ***(Machteld Robichon and Bente van Kan. The Cyber Security Act in practice: the duty of care, ISO certification and the role of the board // bureau Brandeis (https://bureaubrandeis.com/the-cybersecurity-act-in-practice-the-duty-of-care-iso-certification-and-the-role-of-the-board/). 07.04.2026).***

***

«3 квітня 2026 року в Польщі набув чинності змінений Закон про національну систему кібербезпеки, спрямований на імплементацію Директиви ЄС NIS2. Цей закон суттєво розширює зобов'язання у сфері кібербезпеки для критично важливих секторів, таких як енергетика, транспорт, виробництво та цифрові послуги, поширюючи відповідальність не лише на саму організацію, а й на її ланцюг постачання. За новою системою суб'єкти господарювання, класифіковані як такі, що мають стратегічне значення або є важливими, повинні визначити ключових постачальників, оцінити ризики, які вони становлять, та управляти цими ризиками за допомогою структурованих внутрішніх політик, причому контракти з постачальниками стають ключовим інструментом забезпечення відповідності завдяки положенням щодо аудитів, субпідрядників та повідомлення про інциденти. Оцінка ризиків має бути постійною, а не одноразовою процедурою під час налагодження співпраці, тому компаніям знадобиться постійний моніторинг, періодичні перегляди та перевірка того, чи дотримуються постачальники узгоджених стандартів…

Реформа також покладає особисту відповідальність на керівні органи, перетворюючи кібербезпеку на питання, що вирішується на рівні ради директорів, та передбачаючи для організацій і керівників значні санкції, зокрема штрафи у розмірі до 10 млн євро або 2 % від глобального обороту для суб'єктів, що мають особливе значення, 7 млн євро або 1,4 % для важливих суб'єктів, а також особисті штрафи для керівників у розмірі до 300 % місячної заробітної плати. Перехідні терміни надають суб'єктам, що нещодавно потрапили під дію реформи, 12 місяців на впровадження системи управління інформаційною безпекою, шість місяців на подання заявки на реєстрацію, а ключовим суб'єктам — 24 місяці на проведення першого аудиту кібербезпеки. Загальний висновок полягає в тому, що регулювання кібербезпеки в Польщі тепер глибоко зачіпає відносини з постачальниками та управління, роблячи управління ланцюгом поставок центральною частиною

дотримання законодавчих вимог та контролю ризиків». ***(Marcin Bejm, Łukasz Szatkowski, Karol Jaworecki and Marta Klopotowska. Cybersecurity in the supply chain: what NIS2 changes in Poland // CMS Legal (https://cms.law/en/pol/legal-updates/cybersecurity-in-the-supply-chain-what-nis2-changes-in-poland). 09.04.2026).***

***

«За словами Річарда Горна, виконавчого директора Національного центру кібербезпеки (NCSC), Велика Британія стикається із серйозною і дедалі більшою загрозою з боку «масштабних атак хактивістів», особливо якщо країна опиниться втягнутою в геополітичний конфлікт. Виступаючи на конференції CyberUK, Горн попередив, що такі атаки можуть мати наслідки та рівень складності, подібні до нещодавніх гучних інцидентів із використанням програм-вимагачів, які паралізували роботу таких великих компаній, як Royal Mail та Jaguar Land Rover, але без можливості сплатити викуп для відновлення систем… Він наголосив, що зараз саме національні держави є причиною найсерйозніших кіберінцидентів і що Велика Британія опинилася в епіцентрі «ідеального шторму», спричиненого стрімкими технологічними змінами — зокрема появою моделей штучного інтелекту, здатних швидко виявляти вразливі місця, — та зростанням геополітичної напруженості. Щоб протистояти цій загрозі, Горн закликав усі організації державного та приватного секторів включити кібербезпеку до своєї корпоративної місії, усвідомити весь обсяг ризиків, на які вони наражаються, та розробити стратегію глибокої оборони, готуючись до майбутнього, в якому просто «викупити» себе від атаки не буде можливим». ***(Dan Milmo. UK could face 'hacktivist attacks at scale', says head of security agency // Guardian News & Media Limited (https://www.theguardian.com/technology/2026/apr/22/uk-hacktivist-attacks-at-scale-security-agency). 22.04.2026).***

***

«Британські підприємства закликають посилити заходи кібербезпеки на випадок хакерських атак, пов'язаних із Китаєм, які використовують повсякденні підключені до Інтернету пристрої для створення прихованих ботнетів, що застосовуються для шпигунства та кібератак. Національний центр кібербезпеки Великобританії (NCSC) спільно з агентствами дев'яти країн-союзників виявив «істотну зміну» в тактиці Китаю, спрямовану на компрометацію вразливих маршрутизаторів, принтерів, веб-камер та інших пристроїв Інтернету речей (IoT) у невеликих офісах та домашніх офісах з метою приховування джерела атак. Ці захоплені пристрої функціонують аналогічно до домашніх проксі-мереж, дозволяючи зловмисникам маскувати своє місцезнаходження та використовувати нічого не підозрюючі домогосподарства або малі підприємства як відправні точки для атак на великі корпоративні системи або системи критичної інфраструктури…

NCSC вважає, що більшість зловмисників, пов'язаних із Китаєм, використовують такі приховані мережі, які, за повідомленнями, створюють і підтримують приватні китайські компанії; одним із прикладів є зараження 200 000 пристроїв по всьому світу. Відому групу Volt Typhoon пов'язують із проникненням у ключові сектори інфраструктури США, зокрема залізничний, авіаційний та

водопостачальний. Хоча це попередження не спрямовано на окремих споживачів, воно закликає організації скласти карту своїх ІТ-середовищ, забезпечити безпеку підключень до широкосмугових мереж для споживачів, впровадити багатофакторну автентифікацію для віддаленого доступу, обмежити підключення зовнішніх пристроїв та забезпечити оновлення програмного забезпечення для зменшення вразливостей. Це попередження відображає зростаючу стурбованість щодо кібероперацій, що фінансуються державою, які використовують незахищене споживче обладнання в рамках складних глобальних шпигунських кампаній». ***(Dan Milmo. Chinese hackers using everyday devices to target UK firms, warns cybersecurity agency // Guardian News & Media Limited (https://www.theguardian.com/technology/2026/apr/23/china-cyber-hacker-using-everyday-devices-hack-uk-firms). 23.04.2026).***

***

«ENISA, Агентство Європейського Союзу з кібербезпеки, запустило оновлену Національну рамку можливостей у сфері кібербезпеки (NCAF 2.0) — структуровану методологію та онлайн-інструмент, призначені для надання допомоги державам-членам ЄС в оцінці та посиленні реалізації їхніх національних стратегій у сфері кібербезпеки (NCSS). Ця рамка дозволяє національним органам влади оцінювати ступінь зрілості своїх цілей у сфері кібербезпеки, виявляти сильні сторони та прогалини, визначати пріоритети вдосконалень та відстежувати прогрес як на стратегічному, так і на оперативному рівнях… На рівні ЄС NCAF 2.0 забезпечує загальну еталонну модель, яка сприяє взаємному навчанню, обміну передовим досвідом та узгодженню з мінливим законодавством ЄС у сфері кібербезпеки, включаючи Директиву NIS2. Вона також допомагає державам-членам готуватися до процесу добровільного взаємного огляду відповідно до статті 19 Директиви NIS2. Ця концепція в першу чергу призначена для політиків, експертів та урядовців, відповідальних за розробку, впровадження та оцінку національних стратегій у сфері кібербезпеки… Поєднуючи гнучкість із структурованою оцінкою, NCAF 2.0 має на меті зміцнити колективну стійкість Європейського Союзу до кіберзагроз, водночас забезпечуючи можливість адаптації до національних умов та пріоритетів». ***(Assess your National Cybersecurity Capabilities and Maturity with the updated ENISA Framework // European Union Agency for Cybersecurity (https://www.enisa.europa.eu/news/assess-your-national-cybersecurity-capabilities-and-maturity-with-the-updated-enisa-framework). 22.04.2026).***

***

Австралія та Нова Зеландія

«Австралія ухвалила історичний Закон про кібербезпеку 2024 року, який отримав королівське схвалення наприкінці листопада 2024 року після тривалих парламентських дебатів. Законодавство запроваджує обов’язкове повідомлення про значні кіберінциденти до Австралійського управління зв’язку

(ASD) у стислі терміни — з вимогою провести попередню оцінку протягом 24 годин та надати повний звіт протягом 72 годин — для організацій у критично важливих секторах, зокрема енергетики, телекомунікацій, фінансів, охорони здоров'я та транспорту. Воно також обмежує виплати викупу за програмним забезпеченням-вимагачем з боку суб'єктів Співдружності та визначених операторів критичної інфраструктури, вимагаючи попереднього дозволу від міністра внутрішніх справ, та розширює регуляторний нагляд шляхом розробки галузевих кодексів практики з кібербезпеки… Ці кодекси, які будуть розроблені у співпраці з представниками галузі та під наглядом Міністерства внутрішніх справ, визначатимуть вимоги щодо реагування на інциденти, управління вразливостями та безпеки ланцюгів постачання; перші проекти планується винести на громадське обговорення в середині 2025 року, а термін їхнього впровадження становитиме 12 місяців після цього. Закон посилює роль координатора з питань кібербезпеки, створює Національне кібербюро як центральний центр координації політики та кризових ситуацій, а також сприяє більш активному обміну інформацією між урядом та операторами приватного сектору. Реакція зацікавлених сторін була в основному позитивною: Бізнес-рада Австралії вітає чіткість положень, водночас закликаючи до пропорційних вимог та підтримки малих і середніх підприємств; фахівці з кібербезпеки в цілому підтримують рух у напрямку підзвітності та прозорості, хоча багато хто наголошує на необхідності належного фінансування регуляторних органів, таких як ASD та ACSC (Австралійський центр кібербезпеки)…

На міжнародному рівні цей закон розглядається як крок, що приводить Австралію у відповідність до аналогічних законодавчих систем, таких як американський CIRCIA та оновлене законодавство Японії щодо критичної інфраструктури, що позиціонує країну як регіонального лідера у сфері кіберуправління. Організаціям зараз рекомендується оцінити, чи поширюються на них нові правила, переглянути та оновити плани реагування на інциденти й договори з постачальниками, а також підготуватися до періодичної сертифікації відповідності вимогам. На 2025 рік заплановано проведення інформаційних кампаній для громадян з питань кібергігієни та повідомлення про інциденти, а перші основні терміни дотримання вимог встановлено на середину 2026 року. Загалом Закон про кібербезпеку 2024 року є значним переходом від добровільних рекомендацій до обов'язкових стандартів, спрямованих на посилення національної кіберстійкості та координації в умовах зростаючих цифрових загроз». ***(Linda Park. Australia Cyber Security Act: New Ransomware & Incident Reporting Rules // World Today Journal (https://www.world-today-journal.com/australia-cyber-security-act-new-ransomware-incident-reporting-rules/). 21.04.2026).***

***

«Австралійський Центр кібербезпеки та безпеки інфраструктури (CISC) роз'яснив, як регуляторні зобов'язання, передбачені Законом про безпеку критичної інфраструктури 2018 року, покликані інтегрувати управління ризиками, готовність до надзвичайних ситуацій та стійкість у повсякденну діяльність власників та операторів критичної інфраструктури. Відповідно до

зобов’язання щодо повідомлення про інциденти кібербезпеки (NSCI), передбаченого частиною 2B Закону, яке зазвичай називають обов’язковим повідомленням про кіберінциденти (MCIR), суб’єкти господарювання повинні повідомляти Міністерству внутрішніх справ про інциденти кібербезпеки — у тому числі ті, що пов’язані зі штучним інтелектом — які мають значний або істотний вплив на критичні активи, що дозволяє уряду формувати консолідовану картину національних загроз та реагувати на них у режимі реального часу…

Ця система вимагає від відповідальних суб’єктів надавати оперативну інформацію, підтримувати програми управління ризиками та покращувати обмін інформацією між галуззю та урядом, причому режим регулювання масштабується відповідно до критичності активів і накладає посилені зобов’язання на найважливіші системи. CISC надав знеособлені приклади нещодавніх інцидентів, пов’язаних зі штучним інтелектом, зокрема випадок, коли співробітник з привілейованим доступом встановив на хості бази даних кілька розширень AI Visual Studio Code, що підключалися до зовнішніх платформ штучного інтелекту, а також випадок, коли співробітник завантажив до ChatGPT конфіденційні документи, що містили дані про користувачів з привілейованим доступом; обидва випадки викликали занепокоєння щодо витоку даних та управління ними. З метою мінімізації ризиків, пов’язаних зі штучним інтелектом, CISC рекомендує застосовувати перевірені практики кібербезпеки, викладені в «Посібнику з інформаційної безпеки» Австралійського управління радіозв’язку, приділяючи особливу увагу питанням управління, безпечного адміністрування систем, підвищення обізнаності персоналу, а також забезпеченню того, щоб системи штучного інтелекту були безпечними, керованими, підлягали людському нагляду та використовувалися етично й відповідально. На оперативному рівні це передбачає можливість аудиту адміністративних процесів, використання базових налаштувань безпеки, запуск виключно перевіреного програмного забезпечення, а також навчання персоналу з урахуванням їхніх посадових обов’язків щодо загроз, пов’язаних зі штучним інтелектом…

Агентство також проводить консультації щодо реформ, спрямованих на посилення повноважень міністерських керівництв відповідно до Закону про SOCI, щоб забезпечити швидше та рішучіше реагування уряду під час серйозних кіберінцидентів, які можуть спричинити ланцюгові порушення у різних секторах та істотно вплинути на національну безпеку, економічну стабільність або функціонування життєво важливих служб. Загалом, ця система має на меті забезпечити стійкість критичної інфраструктури до різноманітних загроз, зокрема кібератак, з урахуванням взаємопов’язаного характеру сучасних систем». ***(Anna Ribeiro. Australia’s CISC tightens cyber reporting rules to capture AI-driven incidents in critical infrastructure // Industrial Cyber (https://industrialcyber.co/regulation-standards-and-compliance/australias-cisc-tightens-cyber-reporting-rules-to-capture-ai-driven-incidents-in-critical-infrastructure/). 22.04.2026).***

***

«Опитування, проведене компанією Datacom серед 714 керівників служб безпеки в Новій Зеландії та Австралії, виявило значний розрив між

впевненістю у власних кіберможливостях та фактичною готовністю до відновлення роботи після серйозних інцидентів. Хоча 73% респондентів з Нової Зеландії вважають, що мають достатній огляд ризиків, вразливостей та дотримання нормативних вимог, а 78% заявляють, що мають внутрішні ресурси для протидії кібератакам, лише 30% мають офіційний план забезпечення безперервності бізнесу або план реагування на кіберінциденти. Схожі тенденції спостерігаються в Австралії, де 77% респондентів висловлюють впевненість у рівні обізнаності, а 70% — у наявності ресурсів, але лише 32% мають плани забезпечення безперервності діяльності. Дослідження показує, що організації інвестували значні кошти в моніторинг та виявлення, але не досягли достатнього рівня технічної стійкості, відпрацьованих процесів відновлення, чітких повноважень щодо прийняття рішень та показників, пов'язаних із відновленням послуг, а не лише з виявленням інцидентів…

Марк Хайл із компанії Datacom зазначив, що коли організації не можуть працювати протягом днів або тижнів, наслідки є значними і позначаються на клієнтах, ланцюгах постачання та довірі до бренду. Колін Пенман, директор з інформаційної безпеки Datacom, наголосив на розбіжності між очікуваним і фактичним часом відновлення, наводячи приклади, такі як атака програм-вимагачів у 2025 році на компанію Jaguar Land Rover, яка зупинила виробництво на п'ять тижнів, а повне відновлення зайняло майже п'ять місяців. Атаки з використанням штучного інтелекту, включаючи фішинг, є головною проблемою для керівників служб безпеки в обох країнах, а автоматизація, діпфейки та синтетичні ідентичності скорочують терміни атак…

Опитування також вказує на більш широкі структурні проблеми: 51 % респондентів із Нової Зеландії висловили занепокоєння щодо суверенітету даних та життєздатності локальних обчислювальних потужностей, а 43 % повідомили про ознаки «кібервигорання» у своїх командах. Ці висновки узгоджуються з останніми даними Національного центру кібербезпеки, які свідчать про зростання фінансових збитків та кількості інцидентів, зокрема про збільшення прямих фінансових збитків на 118 % у третьому кварталі 2025 року та майже подвоєння кількості інцидентів, що потребували спеціалізованої підтримки. Загалом результати підкреслюють необхідність для організацій перейти від інвестицій, зосереджених на виявленні, до перевірених планів забезпечення безперервності роботи, чіткішого управління та сильніших внутрішніх можливостей для забезпечення справжньої кіберстійкості». ***(Roxanne Libatique. NZ cyber-ready on paper, but few have recovery plans // KM Business Information NZ (https://www.insurancebusinessmag.com/nz/news/cyber/nz-cyberready-on-paper-but-few-have-recovery-plans-572477.aspx). 21.04.2026).***

***

Китай, Індія, Японія, Південна Корея та країни Індо-тихоокеанського регіону

«Ситуація з кіберзагрозами в Малайзії зазнає значних змін, зумовлених стрімким розвитком цифрових технологій та зростанням геополітичного

значення країни, що разом призводить до розширення площі атаки швидше, ніж захисні системи встигають за цим темпом. Ключові сектори країни — такі як енергетика, телекомунікації, транспорт, фінанси та виробництво напівпровідників — стали головними цілями як для шпигунства, що фінансується державою, так і для кіберзлочинності з фінансовою мотивацією…

Групи, пов'язані з Китаєм, такі як APT41 та Mustang Panda, зосереджуються на довгостроковому зборі розвідувальної інформації та спостереженні за ланцюгами постачання, тоді як такі суб'єкти, як північнокорейська група Lazarus та злочинні угруповання на кшталт FIN7, націлюються на фінансові системи та використовують програми-вимагачі. Атаки здебільшого носять ситуативний характер, але є дуже поширеними: серед них переважають програми-вимагачі, фішинг та соціальна інженерія, причому на останню припадає до 75 % випадків шахрайства. Масштаби загроз є значними: це десятки мільйонів веб-атак, зростання збитків від шахрайства та дедалі більш витончені методи, такі як фішинг на основі штучного інтелекту, «діпфейки» та багатовекторні DDoS-атаки. Стратегічне розташування Малайзії та її роль у глобальних торговельних і технологічних ланцюгах постачання ще більше підвищують її вразливість до кібератак, спрямованих як на отримання економічної вигоди, так і на здійснення геополітичного впливу… Як наслідок, ризики у сфері кібербезпеки поширюються на всю економіку, що вимагає посилення захисту інфраструктури, вдосконалення механізмів реагування на інциденти, запровадження більш суворих заходів аутентифікації та підвищення обізнаності для протидії складному та мінливому середовищу загроз». ***(Anna Ribeiro.Malaysia's digital growth and geopolitics widen cyber attack surface, raising critical infrastructure risks // Industrial Cyber (https://industrialcyber.co/reports/malaysias-digital-growth-and-geopolitics-widen-cyber-attack-surface-raising-critical-infrastructure-risks/). 07.04.2026).***

***

«Десять японських компаній, серед яких виробники продуктів харчування та роздрібні мережі, заявили в понеділок, що спільно створять організацію для підвищення рівня кібербезпеки.

Організація займатиметься аналізом та обміном інформацією про ознаки та наслідки кібератак, а також розвитком кадрового потенціалу.

До складу цих 10 компаній входять телекомунікаційна компанія NTT Inc., Asahi Group Japan Ltd. (підрозділ компанії з виробництва напоїв Asahi Group Holdings Ltd.), мережа дисконтних магазинів Trial Holdings Inc., оптовий продавець продуктів харчування Mitsubishi Shokuhin Co., група компаній з виробництва напоїв Suntory Holdings Ltd. та постачальник товарів повсякденного вжитку Kao Corp.

Вони планують запросити до участі й інші компанії.

Кібератака на виробника продуктів харчування або роздрібного продавця спричинить значні збитки, оскільки їхні ланцюги постачання охоплюють багато компаній. Asahi Group Holdings була змушена скоротити поставки після того, як у вересні зазнала кібератаки». ***(Japanese Food Makers, Others to Jointly Enhance***

Cybersecurity // Nippon Communications Foundation (https://www.nippon.com/en/news/yjj2026040600693/). 07.04.2026).

***

«Командування з питань інформації, зв'язку та електронних сил Збройних сил Тайваню реалізує плани щодо посилення кібербезпеки та стійкості систем зв'язку, зокрема уклало новий контракт на суму 5,457 млрд тайваньських доларів з компанією Chunghwa Telecom на надання «послуг виділеної пропускної здатності мережі зв'язку», спрямованих на покращення моніторингу та захисту мережі, забезпечення підтримки спільних операцій та підвищення загальної стійкості оборонної системи. Фінансування здійснюється за рахунок спеціального бюджету на забезпечення стійкості національної безпеки…

У рамках частки Міністерства національної оборони в цьому спеціальному бюджеті більш широка «Програма підвищення стійкості військово-цивільного інформаційно-комунікаційного оперативного середовища та покращення характеристик обладнання» розподіляє ресурси між п’ятьма проектами, включаючи масштабну модернізацію військово-цивільного комунікаційного обладнання та оперативних середовищ з метою зменшення ризику порушення бойового командування китайськими кіберзасобами — за допомогою нових супутників, зашифрованих мобільних і тактичних систем зв’язку з високою пропускною здатністю, ширше використання хмарних/віртуальних середовищ та покращене управління безпекою — поряд із вдосконаленням систем управління та IT-захисту, розширеними можливостями моніторингу, мобільними резервними серверами та розподіленими системами зв’язку управління (включаючи мікрохвильові лінії зв’язку великої дальності та новий центр управління мережею), а також додатковими потужностями з ремонту кабелів та ретрансляції інтернету…» ***(Lo Tien-pin and Jake Chung. Taiwan implementing cybersecurity projects: source // The Taipei Time (https://www.taipeitimes.com/News/front/archives/2026/04/04/2003855001). 04.04.2026).***

***

«Командування з питань інформації, зв'язку та електронних сил Тайваню посилює кіберзахист, зокрема уклавши новий контракт із компанією Chunghwa Telecom на суму 5,457 млрд тайваньських доларів щодо надання «послуг виділеної пропускної здатності мережі зв'язку» з метою покращення моніторингу мережі, її захисту, проведення спільних операцій та загальної стійкості оборони; фінансування здійснюється за рахунок спеціального бюджету на забезпечення стійкості національної безпеки. У рамках загального спеціального бюджету в розмірі 550 млрд тайваньських доларів Міністерство національної оборони контролює 113,2 млрд тайваньських доларів і виділило 70,33 млрд тайваньських доларів на п’ятикомпонентну програму підвищення стійкості військово-цивільного інформаційно-комунікаційного операційного середовища та покращення характеристик обладнання…

Серед ключових елементів — проект вартістю 56 млрд тайваньських доларів, спрямований на запобігання паралізації бойової структури управління Тайваню з боку китайських кіберсил шляхом закупівлі супутників, зашифрованих мобільних і тактичних засобів зв'язку з високою пропускною здатністю, хмарних/віртуальних середовищ та засобів підтримки управління безпекою; ініціатива вартістю 2,48 млрд тайваньських доларів, спрямована на зміцнення систем управління та ІТ-захисту за допомогою мобільних резервних систем для морських командних центрів; цивільно-військова система моніторингу зображень вартістю 500 млн тайваньських доларів для модернізації системи моніторингу Тайванської тактичної мережі; ініціативу з мобільності вартістю 10,758 млрд тайваньських доларів, спрямовану на закупівлю мобільних серверів для розподіленого командування, встановлення мікрохвильового каналу зв'язку великої дальності у Вуцю та будівництво регіонального центру управління мережею; а також проект вартістю 284,45 млн тайваньських доларів, спрямований на збільшення допоміжної пропускної здатності Інтернету за допомогою інструментів для з'єднання волоконно-оптичних кабелів та їх ремонту.

Тайвань також розширює міжнародне співробітництво, про що свідчить візит колишнього голови Національного кіберуправління Ізраїлю Габріеля Портноя, метою якого було обговорення питань кібербезпеки, стійкості критичної інфраструктури та розвитку кадрового потенціалу; при цьому Міністерство оборони наголошує на необхідності поглиблення обміну досвідом із країнами-однодумцями та інтегрованих військово-цивільних зусиль, спрямованих на розвиток навичок та підвищення стійкості». ***(Lo Tien-pin, Jake Chung. Taiwan implementing cybersecurity projects: source // The Taipei Times (https://www.taipeitimes.com/News/front/archives/2026/04/04/2003855001). 04.04.2026).***

***

«Департамент інформаційних технологій уряду Делі видав вичерпний набір рекомендацій з кібербезпеки для захисту ІТ-інфраструктури у понад 60 своїх департаментах. Підкреслюючи необхідність захисту репутації уряду та ІТ-активів, циркуляр зобов'язує кожен департамент призначити помічника головного спеціаліста з інформаційної безпеки (ACISO), який буде єдиною контактною особою та забезпечуватиме наявність у всіх веб-сайтів і додатків дійсних сертифікатів аудиту безпеки. Крім того, департаменти зобов'язані вести точний облік своєї ІТ-інфраструктури, регулярно створювати резервні копії даних та оновлювати все програмне забезпечення й пристрої…

Для окремих співробітників ці рекомендації встановлюють суворі робочі протоколи: офіційне листування має здійснюватися виключно через електронні поштові акаунти Національного інформаційного центру (NIC), тоді як використання сторонніх каналів, піратського програмного забезпечення, а також перехід за підозрілими посиланнями чи відкриття підозрілих вкладень суворо заборонено. Співробітники зобов'язані використовувати антивірусний захист, використовувати надійні паролі з багатофакторною автентифікацією (MFA) та гарантувати, що ці облікові дані ніколи не будуть передані іншим особам. Крім

того, уряд встановив чіткий протокол управління інцидентами, який зобов'язує співробітників правильно вимикати свої комп'ютери при виході з офісу та негайно повідомляти про будь-які потенційні кіберінциденти до відповідних органів…» ***(Delhi govt issues guidelines to shield its departments from cyber attacks // The Indian Express [P] Ltd. (https://indianexpress.com/article/cities/delhi/delhi-govt-issues-guidelines-to-shield-its-departments-from-cyber-attacks-10624477/). 08.04.2026).***

***

«Китай попередив, що вживе відповідних заходів, зокрема розпочне розслідування та, можливо, судові процеси, якщо Європейський Союз продовжить реалізацію запропонованих правил у сфері кібербезпеки, які можуть визнати Китай «країною, що викликає занепокоєння з точки зору кібербезпеки», або внести китайські компанії, такі як Huawei та ZTE, до списку постачальників високого ризику, фактично виключивши їх з ринку ЄС. У 30-сторінковому поданні до Європейської комісії Пекін охарактеризував проект правил як «надзвичайно суб'єктивний та дискреційний», стверджуючи, що вони порушують численні правила СОТ і не можуть бути виправдані винятками з міркувань національної безпеки, оскільки національна безпека залишається у компетенції держав-членів…

Ці нормативні акти передбачають обов'язкове виключення постачальників з високим рівнем ризику з мереж 5G протягом трьох років і можуть поширити обмеження на інші чутливі сектори, зокрема на підключені автомобілі, інфраструктуру електропостачання та водопостачання, хмарні обчислення, медичні прилади, космічні послуги та напівпровідники. Ця ескалація є частиною ширшого циклу правових погроз та контрзаходів у відносинах між ЄС та Китаєм, причому Пекін також заперечує проти запропонованого ЄС закону про промисловий акселератор та висловлює занепокоєння щодо вимог до належної перевірки ланцюгів постачання, які можуть суперечити китайським законам, що регулюють потоки даних та державні таємниці.

Китайські компанії, такі як виробник сканерів для аеропортів Nuctech, вже розпочали судові процеси проти регламенту ЄС щодо іноземних субсидій, що підкреслює зростаючу регуляторну плутанину, яка впливає на передачу технологій, інвестиції у сфері інтелектуальної власності та транскордонну діяльність компаній з обох сторін. Торговельна палата ЄС у Китаї попередила, що європейським компаніям може бути складно одночасно дотримуватися європейських директив та китайського законодавства, особливо коли аудити ланцюгів постачання можуть порушувати китайські норми щодо даних та державної таємниці… Загалом цей спір підкреслює, що заходи з економічної безпеки дедалі частіше перетинаються з питаннями інтелектуальної власності, передачі технологій та торговельних правил, що ускладнює доступ до ринків та дотримання відповідних вимог для технологічних компаній в обох регіонах». ***(Finbarr Bermingham. China threatens EU firms over cybersecurity plans targeting Chinese companies // South China Morning Post Publishers Ltd. (https://www.scmp.com/news/china/diplomacy/article/3350763/china-threatens-eu-firms-over-cybersecurity-plans-targeting-chinese-companies). 20.04.2026).***

***

«Кіберризики стали одним із головних викликів для компаній, що ведуть діяльність в Азії, де кібератаки та витоки даних постійно входять до числа найбільших бізнес-ризиків поряд із порушеннями ланцюгів постачання, стихійними лихами та геополітичною нестабільністю. На високоцифрових та взаємопов'язаних ринках регіону кіберінциденти часто призводять до зупинки операцій, порушують роботу логістичних мереж, викликають транскордонний регуляторний контроль та наражають компанії на договірні збитки й репутаційні втрати, які можуть мати глобальні наслідки… Для транснаціональних організацій, що мають операції або ланцюги постачання в Азії, рішення щодо кіберстійкості та страхування зараз суттєво впливають на нагляд з боку ради директорів, розкриття інформації про цінні папери, розміщення капіталу та розподіл договірних ризиків… Перебої в роботі бізнесу, спричинені кібератаками, стали одним із головних ризиків, що часто завдають більших фінансових збитків, ніж сам початковий злом, через зупинку виробництва, пропущені поставки, збій транзакцій клієнтів, розслідування з боку регуляторних органів та подальші судові спори. Традиційне планування безперервності бізнесу, зосереджене на фізичних перебоях, поступається місцем необхідності враховувати цифрову взаємозалежність, особливо в тих випадках, коли основна діяльність залежить від спільних хмарних сервісів, платіжних систем, аутсорсованих логістичних платформ або транскордонних потоків даних. Кіберстрахування зазвичай забезпечує пряме покриття витрат на реагування на інциденти, відновлення даних, переривання діяльності та додаткові витрати, кібершантаж та кризові комунікації, тоді як непряме покриття переривання діяльності може поширюватися на перебої у роботі постачальників або сервіс-провайдерів…

Однак формулювання в полісах щодо «залежних систем», періодів очікування та виключень у разі недотримання мінімальних стандартів безпеки або договірної відповідальності вимагають ретельного аналізу, щоб уникнути прогалин у страховому покритті. В Азії регуляторні заходи у відповідь на кіберінциденти часто передбачають обов'язкове повідомлення про порушення, розслідування з боку органів захисту даних, адміністративні санкції та перевірки щодо транскордонної передачі даних, що збільшує витрати на захист та ускладнює координацію дій…

Ради директорів та головні юристи повинні забезпечити, щоб положення про відшкодування збитків у договорах, укладених з азіатськими партнерами, відповідали наявним страховим покриттям, а інструкції з реагування на інциденти враховували вимоги політики щодо повідомлення, згоди та затверджених постачальників. У міру того як цифрова трансформація та складні ланцюги постачання посилюють взаємозалежність, кіберризики в Азії перетворюються з технічних інцидентів на стратегічні ризики для підприємств, що впливають на стабільність доходів, виконання договірних зобов'язань, дотримання нормативних вимог, розкриття інформації для інвесторів та цінність бренду, що вимагає комплексних юридичних, операційних та фінансових заходів реагування». ***(Emily E. Garrison, Wendy Tan. Cyber Risk in Asia Moves from Technical Threat to Enterprise Liability and Insurance Imperative // Morgan, Lewis & Bockius LLP.***

(https://www.morganlewis.com/pubs/2026/04/cyber-risk-in-asia-moves-from-technical-threat-to-enterprise-liability-and-insurance-imperative). 23.04.2026).

***

«Міністр фінансів Нірмала Сітхараман закликала фінансовий сектор Індії та Раду з цінних паперів та бірж Індії (SEBI) терміново посилити заходи з кібербезпеки на тлі зростаючої загрози складних атак на основі штучного інтелекту. Виступаючи на Дні заснування SEBI, вона наголосила, що штучний інтелект дозволяє зловмисникам виявляти та використовувати вразливості програмного забезпечення з безпрецедентною швидкістю, знижуючи бар'єр для складних атак на критичну фінансову інфраструктуру. Щоб протидіяти цим ризикам, зокрема поширенню створених за допомогою штучного інтелекту фейкових відео та шахрайського контенту, міністр закликала SEBI застосувати проактивний, орієнтований на розвиток підхід до захисту інвесторів, що включає міжнародну співпрацю в галузі регулювання та швидке видалення фейкових матеріалів у ЗМІ…

Окрім нагальних питань безпеки, Сітараман наполягала на проведенні структурних реформ, таких як стандартизація правил «знай свого клієнта» (KYC) та поглиблення ринків корпоративних і муніципальних облігацій з метою розширення доступу та підвищення якості кредитів. Її виступ був зосереджений на ідеї, що сталий ринковий ріст має ґрунтуватися на доброчесності та надійному управлінні, що забезпечить стійкість індійських фінансових систем в епоху стрімких технологічних змін…» ***(Riya Kapoor. India Ramps Up AI Cyber Defense Amid Growing Threats // whalesbook (https://www.whalesbook.com/news/English/bankingfinance/India-Ramps-Up-AI-Cyber-Defense-Amid-Growing-Threats/69ecac195a43f6b807bbb4b3). 25.04.2026).***

***

Ізраїль, Туреччина та країни Близького сходу

«1 квітня 2026 року Туреччина офіційно запустила свою мережу 5G — це крок, який є значною стратегічною інвестицією як у національну безпеку, так і в економічну конкурентоспроможність, а не простою технологічною модернізацією… Цей перехід відбувається в рамках доктрини президента Ердогана «Кібербатьківщина», яка розглядає кіберпростір як продовження національного суверенітету та передбачає жорсткий контроль над цифровими кордонами. На тлі посилення регіональної нестабільності, зокрема конфлікту між США, Ізраїлем та Іраном, Туреччина розглядає безпечну інфраструктуру 5G як оборонну необхідність для протидії гібридним загрозам та «масштабним, але малоефективним» кібероперація̆м, спрямованим на зривання роботи критично важливих служб та підрив довіри громадськості…

Ця національна стратегія підкріплюється значними інституційними інвестиціями, такими як створення Управління з питань кібербезпеки у 2025 році та масштабне розширення оптоволоконної мережі. З економічної точки зору,

інтеграція 5G, за прогнозами, додасть до 100 мільярдів доларів до економіки Туреччини до 2030 року, прискорюючи інновації у таких ключових секторах, як інтелектуальне виробництво, автономна мобільність та оборона, завдяки забезпеченню обробки даних у реальному часі, необхідної для передових застосувань штучного інтелекту. Беручи до уваги досвід війни в Україні, де цифрові платформи, такі як додаток електронного урядування «Дія», виявилися вирішальними для забезпечення інституційної безперервності та стійкості суспільства в умовах фізичних і кібератак, Туреччина усвідомлює, що надійні комунікаційні мережі є стратегічною перевагою. Інвестуючи в 5G, Туреччина прагне підвищити свою національну стійкість і стратегічну автономію, зміцнивши свої позиції як активного та впливового гравця у новому «технополярному» світовому порядку, де контроль над даними та цифровою інфраструктурою дедалі більше визначає глобальну потужність». ***(Merve Ayşe Kızılaslan. How will 5G reshape Türkiye's cybersecurity and economy? // Turkuvaz Haberleşme ve Yayıncılık (https://www.dailysabah.com/opinion/op-ed/how-will-5g-reshape-turkiyes-cybersecurity-and-economy). 05.04.2026).***

***

«Національний центр кібербезпеки Кувейту запровадив новий набір основних національних заходів контролю у сфері кібербезпеки, покликаних підвищити інституційну зрілість та посилити захист цифрового середовища країни. Завдяки встановленню єдиних національних базових вимог ці заходи спрямовані на захист даних, систем та технічних активів, а також на поліпшення позицій Кувейту у світових рейтингах кібербезпеки… Ця система покликана підвищити готовність до кіберзагроз, забезпечити безперебійність ділової діяльності та зміцнити довіру до цифрового середовища. Засновані на найкращих міжнародних практиках, але адаптовані до конкретних регуляторних потреб Кувейту, ці заходи забезпечують масштабовану основу, яка покращує підзвітність, уточнює ролі та обов'язки, а також підвищує як реагування на інциденти, так і загальну обізнаність з питань кібербезпеки в установах країни». ***(New cybersecurity controls to boost digital protection // Kuwait Times (https://kuwaittimes.com/article/41978/kuwait/other-news/new-cybersecurity-controls-to-boost-digital-protection/). 06.04.2026).***

***

«Швидка цифрова трансформація Саудівської Аравії, що здійснюється завдяки таким ініціативам, як «Vision 2030», значно розширила спектр державних онлайн-послуг, фінтех-платформ та інтелектуальної інфраструктури, що призвело до відповідного зростання попиту на послуги з кібербезпеки. Національне управління з кібербезпеки Саудівської Аравії повідомляє, що Королівство щорічно стикається з мільйонами кіберзагроз у міру того, як такі критично важливі сектори, як державні послуги, енергетика та фінанси, дедалі більше переходять на цифрові технології…

За прогнозами, до 2025 року глобальні витрати, пов'язані з кіберзлочинністю, перевищать 10,5 трлн доларів на рік, а Близький Схід залишається одним із

регіонів, що найчастіше стають мішенями кібератак, особливо на урядову, фінансову та промислову інфраструктуру. У відповідь на це інвестиції в кібербезпеку в регіоні Близького Сходу та Північної Африки (MENA) стабільно зростають, а Саудівська Аравія стає ключовим центром для стартапів у сфері кібербезпеки, які отримують підтримку від венчурних капіталістів та інноваційних фондів, що фінансуються урядом. Фінансування все частіше спрямовується на компанії, що розробляють системи виявлення загроз на основі штучного інтелекту, хмарні рішення з безпеки та платформи для забезпечення відповідності вимогам, адаптовані до регіональних нормативних вимог, що робить кібербезпеку стратегічним стовпом зростаючої цифрової економіки Королівства». ***(Saudi Arabia's Cybersecurity Startups Guard the Region's Digital Shift // Cybersecurity Ventures (https://cybersecurityventures.com/saudi-arabias-cybersecurity-startups-guard-the-regions-digital-shift/). 22.04.2026).***

***

«Рада з кібербезпеки ОАЕ визначила стійкий розрив між наявними засобами безпеки та повсякденною поведінкою користувачів як головну вразливість у хмарних та цифрових середовищах. Незважаючи на постійні інвестиції в інфраструктуру, такі елементарні недоліки, як неналежне управління правами доступу, залишаються значним ризиком: за оцінками, від 68% до 77% файлів, що передаються у приватному режимі, можуть залишатися доступними для сторонніх користувачів через стандартні налаштування конфіденційності. Рада наголошує, що шифрування слід розглядати як базову вимогу, а не як додатковий засіб захисту, зазначаючи, що хмарне сховище не забезпечує безпеку даних за своєю суттю, особливо під час передачі або спільного використання файлів у мережах…

У практичних рекомендаціях наголошується на важливості дотримання таких стабільних звичок, як використання надійних паролів, що часто оновлюються, увімкнення двофакторної автентифікації, обмеження поширення посилань, проведення регулярних перевірок дотримання конфіденційності, захист мереж Wi-Fi, оновлення програмного забезпечення, обмеження дозволів для додатків та використання VPN у публічних мережах. Також підкреслюється важливість дотримання правил «гігієни даних», зокрема видалення невикористовуваних файлів і посилань, регулярного створення резервних копій та дисциплінованого управління базами даних для зменшення загальної площі атаки. Кампанія «Cyber Pulse», яка проводиться вже другий рік поспіль, сигналізує про більш широкий перехід від кібербезпеки, орієнтованої на інфраструктуру, до зменшення ризиків, орієнтованого на користувача, підкреслюючи, що в системах, які стають дедалі більш розподіленими та залежними від хмари, найслабшою ланкою часто є не сама технологія, а повсякденні рішення, які приймають її користувачі». ***(UAE Cyber Security Council Flags Human Error as Primary Cyber Risk // MIT Sloan Management Review Middle East (https://www.mitsloanme.com/article/uae-cyber-security-council-flags-human-error-as-primary-cyber-risk/). 20.04.2026).***

***

«У міру прискорення цифрової трансформації Африки, де кількість інтернет-користувачів перевищує 500 мільйонів, а поширення мобільного банкінгу стрімко зростає, інфраструктура кібербезпеки не встигає за цими змінами, що призведе до фінансових збитків на суму понад 3 мільярди доларів у період з 2019 по 2025 рік. Оскільки кілька африканських країн входять до числа тих, що найчастіше стають мішенями для шкідливого програмного забезпечення, стало очевидно, що ізольовані національні засоби захисту є недостатніми для боротьби з транснаціональними угрупованнями кіберзлочинців, такими як «Black Axe»…

Успіх «Operation Serengeti» — ініціативи INTERPOL-AFRIPOL 2024 року, в якій взяли участь дев'ятнадцять африканських країн, — демонструє ефективність транскордонної співпраці; це державно-приватне партнерство дозволило ліквідувати 134 000 шкідливих онлайн-інфраструктур та призвело до понад 1 000 арештів. Хоча це є значною реактивною перемогою, наступним важливим кроком є створення проактивної континентальної системи запобігання. Це вимагає гармонізації нормативно-правових баз на основі конвенції Африканського союзу з кібербезпеки для встановлення сумісних стандартів безпеки, зокрема для критичної інфраструктури…

Це також вимагає постійного зміцнення потенціалу для підготовки фахівців правоохоронних органів, прокуратури та приватного сектору, а також проведення загальнонаціональних інформаційних кампаній, подібних до тих, що проводилися в Руанді та Марокко. Нарешті, необхідні економічні стимули, щоб зробити значні інвестиції в безпеку фінансово вигідними для малих і середніх підприємств, змінивши сприйняття кібербезпеки з простої статті витрат на конкурентну перевагу.

Ця колективна континентальна оборонна стратегія має доповнюватися індивідуальною та організаційною відповідальністю; з огляду на те, що на фішинг припадає 34 % усіх виявлених інцидентів, дотримання елементарних правил кібергігієни — таких як надійні паролі, багатофакторна автентифікація та своєчасне оновлення програмного забезпечення — залишається надзвичайно важливим. Зрештою, цифрове майбутнє Африки залежить від того, чи зможуть її 54 країни діяти як злагоджена команда, обмінюючись інформацією та узгоджуючи законодавство, щоб спільно протистояти загрозам, які не визнають кордонів». ***(Yasmine Abdillahi. Why African cybersecurity requires a continental approach // Atlantic Council (https://www.atlanticcouncil.org/blogs/africasource/why-african-cybersecurity-requires-a-continental-approach/). 06.04.2026).***

***

«Наразі Африка переживає стрімку цифрову трансформацію, яка відбувається завдяки інноваціям у сферах мобільних грошових переказів, електронного урядування та цифрової охорони здоров'я, особливо в таких регіональних лідерах, як Гана, Кенія, Нігерія та Руанда. Однак цей технологічний стрибок супроводжується різким зростанням кіберзагроз, що часто

ускладнюється слабким контролем за дотриманням нормативних вимог та загальною недостатньою зрілістю систем кібербезпеки. Особливо вразливими є такі критично важливі сектори, як фінтех, охорона здоров'я та державні послуги, де програмне забезпечення для вимагання викупу, шахрайство та витоки даних становлять загрозу фінансовій інклюзії, безпеці пацієнтів та національній безпеці…

Залишається системна проблема: кібербезпека часто розглядається як другорядне питання, а не як фундаментальна вимога, причому складні системи часто впроваджуються ще до того, як взагалі починають думати про заходи безпеки. Такий реактивний підхід призводить до недосконалого проектування систем, недостатніх можливостей реагування на інциденти та невиконання чинного законодавства про захист даних. Щоб забезпечити безпечне цифрове майбутнє, необхідна фундаментальна зміна парадигми у бік підходу «безпека понад усе». Це передбачає інтеграцію кібербезпеки в національні цифрові стратегії з самого початку, узгодження з міжнародно визнаними стандартами, такими як NIST або ISO 27001, та перехід від моделі реактивного реагування до моделі проактивного запобігання…

Окрім політичних реформ, технічну стійкість необхідно зміцнювати за допомогою принципів «безпеки від самого початку», надійного управління ідентифікацією та доступом — зокрема багатофакторної автентифікації — а також регулярних і проактивних оцінок ризиків. Крім того, надзвичайно важливо вирішувати проблему гострого дефіциту кваліфікованих місцевих фахівців шляхом розвитку освіти та нарощування потенціалу. Зрештою, успіх цифрової трансформації Африки залежить від розвитку державно-приватного партнерства та забезпечення того, щоб інфраструктура майбутнього була не лише інноваційною, а й стійкою та надійною. Лише зробивши безпечні системи основою розвитку, континент зможе повністю реалізувати потенціал свого цифрового майбутнього». ***(Abubakari Saddiq Adams. Securing Africa's Digital Future: Why Cybersecurity Must Lead Digital Transformation // CircleID (https://circleid.com/posts/securing-africaas-digital-future-why-cybersecurity-must-lead-digital-transformation). 06.04.2026).***

***

«Нігерія створила Національну міністерську консультативну раду для координації заходів із запобігання кіберзагрозам у ключових секторах, об'єднавши в ній багатосторонні агентства, приватний сектор, наукові кола та інші установи з метою забезпечення ефективного реагування на нові кіберзагрози. Міністр комунікацій, інновацій та цифрової економіки Босун Тіджані підкреслив, що з 163 мільйонами інтернет-користувачів, 157 мільйонами мобільних ліній та 84% покриттям населення 4G, країна стикається з приблизно 4 200 кібератаками на тиждень, спрямованими на урядові організації та інші установи, і ця тенденція, як очікується, посилиться у міру прискорення цифровізації та переходу до цифрової економіки…

Рада буде виявляти нові ризики, покращувати узгодженість політик, зміцнювати співпрацю між державним і приватним секторами, та покращить скоординовану національну реакцію без дублювання існуючих зусиль, що відповідає амбіціям уряду щодо побудови економіки обсягом у один трильйон

доларів, підкріпленої значними інвестиціями у цифрову інфраструктуру, включаючи 2 мільярди доларів на 90 000-кілометрову оптоволоконну мережу та 3 700 телекомунікаційних веж для розширення покриття майже до 98–99% населення. Генеральний директор Національного агентства з розвитку інформаційних технологій (NITDA) Кашіфу Інува наголосив, що штучний інтелект змінює ландшафт кібербезпеки, створюючи більш складні загрози, такі як фішинг «zero-click», шкідливе програмне забезпечення, створене ШІ, автоматизовані програми-вимагачі та витончені методи соціальної інженерії, включаючи «діпфейки», які стає дедалі складніше виявити. Він наголосив, що питання кібербезпеки не можна розглядати ізольовано, а співпраця та обмін інформацією між урядом і приватним сектором мають вирішальне значення, оскільки «наша сила залежить від найслабшої ланки». Загалом ця ініціатива відображає прихильність до постійної підзвітності, обміну розвідданими, національної координації та стратегічного прогнозування ризиків з метою зміцнення національної кіберстійкості в умовах зростаючих загроз». ***(FG inaugurates advisory council to coordinate cybersecurity efforts // Peoples Gazette™ Limited. (https://gazettengr.com/fg-inaugurates-advisory-council-to-coordinate-cybersecurity-efforts/). 22.04.2026).***

***

Кіберстрахування

«Інститут страхової інформації (Triple-I) спільно з компанією Fenix24 опублікував звіт «Кібербезпека для страховиків: баланс між безпекою та сервісом» (Cybersecurity for Insurers: Squaring Safety with Service), в якому оцінюється, як страховики у сфері майнового та особистого страхування управляють власними кіберризиками, та виявляються слабкі місця, що зберігаються попри значні інвестиції. На основі інтерв'ю з керівниками страхових компаній, які відповідають найкращим практикам, регуляторним очікуванням та загальним заходам контролю кіберстрахування, у звіті висвітлено прогалини у частоті встановлення оновлень, виборі методів автентифікації та реалістичному тестуванні відновлення — особливо щодо програм-вимагачів, які часто руйнують не лише резервні копії, а й основну інфраструктуру, таку як Active Directory, системи ідентифікації, віртуальні машини та засоби зв'язку…

У звіті наводяться дані щодо ринку, що активно зростає (чисті премії у 2024 році становитимуть 15,3 млрд доларів, а у 2025 році, за прогнозами, — 16,3 млрд доларів). При цьому зазначається, що у 2023 році 19 % страхових випадків у сфері кібербезпеки були пов'язані з програмним забезпеченням-вимагачем, тоді як на випадки компрометації корпоративної електронної пошти та шахрайства з переказом коштів припадало 56 %; при цьому збитки від переривання діяльності становлять приблизно половину середнього збитку від програм-вимагачів, який становить близько 1 млн доларів. Серед основних спостережень — широке використання незмінних резервних копій та дотримання цілей щодо часу відновлення для систем найвищого рівня, але тести відновлення часто

обмежуються ідеальними сценаріями з однією системою, а не відновленням всієї мережі; надійні практики щодо паролів та їх зберігання з багатофакторною автентифікацією (MFA) для адміністраторів, проте в деяких випадках продовжується використання слабших методів MFA, таких як SMS або електронна пошта; поширене використання фільтрування DNS та блокування ризикованих веб-сервісів, поряд із вразливістю, що створюється «роздільним тунелюванням», яке обходить захист VPN; а також регулярні тестування на проникнення (включно із соціальною інженерією), але лише близько половини страховиків щомісяця встановлюють виправлення, хоча зловмисники можуть використати нові вразливості як зброю вже за кілька днів. Загалом у звіті стверджується, що стійкість залежить не стільки від «ідеальної» профілактики, скільки від систематичної підготовки, швидших циклів оновлення та перевірених можливостей відновлення «від початку до кінця», при цьому забезпечуючи баланс між безпекою, зручністю використання та операційною діяльністю». ***(Triple-I/Fenix24 Report Identifies Emerging Cybersecurity Priorities for Insurers // Business Wire, Inc. (https://www.businesswire.com/news/home/20260402960701/en/Triple-IFenix24-Report-Identifies-Emerging-Cybersecurity-Priorities-for-Insurers). 02.04.2026).***

***

«Ринок кіберстрахування в Кореї залишається значно недорозвиненим, незважаючи на різке зростання кількості кіберінцидентів: у 2025 році було зафіксовано 2 383 атаки — майже вдвічі більше, ніж двома роками раніше — а серйозні порушення безпеки, що зачепили такі компанії, як SK Telecom, Coupang, YES24 та Lotte Card, підкреслили вразливість ключових секторів, зокрема телекомунікацій, електронної комерції та фінансів. За даними Gallagher Re, премії за кіберстрахування в Кореї у 2024 році становили лише близько 3 млн доларів США, що становить приблизно 0,02% від загального світового обсягу, порівняно з 39 млн доларів США у Сінгапурі та 5 млн доларів США у Таїланді, тоді як світовий ринок кіберстрахування у 2025 році оцінюється у 16–20 млрд доларів США, а до 2030 року, за прогнозами, досягне 30–50 млрд доларів США… З боку попиту багато корейських компаній спрямовують витрати на технічні засоби захисту, такі як програмне забезпечення, апаратне забезпечення та консультаційні послуги, а не на страхування, часто розглядаючи кіберризик як проблему ІТ, а не як більш широку фінансову загрозу, і вважаючи за краще вирішувати інциденти внутрішніми силами, щоб мінімізувати репутаційні наслідки. З боку пропозиції страховики стикаються з викликами, пов'язаними з швидко мінливими загрозами, обмеженою історією збитків на внутрішньому ринку для проведення точного актуарного аналізу та потенційною можливістю взаємопов'язаних збитків у взаємопов'язаних системах, що призводить до обережного страхування, жорсткіших умов полісів та повільнішого розвитку продуктів…

На міжнародному рівні Північна Америка продовжує лідирувати за обсягом премій за кіберстрахування, тоді як інциденти, пов’язані зі штучним інтелектом (ШІ) — на які припадає дедалі більша частка страхових виплат через порушення безпеки ланцюгів постачання, інверсію моделей та обхід систем захисту —

спонукають до запровадження більш жорстких умов страхування, окремих полісів щодо ШІ та додаткових умов щодо покриття витрат на перепідготовку персоналу. У США майбутній Закон про повідомлення про кіберінциденти щодо критичної інфраструктури та законодавство на рівні штатів ще більше ускладнюють дотримання нормативних вимог для транснаціональних компаній.

Аналітики вважають, що низький рівень проникнення страхування в Кореї порівняно з розвитком цифрової економіки та кількістю інцидентів вказує на необхідність організованого обміну інформацією, стандартизованих механізмів оцінки ризиків, а також розгляду можливості створення підтримуваних урядом пулів перестрахування для підвищення страхуваності кіберзагроз та підтримки більш стабільного й масштабованого ринку. Загалом розрив між зростаючим ризиком та доступним страховим покриттям підкреслює важливість перетворення підвищеної обізнаності про гучні випадки порушень у більш систематичне використання страхування серед корейських страховиків, перестраховиків, посередників та корпоративних клієнтів». ***(Roxanne Libatique. Korea falls behind on cyber insurance amid surge in attacks // KM Business Information Australia Pty Ltd (https://www.insurancebusinessmag.com/asia/news/cyber/korea-falls-behind-on-cyber-insurance-amid-surge-in-attacks-572879.aspx). 23.04.2026).***

***

«Згідно з результатами третього щорічного глобального опитування EY щодо управління ризиками у страховій галузі, більшість керівників з управління ризиками (CRO) у страховій галузі визнають кібербезпеку своїм головним пріоритетом на наступний рік, а значна частина з них також вважає кіберризики, пов'язані з третіми сторонами та постачальниками, однією з головних проблем. Щоб впоратися з цими зростаючими та взаємопов'язаними загрозами, на які дедалі більший вплив мають геополітична нестабільність та технологічні зміни, багато керівників з управління ризиками надають пріоритет інтеграції генеративної штучної інтелекту та великих мовних моделей у свої функції управління ризиками. Цей технологічний зсув супроводжується структурними змінами у кадровому складі, оскільки більшість страховиків планують скоротити кількість посад, що передбачають ручну працю, одночасно збільшуючи інвестиції в аналітику даних та навички роботи зі штучним інтелектом…

У відповідь на зростаючу складність середовища ризиків страхові компанії переходять до більш інтегрованих систем, що поєднують кіберризики, операційну стійкість та контроль за діяльністю третіх сторін. Цей підхід передбачає посилення систем управління, розширення безперервного моніторингу та проведення більш ретельних тестувань за різними сценаріями. EY також наголошує, що якісні та узгоджені дані мають вирішальне значення для отримання практичних висновків, що зумовлює збільшення інвестицій у централізовані платформи даних. Зрештою, роль CRO еволюціонує у більш стратегічну позицію в організації, зосереджену на передбаченні того, як інновації та руйнівні зміни можуть перетворити бізнес-моделі. Компанії, які успішно покращують своє управління, можливості роботи з даними та цифрову експертизу, матимуть найкращі шанси зберегти стійкість у

цьому швидкозмінному середовищі…» ***(Taylor Mixides. Insurance CROs flag cybersecurity as top risk while AI and data investment surge, EY/IIF survey finds // Steve Evans Ltd. (https://www.reinsurancene.ws/insurance-cros-flag-cybersecurity-as-top-risk-while-ai-and-data-investment-surge-ey-iif-survey-finds/). 24.04.2026).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Національний центр кібербезпеки Великої Британії (NCSC) опублікував нове попередження про те, що російська кібергрупа APT28, яка діє за підтримки держави та відома також як Fancy Bear, захоплює звичайні інтернет-маршрутизатори, щоб таємно перенаправляти трафік користувачів через шкідливі сервери… Використовуючи вразливості пристроїв, ця група, пов'язана з російською військовою розвідкою ГРУ, здатна перехоплювати трафік і викрадати облікові дані та токени доступу до особистих веб-сервісів та електронної пошти. Ця опортуністична кампанія широкого охоплення дозволяє зловмисникам здійснювати захоплення системи доменних імен (DNS), направляючи нічого не підозрюючих користувачів на підроблені веб-сайти, призначені для збору їх конфіденційної інформації, перш ніж зосередитися на конкретних цілях, що представляють інтерес для розвідки… NCSC закликає організації та захисників мереж захищати свої системи шляхом забезпечення безпеки інтерфейсів управління, оновлення всього програмного забезпечення та пристроїв, а також впровадження двоступеневої верифікації для зменшення загрози». ***(UK exposes Russian military intelligence hijacking vulnerable routers for cyber attacks // National Cyber Security Centre (NCSC) (https://www.ncsc.gov.uk/news/uk-exposes-russian-military-intelligence-hijacking-vulnerable-routers-for-cyber-attacks). 07.04.2026).***

***

«У новому аналізі Центру стратегічних і міжнародних досліджень (CSIS) міститься застереження, що кібердоктрина Ірану перетворилася на стійку стратегічну позицію, яка розглядає кіберпростір як важливе продовження державної влади, причому особлива увага приділяється підготовці до майбутніх атак на критичну інфраструктуру США. Цей підхід, який віддає перевагу асиметричним кібероперація̈м, що не залишають слідів, над прямим військовим втручанням, використовує поєднання пов'язаних з державою та проксі-груп «хактивістів» для експлуатації вразливостей у таких секторах, як енергетика, водопостачання та транспорт. Енергетична мережа США є особливо вразливою через її величезні розміри, старіння та дедалі більшу взаємопов'язаність, що створює величезну площину атаки, на яку активно націлюються супротивники, зокрема Китай та Росія…

Хоча китайська кампанія «Volt Typhoon» домінувала в заголовках новин завдяки постійному проникненню в критично важливі системи, Іран також продемонстрував як намір, так і здатність здійснювати руйнівні атаки, про що свідчить нещодавній злом медичної компанії Stryker… У міру ескалації

геополітичної напруженості на Близькому Сході уряд США та компанії з кібербезпеки закликають енергетичні компанії, яким належить 80% енергетичної інфраструктури країни, посилити свою оборону, попереджаючи, що навіть помірні кіберзбої можуть мати ланцюгові економічні та операційні наслідки, особливо якщо вони збігаються у часі з військовими діями. Це призвело до закликів до більш тісної співпраці між державним і приватним секторами та до введення більш суворих обов'язкових стандартів кібербезпеки для усунення роздробленості та нерівномірності захисних систем, які наразі захищають життєво важливі енергетичні системи країни». ***(Anna Ribeiro. CSIS flags Iran's shift from episodic cyberattacks to sustained campaign against critical infrastructure // Industrial Cyber (https://industrialcyber.co/industrial-cyber-attacks/csis-flags-irans-shift-from-episodic-cyberattacks-to-sustained-campaign-against-critical-infrastructure/). 07.04.2026).***

***

«На тлі загострення геополітичної напруженості між Іраном та Ізраїлем, який підтримують США, американські експерти з кібербезпеки та федеральні агентства висловлюють серйозні застереження щодо підвищеного ризику іранських кібератак на критичну інфраструктуру США, зокрема на сектори водопостачання та енергетики. ФБР спеціально попередило муніципалітети та операторів про загрозу з боку кіберзлочинців, які можуть скористатися доступом інсайдерів у компаніях, що постачають апаратне та програмне забезпечення для операційних технологій (ОТ). Ці групи, що фінансуються державою, підозрюються у використанні витончених тактик соціальної інженерії для вербування інсайдерів, що дозволяє їм обходити традиційні системи безпеки та безпосередньо маніпулювати важливими комунальними службами… Агентство з охорони навколишнього середовища (EPA) підтримало ці занепокоєння, наголосивши, що атаки на системи водопостачання становлять пряму та серйозну загрозу для здоров'я населення та безпеки громад. У спільній федеральній рекомендації було вказано на вразливість певних програмованих логічних контролерів, зокрема деяких моделей від Rockwell Automation, які можуть бути використані для порушення фізичних промислових процесів. Ця загроза не є суто теоретичною, про що свідчить інцидент 2023 року, коли пов'язана з Іраном група CyberAv3ngers успішно атакувала системи водопостачання в Пенсильванії, тимчасово вивівши з ладу десятки пристроїв. Цей інцидент є наочним нагадуванням про те, що в умовах коливань у дипломатичних зусиллях цифрове поле бою стає основною ареною конфлікту, що робить захист критичної інфраструктури надзвичайно важливим питанням національної безпеки». ***(Naveen Goud. US anticipates Iran Cyber Attacks and Water and Energy Sectors // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/us-anticipates-iran-cyber-attacks-and-water-and-energy-sectors/). 09.04.2026).***

***

«…ФБР визнало нещодавнє китайське кібервтручання в систему спостереження уряду США «серйозним інцидентом» — цей статус присвоюється лише тим порушенням, які завдають очевидної шкоди

національній безпеці. За даними джерел, обізнаних із ситуацією, в результаті хакерської атаки було викрадено конфіденційну інформацію внутрішніх правоохоронних органів; при цьому, судячи з усього, використовувалися тактики, схожі на ті, що застосовувалися в рамках попередньої кампанії «Salt Typhoon», пов'язаної з Китаєм, під час якої у 2024 році було отримано доступ до записів телефонних дзвінків мільйонів американців та викрадено дані про прослуховування ФБР…

Колишні урядовці розглядають цей останній випадок порушення безпеки як серйозну невдачу контррозвідки, що свідчить про те, що Китай безкарно продовжує свої агресивні хакерські операції, незважаючи на попереднє викриття на міжнародному рівні та поточні дипломатичні зусилля. Сенатор Марк Уорнер, заступник голови Сенатського комітету з розвідки, заявив, що цей інцидент є частиною чіткої схеми, за якою супротивники використовують слабкі місця США, і попередив, що систематичне скорочення адміністрацією Трампа штату федеральних співробітників з кібербезпеки небезпечно підриває цифрову оборону країни в час ескалації загроз». ***(Dan De Luce, Michael Kosnar and Kevin Collier. FBI labels suspected China hack of law enforcement data 'a major cyber incident' // NBC News (https://www.nbcnews.com/news/us-news/fbi-labels-suspected-china-hack-law-enforcement-data-major-cyber-incid-rcna266495). 03.04.2026).***

***

«Кібербезпека перетворилася з вузькотехнічної проблеми на одну з головних сил у геополітиці, оскільки глобальна влада дедалі більше залежить від програмного коду, даних та мережевих систем. На відміну від традиційних полів бою, кіберпростір не має чітких кордонів чи видимих армій і характеризується постійною прихованою конкуренцією, в рамках якої державні та недержавні суб'єкти зондують мережі та ланцюги постачання, порушують роботу державних служб, викрадають дані та маніпулюють інформацією, створюючи постійну «сіру зону», здатну підірвати економіку, демократичні інститути та довіру громадськості. Це змусило уряди розглядати цифрову вразливість як ризик для національної безпеки — не стільки через побоювання вторгнення, скільки через побоювання виведення з ладу внаслідок втрати контролю над критичними системами, такими як енергомережі, транспорт, лікарні, фінанси та вибори…

Як наслідок, альянси переформатуються навколо «технологічної довіри» до практик безпеки партнерів та цілісності спільної інфраструктури й постачальників, що сприяє створенню кіберорієнтованих коаліцій, заснованих на спільних стандартах, безпечних ланцюгах постачання та сумісних системах безпеки. США та ЄС поглибили співпрацю у сфері кібербезпеки та управління технологіями, тоді як Китай і Росія дотримуються іншої моделі, що наголошує на кіберсуверенітеті, державному контролі та альтернативних технологічних стеках; багато регіонів також розробляють власні рамки, пристосовані до розбудови потенціалу, захисту даних та цифрової автономії. Стратегічні технології — 5G, хмарні технології, напівпровідники, штучний інтелект та квантові технології — стали інструментами впливу, що спонукає деякі держави до диверсифікації постачальників («цифровий неучасть») та інші — до приєднання до єдиної екосистеми з міркувань безпеки чи

економіки, поряд із посиленням багатонаціонального обміну інформацією та механізмів колективного реагування.

У цих умовах цифрові можливості дозволяють здійснювати приховане проєктування сили та формувати нові глобальні ієрархії, економічна конкурентоспроможність пов'язана з цифровою стійкістю, а цілісність інформації стала ключовим активом, оскільки маніпуляції в Інтернеті та дезінформація загрожують політичній стабільності. У перспективі поглиблення цифрової взаємозалежності та розвиток нових технологій посилять конкуренцію, водночас збільшивши стимули для встановлення норм, стандартів та колективної оборони, навіть попри те, що деякі країни створюють більш ізольовані цифрові простори — завдяки чому кібербезпека залишатиметься визначальним елементом міжнародних відносин, економічної політики та суспільної безпеки». ***(Liesbeth Jové Lettens. The new geopolitics of cyberspace // Meer (https://www.meer.com/en/102481-the-new-geopolitics-of-cyberspace). 04.04.2026).***

***

«Німецькі спецслужби звинуватили пов'язану з російськими військовими хакерську групу APT28, також відому як Fancy Bear, у проведенні нової кампанії, спрямованої на вразливі інтернет-маршрутизатори TP-Link з метою викрадення конфіденційних даних військових, урядових структур та об'єктів критичної інфраструктури. Внутрішня розвідка Німеччини (BfV) у спільному попередженні з партнерами, серед яких ФБР, заявила, що хакери скористалися кількома тисячами загальнодоступних маршрутизаторів по всьому світу, причому в Німеччині було виявлено близько 30 вразливих пристроїв… Цей останній інцидент є частиною ширшої схеми ймовірних російських кібершпигунських та диверсійних дій, спрямованих проти Німеччини, ключового союзника України, які раніше включали спроби порушити роботу системи управління повітряним рухом та поширити дезінформацію. Хоча Росія заперечує свою причетність, німецькі органи влади попередили операторів уражених маршрутизаторів і перебувають у стані підвищеної готовності до подальших ворожих кібероперацій». ***(German spy agency accuses Russia of new cyberattacks // Euractiv (https://www.euractiv.com/news/german-spy-agency-accuses-russia-of-new-cyberattacks/). 08.04.2026).***

***

«Хакери, пов'язані з Іраном, нещодавно здійснили кібератаки на кілька американських організацій, зокрема на постачальника програмного забезпечення для оборонного та аерокосмічного секторів, що підкреслює: зростання геополітичної напруженості, ймовірно, спричинить збільшення кількості атак на урядові установи, підрядників та їхні ланцюги постачання. Очікується, що значна частина цієї діяльності матиме опортуністичний характер — націлена на незахищені системи, слабкі облікові дані та незахищені вразливості — тоді як хактивісти та проксі-групи можуть також прагнути дестабілізації шляхом залякування та психологічного впливу; навіть обмежене проникнення в середовища ланцюгів постачання може спричинити серйозні операційні наслідки…

Рекомендованим підходом є прийняття позиції «виходити з припущення про злом» у відносинах з постачальниками, визнаючи, що запобігти кожному вторгненню нереально, і зосередитися натомість на швидкому виявленні, локалізації, обмеженні горизонтального поширення та підтримці безперебійної роботи. Для цього агентства, підрядники та постачальники повинні покращити прозорість шляхом картографування системних з'єднань та потоків даних для встановлення базових показників та виявлення прихованих залежностей, ідентифікації та визначення пріоритетності захисту найцінніших критично важливих активів та ризикованих шляхів доступу партнерів, а також посилення таких основних заходів, як своєчасне встановлення виправлень, видалення стандартних облікових даних, надійна багатофакторна автентифікація, зменшення кількості відкритих служб та активний моніторинг журналів. Відповідність вимогам Zero Trust та стандартам, таким як ISO 27001 та CMMC Міністерства оборони США, розглядається як ключ до переходу від рекомендацій до відповідальності, з загальною метою побудови стійкості ланцюга поставок, що захищає федеральні місії та національну безпеку». ***(Gary Barlet. Stop trying to prevent every cyberattack. Start planning to survive one // Government Media Executive Group LLC (https://www.washingtontechnology.com/opinion/2026/04/stop-trying-prevent-every-cyberattack-start-planning-survive-one/412476/). 03.04.2026).***

***

«У нещодавно опублікованому Спільному попередженні з питань кібербезпеки, виданому федеральними агентствами, зокрема Міністерством енергетики США, учасників енергетичного сектору попередили про зростання загрози з боку суб'єктів, що підтримуються Іраном, які активно використовують операційні технології, підключені до Інтернету. Ці супротивники спеціально націлюються на програмовані логічні контролери на об'єктах виробництва та розподілу електроенергії, щоб маніпулювати даними системи та спричиняти перебої в роботі на тлі триваючих геополітичних конфліктів. Оскільки підприємства енергетичного сектору значно різняться за розмірами та наявними ресурсами, у рекомендаціях наголошується, що всі учасники є важливими цілями, які повинні надавати пріоритет кібербезпеці. Щоб зменшити ці ризики та мінімізувати потенційні збитки, автори рекомендацій та експерти з безпеки радять організаціям регулярно переглядати та впроваджувати п'ять основних найкращих практик…

По-перше, підприємствам слід посилити технічну безпеку за допомогою шифрування даних, систем виявлення загроз на кінцевих точках та багатофакторної автентифікації, доповнюючи ці заходи регулярним моніторингом на предмет аномальної активності. По-друге, організації повинні дотримуватися комплексних заходів з управління даними, щоб точно знати, яка інформація зберігається, де вона знаходиться та які постачальники мають до неї доступ. По-третє, компаніям слід створювати ізольовані або зовнішні резервні копії та перевіряти можливість відновлення систем з цих копій. По-четверте, необхідно розробити офіційний план реагування на інциденти (IRP), який чітко визначає ключові внутрішні та зовнішні контактні особи та окреслює негайні кроки, які слід вжити під час порушення

безпеки. Нарешті, організації повинні регулярно тестувати та проводити навчання щодо свого IRP, щоб виявити прогалини та ризики до того, як трапиться реальний інцидент. Впровадивши ці проактивні заходи, учасники енергетичного сектору зможуть краще захищати свою критичну інфраструктуру та захищати свою діяльність від кіберзагроз, що постійно еволюціонують». ***(Erin M. Prest, Kevin J. Conoscenti, Allen R. O'Neil. Protecting Critical Energy Infrastructure and Data from Cyberthreats // McCarter & English, LLP (https://www.mccarter.com/insights/protecting-critical-energy-infrastructure-and-data-from-cyberthreats/). 15.04.2026).***

***

«Спільна американо-ізраїльська кампанія повітряних ударів проти Ірану наприкінці лютого 2026 року (під кодовою назвою «Операція Епічна лють/Ревучий лев») швидко спровокувала масові кібератаки у відповідь з боку іранських державних структур, проіранських хактивістських угруповань та хакерів-опортуністів. Вже через кілька годин після ударів Іран ввів блокування інтернету, що тимчасово порушило координацію, дозволивши десяткам пов'язаних між собою хактивістських угруповань втрутитися та активізувати операції, спрямовані проти урядових і оборонних структур Ізраїлю, західних компаній (включно з руйнівною атакою типу «wiper» на американську медичну технологічну фірму Stryker) та регіональної інфраструктури в таких країнах, як Йорданія, Саудівська Аравія, ОАЕ, Бахрейн і Кувейт…

Понад 60 різних хактивістських угруповань активізували свою діяльність, багато з яких координували свої дії через «електронні оперативні штаби» у Telegram, поєднуючи тактику державного рівня з кримінальними інструментами, такими як інфостілер Rhadamanthys та спеціальні програми для знищення даних. Серед найвідоміших гравців — Handala (яку вважають пов'язаною з МЗС і відповідальною за атаку на Stryker), Cyber Islamic Resistance (об'єднання, що координує синхронізовані DDoS-атаки та кампанії з дефейсингу), FAD Team (що спеціалізується на руйнуванні ICS/SCADA) та Dark Storm (відома масштабними DDoS-атаками та вимаганням). Навіть проросійські групи, такі як NoName057(16), приєдналися до солідарних атак на ізраїльські цілі. Хоча багато заяв хактивістів є перебільшеними або недоведеними, ширші кібернаслідки поширилися далеко за межі зони конфлікту, вразивши організації, які, як вважається, мають зв'язки з Ізраїлем, і продемонструвавши, що географічна відстань забезпечує обмежений захист у сучасній гібридній війні…

З огляду на триваючі переговори щодо крихкого перемир'я та ймовірність подальшої ескалації конфлікту, організаціям настійно рекомендується скористатися цією нагодою для проактивного захисту: зменшити площу зовнішньої атаки шляхом встановлення оновлень для систем, підключених до Інтернету, та посилення захисту віддаленого доступу; впровадити багатофакторну автентифікацію (MFA), стійку до фішингу; покращити виявлення та моніторинг тактик, технік і процедур (TTP), пов'язаних із конфліктом; провести навчання персоналу щодо протидії фішингу та соціальному інжинірингу на військову тематику; а також переглянути ризики, пов'язані зі сторонніми постачальниками та

ланцюгом поставок. Експерти попереджають, що поєднання державних суб'єктів та децентралізованих проксі-серверів хактивістів створює надзвичайно динамічне середовище загроз, яке може швидко розширюватися з мінімальним попередженням». ***(Filip Dimitrov. Cyber Warfare Amid the Israel-Iran Conflict: What Organizations Need to Know // OP Innovate (https://op-c.net/blog/israel-iran-cyber-war-threats-2026/). 16.04.2026).***

***

«Швеція публічно приписала кібератаку на свою енергетичну інфраструктуру проросійській групі, що стало першим офіційним визнанням країни такого інциденту. Атака, що сталася минулого року, призвела до збою в роботі теплоелектростанції на заході Швеції та викликала серйозну стурбованість щодо вразливості національної критичної інфраструктури перед кібероперaціями, пов'язаними з державою… Ця інформація, оприлюднена міністром цивільної оборони Швеції, вказує на чіткі геополітичні мотиви, пов'язані з загальним напруженням у відносинах між Росією та західними країнами, в умовах яких енергетичні системи дедалі частіше розглядаються як цінні цілі. У відповідь на це шведські органи влади та лідери галузі прискорюють зусилля з посилення кібербезпеки в усьому секторі за допомогою законодавчих заходів, технічних оновлень, посилення співпраці з міжнародними союзниками, спільних навчань та покращення обміну інформацією про загрози… Цей крок відображає зростаючу західну тенденцію до публічного викриття як інструменту стримування та притягнення до відповідальності, водночас підкреслюючи нагальну потребу енергетичних операторів усунути прогалини в безпеці, інтегрувати передові засоби виявлення та створити більшу колективну стійкість до мінливого та політично мотивованого ландшафту загроз». ***(Gabby Lee. Sweden Points to Pro-Russian Group in Cyberattack on Energy Infrastructure // Daily Security Review (https://dailysecurityreview.com/cyber-security/sweden-points-to-pro-russian-group-in-cyberattack-on-energy-infrastructure/). 16.04.2026).***

***

«З моменту початку війни в лютому 2026 року Іран значно посилив свої кібероперації проти Сполучених Штатів та їхніх союзників, причому підтримувані Іраном угруповання зловмисників — від суб'єктів, що діють за підтримки держави, до проіранських хактивістів та хакерів, які керуються фінансовими мотивами — демонструють все більш руйнівні можливості та еволюцію мотивів… Аналітики відзначають явний перехід до атак, спрямованих на завдання більшого фізичного та оперативного впливу, зокрема до більш широкого використання шкідливого програмного забезпечення для знищення даних проти ізраїльських цілей та появи складних штамів, таких як ZionSiphon, який дослідники з Darktrace визначили як такий, що потенційно здатний втручатися у рівні хлору та регулятори тиску на ізраїльських водопровідних об'єктах, одночасно вбудовуючи проіранські та палестинські повідомлення для досягнення психологічного ефекту…

Дослідники з компаній Palo Alto Networks та Check Point Research також зафіксували вдосконалені методи ухилення від виявлення та ознаки координації між кібератаками (такими як взлом відеокамер) і військовими ударами, що свідчить про вищий рівень інтеграції між кібероперaціями та звичайними військовими операціями Ірану. Ці дії використовуються не лише для шпигунства та дестабілізації, а й для надсилання політичних сигналів сусіднім державам Перської затоки, Ізраїлю, США та внутрішнім дисидентам… У відповідь групи з обміну інформацією про кіберзагрози у США в березні опублікували спільне попередження про підвищені ризики для секторів критичної інфраструктури, а ФБР та CISA згодом опублікували конкретні попередження про суб'єктів, пов'язаних з Іраном, які націлені на вразливості у водо- та енергопостачальних компаніях. IT-ISAC підтвердила постійні повідомлення про таку діяльність від спільноти критичної інфраструктури, підкресливши стійкий та еволюційний характер загрози». ***(David Jones. Iran-nexus threat groups refine attacks against critical infrastructure // TechTarget, Inc. (https://www.cybersecuritydive.com/news/iran-nexus-threat-groups-refine-attacks-against-critical-infrastructure/818299/). 23.04.2026).***

***

«Згідно з щорічним звітом за 2025 рік, опублікованим Службою оборонної розвідки та безпеки Нідерландів (MIVD), Росія все частіше використовує штучний інтелект для прискорення та розширення масштабів своїх кібератак на Європу. Агентство попередило, що російські суб'єкти тепер можуть проводити операції у високому темпі завдяки частковій автоматизації атак за допомогою ШІ, що дозволяє здійснювати швидші та більш синхронні удари по декількох цілях… Цей розвиток подій відбувається в час посиленого занепокоєння щодо передових моделей ШІ, таких як Mythos від Anthropic, яка, як побоюються, може перевершити людей у виявленні та використанні вразливостей програмного забезпечення; її розробники наразі обмежують доступ до невеликої групи надійних організацій, оцінюючи ризики…

Інструменти штучного інтелекту також дають хакерам можливість створювати надзвичайно переконливі фішингові листи, голосові клони та відеоролики з використанням технології «діпфейк», які здатні обійти традиційні перевірки безпеки, що здійснюються людьми, тоді як фахівці з кібербезпеки водночас використовують штучний інтелект для швидшого виявлення аномалій та моніторингу мережі. Загалом, оцінка MIVD підкреслює, як штучний інтелект кардинально змінює швидкість та рівень складності кіберзагроз, що підтримуються державою, в Європі». ***(Antoaneta Roussi. Russia uses AI to hack Europe, Dutch intelligence warns // Politico (https://www.politico.eu/article/russia-uses-ai-hack-eu-europe-dutch-intelligence-warns/). 21.04.2026).***

***

«У попередженні Агентства з кібербезпеки та безпеки інфраструктури (CISA) від 7 квітня було повідомлено, що кіберзлочинці, пов'язані з Іраном, отримали доступ до підключених до Інтернету програмованих логічних контролерів, які використовуються в критичній інфраструктурі США,

зокрема у системах водопостачання та енергопостачання, з метою спричинення збою в роботі. Це підкреслює, що навіть попри призупинення військового конфлікту та оголошення перемир'я, кіберконфлікт триває як постійний і безмежний вимір геополітики. У статті стверджується, що хакерські атаки з боку національних держав є постійними, а не епізодичними, і що Іран роками досліджував інфраструктуру США, включаючи минулі вторгнення в греблю в Нью-Йорку та систему водопостачання в Пенсильванії, часто використовуючи недофінансовані та погано захищені муніципальні мережі як для збору розвідданих, так і для демонстрації більш широкої вразливості…

Хоча експерти сумніваються, що Іран на даний момент має можливості — або мотивацію — для здійснення катастрофічної, широкомасштабної атаки на великі міста США, навіть обмежені операції можуть спричинити реальні збитки, фінансові втрати та занепокоєння серед населення, про що свідчать DDoS-атаки, інциденти з використанням програм-вимагачів та інші вторгнення, пов'язані з цим конфліктом. Ще до початку військових дій пов'язана з Іраном група Seedworm (також відома як MuddyWater та іншими назвами) вже проникла в мережі США та їхніх союзників, готуючись до потенційних атак, тоді як інший ймовірний посередник, група Handala, здійснила атаку за допомогою «віпервеару» на медичну компанію Stryker, що призвело до виходу з ладу обладнання, затримки операцій та порушення ділової діяльності… Така кібердіяльність є частиною ширшої асиметричної стратегії, поряд із регіональними атаками та навіть фізичними ударами по інфраструктурі, такій як хмарні центри обробки даних, причому Іран робить ставку на наполегливість і дезорганізацію, а не на надсучасні технології. Також висловлюється занепокоєння щодо ослаблення оборонного потенціалу США через скорочення штату ФБР та запропоновані значні скорочення фінансування CISA, при цьому застерігається, що такі заходи можуть підвищити вразливість у період посилення загрози. Зрештою, перемир'я не припиняють кіберконфлікт, а лише змінюють його темп, причому постійне сканування, атаки на облікові дані та експлуатація в сприятливих умовах продовжують спричиняти зриви, а також невизначеність і політичний тиск…» ***(Sue Halpern. How Big a Threat Are Iranian-Backed Cyberattacks? // Condé Nast (https://www.newyorker.com/news/the-lede/how-big-a-threat-are-iranian-backed-cyberattacks). 24.04.2026).***

***

Створення та функціонування кібервійськ

«У жовтні минулого року ЦРУ перетворило свій Центр кіберрозвідки (CCI) на повноцінний оперативний центр, вивівши цей підрозділ зі складу Управління цифрових інновацій, де він перебував з 2015 року. Директор Джон Ратклiфф ініціював цю реорганізацію, щоб надати пріоритет кіберможливостям агентства, забезпечивши підрозділ прямим підпорядкуванням директору, збільшивши фінансування та посиливши кадрові ресурси. Це стратегічне підвищення відображає більш широке прагнення адміністрації Трампа до агресивнішої та бойовішої позиції у кіберпросторі, як зазначено в її Національній

кіберстратегії, яка виступає за використання як наступальних, так і оборонних операцій для стримування іноземних супротивників…

Як підрозділ агентства, що відповідає за стратегічний кібераналіз та шпигунство, CCI відомий розробкою спеціалізованих хакерських засобів — ця функція особливо проявилася під час інциденту з WikiLeaks «Vault 7» у 2017 році, коли були викриті секретні хакерські інструменти та вразливості ЦРУ. Надавши CCI статус місійного центру, Ратклiфф прагне зменшити небажання агентства йти на ризик та дозволити проводити більш наполегливі цифрові операції, щоб покарати тих, хто здійснює цифрові атаки на США. Хоча цей крок свідчить про більш активну роль ЦРУ у цифровій сфері, експерти з розвідки зазначають, що він викликає питання щодо потенційного дублювання функцій з Кіберкомандуванням США при Пентагоні, особливо з огляду на те, що уряд намагається розмежувати ролі збору розвідданих та наступальних операцій стримування». ***(Martin Matishak. CIA director quietly elevated agency's cyber espionage division // Recorded Future News (https://therecord.media/cia-director-elevated-agency-cyber-espionage-division). 08.04.2026).***

***

«Організований Центром передового досвіду спільної кіберзахисту НАТО (CCDCOE) у Таллінні, Естонія, захід імітував інтенсивні кібератаки в режимі реального часу на критичну інфраструктуру та військові системи, перевіряючи здатність захисників підтримувати роботу життєво важливих служб під тиском.

Кількість учасників була такою ж, як і у 2025 році.

Командам було доручено захищати протиповітряну оборону, платформи електронного голосування та іншу критично важливу інфраструктуру. Окрім технічних навичок, Locked Shields перевіряє здатність боротися з дезінформацією та політичним тиском.

За словами Тиніса Саара, директора Центру кібербезпеки НАТО (CCDCOE), учасники продемонстрували потужні можливості у виявленні та реагуванні на зловмисну діяльність. Саар наголосив на необхідності перетворення уроків навчань на реальну готовність, особливо враховуючи, що штучний інтелект продовжує змінювати як можливості кіберзахисту, так і можливості атак.

Шістнадцять багатонаціональних команд змагалися у вправах. Трьома об'єднаними командами з найвищими балами (у довільному порядку) були Франція та Швеція; Латвія та Сінгапур; а також Німеччина, Австрія, Люксембург та Швейцарія…» ***(Eduard Kovacs. Strengthen Cyber Resilience in World's Biggest Exercise // Wired Business Media (https://www.securityweek.com/locked-shields-2026-41-nations-strengthen-cyber-resilience-in-worlds-biggest-exercise/amp/). 24.04.2026).***

***

«Дослідники з Вищої школи технологій Марокко (Університет Мулай-Ісмаїл) проаналізували нові виклики у сфері кібербезпеки для сучасних енергосистем — особливо для «розумних» мереж на основі відновлюваних джерел енергії з високим рівнем комунікації — та розглянули останні досягнення у сферах виявлення та захисту, підкресливши зростаючу роль штучного інтелекту у вдосконаленні систем управління, захисту та стійкості. Вони класифікують загрози за походженням, впливом та ураженими рівнями, а також описують основні типи атак, включаючи DDoS (які затримують дії з управління), маніпуляції з цілісністю даних, атаки повторення, введення фальшивих даних, що імітують нормальні показники, одночасно дестабілізуючи роботу, приховані та нульово-динамічні атаки на основі моделей, розроблені для збереження прихованості, а також компрометацію пристроїв Інтернету речей, що може поширювати шкідливе програмне забезпечення, викрадати дані або спричиняти відмову в обслуговуванні…

Хоча «розумні» енергомережі підвищують ефективність та гнучкість, дослідники застерігають, що вони розширюють площину атаки та залишаються вразливими до фішингу, шкідливого програмного забезпечення, атак типу «відмова в обслуговуванні» (DoS) та атак типу «відмова в функціонуванні» (FDI), які можуть порушити роботу систем, поставити під загрозу дані та завдати шкоди інфраструктурі. Вони рекомендують стратегії захисту, що забезпечують конфіденційність, цілісність та доступність поряд з автентифікацією, авторизацією, приватністю та надійністю, з особливим акцентом на виявленні вторгнень та аномалій на основі машинного навчання та оптимізації для ідентифікації в режимі реального часу FDI та інших нестандартних дій у SCADA та робочих процесах оцінки стану.

Додаткові заходи включають забезпечення безпеки підстанцій та аналіз вразливостей протоколів, багаторівневі архітектури з використанням брандмауерів, систем виявлення вторгнень (IDS) та сегментації мережі, резервні канали управління для забезпечення безперебійності роботи, а також передові інструменти, такі як блокчейн/розподілені реєстри та методи перетворення Гільберта–Хуанга. Для компонентів Інтернету речей, таких як датчики та інтелектуальні лічильники, вони вимагають надійної аутентифікації, безпечного завантаження, частих оновлень прошивки та стандартизованої безпеки, одночасно захищаючи конфіденційні дані енергомережі під час зберігання та передачі за допомогою таких технологій, як гомоморфне шифрування; вони також наголошують на необхідності узгоджених стандартів, швидкого реагування на інциденти та обміну інформацією між операторами, виробниками та регуляторними органами, а також постійного навчання персоналу з метою зменшення ризиків фішингу та соціальної інженерії». ***(Emiliano Bellini. All emerging cyber threats targeting power infrastructure at a glance // pv magazine (https://www.pv-magazine.com/2026/04/06/all-emerging-cyber-threats-targeting-power-infrastructure-at-a-glance/). 06.04.2026).***

***

«Питання кібербезпеки в промисловості перетворилося з проблеми профілактичних витрат на складний комплекс факторів, що охоплює зупинку виробництва, порушення ланцюгів постачання, порушення договірних зобов'язань, ризики, пов'язані з дотриманням нормативних вимог, та нематеріальні збитки, пов'язані з підривом репутації. Згідно з доповіддю IBM «Вартість порушення безпеки даних у 2024 році», середній світовий показник становить 4,88 млн доларів, при цьому у сфері охорони здоров'я — понад 7 млн доларів, у разі використання програм-вимагачів — 10 млн доларів, а в разі інцидентів, пов'язаних з операційними технологіями (OT), — 4,56 млн доларів; незаплановані простої обходяться виробникам у 50 млрд доларів щорічно, а чверть промислових жертв зазнають збитків, що перевищують 5 млн доларів…

У зв'язку зі зростанням витрат, пов'язаних із порушеннями безпеки, посиленням вимог страхових компаній до рівня зрілості систем безпеки та прогнозованим обсягом світового ринку кібербезпеки у 240 мільярдів доларів до 2026 року, кібербезпека операційних технологій перетворилася з завдання, пов'язаного з дотриманням нормативних вимог, на стратегічний пріоритет на рівні ради директорів, що робить структуроване, орієнтоване на ризики бюджетування вкрай необхідним. Питання вже не полягає в тому, чи варто інвестувати, а в тому, чи відображає стратегія реальні економічні витрати, пов'язані з відмовою від інвестицій.

Джейкоб Марзлофф із компанії Armexa наголошує, що в сфері операційних технологій (OT) порушення безпеки призводять до зупинки виробництва, порушують вимоги безпеки, пошкоджують обладнання або становлять загрозу для життя людей, тому керівникам слід задавати собі питання «Які фінансові ризики несе відсутність належних заходів контролю?», а не «Скільки коштує безпека?» Маартен Оостерінк з Indurex зазначає, що захист життя та довкілля не піддається традиційним розрахункам рентабельності інвестицій; Девід Муссінгтон з Університету Меріленду підкреслює, що постійне попереднє позиціонування національних держав — операція «Volt Typhoon» із середнім часом перебування 393 дні, операція «Salt Typhoon», що проникає у телекомунікації у великому масштабі, та іранські суб'єкти, що компрометують водопостачальні підприємства США — вимагає оцінки з урахуванням повного ланцюга наслідків; а Тоні Тернер з Frenos вказує, що нечисленні дані про інциденти, надзвичайно мінливі наслідки та погана кількісна оцінка кіберфізичних наслідків роблять порівняння «вартість безпеки проти вартості порушення» припущенням, а не моделлю. Окрім виплат за програмне забезпечення-вимагач, справжні витрати включають простої у роботі (понад 500 тис. доларів на годину у виробничій сфері), проведення екстреної криміналістичної експертизи, штрафи за порушення нормативних вимог, порушення ланцюга поставок, підвищення страхових премій, судові позови щодо безпеки та довгострокове підривання репутації. Лідери, які досягають успіху, зосереджуються на подіях із серйозними наслідками та ризиках на основі сценаріїв,

щоб побудувати обґрунтовані аргументи, які перетворюють кіберризик на показники прибутку та збитків — очікувані щорічні збитки, вартість під ризиком та рентабельність заходів із мінімізації ризиків — і зосереджують дискусії на доступності виробництва, середньому часі відновлення та незапланованих простоях, а не на кількості CVE. Інвестиції повинні надавати пріоритет людям з галузевим досвідом, ранньому включенню безпеки в закупівлі, локалізації застарілих систем за допомогою компенсаційних заходів контролю та захисту критичних активів за ступенем тяжкості наслідків, причому зрілість визначається такими рамками, як ISA/IEC 62443 та NIST CSF. Кіберстрахування перетворюється з механізму передачі ризиків на фактичну регулюючу силу: страховики вимагають надавати задокументовані переліки активів, докази сегментації та перевірені плани реагування на інциденти; підвищення страхових премій та виключення з покриття, пов’язані з порушеннями безпеки, тривалими перебоями в роботі та діяльністю державних суб’єктів, виявляють прогалини в зрілості систем та фундаментальну складність моделювання кіберфізичних ризиків, що робить страхування скоріше ринковим сигналом, а не заміною реального контролю. У міру скорочення державно-приватних консультативних структур — наприклад, зменшення залучення зацікавлених сторін CISA — та зменшення обсягу урядової інформації про загрози, функція внутрішньої аналітики ризиків повинна забезпечуватися внутрішніми ресурсами, а керівники служб безпеки повинні підпорядковуватися операційним підрозділам та узгоджувати свої дії з ними, формулюючи інвестиції в термінах операційної безперервності, які фінансові директори та ради директорів розуміють одразу». ***(Anna Ribeiro. Rising breach costs and operational downtime redefine economics of OT cybersecurity making it boardroom priority // Industrial Cyber (https://industrialcyber.co/features/rising-breach-costs-and-operational-downtime-redefine-economics-of-ot-cybersecurity-making-it-boardroom-priority/). 05.04.2026).***

***

«У своєму останньому звіті про загрози для операційних технологій компанія Dragos попереджає, що зловмисники, які націлені на операційні технології, переходять від пасивного доступу та розвідки до більш активної позиції, використовуючи зібрані дані для того, щоб достатньо добре зрозуміти промислові процеси та порушити їх роботу шляхом моделювання контурів управління, виявлення інженерних робочих станцій, викрадення даних конфігурації та сигналізації, а також вивчення принципів функціонування фізичних операцій — тим самим ефективно знижуючи бар’єр між доступом до мережі та реальними фізичними наслідками…

У звіті стверджується, що захисники відстають, оскільки телеметричні дані операційних технологій (OT) мають тимчасовий характер, а багатьом організаціям бракує необхідної видимості для виявлення порушень або навіть розпізнавання кіберінцидентів; за оцінками Dragos, лише близько 10 % мереж OT у світі мають будь-який ефективний моніторинг. У звіті також підкреслюється еволюція ландшафту загроз із появою нових груп, що співпрацюють із національними державами, додаючи AZURITE (зосереджену на довгостроковому спостереженні за

OT та витоку даних) та PYROXENE (групу, пов’язану з IRGC, яка використовує ланцюги постачання та шляхи довірених відносин для переходу з IT в OT/ICS, ризикуючи втратою огляду або контролю)…

З огляду на геополітичну нестабільність — зокрема конфлікт на Близькому Сході — що підвищує рівень загрози, а також повідомлення про те, що майже 80 % британських виробників зазнали принаймні однієї кібератаки протягом минулого року, у звіті закликають виробників та операторів критичної інфраструктури посилити стійкість за допомогою базових засобів контролю, покращення видимості мереж операційної техніки (OT), безпечного віддаленого доступу та підходів «нульової довіри», що підкреслюється пов’язаною з Іраном атакою Handala на компанію Stryker, яка використовувала доступ, пов’язаний із Microsoft Intune, і спричинила зупинку виробництва, незважаючи на те, що почалася на рівні IT». ***(Larry O'Brien. Dragos 2026 OT Cybersecurity Report Notes Disturbing Shifts // ARC Advisory Group (https://www.arcweb.com/blog/dragos-2026-ot-cybersecurity-report-notes-disturbing-shifts). 03.04.2026).***

***

«Опитування, проведене компанією з кібербезпеки ESET, показує, що британська промисловість стикається з різким зростанням кіберризиків: щонайменше 78 % виробників повідомили про один або кілька інцидентів за останній рік, а понад половина жертв зазнала збитків у розмірі шестизначних сум. Операційні наслідки також є значними: приблизно кожна сьома постраждала організація зазнала простою, що може зупинити виробництво та порушити ланцюги постачання; майже половина повідомила про середні збитки близько 1 млн фунтів стерлінгів, причому деякі інциденти перевищували 250 000 фунтів стерлінгів, що становить існувальну загрозу, особливо для малих та середніх підприємств… У звіті (ESET for Manufacturing: Simplified, Scalable, and Secure) також відзначається все більш скоординована діяльність: майже 8 з 10 виробників стикалися з декількома інцидентами одночасно, іноді пов'язаними з одними й тими ж злочинними угрупованнями, що ускладнює заходи реагування. Небезпеку посилює поява атак на основі штучного інтелекту, які характеризуються високим рівнем автоматизації та адаптивності, а їхній рівень успішності, за оцінками, становить близько 88%. Такі атаки здатні не лише викрадати дані, а й втручатися в роботу обладнання, спричиняючи збої або помилкові тривоги, що перетворює порушення безпеки на більш серйозні операційні та безпекові проблеми... Загалом, компанія ESET стверджує, що виробникам необхідні більш надійні системи безпеки, навчання персоналу та проактивний моніторинг, щоб стримати зростання фінансових та операційних ризиків». ***(Naveen Goud. Survey suggests 6 figure financial losses from cyber attacks for UK Manufactures // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/survey-suggests-6-figure-financial-losses-from-cyber-attacks-for-uk-manufactures/). 03.04.2026).***

***

«Компанія Stryker повідомляє, що її глобальна виробнича мережа знову працює в повному обсязі після кібератаки, про яку вона вперше повідомила 11

березня 2026 року, коли збій у роботі середовища Microsoft вплинув на обробку замовлень, виробництво та відвантаження. У повідомленні на початку квітня компанія повідомила, що відновлені комерційні, замовні та дистрибуційні системи допомагають виробництву швидко наближатися до пікової потужності, а загальний обсяг поставок продукції залишається стабільним, причому більшість лінійок продукції доступні, оскільки компанія продовжує підтримувати догляд за пацієнтами, працюючи цілодобово з зовнішніми експертами з кібербезпеки, урядовими установами та партнерами з галузі…

Протягом березня компанія Stryker заявляла, що не має жодних підстав вважати, що інцидент пов'язаний із програмним забезпеченням-вимагачем або шкідливим програмним забезпеченням, і вважала, що ситуація взята під контроль; вона також заявляла, що безпека та захищеність продукції не постраждали, а всі пристрої залишаються безпечними для використання. 23 березня, після співпраці з Palo Alto Networks Unit 42 та іншими організаціями, компанія Stryker повідомила, що зловмисник використовував шкідливий файл, який не поширювався, для виконання команд та приховування своєї діяльності, але слідчі не виявили жодних зловмисних дій, спрямованих проти клієнтів, постачальників або партнерів. Компанія визнала, що клієнти, які покладаються на індивідуальні імплантати, зазнали певних незручностей, оскільки у тижні, що почався 16 березня, через затримки з доставкою було перенесено деякі операції, пов'язані з конкретними пацієнтами». ***(Stryker's global manufacturing network now "fully operational" following cyberattack // BIBA Medical (https://neuronewsinternational.com/strykers-global-manufacturing-network-now-fully-operational-following-cyberattack/). 07.04.2026).***

***

«Нові дані компанії Censys, що займається моніторингом Інтернету, свідчать про те, що хакери, пов'язані з Іраном, атакують понад 5 000 підключених до Інтернету програмованих логічних контролерів (PLC) по всьому світу, причому приблизно 3 900 із цих пристроїв розташовані у Сполучених Штатах. Зловмисники зосереджують свою увагу саме на PLC Allen-Bradley від Rockwell Automation, які виконують роль критично важливих промислових комп'ютерів, що керують заводським обладнанням, розподілом енергії та іншою життєво необхідною інфраструктурою. Ця кампанія, яка відновилася у відповідь на поточні геополітичні напруження за участю США та Ізраїлю, використовує той факт, що ці пристрої часто розгорнуті у віддалених, географічно розрізнених місцях і підключені через стільникові модеми або супутникові термінали Starlink, що ускладнює їх моніторинг та оновлення операторами…

Ризик для безпеки значно посилюється тим, що доступ до багатьох із цих пристроїв здійснюється через незахищені мережеві служби, такі як HTTP, VNC, FTP та Telnet, а не виключно через промислові протоколи, для використання яких вони були розроблені. Експерти з безпеки наголошують на особливо небезпечному характері доступу через VNC та незашифрований Telnet, оскільки ці канали дозволяють здійснювати несанкціоноване втручання в роботу операційних

технологій. У відповідь на ці висновки компанія Censys закликає операторів інфраструктури негайно відключити програмовані логічні контролери (PLC) від загальнодоступного Інтернету за допомогою безпечних шлюзів, впровадити багатофакторну автентифікацію для віддаленого доступу та застосувати суворі брандмауери для блокування незахищених служб, таких як Telnet і FTP. Крім того, операторам рекомендується активно реєструвати трафік, пов'язаний з іранськими хакерськими кампаніями, та розглянути можливість заміни застарілих PLC, які більше не отримують належних оновлень безпеки…» ***(Nearly 4,000 industrial control devices across US vulnerable to Iran-linked hacking campaign // Tech Network (https://www.techcentral.ie/nearly-4000-industrial-control-devices-across-us-vulnerable-to-iran-linked-hacking-campaign/). 10.04.2026).***

***

«Підприємствам у сфері виробництва та машинобудування більше не можна покладатися на оборонні, реактивні заходи кібербезпеки; натомість вони повинні застосовувати проактивний підхід, заснований на аналітичних даних, щоб ефективніше прогнозувати, визначати пріоритети та запобігати атакам програм-вимагачів. Ситуація з програм-вимагачами постійно змінюється і перейшла у стадію «екосистеми після втрати довіри», що характеризується непередбачуваними, взаємопов’язаними загрозами. Про це свідчать стратегічні союзи між такими угрупованнями, як DragonForce, LockBit та Qilin, які обмінюються техніками, ресурсами та інфраструктурою для посилення своїх можливостей... Особливо вразливими є такі високоприбуткові сектори, як виробництво, де зриви у роботі та незаплановані простої можуть мати критичні операційні та фінансові наслідки…

Проводячи аналогію з елітною професійністю Прем'єр-ліги, де тренери використовують передові дані, аналітику та детальну інформацію про суперників для підготовки стратегій матчів, організації повинні аналогічним чином формувати комплексну аналітику загроз, щоб зрозуміти, як діють кіберзлочинці, виявити їхні тактики та передбачити їхні наступні кроки. Витончена розвідка щодо вразливостей та площі атаки, що базується на мільярдах даних з відкритого та даркнету, надає зовнішній погляд на вразливості, неправильні налаштування та нагальні потреби у виправленні, допомагаючи командам безпеки подолати «втому від сповіщень» та зосередитися на найважливіших ризиках. Ставлячись до кіберзахисту як до підготовки до Прем'єр-ліги, підприємства можуть перейти від стану, коли їх пригнічує кожен можливий вектор атаки, до прийняття обґрунтованих та своєчасних рішень, що зменшують ймовірність та вплив інцидентів із програмним забезпеченням-вимагачем». ***(Jason Steer. Comment: Why proactive cybersecurity beats ransomware threats // Mark Allen Holdings Ltd (https://www.theengineer.co.uk/content/opinion/why-proactive-cybersecurity-beats-ransomware-threats). 20.04.2026).***

***

«Оскільки автомобілі перетворилися на «ноутбуки на колесах» із вбудованими можливостями підключення, додатками, бездротовими оновленнями та інформаційно-розважальними системами, підключеними до Інтернету, експерти попереджають, що кіберризики в автомобільній галузі зростають разом із загальним зростанням кількості кібератак (у 2025 році в Великобританії буде зламано 612 000 підприємств, а станом на 2023 рік у країні, за оцінками, буде понад 19 мільйонів підключених до мережі автомобілів). Дослідники вже давно довели, що недостатньо захищені системи автомобілів можна дистанційно маніпулювати таким чином, що це може створити ризики для безпеки, і це сприяло прийняттю таких нормативних актів, як Регламент ООН № 155 (R155), який з 2022 року вимагає від нових автомобілів впровадження структурованого управління кібербезпекою, включаючи шифрування та реагування на інциденти…

Хоча випадки драматичного «дистанційного захоплення» управління залишаються рідкісними, а злочинці, що керуються фінансовими мотивами, часто мають більше стимулів для викрадення даних, ніж для спричинення ДТП, підключені автомобілі все ж залишаються привабливою мішенню для шпигунства та викрадення цінної особистої інформації, що зберігається в облікових облікових записах та інформаційно-розважальних системах — про що свідчать атаки на ланцюги постачання автомобільної галузі та постачальників послуг з обробки даних, а також висновки про те, що покупці вживаних автомобілів часто виявляють у транспортних засобах залишені попередніми власниками дані. Дослідники також виявили архітектурні слабкі місця в деяких підключених до мережі автомобілях, і зростає занепокоєння, що напівавтономні та повністю автономні автопарки — часто пов’язані через централізовані системи — можуть спричинити більш серйозні порушення роботи всього автопарку, якщо їх буде зламано.

Нещодавні реальні збитки вже були спричинені атаками на корпоративні IT-системи автовиробників, наприклад, інцидент із програмним забезпеченням-вимагачем у компанії Jaguar Land Rover, який призвів до зупинки виробництва, затримки поставок та перебоїв у сервісному обслуговуванні й постачанні запчастин, продемонструвавши, як кіберінциденти можуть впливати на клієнтів навіть без безпосереднього злому автомобіля. Рекомендовані практичні заходи зосереджуються на «кібергігієні» для автомобілів: оновлюйте програмне забезпечення автомобіля, вимикайте невикористовувані функції Bluetooth/Wi-Fi/хотспоту, уникайте невідомих мереж та ненадійних додатків або USB-пристроїв, використовуйте надійні унікальні паролі для сервісів автомобіля, захищайте ключі від релейних атак (наприклад, ретельно зберігаючи їх або використовуючи мішечки Фарадея) та видаляйте особисті дані перед продажем або поверненням автомобіля, видаляючи профілі, історію навігації, паркування Bluetooth, а також виходу з додатків та стрімінгових сервісів». ***(Tom Jervis. Is car hacking real? Risks, vulnerabilities and expert cyber security tips // Carwow Studio Limited (https://www.autoexpress.co.uk/features/369308/car-hacking-real-risks-vulnerabilities-and-expert-cyber-security-tips). 04.04.2026).***

***

«Як повідомляється, у період з 4 по 6 квітня складний кіберінцидент вразив спільну ІТ-платформу авіакомпаній та аеропортів і спричинив ланцюгові збої в роботі десятків європейських хабів, паралізувавши системи реєстрації, обробки багажу та посадки в таких великих аеропортах, як Хітроу, «Шарль де Голль», Франкфурт та Копенгаген. Співробітники були змушені перейти на ручні процедури, і лише 6 квітня було скасовано або затримано понад 1 600 рейсів, що змусило авіакомпанії активувати аварійні графіки роботи та порадити пасажирам мати при собі роздруковані документи та прибувати заздалегідь… Хоча Прага не зазнала прямого впливу, ланцюгові наслідки у вигляді неправильного розміщення літаків та екіпажів призвели до затримок кількох рейсів до та з аеропорту імені Вацлава Гавела у понеділок та вівторок після Великодня.

Цей випадок наочно продемонстрував вразливість ланцюгів постачання для чеських підприємств — що загрожує залишенням співробітників за кордоном, затримками вантажів та додатковим навантаженням у вигляді обов'язків щодо забезпечення безпеки — і змусив менеджерів з організації поїздок посилити плани дій у надзвичайних ситуаціях за допомогою гнучких квитків, збережених цифрових/друкованих документів та запасних варіантів маршрутів, тоді як аналітики очікують, що це прискорить зусилля ЄС щодо підвищення стійкості авіаційної галузі та спонукає аеропорти до більшої сегментації мереж і створення офлайн-резервних копій, що додає актуальності інвестиціям аеропорту Праги у створення дублюючих систем». ***(Major cyberattack on aviation IT systems snarls flights across Europe and hits Prague connections // VisaHQ.com, Inc. (https://www.visahq.com/news/2026-04-07/cz/major-cyberattack-on-aviation-it-systems-snarls-flights-across-europe-and-hits-prague-connections/). 08.04.2026).***

***

«У залізничній галузі цілі кібербезпеки та безпеки історично суперечили одна одній і збігалися лише тоді, коли інцидент у сфері безпеки, наприклад, незаконне проникнення на територію, створював загрозу безпеці; однак таке розмежування стає дедалі менш обґрунтованим у міру того, як кібератаки стають дедалі частішими та витонченішими. Транспортний сектор, включаючи залізничний, зараз входить до п'ятірки галузей, що найчастіше стають мішенями атак у Європейському Союзі, на нього припадає 7,5 % проаналізованих кібератак згідно з доповіддю ENISA «Ландшафт загроз до 2025 року», при цьому 12 % значних інцидентів відповідно до Директиви про оператори мереж інформаційної безпеки (NIS) у 2024 році відбудуться у транспортній галузі…

Залізничний транспорт є привабливою мішенню для злочинців, які керуються фінансовими мотивами, хактивістів та представників державних структур через свою високу помітність, застарілі системи без шифрування та можливість здійснення недорогих атак із серйозними наслідками, які можуть поставити під загрозу як операційні технології (OT), так і інформаційні технології (IT). Конвергенція IT та OT розширила площину атаки, про що свідчить інфікування німецької залізниці програмним забезпеченням-вимагачем WannaCry у 2017 році, яке поширилося з застарілої системи Windows XP у корпоративній мережі на

інформаційні табло для пасажирів, системи відеоспостереження та квиткові автомати…

Недавні приклади, такі як атака 2023 року, пов’язана з Росією, на польську залізничну мережу, яка призвела до зупинки 20 поїздів завдяки використанню незашифрованих каналів зв’язку, ілюструють, як кіберінциденти можуть безпосередньо загрожувати безпеці, безперебійності роботи та національній логістиці. Щоб вирішити цю проблему, залізниці повинні застосовувати проактивні стратегії, засновані на аналітичних даних, зокрема обмежувати публічну інформацію про технології, усувати вразливості, проводити регулярне та своєчасне навчання співробітників, приєднуватися до галузевих спільнот з обміну інформацією про загрози, таких як R-ISAC та ER-ISAC, проводити регулярні оцінки вразливості та враховувати питання кібербезпеки в процесах закупівлі. Якщо залізничні компанії розглядатимуть кібербезпеку як одне з основних питань безпеки та застосовуватимуть модель «кібер-ланцюга знищення» для раннього виявлення й запобігання атакам, вони зможуть ефективніше захищати конфіденційні дані, операційні системи та, зрештою, громадську безпеку в умовах дедалі більш взаємопов’язаного цифрового середовища». ***(Erin Plemons, Ruben Pena. The safety case for cybersecurity // Simmons-Boardman Publishing, Inc. (https://www.railjournal.com/in_depth/the-safety-case-for-cybersecurity/). 23.04.2026).***

***

«Компанія Airbus придбає французьку фірму з кібербезпеки Quarkslab, щоб посилити свої захисні механізми, оскільки комерційні літаки дедалі більше залежать від програмного забезпечення та взаємопов’язаних цифрових систем, що підвищує ризик кібератак, які можуть порушити роботу, використати вразливості або поставити під загрозу безпеку польотів. Quarkslab, у складі якої працює близько 100 фахівців, що спеціалізуються на захисті критично важливого програмного забезпечення та систем від сучасних загроз, включаючи реверс-інжиніринг з використанням штучного інтелекту, володіє досвідом як в області наступальної, так і оборонної безпеки, а її флагманський продукт QShield призначений для захисту коду, даних та вбудованих систем… Угода, яку планується укласти у 2026 році, є другим придбанням Airbus у сфері кібербезпеки за менш ніж місяць і є частиною ширшої стратегії з побудови «суверенного» європейського потенціалу у сфері кібербезпеки, який менше залежатиме від іноземних, зокрема американських, технологій, створюючи загальноєвропейську мережу, що охоплюватиме Францію, Німеччину, Велику Британію, Іспанію та Фінляндію… Кібербезпека в авіації пов'язана з унікальними викликами, зумовленими складністю систем, що містять мільйони рядків коду, тривалим терміном експлуатації, поєднанням застарілих і сучасних архітектур, глобальними ланцюгами постачання, оперативними обмеженнями в режимі реального часу та зростаючою загрозою атак на основі штучного інтелекту. Це придбання свідчить про перехід до більш глибокої інтеграції кібербезпеки в процес проектування та експлуатації літаків, а не до її розгляду як допоміжної функції, що потенційно допоможе Airbus виділитися на світовому ринку в умовах геополітичної напруженості, яка змінює технологічні ланцюги постачання. У міру

того, як літаки перетворюються на взаємопов'язані цифрові платформи, кібербезпека стає невіддільною від фізичної безпеки, а експерти попереджають, що галузь повинна випереджати нові загрози, щоб зберегти свій високий рівень безпеки…» ***(Juergen T Steinmetz. Airbus Deepens Cybersecurity Push as Aviation Faces Rising Digital Threats // TravelNewsGroup (https://eturbonews.com/airbus-cybersecurity-quarkslab-aviation-digital-threats/). 21.04.2026).***

***

Кіберзахист закладів охорони здоров'я

«Швидка цифровізація сектору охорони здоров'я у поєднанні з його розгалуженою мережею взаємопов'язаних застарілих систем та цінними даними про пацієнтів зробила його надзвичайно привабливою та вразливою мішенню для кіберзлочинців. Як продемонструвала атака програм-вимагачів 2021 року на Національну службу охорони здоров'я Ірландії (HSE) — яка розпочалася з того, що один співробітник натиснув на посилання у фішинговому листі, і призвела до загальнонаціонального відключення ІТ-систем — навіть одне слабке місце може мати руйнівні наслідки. Зростаюча інтеграція штучного інтелекту, зокрема великих мовних моделей (LLM), створює новий рівень складних загроз…

На відміну від традиційних систем штучного інтелекту, непрозорий характер великих мовних моделей (LLM) робить їх вразливими до нових векторів атак, таких як «введення підказки», коли приховані інструкції в медичних даних можуть маніпулювати діагностичними інструментами на базі штучного інтелекту; «отруєння даних», яке забруднює навчальні дані; та «атаки через «задні двері», які встановлюють приховані шкідливі тригери. Ці вразливості можуть посилити загрозу від програм-вимагачів, оскільки зловмисники пошкоджуватимуть невеликі частини даних, а не шифруватимуть цілі системи, що зробить майже неможливим відрізнити справжню інформацію від підробленої…

Крім того, використання генеративної ШІ для створення синтетичних даних з метою досліджень відкриває шлях до «атак інверсії», під час яких зловмисники можуть змусити модель відтворити впізнавані медичні знімки пацієнтів та їхні особисті дані на основі навчального набору, перетворюючи саму ШІ на легкодоступну точку витоку даних. Щоб протидіяти цій мінливій загрозі, експерти виступають за багатовекторну стратегію захисту. Це включає впровадження принципу мінімальних привілеїв для агентів ШІ, що автоматично обмежуватиме їхні дозволи після обробки ненадійного контенту, а також сувору «пісочницю» для тестування моделей на вразливість в ізольованих середовищах перед розгортанням… Додаткові технічні заходи безпеки, такі як додавання шуму до навчальних даних та використання цифрових водяних знаків, можуть допомогти захистити конфіденційність та цілісність даних. Однак одних лише технологій недостатньо. Усі експерти сходяться на думці, що людський фактор залишається як найбільшою вразливістю, так і найнадійнішим захистом. Тому надзвичайно важливо вийти за межі суто технічних рішень і розвивати культуру проактивної,

колективної безпеки, що включає всебічну освіту персоналу щодо потенціалу ШІ та пов'язаних з ним ризиків, а також залучення клінічних фахівців, таких як радіологи, до навчань «червоної команди» для виявлення та усунення слабких місць системи з точки зору користувача». ***(Wolfgang Behrends. Poisoned pixels, phishing, prompt injection: Cybersecurity threats in AI-driven radiology // HiE (https://healthcare-in-europe.com/en/news/cybersecurity-threats-llm-radiology.html). 02.04.2026).***

***

«Атака програм-вимагачів, що сталася в лютому 2026 року на Медичний центр Університету Міссісіпі (UMMC), продемонструвала, наскільки безпосередньо програми-вимагачі можуть зашкодити роботі закладу та пацієнтам: вона вивела з ладу систему електронних медичних записів Епіс у 35 клініках та на понад 200 телемедичних майданчиках, змусила персонал перейти на паперові робочі процеси, а також призвела до скасування призначень на хіміотерапію та перенесення планових операцій. Цей інцидент відображає більш загальну тенденцію, за якої програми-вимагачі дедалі частіше стають загрозою для безперебійної роботи бізнесу у різних секторах — 93% медичних організацій США повідомили про щонайменше одну кібератаку у 2025 році, а 72% зазначили, що інцидент порушив процес надання медичної допомоги пацієнтам; водночас атака на платіжний процесор BridgePay у лютому 2026 року вивела з ладу критично важливі платіжні API та віртуальні термінали, а кількість публічно розкритих інцидентів із програмним забезпеченням-вимагачем зросла на 49% у порівнянні з попереднім роком у 2025 році — до 1 174 випадків…

Загроза також еволюціонувала від простого вимагання викупу за шифрування файлів до «подвійного вимагання», коли зловмисники спочатку викрадають конфіденційні дані, а потім шифрують системи, змушуючи жертв платити, щоб уникнути як простою, так і витоку даних; також зростає кількість випадків «потрійного вимагання», що передбачає додатковий тиск на клієнтів або партнерів. З огляду на 124 активні групи зловмисників, що використовують програми-вимагачі, виявлені у 2025 році — багато з яких з’явилися нещодавно — та інструменти штучного інтелекту, що знижують бар’єри для входу на ринок, лише периметральні засоби захисту та резервне копіювання вже не є достатніми, і що організаціям потрібні архітектури, які запобігають використанню викрадених даних як зброї, зберігаючи їх у нечитабельному вигляді після витоку, блокуючи доступ програм-вимагачів до файлів та забезпечуючи швидке відновлення… Як приклад такого підходу є платформа D.AMO від Penta Security, яка поєднує шифрування файлів на рівні папок, контроль доступу на основі процесів та користувачів для запобігання несанкціонованому доступу програм-вимагачів, централізований аудит, а також незалежне резервне копіювання та відновлення даних, що дозволяє зменшити залежність від необхідності оплати ключів дешифрування». ***(Evolution of Ransomware: Multi-Extortion Ransomware Attacks // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/evolution-of-ransomware-multi-extortion-ransomware-attacks/). 03.04.2026).***

***

«Компанія Hims & Hers, що спеціалізується на телемедицині та базується в Сан-Франциско, яка налічує близько 2,5 мільйонів передплатників, повідомила, що в лютому стала жертвою складної атаки з використанням методів соціальної інженерії, в результаті якої невідомий зловмисник отримав доступ до сторонньої платформи обслуговування клієнтів та переглянув запити клієнтів у період з 4 по 7 лютого... Компанія виявила підозрілу активність 5 лютого, забезпечила безпеку середовища обслуговування клієнтів та розпочала розслідування, повідомивши, що доступ до її системи електронних медичних записів та комунікацій з медичними працівниками не було отримано; викрадені дані складалися переважно з імен клієнтів та їхніх електронних адрес, хоча документи вказують на те, що хакери також могли отримати доступ до певної інформації про лікування деяких клієнтів, які зверталися до служби підтримки через платформу в період з лютого 2025 року по лютий 2026 року. Атака була спрямована на двох співробітників. Hims & Hers повідомила правоохоронні органи та переглядає політику, щоб запобігти повторенню інциденту, і заявила, що не очікує, що інцидент істотно вплине на фінансові результати…» ***(David Jones. Hims & Hers says limited data stolen in social engineering attack // TechTarget, Inc. (https://www.cybersecuritydive.com/news/hims-hers-data-stolen-social-engineering/816707/). 06.04.2026).***

***

«Сфера охорони здоров'я стрімко переходить на цифрові технології завдяки віртуальній медичній допомозі, хмарним додаткам та інструментам штучного інтелекту — цей процес прискорюється завдяки федеральним стимулам, таким як Програма трансформації охорони здоров'я в сільській місцевості, — однак така модернізація розширює площину вразливості сектору до кібератак, навіть попри те, що вона покращує масштабованість та економічну ефективність. Пропонована реформа Правил безпеки HIPAA має на меті запровадити більш суворі вимоги, механізми контролю за дотриманням та відповідальність, а аргументом на користь цього є те, що проблема безпеки в охороні здоров'я полягає не просто в самозаспокоєності чи недостатньому фінансуванні, а у властивій цій галузі складності надання медичної допомоги…

Сфера охорони здоров'я особливо вразлива, оскільки доступність систем має життєво важливе значення, захищена медична інформація є надзвичайно цінною і її важко «відновити», а медична допомога надається в рамках взаємопов'язаної екосистеми, що включає медичних працівників, страховиків, аптеки та постачальників, де слабкі місця можуть спричинити ланцюгову реакцію. На відміну від «складних» лінійних процесів, які можна виміряти та контролювати, робочі процеси в галузі охорони здоров'я є складними, нелінійними та часто ситуативними, що ускладнює аналіз та стандартизацію стану безпеки; наведені дослідження свідчать, що найскладніші системи охорони здоров'я (з найширшими схемами направлення пацієнтів) мають на 29% вищу ймовірність порушення безпеки, ніж у середньому..

Станом на березень 2026 року Міністерство охорони здоров'я та соціальних служб США (HHS) завершує роботу над найзначнішим оновленням Правил

безпеки HIPAA за останні понад два десятиліття, переходячи від гнучкого підходу на основі контрольних списків до більш суворого стандарту архітектури кібербезпеки та фактично скасовуючи давнє розмежування між «обов'язковими» та «рекомендованими» заходами безпеки. Рекомендованим рішенням є систематичний план дій «Zero Trust», адаптований до складності сфери охорони здоров'я, а Cisco структурує впровадження у три поетапні пріоритетні напрямки — персонал (безпечний віддалений доступ, MFA, контроль на основі ролей, SASE та моніторинг використання ШІ), робоче навантаження (мікросегментація, моніторинг та управління ШІ/захисні механізми DevSecOps для зменшення радіусу ураження) та робоче середовище (краща видимість та контекст, особливо для медичних пристроїв, для забезпечення NAC та сегментації) — за підтримки інструментів Cisco та консультативних оцінок готовності до дотримання вимог». ***(Mary Swigart. Complicated vs. Complex: Why Modern Healthcare Demands a Unique Approach to Cybersecurity // Cisco Systems, Inc. (https://blogs.cisco.com/industries/complicated-vs-complex-why-modern-healthcare-demands-a-unique-approach-to-cybersecurity). 06.04.2026).***

***

«…Майже через десять років після того, як у 2017 році атака програм-вимагачів WannaCry виявила критичні вразливості та спричинила масштабні збої в роботі Національної служби охорони здоров'я (NHS), організація продовжує зміцнювати свою систему кібербезпеки у відповідь на дедалі наполегливіші та складніші загрози. Глобальна атака, яка заблокувала доступ співробітників до систем і змусила повернутися до ручних процесів, стала значним поворотним моментом, прискоривши інвестиції та перетворивши кібербезпеку з нішевої ІТ-проблеми на основний операційний пріоритет. За словами експертів галузі, з того часу NHS досягла значного прогресу, покращивши прозорість систем та розвинувши більш скоординовані національні можливості реагування на інциденти…

Однак проблеми залишаються, зокрема необхідність забезпечення належного фінансування, вирішення питань, пов'язаних із застарілою інфраструктурою, а також чітке пояснення того, як кіберризики безпосередньо впливають на догляд за пацієнтами та їхню безпеку. Консультаційні компанії з питань кібербезпеки, які співпрацюють із Національною службою охорони здоров'я (NHS), наголошують, що кіберзахист — це не лише технологічне питання, а комплексна дисципліна, що охоплює людей, процеси та технології, і що для ефективного захисту системи охорони здоров'я до неї слід ставитися саме так». ***(Alexa Hornbeck. EXCLUSIVE: NHS strengthens cybersecurity resilience following legacy of WannaCry // HPCi Media Limited (https://buildingbetterhealthcare.com/exclusive-nhs-strengthens-cybersecurity-resilience-with-national-strategy). 08.04.2026).***

***

«…Компанія Signature Healthcare, яка управляє лікарнею Brockton Hospital та медичною групою Signature Medical Group, повідомила про інцидент у сфері кібербезпеки після виявлення підозрілої активності в мережі

та запуску процедур реагування на інциденти й забезпечення безперебійної роботи для забезпечення медичного обслуговування та безпеки пацієнтів. Стаціонарне лікування та послуги невідкладної допомоги без попереднього запису продовжували надаватися, проте станом на вівторок карети швидкої допомоги все ще перенаправляли в інші заклади; хірургічні операції та процедури не зазнали змін, однак сеанси хіміотерапії було скасовано, а пацієнтів попередили про можливі затримки у всіх медичних групах та пунктах невідкладної допомоги… Деякі роздрібні аптеки закрилися в понеділок і знову відкрилися у вівторок для консультацій, але не могли відпускати ліки за рецептами. Організація не підтвердила використання програм-вимагачів або мотивів зловмисників, і жодна група хакерів поки що не взяла на себе відповідальність за інцидент. Це відбувається на тлі глобальної хвилі кібератак на об'єкти охорони здоров'я, які спричиняють серйозні витоки даних і, в деяких випадках, пов'язані з нанесенням шкоди пацієнтам». ***(Eduard Kovacs. Massachusetts Hospital Diverts Ambulances as Cyberattack Causes Disruption // SecurityWeek (https://www.securityweek.com/massachusetts-hospital-diverts-ambulances-as-cyberattack-causes-disruption/). 08.04.2026).***

***

«Захист приватного життя та інформаційна безпека стали ключовими складовими захисту інтелектуальної власності у сфері охорони здоров’я, де особисті медичні записи є конфіденційною особистою інформацією, яка потребує надійних правових та технічних заходів захисту. Спочатку сформульоване Уорреном та Брандейсом у 1890 році як право людини, поняття приватного життя перетворилося на комплексну систему захисту даних, покликану захищати громадян від несанкціонованого доступу, розголошення або зловживання їхньою інформацією. У сфері охорони здоров’я це є особливо важливим, оскільки пацієнти часто вагаються ділитися конфіденційною інформацією, такою як діагнози туберкульозу або ВІЛ, через побоювання соціальної або офіційної дискримінації…

Поняття «приватність» стосується права особи контролювати свої персональні дані, тоді як інформаційна безпека охоплює технічні та організаційні заходи — такі як брандмауери, криптографія, біометрія та контроль доступу — що застосовуються для захисту даних, які зберігаються та обробляються. Ці два поняття тісно пов’язані між собою: ефективна інформаційна безпека слугує практичним механізмом для забезпечення прав на приватність. Загальний регламент про захист даних (GDPR) Європейського Союзу, який набрав чинності у травні 2018 року, став основою для медичних закладів, що працюють у країнах-членах ЄС. Він вимагає законної, прозорої та безпечної обробки персональних даних, а також передбачає такі зобов’язання, як призначення відповідальних за захист даних, навчання персоналу та впровадження систем управління ризиками…

Дотримання вимог GDPR — це не лише технічне завдання, а й процес, що вимагає активної участі керівництва та управлінського персоналу для забезпечення конфіденційності пацієнтів поряд із наданням якісної медичної допомоги. Дослідження вказують на постійні виклики в сфері управління, такі як узгодження

вимог щодо конфіденційності з інформаційною безпекою в цифрових середовищах, регулювання політики використання власних пристроїв (BYOD), забезпечення відповідності вимогам під час резервного копіювання даних та виконання запитів на їх видалення, а також вирішення питань щодо неоднозначності прав власності на роботи, виконані на замовлення або в рамках співпраці. Дослідження також підкреслюють важливість методів подвійного підтвердження прав, включаючи офіційну реєстрацію авторських прав та криміналістичний аналіз блокчейну, а також чіткі договірні угоди для встановлення ланцюжків власності… Загалом, захист інтелектуальної власності у сфері охорони здоров'я у формі особистих медичних даних вимагає збалансованого підходу, що поєднує дотримання законодавчих вимог, технічні заходи контролю та організаційне управління, щоб мінімізувати порушення, забезпечити дотримання нормативних вимог та зберегти довіру пацієнтів у дедалі більш цифровому середовищі». ***(Hina Saif. Relationship between Privacy and Information Security and the Role of Government // HackerNoon (https://hackernoon.com/relationship-between-privacy-and-information-security-and-the-role-of-government). 17.04.2026).***

***

«Компанія ChipSoft, провідний нідерландський постачальник програмного забезпечення для ведення електронних медичних карток, підтвердила, що веде активні переговори з кіберзлочинцями, які на початку цього місяця викрали конфіденційні дані пацієнтів. В результаті атаки, яку, як вважається, здійснила хакерська група Embargo, було викрадено медичну інформацію від сімейних лікарів, реабілітаційних центрів та Офтальмологічної лікарні Роттердама. Після зломи хакери розмістили в даркнеті лічильники зворотного відліку, погрожуючи оприлюднити дані, хоча згодом їх було видалено… Хоча компанія ChipSoft зберігає мовчання щодо подробиць переговорів або можливих виплат викупу, щоб захистити інтереси постраждалих, цей інцидент спричинив значні перебої в роботі, через що багато лікарень в якості запобіжного заходу тимчасово закрили свої онлайн-портали для пацієнтів. Цей злом є частиною ширшої хвилі масштабних кібератак, спрямованих останнім часом проти нідерландських установ, зокрема Міністерства фінансів та кількох відомих приватних компаній». ***(Hacked healthcare software firm ChipSoft in negotiations with cybercriminals // NL Times (https://nltimes.nl/2026/04/23/hacked-healthcare-software-firm-chipsoft-negotiations-cybercriminals). 23.04.2026).***

***

«AstraZeneca», світовий фармацевтичний гігант і піонер у розробці вакцини проти COVID-19, нещодавно стала жертвою кібератаки з боку міжнародного хакерського угруповання, відомого під назвою Lapsus$. Факт порушення безпеки підтвердило Британське управління з питань інформації (ICO), яке заявило, що надало компанії рекомендації після «кіберінциденту», що стався у березні 2026 року, а потім закрило справу без вжиття офіційних заходів. Згідно з різними публікаціями в даркнеті, хакерська група, відома своїми попередніми гучними атаками на такі компанії, як Microsoft і Nvidia, стверджує, що викрала 3 ГБ

конфіденційних даних. Сюди нібито входять вихідний код програмного забезпечення, записи про співробітників, деталі хмарної інфраструктури та API-ключі, які, за повідомленнями, хакери намагаються продати тому, хто запропонує найвищу ціну…

Хоча компанія AstraZeneca відмовилася коментувати цю ситуацію, заяви групи викликали серйозну стурбованість щодо безпеки конфіденційних даних у компанії, яка наразі керує важливими ініціативами у сфері охорони здоров'я, зокрема дослідженнями в галузі онкології. Цей інцидент є частиною загального сплеску кіберзагроз, спрямованих проти даних, пов'язаних зі сферою охорони здоров'я; він стався після нещодавнього підтвердження урядом того, що внаслідок окремого злом бази даних Biobank особисті дані 500 000 добровольців були виставлені на продаж на веб-сайті Alibaba. Lapsus$, яку часто характеризують як групу підлітків-хакерів, що використовують як технічні експлойти, так і соціальну інженерію, продовжує становити серйозну загрозу для великих глобальних корпорацій та критичної інфраструктури». ***(Luke Alsford. Global drug company AstraZeneca 'hacked' by teenage cyber gang // Associated Newspapers Limited (https://metro.co.uk/2026/04/23/global-drug-company-astrazeneca-hacked-teenage-cyber-gang-28089598/?ito=newsnow-feed). 23.04.2026).***

***

Захист персональних даних та соціальні мережі

«Сучасна сфера підбору персоналу сповнена ризиків у сфері кібербезпеки, про що свідчать такі інциденти, як витік у 2025 році 26 мільйонів резюме з неправильно налаштованого хмарного сервера, а також постійний потік витончених фішингових атак, спрямованих проти фахівців з управління персоналом… З огляду на те, що середня вартість порушення безпеки даних становить майже 4,9 мільйона доларів, для організацій вкрай важливо забезпечити захист конфіденційних даних кандидатів, не перевантажуючи при цьому рекрутерів технічним жаргоном або громіздкими робочими процесами. Аналіз десятків постачальників рішень з безпеки виявив набір із семи інструментів, спеціально розроблених для реалій дистанційного рекрутингу, що ставлять на перше місце захист даних, простоту використання, безперебійну інтеграцію та реальну ефективність…

Основу цієї архітектури становить VPN-сервіс TorGuard Dedicated IP, який забезпечує шифрування мережевого трафіку та додавання до білого списку єдиної захищеної IP-адреси для критично важливих систем. Далі йде 1Password Business, що дозволяє усунути слабкі та повторно використовувані паролі завдяки спільному зашифрованому сховищу. Потім Okta Workforce Identity створює єдиний вхід із функцією єдиного входу та адаптивною багатофакторною автентифікацією, а CrowdStrike Falcon забезпечує захист кінцевих пристроїв у режимі реального часу від шкідливого програмного забезпечення та програм-вимагачів на ноутбуках рекрутерів… Далі Proofpoint Email Security очищає поштові скриньки, ізолюючи

вкладення в пісочниці та блокуючи шахрайські спроби підробки особи, а Box Shield виконує роль безпечного, зашифрованого сховища файлів, яке забезпечує дотримання правил доступу та автоматизує зберігання даних. Нарешті, програма навчання з питань інформаційної безпеки KnowBe4 Security Awareness Training створює «людський брандмауер», навчаючи співробітників розпізнавати та повідомляти про спроби фішингу та соціальної інженерії, перетворюючи найслабшу ланку на міцну лінію оборони…

Впроваджуючи ці інструменти трьома послідовними етапами — спочатку забезпечуючи безпеку мережі, ідентифікації та паролів, потім посилюючи захист кінцевих пристроїв та електронної пошти, а насамкінець формуючи культуру, орієнтовану на безпеку, — організації можуть ефективно захистити процес підбору персоналу, зменшити операційні труднощі та зберегти довіру кандидатів, не перевищуючи при цьому свій бюджет». ***(7 Best Cybersecurity Tools for Remote Recruitment Teams: Guard Candidate PII // Onrec (https://www.onrec.com/news/news-archive/7-best-cybersecurity-tools-for-remote-recruitment-teams). 07.04.2026).***

***

«…Наші цифрові сліди, зокрема файли cookie веб-сайтів, дають правоохоронним органам потужний інструмент для розкриття злочинів, водночас викликаючи серйозні занепокоєння щодо конфіденційності у широкої громадськості. Про це свідчить нещодавній випадок в Огайо, де слідчі використали видані судом ордери на обшук, щоб отримати доступ до даних файлів cookie Google з iPhone підозрюваного. Ці дані показали, що з цього пристрою здійснювався доступ як до анонімного облікового запису Gmail, пов'язаного з погрозою вибуху в суді, так і до другого, ідентифікованого облікового запису, що в кінцевому підсумку призвело до арешту та пред'явлення звинувачень Донтавіусу Конлі. Хоча заспокоює той факт, що правоохоронні органи повинні отримати ордер для доступу до такої приватної інформації, як це підтверджують прецеденти Верховного суду США, цей інцидент підкреслює, наскільки наші пристрої та додатки відстежують нас, навіть у так званих режимах «інкогніто». Для осіб, стурбованих таким рівнем спостереження, це суворе нагадування про те, що цифрова конфіденційність не є самоочевидною і вимагає свідомих зусиль для її забезпечення…» ***(Joe Oliveto. Police Are Using Cookies To Catch Criminals - Here's How // Static Media. (https://www.bgr.com/2135565/how-police-use-computer-cookies-to-catch-criminals/). 05.04.2026).***

***

«Згідно зі звітом Fairlinked eV та незалежно підтвердженим BleepingComputer, LinkedIn під час кожного завантаження сторінки вбудовує скрипт JavaScript для ідентифікації, який перевіряє браузери відвідувачів на базі Chromium на наявність 6 236 конкретних розширень Chrome та збирає додаткові телеметричні дані про пристрій, такі як кількість ядер процесора, обсяг вільної пам’яті, роздільна здатність екрана, часовий пояс, мовні налаштування, стан акумулятора та інші сигнали для ідентифікації

апаратного та програмного забезпечення. У звіті Fairlinked «BrowserGate» стверджується, що виявлення розширень працює шляхом спроби доступу до ресурсів, пов'язаних із відомими ідентифікаторами розширень, що є задокументованою технікою ідентифікації встановлених розширень, і зазначається, що попереднє публічне відстеження показало, що LinkedIn сканував приблизно 2 000 розширень у 2025 році та близько 3 000 на початку цього року, що свідчить про швидке розширення до нинішніх масштабів… Багато з проаналізованих розширень є інструментами, пов’язаними з LinkedIn або конкуруючими з ним, зокрема продуктами для аналізу продажів, такими як Apollo, Lusha та ZoomInfo. У звіті стверджується, що список налічує понад 200 конкуруючих продуктів, а також розширення з інших категорій (наприклад, інструменти для вивчення мови та граматики, а також розширення, пов’язані з оподаткуванням). Оскільки профілі LinkedIn пов'язані з реальними особами (іменами, роботодавцями, посадами), поєднання даних про розширення та відбитків пристроїв може бути пов'язане з конкретними особами; у звіті також стверджується, що дані надсилаються до HUMAN Security, хоча ця передача не була незалежно перевірена.

Компанія LinkedIn повідомила виданню BleepingComputer, що сканування має на меті виявлення розширень, які збирають дані або порушують її умови використання, позиціонуючи це як захід із забезпечення конфіденційності та стабільності сайту, а також зазначила, що не використовує ці дані для отримання конфіденційної інформації; вона також заперечила контекст публікації, вказавши, що обліковий запис видавця було обмежено через збір даних, пов’язаний із розширенням (Teamfluence), і що німецький суд відмовився видати судову заборону щодо заходів LinkedIn із забезпечення дотримання правил». ***(Luke James. LinkedIn is spying on you, according to a new 'BrowserGate' security report — scripts stealthily scan visitors' browsers for over 6,000 Chrome extensions and harvest hardware data // Future US, Inc. (https://www.tomshardware.com/software/browsers/linkedin-scans-visitors-browsers-for-over-6000-chrome-extensions-and-collects-device-data). 04.04.2026).***

***

«Захист та безпека даних зазнають фундаментальних змін, перетворюючись із вузьких технічних вимог на ключовий принцип «обов’язку дбати», що визначає сучасне управління. Оскільки захищена інформація часто стосується благополуччя окремих осіб, організації переосмислюють управління ризиками як юридичний та етичний обов’язок щодо запобігання передбачуваній шкоді, такій як витік даних, компрометація особистих даних або системні перебої в роботі сервісів. Ця зміна підняла кіберризики та операційні ризики на той самий рівень пріоритетності, що й фінансові та стратегічні ризики на рівні ради директорів, зробивши цифрову довіру стратегічним чинником, що вирізняє компанію серед конкурентів…

Для практичної реалізації цього обов’язку дбайливого ставлення необхідно відійти від статичних щорічних оцінок на користь постійного моніторингу ризиків та міжфункціональної співпраці між юридичним, безпековим, кадровим та операційним відділами. Крім того, оскільки організації стають дедалі більш

залежними від хмарних послуг та складних екосистем постачальників, сфера цієї відповідальності тепер виходить за межі внутрішньої інфраструктури та включає надійне управління постачальниками та моніторинг сторонніх організацій. Відносностійкість — здатність реагувати на інциденти, підтримувати функціонування основних послуг та швидко відновлюватися — стала основним критерієм, за яким зацікавлені сторони оцінюють етичне управління організацією…

Хоча термін «обов'язок дбати» не завжди прямо згадується в нормативних документах, цей принцип глибоко вкорінений у вимогах таких стандартів, як Рамка кібербезпеки NIST, ISO 27001, SOC 2 та CMMC. Ці рамки забезпечують практичну основу для впровадження «розумних заходів захисту» та демонстрації керівного нагляду. Зрештою, оскільки нові технології, такі як штучний інтелект, створюють нові форми ризиків, найбільш успішними будуть ті організації, які вбудують цей проактивний обов'язок дбайливості у свою корпоративну культуру, розглядаючи його як фундаментальну філософію діяльності, а не лише як регуляторну вимогу». ***(Michael Peters. What is the Duty of Care in Cybersecurity? // Techstrong Group Inc. (https://securityboulevard.com/2026/04/what-is-the-duty-of-care-in-cybersecurity/). 24.04.2026).***

***

Масштабні витоки персональних даних

«В результаті злому в освітньому видавництві McGraw Hill було викрадено близько 13,5 мільйонів записів користувачів; цей витік незалежно підтвердив ресурс Have I Been Pwned після аналізу даних, опублікованих в Інтернеті. Інцидент вперше з'явився на сайті здирників ShinyHunters, де група заявила, що отримала доступ до десятків мільйонів записів у системі Salesforce, пов'язаних із McGraw Hill, і висунула ультиматум «плати або ми опублікуємо дані»; після того, як переговори, судячи з усього, провалилися, було опубліковано понад 100 ГБ даних. Витік даних містить приблизно 13,5 мільйонів унікальних електронних адрес і, у багатьох випадках, додаткові особисті дані, такі як імена, номери телефонів та фізичні адреси, хоча ці поля присутні не в кожному записі… Компанія McGraw Hill заявила, що витік інформації стався через неправильну конфігурацію веб-сторінки, розміщеної на платформі Salesforce, а не внаслідок прямого злому її внутрішніх систем, і зазначила, що доступ до основних систем, таких як бази даних клієнтів та платформи навчальних матеріалів, не було отримано, представивши цей випадок як частину більш загальної проблеми з конфігурацією, що зачепила багатьох клієнтів Salesforce… Цей випадок підкреслює системний ризик, пов'язаний із сторонніми розробниками та конфігурацією хмарних сервісів, що відповідає історії ShinyHunters, яка полягає у використанні вразливих хмарних сервісів та інтеграцій, а потім застосуванні тактик викрадення даних та вимагання. Хоча багато електронних листів вже були присутні в попередніх наборах даних про порушення, значна частина з них стала доступною нещодавно, що збільшує ймовірність фішингу та шахрайства, спрямованого на

крадіжку особистих даних; постраждалим користувачам рекомендується бути обережними щодо підозрілих повідомлень, використовувати унікальні паролі, увімкнути багатофакторну автентифікацію та стежити за незвичайною активністю в своїх облікових записах». ***(Amar Ćemanović. McGraw Hill data breach incident exposed 13.5 million accounts // CyberInsider (https://cyberinsider.com/mcgraw-hill-data-breach-incident-exposed-13-5-million-accounts/). 16.04.2026).***

***

«Французьке урядове агентство France Titres, відповідальне за видачу офіційних документів, що посвідчують особу та реєстрацію, таких як водійські посвідчення, національні посвідчення особи, паспорти та імміграційні документи, повідомило про витік даних, внаслідок якого, ймовірно, була розкрита особиста інформація невідомої кількості користувачів. Інцидент було виявлено 15 квітня 2026 року, і наразі триває розслідування. Дані, що потенційно можуть бути скомпрометовані, включають логіни, імена, адреси електронної пошти, дати народження, унікальні ідентифікатори облікових записів, а в деяких випадках — поштові адреси, місця народження та номери телефонів. Агентство підтвердило, що жодні додаткові процедурні дані, такі як вкладення, не були викриті, і що витік не дозволяє отримати несанкціонований доступ до облікових записів користувачів на порталі… Постраждалі особи вже отримали відповідне повідомлення, і агентство порекомендувало їм зберігати пильність щодо можливих фішингових спроб через SMS, дзвінки або електронні листи, в яких зловмисники видають себе за представників France Titres. Про інцидент було повідомлено французькому регулятору з питань захисту даних CNIL відповідно до GDPR, прокурору Парижа для порушення кримінального розслідування, а також національному органу з кібербезпеки ANSSI. France Titres вжила додаткових заходів безпеки для захисту поточних операцій та даних користувачів, а також попередила, що будь-який продаж або розповсюдження викраденої інформації є незаконним». ***(Sinisa Markovic. Cyberattack on French government agency triggers phishing alert // Help Net Security (https://www.helpnetsecurity.com/2026/04/22/france-titres-online-portal-data-breach/). 22.04.2026).***

***

«Нідерландський косметичний гігант Rituals підтвердив витік даних, в результаті якого хакери викрали особисту інформацію з бази даних членів клубу; це торкнулося клієнтів у Європі, Великій Британії та деяких у Сполучених Штатах. Компанія повідомила про інцидент у листі, надісланому постраждалим клієнтам, зазначивши, що в результаті несанкціонованого викрадення даних у квітні були викрадені повні імена, дати народження, стать, поштові та електронні адреси, номери телефонів, улюблені магазини та типи облікових записів. Rituals заявила, що розслідує обставини витоку, але відмовилася надати додаткові деталі, зокрема щодо того, чи вимагали викуп, та точної кількості постраждалих клієнтів, посилаючись на міркування безпеки… Маючи понад 41 мільйон членів та дохід у розмірі 2,4 мільярда євро у 2025 році, Rituals стала

черговою великою торговельною мережею, яка зазнала витоку даних про членство клієнтів. Це сталося після аналогічних інцидентів у британських мережах Co-op та Marks & Spencer, де такі записи стали привабливою мішенню для хакерів, які намагаються шантажувати компанії, погрожуючи оприлюднити інформацію в Інтернеті. Компанія повідомила постраждалих клієнтів та порадила їм бути пильними щодо можливих спроб фішингу». ***(Zack Whittaker. Cosmetics giant Rituals confirms data breach of customer membership records // (https://techcrunch.com/2026/04/22/cosmetics-giant-rituals-confirms-data-breach-of-customer-membership-records/). 22.04.2026).***

***

«Кібератака, що сталася в грудні на компанію Eurail (Нідерланди), яка займається продажем проїзних Interrail для подорожей 33 країнами, призвела до витоку та продажу конфіденційних персональних даних понад 300 000 клієнтів. Викрадена інформація, яка з'явилася в даркнеті та Telegram, включає номери паспортів, повні імена, домашні адреси, контактні дані та дати народження…

Цей витік даних викликав широке занепокоєння та розчарування серед мандрівників, особливо з огляду на те, що уряди різних європейських країн почали радити постраждалим особам анулювати та замінити свої паспорти, щоб запобігти шахрайству з особистими даними. Ці офіційні рекомендації викликали критику з боку клієнтів, які зараз стикаються зі значними витратами на заміну документів та відсутністю чітких вказівок щодо серйозності ризику…

Хоча компанія Eurail висловила жаль з приводу інциденту та закликала користувачів стежити за своїми фінансовими рахунками й оновлювати паролі, багато потерпілих як і раніше критично ставляться до стандартів захисту даних компанії. Відповідно, цей інцидент спричинив заклики до колективних судових позовів та вимагання компенсації відповідно до Загального регламенту про захист даних (GDPR) ЄС. Eurail продовжує повідомляти постраждалих осіб, працюючи над мінімізацією ризиків, пов'язаних із витоком даних». ***(Hazel Belkis Belge. Over 300,000 Europeans' data on sale on dark web after December cyberattack on Eurail: Report // Anadolu Ajansı (https://www.aa.com.tr/en/world/over-300-000-europeans-data-on-sale-on-dark-web-after-december-cyberattack-on-eurail-report/3915890). 23.04.2026).***

***

«Компанія з охорони житла ADT повідомила про витік даних, в результаті якого кіберзлочинці викрали «обмежений набір» інформації про клієнтів та потенційних клієнтів, зокрема імена, номери телефонів, адреси, дати народження та останні чотири цифри номерів соціального страхування й податкових ідентифікаційних номерів; при цьому дані про платежі не були скомпрометовані, а системи безпеки клієнтів не зазнали впливу. Компанія безпосередньо повідомила про це постраждалих осіб, запропонувала безкоштовні послуги із захисту особистих даних у відповідних випадках, повідомила правоохоронні органи та залучила сторонніх експертів з кібербезпеки для

розслідування інциденту. Група кіберзлочинців, відома під назвою ShinyHunters, взяла на себе відповідальність за інцидент і заявила, що викрала 10 мільйонів записів, погрожуючи оприлюднити дані, якщо не буде сплачено викуп… Компанія ADT не підтвердила, чи надходила вимога про викуп і чи ведуться переговори. Цей злом є останнім у серії гучних атак, що приписуються групі ShinyHunters, яка була відносно спокійною після заходів правоохоронних органів у 2025 році, що призвели до тюремних вироків для деяких її членів, але знову з'явилася на початку цього року, взявши на себе відповідальність за інциденти, пов'язані з такими компаніями, як Rockstar, McGraw Hill, Bumble, Match Group, Canada Goose, Університет Пенсильванії та Європейська комісія. Компанія ADT, яка минулого року повідомила про дохід у розмірі 5,1 млрд доларів, протягом останніх двох років неодноразово повідомляла Комісії з цінних паперів і бірж про численні інциденти у сфері кібербезпеки. Цей інцидент підкреслює постійну вразливість великих компаній, що працюють із споживачами, до крадіжок даних та спроб вимагання з боку досвідчених кіберзлочинних угруповань». ***(Jonathan Greig. ADT says customer data stolen in cyber intrusion // Recorded Future News (https://therecord.media/ADT-data-breach-cyberattack). 24.04.2026).***

***

Кібербезпека та хмарні технології

«Всесвітній день безпеки хмарних технологій підкреслює зростаючу необхідність захисту хмарних даних, а цьогорічна дискусія зосереджується на прозорості ідентифікації в кібербезпеці та гнучкому впровадженні хмарних технологій у сфері фізичної безпеки. Джеймс Мод з BeyondTrust зазначає, що багато інцидентів у хмарі пов’язані не стільки з витонченими атаками, скільки з повсякденними рішеннями щодо доступу, неправильними налаштуваннями та зловживанням обліковими даними, дозволами або токенами; оскільки навіть одна скомпрометована ідентичність може спричинити масштабні порушення «зі швидкістю машини», організації повинні надавати пріоритет прозорості ідентифікації та доступу, скорочувати постійні привілеї та посилювати контроль доступу, щоб обмежити радіус ураження, а не просто додавати більше рівнів безпеки…

У сфері фізичної безпеки компанія Genetec наголошує, що стратегії, які передбачають виключно хмарні рішення, часто не враховують реалії експлуатації, а її звіт «Стан фізичної безпеки у 2026 році» показує, що впровадження гібридних хмарних рішень часто зумовлене потребами у забезпеченні відмовостійкості, такими як масштабованість (39%) та надмірність (38%). Франсіс Лашанс із Genetec стверджує, що підприємства зазвичай паралельно використовують хмарні, локальні та гібридні розгортання, тому системи та хмарні стратегії повинні підтримувати безперебійну роботу в усіх моделях, щоб забезпечити довгострокове управління, прозорість та контроль». ***(Jordyn Alger. World Cloud Security Day: Breaking Down the State of Cloud Cybersecurity and Physical Security // BNP Media, Inc.***

(https://www.securitymagazine.com/articles/102204-world-cloud-security-day-breaking-down-the-state-of-the-cloud-cybersecurity-and-physical-security). 03.04.2026).

***

Кібербезпека Інтернету речей. Штучний інтелект

«Штучний інтелект кардинально змінює ландшафт кібербезпеки, створюючи гонку озброєнь з високими ставками, де ШІ виступає як потужна зброя для зловмисників, так і незамінний інструмент для захисників. Наприкінці минулого року компанія Anthropic повідомила про першу відому велику кібератаку, здійснену переважно агентом ШІ, під час якої китайські хакери, що діяли за підтримки держави, проникли приблизно в 30 глобальних організацій, практично не потребуючи людського нагляду. Цей інцидент ознаменував початок нової ери, в якій технології ШІ можуть самостійно писати код, використовувати програмне забезпечення та виявляти вразливості безпеки з безпрецедентною швидкістю та масштабом… У міру стрімкого вдосконалення моделей штучного інтелекту, таких як розробки компаній Anthropic та OpenAI, фахівці з безпеки отримали можливість завчасно виявляти сотні раніше невідомих вразливостей «нульового дня» у критично важливому програмному забезпеченні з відкритим кодом, зокрема серйозну помилку в операційній системі Linux, яка залишалася непоміченою з 2003 року. Однак ця ж сама потужність тепер знаходиться в руках зловмисників, які використовують ШІ для автоматизації розвідки, розробки складних фішингових кампаній, прискорення розробки шкідливого програмного забезпечення та швидкої торгівлі доступом до скомпрометованих систем — скорочуючи час транзакцій з годин до лічених секунд… Хоча компанії, що займаються штучним інтелектом, запровадили заходи безпеки, щоб запобігти використанню їхніх інструментів для атак, хакери вміють обходити ці бар’єри, часто маскуючи свою діяльність під нешкідливі навчальні вправи з безпеки. Поки експерти розходяться в думках щодо того, чи штучний інтелект у кінцевому підсумку сприяє нападу чи обороні, існує чіткий консенсус щодо того, що організації та уряди повинні активно впроваджувати штучний інтелект у оборонних цілях, інакше вони ризикують стати катастрофічно вразливими. Як попередив один із лідерів галузі, це найзначніша зміна, яку коли-небудь бачило кіберсередовище, і єдиний спосіб ефективно боротися з загрозами, пов'язаними зі штучним інтелектом, — це «боротися зі штучним інтелектом за допомогою штучного інтелекту». ***(Cade Metz and Kate Conger. A.I. Is on Its Way to Upending Cybersecurity // The New York Times Company (https://www.nytimes.com/2026/04/06/technology/ai-cybersecurity-hackers.html). 07.04.2026).***

***

«За два тижні до офіційного оголошення компанія Anthropic випадково оприлюднила деталі щодо Claude Mythos Preview — революційної моделі штучного інтелекту, яку визнали надто небезпечною для широкого випуску через її здатність використовувати вразливості в системі кібербезпеки швидше, ніж можуть зреагувати люди, що її захищають. Одночасно з запуском цієї передової системи, яка використовує вдосконалені логічні висновки для поєднання численних програмних вразливостей у складні атаки, компанія Anthropic представила Project Glasswing — спільну ініціативу, до якої долучилися понад 40 провідних технологічних корпорацій, зокрема Apple, Google та Microsoft…

Цей проєкт надає партнерам ранній доступ до моделі, що дозволяє їм завчасно виявляти та усувати вразливості у власних системах та критично важливій інфраструктурі з відкритим кодом. Проєкт підтримується кредитами на використання на суму 100 мільйонів доларів та пожертвою у розмірі 4 мільйонів доларів на підтримку ініціатив з безпеки у сфері відкритого програмного забезпечення. З моменту початку тестування модель виявила тисячі вразливостей високого рівня небезпеки, зокрема критичні недоліки в ядрі Linux та OpenBSD, які залишалися невиявленими протягом десятиліть.

Експерти галузі, такі як Алекс Стамос, застерігають, що моделі з відкритим кодом можуть досягти таких можливостей вже за півроку, що потенційно дасть зловмисникам, які використовують програми-вимагачі, змогу масово застосовувати вразливості, не залишаючи слідів. Хоча Ентоні Гріко з компанії Cisco наголошує на кардинальній зміні пріоритетів у питанні захисту критичної інфраструктури, такий крок викликає серйозні побоювання щодо централізації повноважень і ризиків, оскільки одна приватна організація тепер володіє великим набором експлойтів «нульового дня», які можуть стати об’єктом крадіжки… Крім того, незважаючи на те, що компанія Anthropic проінформувала представників уряду США про ці можливості, напруженість у регуляторній сфері зберігається через минулі судові суперечки щодо ризиків у ланцюгах постачання, що підкреслює складність управління надлюдськими можливостями ШІ в умовах мінімального регулювання, тоді як громадськість дедалі частіше вимагає посилення заходів безпеки». ***(Casey Newton. Why Anthropic’s new model has cybersecurity experts rattled // Platformer (https://www.platformer.news/anthropic-mythos-cybersecurity-risk-experts/). 07.04.2026).***

***

«Міністр фінансів США Скотт Бессент і голова Федеральної резервної системи Джером Пауелл нещодавно попередили лідерів Уолл-стріт про значне загострення кібергонки озброєнь: появу «Mythos» — нової моделі штучного інтелекту від компанії Anthropic, здатної виявляти та експлуатувати вразливості програмного забезпечення з безпрецедентною швидкістю та мінімальним втручанням людини. Ця модель, яка вже виявила тисячі «нульових» вразливостей у основних операційних системах та браузерах — деякі з яких залишалися невиявленими протягом десятиліть — є переломним моментом у кібербезпеці. Через величезну потужність моделі, яка може сприяти руйнівним кібератакам у разі зловживання, компанія Anthropic вирішила не випускати її у

відкритий доступ. Натомість компанія започаткувала «Project Glasswing» — обмежену програму, що надає доступ до перевіреної групи з понад 40 партнерів, серед яких такі технологічні гіганти, як Microsoft, Google та Apple, фінансові установи, як-от JPMorganChase, та Linux Foundation, для використання цього інструменту в оборонних цілях, таких як превентивні тестування на проникнення…

Розробка Mythos відбувається паралельно з аналогічними ініціативами таких компаній, як OpenAI та Google, що свідчить про загальний зсув у галузі в бік автономних засобів безпеки. Хоча Anthropic стверджує, що такі моделі ШІ зрештою стануть на користь захисникам, забезпечуючи швидше зміцнення програмного забезпечення, найближчі перспективи залишаються нестабільними. Компанія визнала, що робота над засобами захисту ще триває, зазначивши тривожні особливості поведінки в ранніх версіях. Крім того, оборонні переваги Mythos наразі нівелюються тим фактом, що хакери використовують ШІ для прискорення власного використання нещодавно виявлених вразливостей, залишаючи організаціям дедалі менший проміжок часу для виправлення систем. Зрештою, хоча Anthropic передбачає довгострокове майбутнє, в якому програмне забезпечення буде значно безпечнішим завдяки коду, написаному ШІ, нинішній перехідний період створює підвищений рівень ризику, оскільки як захисники, так і супротивники стрімко розширюють свої кіберможливості». ***(Andrew Martin Bloomberg. Why officials are so worried about Mythos, Anthropic's new AI tool // Gulf Times (https://www.gulf-times.com/article/723783/opinion/why-officials-are-so-worried-about-mythos-anthropics-new-ai-tool). 11.04.2026).***

***

«Ринок кібербезпеки стикається з посиленою актуальністю проблеми після помилки в налаштуваннях системи безпеки компанії Anthropic, яка на короткий час призвела до витоку «Claude Mythos» — передової моделі штучного інтелекту, здатної самостійно виявляти та використовувати уразливості «нульового дня». Цей інцидент спричинив різке падіння акцій компаній у сфері кібербезпеки та висвітлив критичну слабкість: хоча загрози на основі штучного інтелекту швидко еволюціонують, більшість підприємств досі не мають офіційних дорожніх карт щодо квантово-безпечного шифрування, що залишає конфіденційні хмарні дані вразливими до майбутніх атак з розшифрування. У відповідь на ці ризики, що посилюються, п'ять ключових гравців галузі просувають платформи, орієнтовані на захист на основі штучного інтелекту та модернізацію криптографії…

Компанія Quantum Secure Encryption (QSE) бореться з «квантовою кризою» завдяки запуску QPA v2 — корпоративної платформи, яка надає структуровану основу для організацій з метою оцінки їхніх поточних вразливостей у шифруванні та планування переходу на постквантові стандарти; компанія також розширює свою присутність у муніципальному секторі та секторі оборони. Тим часом SentinelOne поглибила стратегічну співпрацю з Google Cloud з метою розробки масштабних рішень у сфері безпеки на основі штучного інтелекту, зосередившись на суверенітеті даних та автономному захисті кінцевих точок. Elastic зміцнила свої позиції на федеральному ринку, отримавши авторизацію FedRAMP High, що

дозволяє їй обробляти надзвичайно чутливі несекретні робочі навантаження уряду США… Компанія Rapid7 зробила крок у напрямку автономної безпеки, придбавши Kenzo Security — платформу на основі штучного інтелекту з агентами, яка забезпечує розслідування та реагування зі швидкістю роботи машин. Нарешті, компанія Broadcom запустила Symantec CBX — уніфіковану платформу, яка інтегрує технології Symantec і Carbon Black для надання розширених можливостей виявлення та реагування на основі штучного інтелекту, спеціально розроблених для команд з безпеки, що мають обмежені ресурси. У сукупності ці кроки відображають загальногалузевий перехід до прогнозних, автономних та квантово-стійких архітектур безпеки в умовах дедалі більш витончених автоматизованих загроз». ***(Emerging AI-Driven Threats Prompt Renewed Focus on Enterprise Cybersecurity // Cision US Inc (https://www.prnewswire.com/news-releases/emerging-ai-driven-threats-prompt-renewed-focus-on-enterprise-cybersecurity-302739101.html). 10.04.2026).***

***

«У березні 2026 року в галузі кібербезпеки спостерігався сплеск масштабних злиттів і поглинань, зосереджених навколо штучного інтелекту: постачальники ШІ прагнули інтегрувати експертизу з безпеки безпосередньо у свої платформи, а традиційні компанії з безпеки розширювали свої можливості у сфері ШІ. OpenAI оголосила про придбання Promptfoo — компанії, що спеціалізується на тестуванні безпеки агентного ШІ, інструменти якої вже використовує чверть компаній зі списку Fortune 500. Цей крок дозволить OpenAI інтегрувати досвід Promptfoo у виявленні та усуненні вразливостей ШІ безпосередньо у свою платформу Frontier для створення агентів ШІ…

У тому ж дусі компанія DataBricks, що спеціалізується на хмарних технологіях та аналітиці на основі штучного інтелекту, випустила Lakewatch — новий агентський продукт для управління інформацією та подіями безпеки (SIEM) — і підкріпила цей запуск придбанням двох стартапів у сфері штучного інтелекту: Antimatter, що спеціалізується на безпечній аутентифікації та авторизації, та SiftD.ai, компанії з глибоким досвідом у розробці рішень для виявлення загроз у великих масштабах. Тим часом італійський гігант аерокосмічної та оборонної промисловості Leonardo придбав британського постачальника послуг з кібербезпеки Becrypt, щоб розширити свою пропозицію у сфері Zero Trust, отримавши доступ до рішень Becrypt для безпечного захисту настільних комп'ютерів та мобільних пристроїв… Завершуючи перелік значних угод цього місяця, компанія Google завершила придбання платформи безпеки для хмарних технологій та штучного інтелекту Wiz за 32 мільярди доларів — про цю угоду було вперше оголошено у 2025 році. Це масштабне придбання покликане посилити можливості Google Cloud, надавши клієнтам уніфіковану платформу безпеки для захисту складних мультихмарних середовищ та середовищ на базі штучного інтелекту, що зробить надійну безпеку доступнішою для ширшого кола організацій». ***(Danny Palmer. Cybersecurity M&A Round-Up: Big Players Boost AI Security Offerings // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news-features/cyber-ma-roundup-march-26/). 03.04.2026).***

***

«Прогрес у галузі штучного інтелекту трансформує як розробку програмного забезпечення, так і кібербезпеку, відкриваючи перспективу майбутнього, в якому «миттєве програмне забезпечення» можна буде швидко створювати, модифікувати та видаляти, поряд із традиційними довговічними системами. Штучний інтелект уже зараз покращує можливості автоматичного виявлення та використання вразливостей, знижуючи бар'єри для зловмисників і створюючи умови для масштабних автоматизованих кібератак, зокрема на системи з відкритим кодом, Інтернет речей (IoT) та застарілі системи…

Водночас ці самі можливості надають значні переваги захисникам, оскільки ШІ також може виявляти вразливості та потенційно генерувати виправлення, що відкриває перспективу створення більш безпечного коду і навіть систем із функцією «самовідновлення», які постійно виявляють і усувають недоліки. Однак цей баланс залежить від низки ключових невизначеностей, зокрема від того, наскільки ефективно ШІ може писати безпечний код, як швидко можна розгортати виправлення та наскільки ефективно організації управляють застарілими системами, в яких зберігаються вразливості…

Хоча нове та короткочасне програмне забезпечення може зменшити вразливість завдяки обмеженій помітності та коротшому терміну експлуатації, зловмисники й надалі використовуватимуть слабкі місця застарілих систем і переходитимуть до атак вищого рівня, таких як соціальна інженерія, ефективність яких також підвищує штучний інтелект. Зрештою, штучний інтелект прискорює гонку озброєнь у сфері кібербезпеки, посилюючи як атаки, так і засоби захисту, а результат залежить від таких факторів, як обмін інформацією, складність систем та здатність управляти ризиками, що постійно еволюціонують, у дедалі більш автоматизованому цифровому середовищі». ***(Bruce Schneier. Cybersecurity in the age of instant software // FoundryCo, Inc. (https://www.csoonline.com/article/4152133/cybersecurity-in-the-age-of-instant-software.html). 02.04.2026).***

***

«Бум штучного інтелекту дедалі частіше розглядається як виклик для національної стійкості, оскільки державні органи розбудовують інфраструктуру штучного інтелекту та центрів обробки даних швидше, ніж це дозволяють існуючі системи безпеки, особливо в умовах бюджетних обмежень та застарілих систем… Це стрімке розширення збільшує площу атаки на критичну інфраструктуру — насамперед на енергомережу — через впровадження нових підстанцій, міжмережевих з'єднань, цифрових інструментів управління мережею та інтеграції сторонніх систем, кожна з яких додає кінцеві точки, облікові дані та програмні залежності, що можуть виходити за межі існуючих архітектур безпеки. Водночас вимоги до високої доступності створюють компроміс між надійністю та безпекою, в якому заходи контролю, що ускладнюють роботу, такі як багатофакторна автентифікація, сегментація та планове технічне обслуговування, відкладаються або обходять, щоб зберегти час безперебійної роботи, створюючи можливості для досвідчених зловмисників…

Останні попередження CISA та загальні тенденції свідчать про те, що зловмисникам не потрібні нові методи; у 2025 році різко зросла кількість випадків використання вразливостей, а основними точками проникнення залишаються типові слабкі місця — нерівномірна аутентифікація та прогалини в багатофакторній аутентифікації (MFA) у нових розгортаннях, безконтрольне розширення доступу сторонніх користувачів та неефективне управління ідентифікацією, а також обмежені базові моделі поведінки, що уповільнюють виявлення. Рекомендований шлях до забезпечення стійкості полягає у «виправленні основних недоліків» за допомогою перевірених методологій, таких як NIST: посилити ідентифікацію та доступ (універсальна MFA, мінімальні привілеї, доступ «just-in-time», видалення застарілих облікових даних та спільних облікових записів, а також MFA, стійка до фішингу, для критично важливих систем), покращити оперативну видимість за допомогою моніторингу та виявлення аномалій (включно з AI/ML, де це доречно), а також зміцнити надійні канали за допомогою верифікації та позасмугової валідації для змін з високим рівнем ризику, ретельно контролюючи доступ постачальників. У міру прискорення впровадження штучного інтелекту очікується, що державні суб'єкти й надалі будуть націлюватися на об'єкти енергетики, водопостачання та зв'язку, оскільки порушення в їхній роботі можуть спричинити ланцюгові наслідки значного масштабу; тому нагальним є послідовне застосування основних заходів контролю, щоб запобігти перетворенню повсякденних збоїв на серйозні операційні інциденти». ***(Leslie Nielsen. How Cyber Resilience Helps Governments Harness AI Infrastructure // CDW LLC (https://statetechmagazine.com/article/2026/04/how-cyber-resilience-helps-governments-harness-ai-infrastructure). 07.04.2026).***

***

«Штучний інтелект кардинально змінює сферу кібербезпеки, відкриваючи як потужні можливості для захисників, так і нові інструменти для зловмисників. Прогностичний ШІ, який чудово справляється із сортуванням даних та виявленням аномалій, надав захисникам структурну перевагу, дозволивши їм керувати надзвичайно складними сучасними мережами та автоматизувати реагування на загрози. Однак поява генеративного ШІ (GenAI) створює більш складну динаміку подвійного використання: ті самі інструменти, що допомагають командам з безпеки, можуть бути використані зловмисниками для створення переконливих фішингових кампаній, генерування шкідливого коду та експлуатації незахищених вразливостей у безпрецедентних масштабах та різноманітності…

Це викликає особливе занепокоєння, враховуючи, що багато організацій повільно виправляють відомі уразливості типу «N-day», створюючи тим самим величезну площину атаки. Щоб посилити колективну стійкість у цьому середовищі, яке розвивається завдяки штучному інтелекту, необхідний багатоаспектний підхід, що включає ринкові стимули для зменшення ризиків, пов'язаних з уразливостями типу «N-day», перегляд питань прозорості генеративної штучної інтелекту (GenAI) з метою запобігання зловживанням, а також цілеспрямоване впровадження організаціями інструментів штучного інтелекту для зміцнення власної кіберзахисту. Для керівників служб безпеки це

означає вибір технологічних партнерів із доведеною зрілістю у сфері безпеки, максимізацію цінності даних у взаємосумісних екосистемах та стратегічне впровадження GenAI, щоб гарантувати, що інновації зміцнюють, а не підривають їхню оборонну позицію...» ***(Jim Richberg. How Does AI Affect Cyber Resilience for Federal Agencies? // CDW LLC (https://fedtechmagazine.com/article/2026/04/how-does-ai-affect-cyber-resilience-federal-agencies). 07.04.2026).***

***

«Випуск нових моделей штучного інтелекту від Frontier AI означає кардинальний зсув у можливостях кібербезпеки, особливо в галузі виявлення вразливостей та створення експлойтів. Згідно з попередніми тестуваннями компанії Palo Alto Networks таких передових систем, як Mythos від Anthropic та найновіші моделі OpenAI, ці інструменти штучного інтелекту демонструють надзвичайну ефективність у виявленні вразливостей коду, об'єднанні декількох слабких місць у критичні ланцюжки експлойтів та масштабному аналізі логіки додатків у повному стеку. За повідомленнями, менш ніж за три тижні передова ШІ виконала роботу, еквівалентну цілорічному тестуванню на проникнення… Хоча ці моделі розробляються з урахуванням заходів безпеки, очікується, що подібні можливості поширяться й на інші лабораторії штучного інтелекту, зокрема на моделі з відкритим кодом та міжнародні моделі, а це означає, що зловмисники неминуче почнуть їх використовувати. Як наслідок, виявлення вразливостей «нульового дня», автоматичне створення експлойтів та автономні агенти для атак на базі штучного інтелекту можуть незабаром стати звичним явищем, що значно скоротить тривалість атак з тижнів до хвилин…

Таке прискорення несе з собою кілька серйозних ризиків. По-перше, ефект «потопу вразливостей»: штучний інтелект різко збільшить темпи виявлення вразливостей, що створить навантаження на системи управління виправленнями. Невиправлені вразливості швидко стануть цілями для зловмисників. По-друге, все більшого поширення набуватимуть атаки «зсередини», що використовують слабкі місця ланцюга постачання та залежність інфраструктури штучного інтелекту, що вимагатиме більш надійних архітектур на основі моделі «нульової довіри» та засобів захисту ідентичності. По-третє, автоматизація атак на основі ШІ змусить захисників відповідати швидкості супротивників, вимагаючи можливостей виявлення та реагування в режимі реального часу, що вимірюються одиницями хвилин…

Щоб відповісти на ці виклики, організації повинні впровадити комплексну стратегію захисту, що базується на трьох основних компонентах: оцінці, захисті та платформізації. Оцінка передбачає використання штучного інтелекту для проактивного сканування внутрішніх кодових баз, виявлення вразливостей, ідентифікації ланцюжків експлойтів, аудиту залежностей від програмного забезпечення з відкритим кодом та усунення прогалин у телеметрії. Захист вимагає повного впровадження передових рішень для захисту кінцевих точок, безпечних корпоративних браузерів, архітектур «нульової довіри» та систем виявлення з використанням штучного інтелекту як у хмарних, так і в локальних середовищах. Нарешті, операції з забезпечення безпеки повинні перейти від ізольованих ручних

процесів до повністю інтегрованих платформ на базі штучного інтелекту, здатних автоматично виявляти загрози та реагувати на них у всіх відповідних джерелах даних. Загальний висновок очевидний: стійкість кібербезпеки в епоху передових технологій штучного інтелекту вимагає повного, а не часткового захисту, оскільки зловмисники незабаром почнуть діяти зі швидкістю машин». ***(Lee Klarich. Defender's Guide to the Frontier AI Impact on Cybersecurity // Palo Alto Networks (https://www.paloaltonetworks.com/blog/2026/04/defenders-guide-frontier-ai-impact-cybersecurity/). 17.04.2026).***

***

«Йошуа Бенджо, один із «батьків штучного інтелекту», попередив, що передові моделі, такі як Mythos від Anthropic — здатні виявляти тисячі раніше невідомих вразливостей «нульового дня» — наочно демонструють, чому міжнародні інституції повинні терміново об'єднати зусилля для регулювання ризиків подвійного призначення штучного інтелекту. Хоча Mythos є значним кроком вперед у сфері кібербезпеки, допомагаючи захищати критичну інфраструктуру, його випуск, суворо обмежений невеликою групою американських технологічних компаній та урядових агентств, підкреслив концентрацію влади в руках приватних американських компаній та викликав занепокоєння щодо глобального доступу, справедливості та суверенітету в галузі штучного інтелекту…

Бенджо стверджує, що рішення, які можуть мати далекосяжні наслідки для інфраструктури в усьому світі, не слід залишати виключно на розсуд приватних суб'єктів, і закликав створити регуляторний орган на зразок FDA для нагляду за розробкою та впровадженням передових технологій штучного інтелекту, а також встановити чіткіші зобов'язання для компаній щодо запобігання шкоді критично важливим системам в інших країнах. Він наголошує, що будь-яка значуща глобальна реакція має включати угоду з Китаєм, зазначаючи, що хоча провідні китайські моделі наразі відстають від американських аналогів приблизно на шість місяців, стрімкий прогрес Китаю у сфері ШІ з відкритим кодом становить ще більший ризик… На відміну від пропрієтарних систем із вбудованими засобами безпеки, моделі з відкритим кодом може завантажити, модифікувати та позбавити засобів захисту будь-хто, що потенційно може надати потужні кіберможливості безпосередньо зловмисникам. Бенджо, давній прихильник відкритого коду, визнає його переваги у вигляді прозорості, але попереджає, що в епоху кібернападів із використанням ШІ традиція відкритого коду — яка колись вважалася засобом підвищення безпеки завдяки колективному контролю — тепер може стати серйозною проблемою, оскільки високопродуктивні моделі сканують відкритий код у великих обсягах, щоб виявляти вразливості швидше, ніж люди. Загалом він наголошує, що з ростом потужності ШІ міжнародна координація в питаннях управління, безпеки та відповідального впровадження є надзвичайно важливою для запобігання неконтрольованому поширенню технологій подвійного призначення». ***(Beatrice Nolan. Anthropic's Mythos cybersecurity capabilities require urgent international cooperation, 'AI Godfather' Yoshua Bengio says // Fortune Media IP Limited. (https://fortune.com/2026/04/17/anthropic-mythos-cybersecurity-capabilities-***

highlight-problem-of-ais-concentration-of-power-ai-godfather-yoshua-bengio-says/). 17.04.2026).

***

«15 квітня 2026 року представники Європейського Союзу провели зустріч із компанією Anthropic, щоб обговорити занепокоєння щодо її моделі штучного інтелекту Mythos та пов'язаних із нею потенційних ризиків у сфері кібербезпеки; у найближчі тижні заплановано проведення додаткових зустрічей. Європейська комісія наголосила на необхідності детальної інформації щодо можливостей моделі, зазначивши, що компанія Anthropic дотримується Кодексу практики ЄС щодо штучного інтелекту загального призначення та бере участь в обговореннях щодо оцінки та мінімізації ризиків для будь-яких послуг, що можуть пропонуватися в Європі. Mythos призначений переважно для оборонних завдань у сфері кібербезпеки, дозволяючи обраним партнерам виявляти вразливості та зміцнювати системи до їх експлуатації, а також був представлений уряду США щодо своїх наступальних та оборонних кіберможливостей…

Однак на початковому етапі реалізації проєкту Glasswing ранній доступ отримали лише близько 40 провідних американських технологічних компаній, що викликало занепокоєння урядів та фінансових установ інших країн щодо нерівного доступу та обміну інформацією. Міністр фінансів Канади заявив про плани порушити це питання перед своїми колегами з метою забезпечення стійкості фінансової системи, тоді як Великобританія готується надати доступ своїм банкам. Ця ситуація підкреслює більш широкі питання щодо глобального управління штучним інтелектом, розподілу ризиків та необхідності більш інклюзивної міжнародної співпраці у сфері технологій штучного інтелекту подвійного призначення». ***(Anthropic Briefs EU Regulators on Mythos Cybersecurity Concerns // PYMNTS (https://www.pymnts.com/artificial-intelligence-2/2026/anthropic-briefs-eu-regulators-on-mythos-cybersecurity-concerns/). 17.04.2026).***

***

«Останнє глобальне дослідження компанії Kroll щодо кіберстійкості показує, що стрімке впровадження штучного інтелекту значно випереджає розвиток механізмів управління, засобів безпеки та готовності до інцидентів, що створює для організацій нові значні ризики. Дослідження виявило: хоча ШІ все глибше інтегрується в діяльність підприємств, 76 % компаній за останні два роки стикалися з інцидентами безпеки, пов'язаними з додатками або моделями ШІ, причому майже третина (27 %) понесла витрати, пов'язані з такими інцидентами, що перевищують один мільйон доларів. Хоча існує сильне бажання інтегрувати ШІ в інфраструктуру безпеки, 90% респондентів вказали на перешкоди для більших інвестицій, найчастіше це відсутність чіткої окупності інвестицій, недостатнє розуміння керівництвом ризиків ШІ та уявлення про те, що існуючі заходи є достатніми…

Організації виділяють у середньому лише 13 % своїх бюджетів на ініціативи в галузі ШІ на тестування засобів безпеки або самих моделей, що створює критичні прогалини в їхній системі безпеки ШІ. Натомість компанії з високорозвиненими

практиками безпеки в шість разів частіше витрачають понад 20% свого бюджету на ШІ на таке тестування, а 69% організацій з дуже високим рівнем кіберзрілості дотримуються стратегії централізованої платформи ШІ з вбудованими засобами контролю безпеки, порівняно з лише 39% тих, що мають дуже низький рівень зрілості…

Дослідження також показує, що зі зростанням кіберзрілості організації ймовірність виникнення інцидентів безпеки, пов'язаних зі штучним інтелектом, суттєво знижується: 89 % організацій з дуже низьким рівнем зрілості зазнали таких інцидентів, порівняно з 54 % організацій з дуже високим рівнем зрілості, причому 46 % останніх повідомили про відсутність інцидентів, пов'язаних зі штучним інтелектом, протягом останніх двох років... Загалом, результати дослідження підкреслюють, що без надійних основ безпеки ШІ посилює існуючі слабкі місця, і організації повинні надавати пріоритет безпечній архітектурі, управлінню ідентифікацією, реагуванню на інциденти та культурі безпеки, щоб зробити інновації стійкими». ***(AI Innovation Surges as Security Fundamentals Lag, Kroll Research Finds // Cision US Inc. (https://www.prnewswire.com/news-releases/ai-innovation-surges-as-security-fundamentals-lag-kroll-research-finds-302747672.html). 21.04.2026).***

***

«…На конференції RSA 2026 у Сан-Франциско головною темою виступів, панельних дискусій та обговорень став «агентний ШІ» — автономні системи, здатні до самостійного прийняття рішень та виконання багатоетапних операцій. Прикладом цього є модель Mythos від компанії Anthropic, яка може координувати складні кіберзавдання, але наразі перебуває під суворими обмеженнями через свій потенціал подвійного призначення — як для оборонних, так і для наступальних цілей. Лідери галузі, зокрема Cloud Security Alliance, закликають організації боротися з ШІ за допомогою ШІ, тоді як OpenAI розширює свою програму Trusted Access for Cyber, а Gartner прогнозує, що витрати на ШІ зростуть на 44% у 2026 році та досягнуть 47 трильйонів доларів до 2029 року, значно випередивши традиційні бюджети на інформаційну безпеку…

Однак ті самі можливості, що розширюють потенціал захисників, також дозволяють зловмисникам здійснювати автономну розвідку, горизонтальне переміщення, адаптацію в режимі реального часу, а також масштабовані та недорогі атаки з мінімальним втручанням людини, що кардинально змінює модель загрози. Експерти попереджають, що просте додавання спеціалізованих інструментів безпеки на основі штучного інтелекту (ШІ) створює ризик подальшого розростання інструментарію, розрізненої видимості та операційної складності, що в кінцевому підсумку грає на руку зловмисникам. Натомість формується консенсус щодо розгляду агентного ШІ як ідентичності — що здійснює аутентифікацію, отримує доступ до систем, виконує дії та потенційно може бути скомпрометованим або стати зловмисним — що робить виявлення загроз ідентичності та зменшення ризиків логічною площиною контролю…

Такий підхід забезпечує прозорість поведінки, засоби контролю на основі ризиків, єдине застосування політик як для людських, так і для машинних

ідентичностей, а також управління життєвим циклом для виявлення аномалій, дотримання принципу мінімальних привілеїв та автоматизації реагування без створення нових ізольованих систем безпеки. У той час як галузь бореться з нелюдськими суб'єктами, здатними діяти самостійно, інтеграція засобів безпеки на основі штучного інтелекту в існуючі системи управління ідентифікацією пропонує практичний та масштабований спосіб управління новими ризиками, дозволяючи уникнути фрагментації систем захисту». ***(Torsten George. Why Cybersecurity Must Rethink Defense in the Age of Autonomous Agents // SecurityWeek (https://www.securityweek.com/why-cybersecurity-must-rethink-defense-in-the-age-of-autonomous-agents/). 24.04.2026).***

***

Штучний інтелект, як інструмент боротьби із кіберзлочинністю

«Незважаючи на поширений ажіотаж і побоювання, що штучний інтелект кардинально змінить характер кіберконфліктів, надавши зловмисникам нові можливості, більш глибокий аналіз свідчить про те, що автоматизація на основі ШІ, ймовірно, принесе більше користі захисникам, ніж зловмисникам, і в кінцевому підсумку сприятиме заспокоєнню, а не розпалюванню міждержавних кіберконфліктів з високими ставками… Хоча нещодавні хакерські атаки з використанням ШІ — такі як модель ШІ, що очолила рейтинг хакерів, та групи, що фінансуються державою, які використовують агентів ШІ — демонструють, що ШІ може значно підвищити ефективність атак, особливо для менш кваліфікованих учасників, є мало доказів того, що він підвищує їхню результативність. Основна причина полягає в тому, що моделі ШІ чудово справляються з розпізнаванням та виявленням закономірностей, але мають труднощі з творчим обманом та розробкою нових експлойтів, що є характерними для складних наступальних операцій з високими ставками… Це створює «розрив в автоматизації», коли ШІ забезпечує значні переваги для оборони, яка базується на масовому виявленні, але приносить все меншу віддачу та підвищує ризики невдач для нападу, що спирається на приховання та хитрість. Хоча ШІ значно посилить кіберзлочинність та репресії проти «м'яких» цілей, що не мають сучасних засобів захисту, на рівні протистояння між державами захисні системи на базі ШІ, ймовірно, ускладнять кібератаки, зменшивши їхню корисність як інструменту державної політики порівняно з іншими варіантами». ***(Lennart Maschmeyer. The AI Revolution in Cyber Conflict // The Lawfare Institute (https://www.lawfaremedia.org/article/the-ai-revolution-in-cyber-conflict). 08.04.2026).***

***

«За даними останнього дослідження ISC2, в якому взяли участь понад 950 респондентів із Великої Британії, фахівці з кібербезпеки у цій країні стрімко впроваджують інструменти на основі штучного інтелекту (ШІ), проте через значний дефіцит кваліфікованих кадрів команди не готові до їх безпечного впровадження або захисту від зростаючої хвилі загроз, пов'язаних із ШІ. Хоча

74% команд з кібербезпеки вже використовують, тестують або оцінюють інструменти безпеки на основі штучного інтелекту, саме у цій сфері спостерігається найгостріший дефіцит кваліфікованих кадрів (42%), причому 95% організацій вказують принаймні одну сферу, де співробітники потребують додаткового навчання. Бюджетні обмеження залишаються основною перешкодою для найму персоналу (28%), навіть попри стабілізацію фінансового тиску… Організації з оптимізмом оцінюють потенціал штучного інтелекту в поліпшенні моніторингу мереж (38%), операцій з безпеки (34%) та моделювання загроз (30%), а 70% відзначають підвищення ефективності після впровадження. Однак загрози, пов'язані з ШІ, різко зростають: 43% стикаються з соціальною інженерією на основі ШІ, 29% повідомляють про витік даних, 23% підозрюють атаки на основі ШІ, а 26% підтверджують порушення, пов'язані з ШІ, — це особливо впливає на менші організації (67% повідомили про численні інциденти)… Щоб подолати цей розрив і посилити стійкість, у звіті наголошується на необхідності більших інвестицій у підвищення кваліфікації персоналу, обізнаність у питаннях хмарних технологій та ШІ, структуровані програми навчання, а також на необхідності зосередити увагу керівництва на інтеграції планування з урахуванням ШІ у більш широкі стратегії безпеки, а не покладатися виключно на зовнішній підбір персоналу». ***(Elizabeth Greenberg. AI Adoption Outpacing AI Skills in Cybersecurity // DIGIT (https://www.digit.fyi/__trashed-4/). 23.04.2026).***

***

«Vodafone Business та Google Cloud розширили своє десятирічне стратегічне партнерство на суму 1 мільярд доларів, запропонувавши два нових рішення, покликані допомогти малим та середнім підприємствам (МСП) посилити кібербезпеку та впровадити агентний штучний інтелект. Першим з них є послуга керованого виявлення та реагування (MDR) на базі Google Security Operations, призначена для захисту клієнтів від дедалі частіших і витонченіших кіберзагроз; спочатку вона буде запущена в Німеччині з метою дотримання місцевих стандартів захисту даних, а пізніше цього року — на інших європейських ринках…

Другим є Vodafone Business AI Concierge, створений на базі Google Gemini — мультимодального агента штучного інтелекту, що працює на платформі Gemini Enterprise Agent Platform від Google Cloud. Цей агент здатний самостійно обробляти запити клієнтів, призначати зустрічі та забезпечувати голосові та інформаційні взаємодії з низькою затримкою, що дозволяє малим та середнім підприємствам не втрачати потенційних клієнтів поза стандартними робочими годинами та дає можливість власникам зосередитися на розвитку бізнесу. Спочатку AI Concierge буде доступний у Німеччині та Греції. Директор з продуктів та міжнародного бізнесу Vodafone Business Фанан Генрікес описав ці пропозиції як такі, що роблять передовий штучний інтелект практичним для щоденного використання в бізнесі, тоді як Олівер Паркер з Google Cloud зазначив, що ця співпраця поєднує моделі Gemini та безпеку корпоративного рівня з можливостями підключення Vodafone, щоб краще підготувати малі та середні підприємства до швидкозмінного цифрового середовища. Ця заява є важливою віхою в історичному партнерстві, підписаному в

жовтні 2024 року». ***(Annie Turner. Vodafone Business, Google Cloud offer SMEs cybersecurity, agentic AI // Mobile Europe (https://www.mobileeurope.co.uk/vodafone-business-google-cloud-offer-smes-cybersecurity-agentic-ai/). 22.04.2026).***

***

Штучний інтелект, як зброя кіберзлочинців

«Галузь кібербезпеки перейшла від гіпотез до нової реальності, в якій активно застосовуються засоби кібервійни на основі штучного інтелекту. Останні дані свідчать, що 64 % керівників IT-підрозділів у США за останній рік зазнали атак, керованих або ініційованих штучним інтелектом, що підкреслює небезпечний розрив у швидкості: зловмисники зараз діють зі швидкістю машин, використовуючи автономних агентів, тоді як більшість захисників залишаються прив'язаними до статичних процесів, керованих людьми. Державні суб'єкти все частіше використовують агентний ШІ як зброю для масштабування своїх зусиль, як це було видно, коли китайська група GTG-1002, що фінансується державою, використовувала помічника Claude Code для самостійного виконання майже 90% кібератаки, проводячи розвідку та витяг даних зі швидкістю, яку неможливо досягти хакерам-людям…

Незважаючи на ці технологічні досягнення, зловмисники продовжують використовувати базові вразливості, такі як застарілі системи та неправильно налаштовані хмарні середовища, про що свідчить поточна діяльність групи Salt Typhoon. Це доводить, що традиційний захист на основі сигнатур є недостатнім для протидії як давнім точкам проникнення, так і автономним загрозам майбутнього. Щоб ефективно реагувати на ці виклики, галузь кібербезпеки повинна перейти до архітектурної моделі, відомої як «колективний захист» або підхід «колективного розуму». Ця модель замінює ізольовані ручні засоби безпеки на автономну, розподілену розвідку в режимі реального часу, використовуючи федеративне навчання та поведінкову аналітику для виявлення аномальних патернів у величезних спільних наборах даних. Автоматизувавши захист відповідно до швидкості та контексту супротивника, галузь може еволюціонувати від реактивних, поступових оновлень до архітектури, що примножує сили, необхідної для протистояння епосі агентних кіберзагроз». ***(Nadir Izrael. The New Rules of Engagement: Matching Agentic Attack Speed // SecurityWeek (https://www.securityweek.com/the-new-rules-of-engagement-matching-agentic-attack-speed/). 07.04.2026).***

***

«Gartner прогнозує, що до 2028 року половина всіх зусиль підприємств з реагування на інциденти буде спрямована на загрози, пов'язані з індивідуально розробленими додатками штучного інтелекту, оскільки організації впроваджують системи штучного інтелекту набагато швидше, ніж команди з безпеки встигають розробити необхідні тести, процеси та набути спеціалізованих навичок для їхнього захисту. Крістофер Мікстер, віце-президент

та аналітик Gartner, попереджає, що спеціальні інструменти ШІ важко контролювати з часом і що більшості команд з безпеки наразі бракує стандартизованих процесів для вирішення інцидентів, пов'язаних саме з ШІ, закликаючи керівників залучатися до проектів ШІ на ранніх етапах, щоб забезпечити вбудовування відповідних ресурсів та засобів контролю з самого початку. Очікується, що до 2028 року понад половина підприємств впровадить спеціалізовані платформи безпеки ШІ для централізованого управління ризиками, такими як введення підказок та зловживання даними, як у сторонніх, так і у внутрішніх додатках ШІ…

За прогнозами Gartner, до 2027 року 75% організацій, що підлягають регулюванню, будуть змушені сплачувати штрафи, які перевищуватимуть 5% їхнього глобального доходу, через використання ручних процесів забезпечення відповідності вимогам у сфері ШІ. Компанія рекомендує посилити автоматизацію та запровадити надійне кіберуправління, щоб відповідати мінливим нормам безпеки ШІ. До 2030 року третина ІТ-роботи буде витрачена на усунення «боргу даних ШІ», причому неструктуровані та погано захищені дані стануть основною перешкодою для безпечного впровадження ШІ; тому команди з кібербезпеки розширюють можливості запобігання втраті даних (DLP) для моніторингу потоків даних GenAI та Agentic AI і посилюють співпрацю з лідерами у сфері даних та ШІ щодо структурованого виявлення та контролю доступу. Тривала геополітична нестабільність та місцеві нормативні вимоги змусять 30% організацій вимагати повного суверенітету над своїми засобами контролю безпеки хмарних середовищ до 2027 року, що вплине на вибір постачальників та вимагатиме від керівників служб інформаційної безпеки чітко визначити вимоги щодо суверенітету…

Зрештою, до 2028 року 70 % керівників служб інформаційної безпеки (CISO) використовуватимуть платформи для моніторингу та аналізу ідентифікаційних даних, щоб зменшити площу атаки в системі управління ідентифікацією та доступом (IAM), застосовуючи інструменти на базі штучного інтелекту для усунення прогалин у моніторингу та виявлення помилок у налаштуваннях у дедалі складніших середовищах, що охоплюють як людські, так і машинні ідентифікаційні дані». ***(AI to Dominate 50% of Cyber Incident Response by 2028: Gartner // The Story Thailand (https://www.thestorythailand.com/en/gartner-ai-applications/). 21.04.2026).***

***

Кіберзлочинність та кібертероризм

«Група хакерів-вимагачів, пов'язана з Росією та відома під назвою «Play», заявила, що зламала систему шведського виробника дистанційно керованих роботів для знесення будівель «Brokk», які використовуються в небезпечних умовах, зокрема на атомних об'єктах та під час ліквідації наслідків катастроф, і погрожує оприлюднити більше викрадених даних, якщо компанія не сплатить викуп. Заява з'явилася на сайті Play, присвяченому витокам, кілька днів тому разом із нібито частковим оприлюдненням 4 ГБ даних. Угруповання стверджує, що викрало внутрішню корпоративну інформацію, таку як документи

клієнтів, бюджети, відомості про заробітну плату, ідентифікаційні дані, податкові матеріали та інші фінансові дані, і попереджає, що без відповіді буде опубліковано «повний дамп». Витік даних не вдалося перевірити незалежно, оскільки їх не вдалося відкрити за допомогою наданого пароля, а Brokk на момент публікації не відповіла на запити ЗМІ, але якщо крадіжка справжня, це може завдати шкоди репутації компанії та її клієнтів, створити ризики для конфіденційності та спричинити подальші шахрайські дії… Компанія Brokk, заснована в 1976 році, відома своїми машинами, що використовуються для проведення робіт з очищення та виведення з експлуатації на об'єктах підвищеного ризику, таких як Селлафілд, Айдахо-Фолс, Чорнобильська зона відчуження та атомна електростанція Траусфіннід; вона позиціонує модель Brokk 900 як найпотужнішого у світі робота для знесення будівель. Play залишається однією з найактивніших операцій з використанням програм-вимагачів: моніторинг даркнету показує, що з 2023 року вона зафіксувала понад тисячу жертв, включаючи нещодавні атаки на організації в ланцюгах постачання модної індустрії, аерокосмічної галузі та оборонної промисловості». ***(Paulina Okunytė. Russian hackers target firm behind robot that cleaned up Chornobyl // Cybernews (https://cybernews.com/security/brokk-ransomware-data-breach/). 02.04.2026).***

***

«Зловмисники, пов'язані з Корейською Народно-Демократичною Республікою (КНДР), здійснюють складні багатоетапні кібератаки на південнокорейські організації, дедалі частіше використовуючи легітимні платформи та вбудовані засоби Windows для уникнення виявлення. Було зафіксовано, що такі угруповання, як Kimsuky, використовують зашифровані файли ярликів Windows (LNK), які розповсюджуються через фішингові листи, для розміщення приманкових документів та шкідливих скриптів PowerShell, призначених для уникнення аналізу та забезпечення стійкості шляхом виконання завдань через регулярні проміжки часу. Ключовою інновацією в цих кампаніях є використання надійних платформ, таких як GitHub і Dropbox, як інфраструктури управління та контролю (C2), що дозволяє зловмисникам викрадати дані та отримувати додаткові інструкції, маскуючись під легітимний мережевий трафік… У цих кампаніях часто відмовляються від складного спеціалізованого шкідливого ПЗ на користь тактики «Living off the Land» (LolBins), використовуючи вбудовані системні інструменти для розгортання та забезпечення стійкості, що значно знижує рівень виявлення. Подальше вдосконалення своїх методів дозволило таким групам, як ScarCruft, перейти від традиційних ланцюжків LNK до використання дроперів у форматі HWP (Hangul Word Processor) із вбудованими об'єктами OLE для доставки трояна віддаленого доступу RokRAT шляхом бічного завантаження DLL, що свідчить про зростаючу залежність КНДР від передових, адаптивних технік для забезпечення довгострокового, стійкого доступу до цільових систем». ***(Ravie Lakshmanan. DPRK-Linked Hackers Use GitHub as C2 in Multi-Stage Attacks Targeting South Korea // The Hacker News (https://thehackernews.com/2026/04/dprk-linked-hackers-use-github-as-c2-in.html). 06.04.2026).***

***

«…Північнокорейські хакери, що діють за підтримки держави та належать до групи «Lazarus», наприкінці березня зламали популярну бібліотеку JavaScript Axios, провівши двотижневу кампанію з соціальної інженерії, щоб обдурити розробника та змусити його встановити шкідливе програмне забезпечення, яке надало їм доступ до системи. Потім вони опублікували два заражені пакети Axios, які були доступні протягом приблизно трьох годин, перш ніж їх було видалено, створивши короткий, але небезпечний проміжок часу, протягом якого будь-хто, хто встановлював оновлення, міг зазнати загрози… Оскільки Axios широко використовується — мільйони завантажень щотижня та залежності у понад 115 000 репозиторіях GitHub — навіть короткочасне порушення безпеки могло вплинути на тисячі систем нижчого рівня…

Тактика, інфраструктура та шкідливе програмне забезпечення, використані в цій атаці, збігаються з попередніми операціями угруповання «Lazarus», зокрема з використанням підроблених даних про компанії, фальшивих робочих просторів Slack та шкідливого програмного забезпечення для проведення зустрічей, що підтверджує висновки США та представників галузі про причетність Північної Кореї. Цей інцидент подається як доказ того, що програмне забезпечення з відкритим кодом залишається важливою стратегічною ціллю, оскільки критична інфраструктура часто підтримується однією особою або невеликою командою волонтерів, що робить базові пакети вразливими до виважених, добре забезпечених ресурсами атак на ланцюг постачання, спрямованих на викрадення облікових даних та криптовалюти або обхід санкцій». ***(Tommy Baker. A three-hour window: North Korean hackers compromised the Axios library and exposed thousands of systems // Silicon Canals (https://siliconcanals.com/sc-n-a-three-hour-window-north-korean-hackers-compromised-the-axios-library-and-exposed-thousands-of-systems/). 07.04.2026).***

***

«Кібератаки на політичні партії стають дедалі більш тривожною рисою цифрового простору, викликаючи занепокоєння щодо конфіденційності даних, чесності виборів та національної безпеки. Яскравим прикладом цієї тенденції є нещодавній злом серверів німецької демократично-соціалістичної партії «Ді Лінке» групою-вимагачами «Qilin», яка 27 березня 2026 року проникла на сервери партії та погрожувала оприлюднити конфіденційні дані в даркнеті. Однак цей інцидент є частиною ширшої тенденції кібершпигунства та злочинності, спрямованої проти політичних організацій. Одним із найвідоміших прецедентів є злом серверів електронної пошти Гілларі Клінтон у 2015 році, який, на думку багатьох аналітиків, вплинув на результат президентських виборів у США 2016 року… Складність цих атак також зросла, про що свідчить випадок 2024 року, коли пов'язана з Росією хакерська група APT29 (або «Cozy Bear») здійснила атаку на німецький Християнсько-демократичний союз із використанням сучасного шкідливого програмного забезпечення з функцією «задніх дверей». У сукупності ці події вказують на чітку й тривожну тенденцію: політичні організації є особливо цінними

цілями, і без надійних засобів кіберзахисту та міжнародної співпраці демократичні інститути залишатимуться вкрай вразливими в цифрову епоху». ***(Naveen Goud. Qilin Ransomware targets Die Linke of Germany // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/qilin-ransomware-targets-die-linke-of-germany/). 06.04.2026).***

***

«Kubernetes, хоча й є незамінним інструментом для управління сучасними контейнеризованими додатками, став основною мішенню зловмисників, які використовують слабкі місця в конфігурації для організації проривів з контейнерів та подальшого проникнення в ширшу хмарну інфраструктуру. Дані телеметрії свідчать про 282-відсотковий сплеск операцій, пов'язаних із загрозами для Kubernetes, за останній рік — особливо в секторі інформаційних технологій — причому зловмисники дедалі частіше виходять за межі простого виходу з контейнерів, зловживаючи слабкими налаштуваннями ідентифікації та надто ліберальними засобами контролю доступу. Ці зловмисники дотримуються продуманого алгоритму дій: вони отримують початковий доступ через виконання коду, витягують конфіденційні токени облікових записів служб (JSON Web Tokens), перевіряють дозволи API і, зрештою, проникають у цінні хмарні ресурси…

Про серйозність цієї загрози свідчать реальні випадки вторгнень, такі як діяльність пов'язаної з Північною Кореєю групи «Slow Pisces», яка використовувала викрадені токени з облікового запису служби управління з високим рівнем привілеїв для горизонтального переміщення з кластера Kubernetes у основні фінансові системи криптовалютної біржі, що призвело до збитків на мільйони доларів. Аналогічно, експлойт «React2Shell» (CVE-2025-55182) дозволив зловмисникам перейти з контейнерів додатків у хмарні облікові записи для встановлення бекдорів та криптомайнерів вже через кілька днів після розкриття уразливості. Оскільки один викрадений токен може надати повний контроль, команди з безпеки повинні застосовувати проактивну стратегію захисту. Це включає впровадження суворого контролю доступу на основі ролей (RBAC) для забезпечення мінімальних привілеїв, заміну довготривалих статичних токенів на короткотривалі, прогнозовані альтернативи, а також впровадження надійного моніторингу під час виконання для виявлення аномальних вихідних з'єднань або несанкціонованого доступу до системи. Нарешті, ведення та перегляд журналів аудиту Kubernetes є надзвичайно важливим для виявлення ранніх ознак зловживання API та горизонтального переміщення, перш ніж порушення ескалує до хмарного рівня». ***(Tushar Subhra Dutta. Hackers Exploit Kubernetes Misconfigurations to Move From Containers to Cloud Accounts // Cyber Security News (https://cybersecuritynews.com/hackers-exploit-kubernetes-misconfigurations/). 07.04.2026).***

***

«Галерея Уффіці у Флоренції підтвердила, що близько 1 лютого вона зазнала кібератаки (після повідомлень про те, що вона сталася в період з кінця січня до початку лютого і зачепила не лише Уффіці, а й Палаццо Пітті та

Боболійський сад), але наголосила, що жодні твори мистецтва не були пошкоджені чи викрадені, а основні системи безпеки музею не зазнали зломів…

Італійська щоденна газета «Corriere della Sera» повідомила, що зловмисники проникли в ІТ-середовище музею, нібито викравши конфіденційну інформацію, таку як коди доступу, внутрішні плани та розташування камер відеоспостереження й сигналізації, а потім надіслали вимогу про викуп на особистий телефон директора Сімоне Верде, погрожуючи продати ці дані в даркнеті; Уффіці заперечили цю версію, заявивши, що системи безпеки є внутрішніми, замкнутими і недоступними ззовні, що жодних паролів викрадено не було і що немає доказів того, що хакери отримали карти систем безпеки (зазначивши, що камери й так видно у громадських місцях). Музей повідомив, що прискорив поточні роботи з підвищення безпеки — незалежно від проблем, що виникли в Луврі — та наголосив на таких оновленнях, як заміна аналогових камер на цифрові відповідно до рекомендацій поліції у 2024 році. Він також спростував твердження про те, що весь його цифровий фотоархів було викрадено, зазначивши, що фотосервер залишився неушкодженим завдяки резервним копіям, а будь-яке відключення було пов’язане з відновленням даних із резервної копії, без втрати інформації…

Повідомлення про закриття, замуровані двері та тимчасове переміщення «Скарбниці Медічі» з Палаццо Пітті до сховища Банку Італії музей пов’язав із запланованою реконструкцією, заходами з пожежної безпеки та потребами управління будівлею, а не з хакерською атакою. Незважаючи на цей інцидент і суперечки, галерея Уффіці залишається відкритою, а робота кас та доступ до громадських зон практично не зазнали змін». ***(Davide Ghiglione. Italy's Uffizi Galleries targeted in cyber-attack but deny security breach // BBC (https://www.bbc.com/news/articles/cy51wzeq6g5o). 03.04.2026).***

***

«Кібератака на шкільну ІТ-мережу C2K Північної Ірландії, яку адмініструє Управління освіти (ЕА) і яка використовується для забезпечення онлайн-систем для всіх шкіл, призвела до того, що під час великодніх канікул багато учнів втратили доступ до своїх облікових записів, що перешкодило їм користуватися навчальними матеріалами, матеріалами для повторення та спілкуватися з вчителями через такі платформи, як Microsoft Teams… Деякі школи, зокрема Regent House у Ньютаунардсі, відкрилися під час канікул, щоб допомогти учням скинути паролі та відновити доступ, оскільки кандидати на іспити GCSE, AS та A-level повідомляли про занепокоєння та втрачений час на навчання з наближенням термінів та іспитів. ЕА провела вебінар, у якому взяли участь понад 300 шкіл, заявила, що немає доказів того, що дані персоналу або учнів були скомпрометовані або викрадені, та повідомила, що інцидент було виявлено на ранній стадії, його вдалося локалізувати і розпочато відновлення роботи: близько 80 % шкіл після початкової школи знову підключено до мережі, а персонал працює цілодобово, щоб відновити послуги…» ***(Robbie Meredith. Pupils back to school in holidays to deal with fallout from cyber attack // BBC (https://www.bbc.com/news/articles/cd6l7y8lngno). 07.04.2026).***

***

«Компанія Jaguar Land Rover (JLR) повідомила про значне відновлення обсягів продажів у першому кварталі цього року після масштабної кібератаки, яка наприкінці 2024 року призвела до зупинки виробництва на п'ять тижнів. Найбільший британський автовиробник продав 95 300 автомобілів дилерам і 92 700 — кінцевим споживачам за три місяці до 31 березня, що становить квартальне зростання на 61,1% і 16,2% відповідно, після відновлення виробництва на заводах у Соліхаллі, Халвуді та Вулвергемптоні до нормального рівня. Однак, незважаючи на це відновлення, результати компанії все ще відстають від показників попереднього року. У порівнянні з аналогічним періодом 2024 року продажі JLR як споживачам, так і дилерам знизилися більш ніж на 14%, причому на китайському ринку спостерігалося значне падіння на 29,8%, що відображає триваючі труднощі, пов'язані з американськими митами, ринковими викликами та запланованим виведенням з обігу старих моделей Jaguar». ***(JLR sees sales recover after cyber attack // BBC (https://www.bbc.com/news/articles/c5yj9g89362o). 02.04.2026).***

***

«Як повідомляється, стався серйозний витік корпоративних даних після того, як зловмисники проникли в захищену мережу, скориставшись підключеною до Інтернету кавоваркою. За словами експерта з цифрової криміналістики, пристрій був підключений до мережі компанії з використанням пароля за замовчуванням, працював на застарілій операційній системі та не мав брандмауера. Це дозволило зловмисникам викрасти конфіденційні дані, надсилаючи пакети даних за кордон щоразу, коли співробітник готував каву, фактично обходячи стандартні засоби безпеки… Цей інцидент є суворим нагадуванням для керівників служб інформаційної безпеки про те, що проігноровані активи Інтернету речей (IoT), такі як розумна побутова техніка, принтери та камери, можуть створювати критичні вразливості в інакше захищених середовищах. Щоб зменшити цей ризик, команди з безпеки повинні проактивно перевіряти та захищати всі підключені пристрої, ізолювати їх від конфіденційних мереж та включити ці нетрадиційні кінцеві точки до своїх основних програм моніторингу та управління поверхнею атаки». ***(Evan Rowe. Internet-Connected Coffee Machine Reportedly Led to Corporate Data Breach // Techstrong Group Inc. (https://securityboulevard.com/2026/04/internet-connected-coffee-machine-reportedly-led-to-corporate-data-breach/). 04.04.2026).***

***

«Зловмисник заявив, що продає набір даних, нібито викрадених з торгової платформи Forex, зазначивши, що він містить близько 438 000 записів про користувачів та 185 000 записів про транзакції. Дослідники зазначили, що зловмисник надав лише невеликий зразок — один запис користувача та 16 записів транзакцій — із такими полями, як електронні адреси, імена користувачів, ідентифікатори користувачів, ідентифікатори транзакцій, номери довідок та суми платежів, а відсутність посилань для завантаження свідчить про те, що зловмисник, ймовірно, прагне домовитися про продаж, а не оприлюднити дані… Витік даних не

підтверджено, і немає підтвердження, що дані походять саме з Forex, але якщо вони справжні, це може наражати користувачів на подальше шахрайство, оскільки суми транзакцій та ідентифікатори можуть розкривати торгові моделі та уможливлювати більш цілеспрямовані шахрайські дії у поєднанні з іншою інформацією. Рекомендовані кроки: швидко перевірити, чи дані справжні та пов'язані з організацією; розглядати ідентифікатори транзакцій та суми як конфіденційні операційні дані; та підготуватися до спроб шахрайства, пов'язаних із витоком інформації про торгову діяльність». ***(Evan Rowe. Hackers Claim Massive Forex Trading Data Leak Could Expose 438,000 User Records // Techstrong Group Inc. (https://securityboulevard.com/2026/04/hackers-claim-massive-forex-trading-data-leak-could-expose-438000-user-records/). 04.04.2026).***

***

«Дослідники у сфері кібербезпеки виявили «Masjesu», також відомий як «XorBot» — нову бот-мережу, яка з 2023 року функціонує як сервіс DDoS-атак на замовлення. Ця бот-мережа, реклама якої поширюється переважно через Telegram, націлена на широкий спектр пристроїв Інтернету речей (IoT), зокрема маршрутизатори, шлюзи, камери та відеореєстратори від багатьох провідних виробників. На відміну від багатьох ботнетів, які надають пріоритет гучним, широкомасштабним інфікуванням, Masjesu вирізняється стратегією стійкості та низької помітності. Він навмисно уникає націлювання на відомі критично важливі організації, такі як Міністерство оборони США, щоб уникнути уваги правоохоронних органів та забезпечити свою довгострокову життєздатність. Щоб зберегти цю прихованість, шкідливе програмне забезпечення використовує шифрування на основі XOR для приховування своїх рядків та даних конфігурації…

З моменту виявлення ця бот-мережа еволюціонувала, інтегрувавши різні експлойти для різних апаратних архітектур, зокрема для маршрутизаторів Realtek. Після зараження пристрою шкідливе ПЗ забезпечує свою стійкість, припиняє роботу конкуруючих процесів бот-мереж, таких як wget і curl, та прив'язується до певного TCP-порту, очікуючи команд від своїх операторів… Крім того, Masjesu має здатність до саморозповсюдження, що дозволяє їй сканувати випадкові IP-адреси та залучати нові пристрої до своєї інфраструктури. Ботнет запускає об'ємні DDoS-атаки на такі цілі, як корпоративні системи, ігрові сервери та мережі доставки контенту. Хоча його діяльність охоплює весь світ, трафік переважно походить із В'єтнаму — на який припадає майже половина всієї спостережуваної активності — а також з України, Ірану, Бразилії, Кенії та Індії. Постійно розширюючи список експлойтів для апаратного забезпечення та обережно уникаючи чутливих цілей, Masjesu залишається зростаючою та постійною загрозою у сфері Інтернету речей». ***(Ravie Lakshmanan. Masjesu Botnet Emerges as DDoS-for-Hire Service Targeting Global IoT Devices // The Hacker News (https://thehackernews.com/2026/04/masjesu-botnet-emerges-as-ddos-for-hire.html). 08.04.2026).***

***

«У звіті за квітень 2026 року, опублікованому постачальником програмного забезпечення для індустрії iGaming компанією Digitain,

наголошується на зростаючій глобальній загрозі кіберзлочинності, яка зараз обходиться світовій економіці у понад 1 трильйон доларів щорічно, а також наводиться рейтинг країн за рівнем їхньої стійкості до кібератак із використанням штучного інтелекту. У ході дослідження країни оцінювалися за такими ключовими факторами, як ВВП для фінансування, державна політика у сфері безпеки, технологічна інфраструктура та впровадження штучного інтелекту, що стає дедалі важливішим для автоматизованого виявлення загроз…

Уругвай виявився найстійкішою країною світу, забезпечивши захист майже 98 % своїх пристроїв від вірусів та програм-вимагачів, що значною мірою стало можливим завдяки суворим державним вимогам щодо безпеки. На другому місці опинився Катар, який, використовуючи значні національні ресурси та 40-відсотковий рівень впровадження штучного інтелекту в корпоративному секторі, забезпечив захист приблизно 95 % пристроїв. Болгарія посіла третє місце, досягнувши рівня захисту, аналогічного Катару, завдяки жорстким нормам щодо конфіденційності, незважаючи на нижчий рівень доходів. Швейцарія посіла четверте місце, скориставшись значними інвестиціями у брандмауери, 35% впровадженням штучного інтелекту та високим рівнем цифрової грамотності населення, а Франція замикає п’ятірку лідерів, маючи найвищий у світі показник індексу кібербезпеки та 44% рівень впровадження штучного інтелекту, що дозволяє ботам виявляти загрози.

У висновках звіту експерти висловлюють серйозне застереження: кіберзлочинність увійшла до двадцятки найбільших галузей світової економіки, а штучний інтелект дає змогу злочинним угрупованням здійснювати одночасні автоматизовані атаки в безпрецедентних масштабах, через що надійна державна політика у сфері кібербезпеки стає важливішою, ніж будь-коли». ***(Which Countries Are Most Prepared for AI-Powered Cyberattacks? // Investorideas.com (https://www.investorideas.com/news/2026/defense/04082-ai-cyberattack-resilience-global-ranking.asp). 08.04.2026).***

***

«Проіранська кіберзлочинна група взяла на себе відповідальність за серію атак типу «розподілена відмова в обслуговуванні» (DDoS), які тимчасово вивели з ладу веб-сайти фінтех-компанії Chime Financial та соціальної мережі Pinterest… Компанія Chime підтвердила, що 1 квітня у неї стався короткочасний збій у роботі, який було швидко усунуто без жодних наслідків для коштів або даних користувачів, тоді як Pinterest повідомила про відбиття подібної атаки у вівторок, яка зачепила менше 2% її трафіку… Ці інциденти збігаються з більш широким урядовим попередженням від Агентства з кібербезпеки та безпеки інфраструктури (CISA), яке попередило, що хакери, пов'язані з Іраном, активно націлюються на операційні технологічні системи в секторі критичної інфраструктури США та порушують їхню роботу, особливо в енергетичній та водопостачальній галузях. Кіберзбої сталися на тлі загострення геополітичної напруженості, коли президент Дональд Трамп виступив із суворим попередженням на адресу Ірану щодо Ормузької протоки, а потім відклав його». ***(Margi Murphy and Paige Smith. Pro-Iran Group Takes Credit for Cyberattacks on Chime, Pinterest //***

Bloomberg L.P. (https://www.bloomberg.com/news/articles/2026-04-07/pro-iran-group-takes-credit-for-cyberattacks-on-chime-pinterest). 08.04.2026).

***

«Недавні збої, такі як зупинка виробництва Jaguar Land Rover наприкінці 2025 року та масовий хаос у європейських аеропортах після того, як зловмисники зламали програмне забезпечення MUSE компанії Collins Aerospace, ілюструють, як операційна вразливість дедалі більше зумовлюється цифровою взаємозалежністю, а не дефіцитом комплектуючих: навіть якщо основні системи компанії залишаються захищеними, злом одного постачальника може зупинити виробництво, затримати поставки або призвести до витоку даних. Кількість атак на ланцюги постачання перевищила попередні прогнози — прогноз Gartner на 2021 рік, згідно з яким до 2025 року 45 % організацій зіткнуться з атаками на ланцюги постачання програмного забезпечення, зараз видається заниженим, оскільки дослідження показують, що 61 % підприємств зазнали порушень у ланцюгах постачання протягом останнього року, що часто призводило до зривів у роботі або фінансових втрат…

Зловмисники все частіше обирають мішенню невеликих постачальників, розглядаючи їх як «слабке місце» екосистем, побудованих на хмарних провайдерах, інструментах SaaS, логістичних партнерах та операторах обробки даних; наприклад, компанія Mango повідомила про викрадення даних клієнтів через зовнішнього постачальника маркетингових послуг. Дослідження показують, що невеликі фірми непропорційно сильно страждають від каскадних наслідків, проте багато керівників служб безпеки залишаються надто впевненими в собі та не надають належного пріоритету компрометації ланцюга поставок (лише 23% вважають це однією з головних нових загроз), незважаючи на реальні наслідки, включаючи витік даних клієнтів, співробітників та партнерів, незаплановані витрати та перебої в роботі…

Одноразові сертифікації постачальників та формальне дотримання вимог вже не є достатніми, і закликається до «постійного забезпечення»: включення до контрактів вимог щодо кібербезпеки, що підлягають примусовому виконанню; перехід від одноразової перевірки до постійної верифікації за допомогою аудитів, моніторингу та оцінки ризиків у реальному часі; а також приведення управління сторонніми організаціями у відповідність до таких стандартів, як NIST 800-53 та ISO 27001 (а також базових програм, таких як Cyber Essentials), щоб підвищити рівень зрілості безпеки в усій екосистемі». ***(Sam Peters. Why the Next Supply Chain Shock Will Come From Cyber, Not Shortages // Keller International Publishing Corp (https://www.supplychainbrain.com/blogs/1-think-tank/post/43701-why-the-next-supply-chain-shock-will-come-from-cyber-not-shortages). 08.04.2026).***

***

«Хакери заявили про масштабний кіберзлом великого китайського суперкомп'ютерного центру, ймовірно, Національного суперкомп'ютерного центру в Тяньцзіні, в результаті якого, за повідомленнями, було викрадено понад 10 петабайтів даних. Центр обслуговує тисячі клієнтів у науковій,

промисловій та оборонній галузях, тому будь-яке порушення безпеки має надзвичайно серйозні наслідки. За повідомленнями, серед викрадених зразків є конфіденційна інформація, пов'язана з обороною, така як дані про конструкцію ракет, що викликає серйозні побоювання щодо національної безпеки. Хоча повний масштаб зломів не був незалежно перевірений, експерти вважають наявні докази достатньо надійними, щоб викликати занепокоєння… Зловмисники стверджують, що отримали доступ через зламану VPN-мережу і протягом місяців залишалися непоміченими, використовуючи ботнети для викачування даних. Цей інцидент також, схоже, відповідає схемі часткових витоків даних, спрямованих на залучення покупців або монетизацію порушення. Якщо це підтвердиться, цей випадок продемонструє вразливість централізованої високоцінної обчислювальної інфраструктури та її потенціал одночасно наражати на небезпеку численні організації, підкреслюючи зростаючі ризики у глобальному кіберконфлікті». ***(Guru Baran. Hackers Claim to Have Stolen 10 Petabytes of Data from China's Tianjin Supercomputer Center // Cyber Security News (https://cybersecuritynews.com/supercomputing-center-data-breach/). 09.04.2026).***

***

«Перший тиждень квітня 2026 року продемонстрував загострення загроз кібербезпеці, з якими стикаються об'єкти критичної інфраструктури та конфіденційні дані в багатьох секторах. Атака програм-вимагачів на водоочисну станцію в місті Мінот (штат Північна Дакота) змусила підприємство повернутися до ручного управління, що призвело до перебоїв у роботі та викрило вразливі місця в критичній інфраструктурі. У відповідь ФБР розпочало операцію «Winter Shield» для боротьби зі зростаючою кількістю атак програм-вимагачів на об'єкти комунального господарства, наголосивши на необхідності державно-приватного партнерства між урядовими органами та приватними організаціями для посилення колективної оборони. Одночасно зловмисники скористалися витоком вихідного коду з Claude Code компанії Anthropic для створення фальшивих репозиторіїв GitHub, що розповсюджували шкідливе програмне забезпечення, зокрема інфостілер Vidar та шкідливе програмне забезпечення GhostSocks, націлене на розробників… Інфостілер «Vidar» призначений для викрадення конфіденційної інформації, такої як облікові дані та особисті дані, тоді як «GhostSocks» створює проксі-сервер на заражених комп'ютерах, що дозволяє зловмисникам приховувати свою особу під час здійснення подальших атак. Ця тенденція до використання витоків вихідного коду підкреслює нагальну необхідність для організацій захищати інтелектуальну власність та забезпечувати безпеку своїх ресурсів з розробки програмного забезпечення, оскільки розробники є головними мішенями через їхній доступ до конфіденційної інформації та інструментів. В іншому значному інциденті Управління лікарень Гонконгу 2 квітня 2026 року повідомило про витік даних, що поставив під загрозу конфіденційну інформацію приблизно 56 000 пацієнтів, що спонукало до розслідування з боку Управління комісара з питань конфіденційності та місцевої поліції… Цей випадок підкреслює нагальну необхідність для організацій сфери охорони здоров'я надати пріоритет кібербезпеці, оскільки дані пацієнтів є особливо цінними для кіберзлочинців, які

прагнуть використати особисту інформацію з метою отримання фінансової вигоди. Ці інциденти, що сталися у квітні 2026 року, у сукупності свідчать про більш загальну тенденцію: критична інфраструктура та конфіденційні дані дедалі більше наражаються на ризик у міру стрімкого розвитку кіберзагроз. Організації у всіх секторах повинні прийняти проактивну стратегію кібербезпеки, яка включає регулярні аудити безпеки, добре розроблені та регулярно оновлювані плани реагування на інциденти, постійне навчання співробітників щодо розпізнавання фішингу та тактик соціального інжинірингу, а також інвестиції в передові технології безпеки, такі як системи виявлення вторгнень та шифрування. У міру розширення цифрового простору та ускладнення дій зловмисників збереження пильності та готовності реагувати на постійно мінливе середовище загроз стало необхідним для забезпечення стійкості організацій та захисту даних». ***(Matthew Lynch. Surge in Cybersecurity Incidents: April 2026 Highlights Major Threats // Matthew Lynch (https://www.theedadvocate.org/surge-in-cybersecurity-incidents-april-2026-highlights-major-threats/). 12.04.2026).***

***

«Компанія Vercel повідомила про інцидент безпеки після того, як зловмисник заявив, що проник у її системи, і намагається продати викрадені дані на хакерському форумі. Хмарна платформа для розробки, відома завдяки Next.js та таким сервісам, як безсерверні функції, периферійні обчислення та конвеєри CI/CD, підтвердила несанкціонований доступ до певних внутрішніх систем і заявила, що залучила експертів з реагування на інциденти, повідомила правоохоронні органи та активно проводить розслідування. Порушення безпеки сталося внаслідок компрометації облікового запису Google Workspace співробітника Vercel за допомогою стороннього інструменту штучного інтелекту Context.ai, після чого зловмисник підвищив свої привілеї та отримав доступ до змінних середовища, які не були позначені як конфіденційні і, отже, не шифрувалися під час зберігання… Vercel наголосив, що всі змінні середовища клієнтів зберігаються у повністю зашифрованому вигляді з використанням багаторівневих засобів захисту, що це не вплинуло на основні сервіси компанії, а також що проекти з відкритим кодом, зокрема Next.js і Turbopack, залишилися незачепленими. Компанія порадила клієнтам перевірити свої змінні середовища, позначити конфіденційні для шифрування, а також впровадила вдосконалення в панелі управління для кращого управління ними. Зловмисник, який стверджував, що належить до групи ShinyHunters (хоча група заперечила свою причетність), опублікував зразки, що містили 580 записів про співробітників та знімок екрана внутрішньої панелі управління, і запропонував продати ключі доступу, вихідний код, дані бази даних, внутрішні розгортання та ключі API (включно з токенами NPM та GitHub), вимагаючи, за повідомленнями, викуп у розмірі 2 мільйонів доларів. Vercel не підтвердила жодних переговорів щодо викупу». ***(Lawrence Abrams. Vercel confirms breach as hackers claim to be selling stolen data // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/vercel-confirms-breach-as-hackers-claim-to-be-selling-stolen-data/). 19.04.2026).***

***

«За останні роки різко зросла кількість кіберзагроз, спрямованих проти освітнього сектору. Згідно з доповіддю Quorum Cyber, кількість кіберінцидентів, що зачепили університети, коледжі та школи, зросла на 63% у період з листопада 2023 року по жовтень 2025 року. На основі даних про загрози від FalconFeeds.io у 67 країнах у звіті «Глобальний прогноз кіберризиків для вищої освіти на 2026 рік» наголошується на тривожному зростанні як частоти, так і складності атак, що значною мірою зумовлено хактивізмом, геополітичною напруженістю та еволюцією кампаній із використанням програм-вимагачів. Тільки кількість випадків витоку даних зросла на 73%, що призвело до витоку особистої інформації, даних досліджень та фінансових записів, тоді як кількість інцидентів, пов'язаних з хактивізмом, зросла на 75%, а кількість атак з використанням програм-вимагачів — на 21%...

До додаткових загроз належать частіші атаки типу «розподілена відмова в обслуговуванні» (DDoS), що проводяться з метою зриву важливих навчальних періодів, а також все ширше використання генеративної штучної інтелекту для створення переконливих фішингових листів, автоматизації атак та розробки вдосконаленого шкідливого програмного забезпечення. Також зросла кількість шпигунських програм та шкідливого програмного забезпечення для викрадення інформації, що поширюються через фішингові кампанії, які використовують людські помилки студентів, викладачів та співробітників для отримання облікових даних та горизонтального переміщення по системах. У звіті підкреслюється, що навчальні заклади з їхніми відкритими мережами, величезними цифровими екосистемами та масивами конфіденційних даних стали привабливими цілями як для злочинців, що керуються фінансовими мотивами, так і для хактивістів, що керуються ідеологічними мотивами. Без проактивних інвестицій у підвищення обізнаності з питань безпеки, інфраструктуру та виявлення загроз розширення площі атаки в цьому секторі продовжуватиме робити його вразливим до дедалі більш витончених і руйнівних кібероперацій». ***(Naveen Goud. Universities and Schools were badly hit by Cyber Attacks in 2025 // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/universities-and-schools-were-badly-hit-by-cyber-attacks-in-2025/). 23.04.2026).***

***

«15 квітня у мережі Bluesky стався масштабний збій, спричинений складною розподіленою атакою типу «відмова в обслуговуванні» (DDoS), яка порушила роботу основних функцій, зокрема стрічок новин, сповіщень, тем та пошуку. Представники децентралізованої соціальної мережі повідомили, що їхні інженери працювали всю ніч, аби нейтралізувати атаку, яка протягом дня набирала сили, та підтвердили, що з 16 квітня платформа працює стабільно, незважаючи на триваючі спроби атак. Bluesky заявила, що немає доказів того, що інцидент пов'язаний з несанкціонованим доступом до приватних даних користувачів. DDoS-атаки працюють шляхом затоплення онлайн-сервісів великими обсягами трафіку, що робить їх повільними або недоступними для законних користувачів…

Хоча компанія не пов’язала цю атаку з жодним конкретним суб’єктом, пов’язана з Іраном хакерська група під назвою «313 Team» взяла на себе відповідальність на своєму каналі в Telegram, назвавши її «масштабною кібератакою», спрямованою проти інтерфейсу прикладного програмування (API) Bluesky. Ця група, яка, як вважається, діє з території Іраку та підтримує шиїтські міліції, що фінансуються Іраном, раніше вже проводила операції у відповідь проти організацій, які, на її думку, підтримують США або Ізраїль. Bluesky відмовилася висловлювати припущення щодо авторства атаки. Інцидент стався на тлі стрімкого зростання Bluesky з 2024 року, коли користувачі почали мігрувати з X Ілона Маска після переобрання Дональда Трампа, досягнувши приблизно 43,7 мільйона користувачів — хоча це значно менше, ніж у X та Threads від Meta, кожна з яких має сотні мільйонів активних користувачів щомісяця». ***(Daryna Antoniuk. Bluesky blames app outage on ‘sophisticated’ DDoS attack // Recorded Future News (https://therecord.media/bluesky-blames-app-outage-on-ddos). 20.04.2026).***

***

«У сучасному взаємопов’язаному цифровому середовищі, де межі між професійним та особистим життям значною мірою стираються, кіберзлочинці дедалі частіше обходять захищені корпоративні периметри, націлюючись на керівників та їхні сім’ї за допомогою «ланцюга особистих атак» — складного багатоетапного процесу, який використовує загальнодоступні особисті дані для того, щоб у кінцевому підсумку отримати доступ до корпоративних систем та інтелектуальної власності. Цей ланцюг зазвичай починається з розвідки, під час якої зловмисники збирають дані про особу з джерел, таких як брокери даних, соціальні мережі, публічні реєстри та інші джерела, після чого відбувається вторгнення в часто вразливе домашнє середовище через незахищені пристрої Інтернету речей (IoT), слабкі мережі Wi-Fi або скомпрометовані особисті пристрої…

Опинившись всередині, зловмисники здійснюють горизонтальне переміщення, щоб отримати доступ до конфіденційних особистих облікових записів і відстежувати комунікації в пошуках сприятливих моментів, а в підсумку реалізують такі цілі, як фінансове шахрайство, крадіжка особистих даних, підробка особи за допомогою технології «діпфейк» або повне захоплення корпоративного облікового запису. Цей підхід є особливо ефективним, оскільки використовує легітимний доступ і соціальну інженерію, а не пряме шкідливе програмне забезпечення, що діє на рівні файлів, через що традиційні реактивні засоби, такі як антивіруси або базові VPN, виявляються недостатніми. Щоб протидіяти цьому, організації впроваджують стратегії цифрового захисту керівників (DEP), які розглядають особисту кібербезпеку як основний корпоративний імператив. Це включає зменшення цифрового сліду за допомогою очищення даних у брокерах, посилення захисту домашніх мереж та пристроїв, забезпечення моніторингу крадіжок особистих даних та кредитів, надання індивідуального навчання та підготовки для керівників та їхніх сімей, а також швидке реагування на інциденти… Експерти наголошують на необхідності активного збору розвідувальної інформації, постійного моніторингу «темного вебу» на предмет

витоку облікових даних, незалежної перевірки постачальників та домашніх систем, а також проведення аудитів безпеки до та після поїздок, щоб перервати ланцюжок загроз, перш ніж він досягне підприємства. Зрештою, захист інтелектуальної власності сьогодні вимагає комплексного підходу, що забезпечує безпеку як в офісі, так і вдома, з урахуванням того, що в сучасному цифровому світі, який ніколи не спить, особисті вразливості стали шлюзами для компрометації організацій». ***(Mark A. Houpt. When the Attack Comes Faster: What Security Leaders Need to Know About AI-Powered Threats // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/when-the-attack-comes-faster-what-security-leaders-need-to-know-about-ai-powered-threats/). 20.04.2026).***

***

«…У 2025 році збитки від кіберзлочинності у США досягнуть рекордного рівня — майже 21 мільярд доларів, а загальні збитки приватного сектору від зловмисної кібердіяльності часто перевищують 200 мільярдів доларів на рік, тоді як суб'єкти, що діють за підтримки держави, дедалі частіше націлюються на економічні цінності, стираючи межу між кіберпростором та економічною конкуренцією як аренами конфлікту. У аналізі стверджується, що Китай є одночасно найзначнішою економічною та кіберзагрозою для Сполучених Штатів, використовуючи кібершпигунство, цифрове крадіжки та компрометацію ланцюгів постачання як основні інструменти економічної політики, тому Вашингтон повинен інтегрувати економічну та кіберпотужність у скоординовані кампанії, а не розглядати їх окремо… У ній економічна політика (санкції, експортний контроль, мита, інвестиції та допомога) та кіберполітика (формування стимулів і забезпечення безпеки цифрової інфраструктури, включаючи кібероперації) розглядаються як дисципліни, що зближуються, які вимагають як загальнодержавних заходів, так і тісної координації з приватним сектором, оскільки саме приватний сектор управляє більшістю інфраструктури та несе на собі значну частину ризиків; залежність фінансів від цифрових систем — від щоденних операцій з акціями на трильйони доларів і величезних обсягів банківських переказів/ACH до глобального обміну повідомленнями через SWIFT — робить ставки особливо високими, про що свідчать серйозні порушення безпеки та високі середні витрати на один інцидент. Кібероперації можуть безпосередньо сприяти досягненню економічних цілей (крадіжка інтелектуальної власності, комерційних таємниць, викрадення криптовалюти з метою ухилення від санкцій), а також те, що економічні органи влади також лежать в основі кіберзаходів (наприклад, кіберсанкції на підставі IEEPA та NDAA, застосовані проти Росії та у відповідь на інцидент із SolarWinds), що підсилює їхню взаємну залежність…

Виходячи з досвіду становлення кіберполітики США, у доповіді стверджується, що економічна політика США залишається стратегічно незрілою, гальмуючись бар'єрами в обміні інформацією та роздробленою бюрократією, і рекомендується три реформи: розробити об'єднуючу, довгострокову стратегічну парадигму, подібну до зміни кіберполітики 2018 року в бік «наступальної оборони» та постійної взаємодії; переформатувати стимули для обміну інформацією між державним і приватним секторами за допомогою правових гарантій, подібних до

Закону про обмін інформацією з питань кібербезпеки 2015 року (який створив загальні визначення, «обов'язок уряду щодо обміну» та захист у сфері відповідальності, доступу до інформації та антимонопольного законодавства); а також централізувати та координувати розрізнені обов'язки через стабільні інституційні координаційні центри, беручи до уваги досвід створення CISA, Кіберкомандування США та посади Національного директора з питань кібербезпеки — водночас визнаючи їхні поточні обмеження та ризики реорганізації без чіткої мети. Загалом, суть аргументу полягає в тому, що економічне процвітання та національна безпека сьогодні залежать від того, щоб розглядати економічну та кіберполітику як взаємопов'язані та взаємодоповнюючі сфери, що вимагає комплексної стратегії, ефективніших стимулів для співпраці та злагодженої координації, аби ефективно протистояти супротивникам». ***(Jason Blessing. Seeing the Cyber in Economic Statecraft // Metamorphic Media (https://warontherocks.com/seeing-the-cyber-in-economic-statecraft/). 23.04.2026).***

***

«Північна Корея протягом останніх років проводить одну з найбільш непомітних, але ефективних операцій з кібершахрайства: агенти, що діють за підтримки держави, видають себе за законних ІТ-фахівців, які працюють віддалено, щоб отримати роботу в сфері розробки програмного забезпечення в компаніях по всьому світу, особливо у США та Європі. Використовуючи викрадені особисті дані, сфабриковані резюме та підроблені посвідчення, ці «працівники» часто перенаправляють відеоспівбесіди на телефон або в текстовий формат, посилаючись на технічні проблеми, а перед камерою з'являється їхній спільник. Заробітна плата, яка може сягати до 300 000 доларів на рік на одного агента, перераховується до Північної Кореї, де режим утримує до 90% цих коштів для фінансування своїх програм з розробки ракет та зброї масового знищення…

Ця операція, яка діє щонайменше з 2017 року та поширюється на нові галузі й великі організації, пов'язана з доменом luckyguys[.]site, який дослідники з Team Cymru проаналізували після отримання інформації від дослідника з питань безпеки криптовалют ZachXBT. Аналіз трафіку показав значну залежність від VPN-сервісів, таких як Astrill (37,5%), Mullvad (32,25%) та Proton VPN (6,25%), для маршрутизації з'єднань через вихідні вузли у США, що дозволяє оперативникам виглядати як звичайні місцеві співробітники, а також з'єднання з Gmail, ChatGPT та фріланс-платформою Workana. З кінця 2024 року оперативники посилили тактику вимагання, викрадаючи конфіденційні дані та вихідний код у роботодавців і вимагаючи викуп…

У березні 2026 року Управління з контролю за іноземними активами Міністерства фінансів США наклало санкції на шістьох осіб та дві організації за їхню причетність до схеми, яка відома під такими назвами, як Coral Sleet, PurpleDelta та Wagemole. Організаціям рекомендується з обережністю ставитися до IP-адрес, що належать до приватних мереж, оскільки вони можуть бути частиною проксі-мереж або мереж для відмивання коштів, відстежувати використання VPN від провайдерів, які раніше були пов'язані з діяльністю КНДР, ретельно перевіряти канали найму фрілансерів та досліджувати зв'язки з конкретними IP-адресами,

такими як 216.158.225[.]144 та 163.245.219[.]19. Різке падіння мережевого трафіку після публічного розкриття домену luckyguys[.]site підтверджує, що оператори швидко покидають інфраструктуру, щойно вона викрита». ***(Tushar Subhra Dutta. North Korean Hackers Use Fake IT Worker Scheme to Infiltrate Companies and Evade Sanctions // Cyber Security News (https://cybersecuritynews.com/north-korean-hackers-use-fake-it-worker-scheme/). 23.04.2026).***

***

«Раніше не задокументований зловмисник, пов'язаний з Китаєм, якого компанія ESET відстежує під назвою GopherWhisper, проводить операції з кібершпигунства щонайменше з листопада 2023 року, націлюючись на урядову установу Монголії та, ймовірно, десятки інших жертв у різних регіонах і секторах. Група була виявлена в січні 2025 року після того, як дослідники ідентифікували раніше невідомий бекдор під назвою LaxGopher, розгорнутий приблизно на десятку систем у монгольській установі. GopherWhisper активно використовував легітимні онлайн-сервіси, такі як Discord, Slack та Microsoft 365 Outlook, щоб приховати свою діяльність, застосовуючи їх для управління та передачі даних…

Зловмисники використовували набір спеціально розроблених інструментів, написаних переважно на мові програмування Go, зокрема бекдор RatGopher, BoxOfFriends, інжектор JabGopher, завантажувач FriendDelivery та інструмент для викрадення даних CompactGopher, який стискав викрадені файли та завантажував їх на сервіс обміну файлами File.io. Ця операція відповідає ознакам кібершпигунства, що фінансується державою, хоча компанія ESET не пов’язує її з конкретною організацією. Ця кампанія підкреслює, як групи, що представляють собою складні постійні загрози, все частіше використовують популярні платформи для співпраці та спеціальні інструменти, щоб залишатися непомітними під час викрадення конфіденційних даних з урядових та інших важливих об’єктів». ***(Daryna Antoniuk. China-linked hackers targeted Mongolian government using Slack, Discord for covert communications // Recorded Future News (https://therecord.media/china-linked-hackers-target-mongolian-gov-slack-discord). 23.04.2026).***

***

«Управління генерального інспектора (OIG) NASA оприлюднило подробиці складної багаторічної кампанії зі spear-phishing, яку очолював громадянин Китаю Сонг Ву, який видавав себе за американських дослідників з метою незаконного отримання секретних оборонних технологій. У період з 2017 по 2021 рік Сонг, інженер державного китайського оборонного конгломерату AVIC, націлився на десятки інженерів та професорів у державних установах — зокрема в NASA, армії та флоті — а також в університетах і приватних компаніях. Видаючи себе за надійного колегу, Сонг успішно обдурив жертв, змусивши їх поділитися власницьким програмним забезпеченням для моделювання та вихідним кодом, що використовуються для критично важливих військових застосувань, таких як розробка тактичних ракет та проектування аеродинамічної зброї…

У 2024 році Міністерство юстиції США висунуло Сонгу звинувачення у шахрайстві з використанням засобів зв'язку та крадіжці особистих даних з обтяжуючими обставинами, проте він досі перебуває на волі і був внесений до списку найбільш розшукуваних осіб ФБР. Інспекція генерального інспектора НАСА зазначила, що, хоча кампанія була дуже ефективною, були присутні ледь помітні тривожні сигнали, такі як неодноразові запити Сонга на одне й те саме програмне забезпечення без обґрунтування та використання нетрадиційних методів передачі даних для уникнення виявлення. Цей інцидент підкреслює постійну загрозу схем «експортного шахрайства» та наголошує на нагальній потребі дослідників і державних службовців залишатися пильними щодо витончених спроб підробки особи, спрямованих на обхід законів про експортний контроль та незаконне привласнення конфіденційних технологій США». ***(Ravie Lakshmanan. NASA Employees Duped in Chinese Phishing Scheme Targeting U.S. Defense Software // The Hacker News (https://thehackernews.com/2026/04/nasa-employees-duped-in-chinese.html). 24.04.2026).***

***

Діяльність хакерів та хакерські угруповування

«Компанія Microsoft виявила масштабну кампанію російської групи військової розвідки «Forest Blizzard», яка зламує незахищені інтернет-маршрутизатори для малих офісів та домашніх офісів (SOHO) з метою перехоплення запитів до системи доменних імен (DNS). Принаймні з серпня 2025 року зловмисник змінював мережеві налаштування вразливих пристроїв, перетворюючи їх на частину своєї шкідливої інфраструктури для пасивного шпигунства за понад 200 організаціями та 5 000 споживчих пристроїв… Це широкомасштабне перехоплення DNS дозволяє зловмиснику здійснювати складні атаки типу «супротивник посередині» (AiTM), спрямовані конкретно на TLS-з'єднання з веб-версією Microsoft Outlook та іншими урядовими серверами з метою перехоплення даних у вигляді звичайного тексту, включаючи електронні листи та інший конфіденційний вміст…

Використовуючи ці менш захищені периферійні пристрої, Forest Blizzard отримує стійкий плацдарм для проведення подальших атак на важливі об’єкти урядового, IT- та енергетичного секторів. Microsoft закликає організації мінімізувати цю загрозу шляхом впровадження моделі Zero Trust DNS, суворого дотримання багатофакторної автентифікації, централізації управління ідентифікацією, а також усвідомлення того, що некеровані пристрої класу SOHO, якими користуються віддалені співробітники, можуть наражати захищені корпоративні мережі на значний ризик». ***(SOHO router compromise leads to DNS hijacking and adversary-in-the-middle attacks // Microsoft (https://www.microsoft.com/en-us/security/blog/2026/04/07/soho-router-compromise-leads-to-dns-hijacking-and-adversary-in-the-middle-attacks/). 07.04.2026).***

***

«Іранська хакерська група під назвою «Handala» нещодавно проникла в мережі медичної технологічної компанії «Stryker», що базується в штаті Мічиган, знищивши дані та вивівши з ладу тисячі пристроїв, зокрема ті, що використовуються працівниками служб екстреної допомоги, а потім проголосила цей інцидент початком «нової ери кібервійни». Однак цей епізод подається як доказ того, що іранська кібервійна залишається більш обмеженою та опортуністичною, ніж давно роздуті уявлення про «цифровий Перл-Харбор»: незважаючи на оцінки американських розвідок, які попереджають, що зростаючий досвід Ірану робить його серйозною загрозою, та на багаторічне вивчення критичних систем командами, пов'язаними з Іраном, кібернаслідки, які спостерігалися досі, здебільшого зводилися до кіберзлочинності, пропаганди та незначних зривів, а не до стратегічно вирішальних атак… Хоча деякі дії можуть залишатися непоміченими (швидше шпигунство, ніж операції з порушенням роботи), у спільній консультативній записці США з питань кібербезпеки найбільш помітні іранські інциденти описано як поодинокі хакерські атаки на слабозахищені системи, які інколи спричиняють перебої в роботі та фінансові збитки, що свідчить про відсутність цілісної, скоординованої кампанії… Можливості Ірану можуть бути переоцінені або знижені, особливо після того, як дії США та Ізраїлю під час війни, як повідомляється, були спрямовані проти іранського кіберкерівництва та інфраструктури, при цьому підкреслюється, що ефективна кібервійна не є ні дешевою, ні легкою, і що США та Ізраїль мають набагато глибший досвід інтеграції кібероперацій у військові кампанії… Іран здійснював деструктивні хакерські атаки — зокрема, спроби втручання в роботу промислових контролерів та атаки на камери й системи моніторингу — але їхній вплив було стримано або обмежено порівняно з більш дестабілізуючими традиційними засобами, такими як ракети, безпілотники та загрози морським вузьким місцям; будь-яка майбутня кіберзагроза може залежати від того, чи зможе Іран адаптуватися та відновити свої сили у разі відновлення конфлікту». ***(Jon R. Lindsay. Iran Is Losing the Cyberwar, Not the Real War // The New York Times Company (https://www.nytimes.com/2026/04/11/opinion/iran-war-cyber-warfare-attacks.html). 11.04.2026).***

***

Вірусне та інше шкідливе програмне забезпечення

«Вірус NoVoice для Android — це складне шкідливе програмне забезпечення, яке становить серйозну загрозу для користувачів смартфонів у всьому світі, насамперед атакуючи акаунти WhatsApp з метою викрадення даних та клонування сеансів користувачів. На відміну від типових шкідливих програм, NoVoice працює непомітно у фоновому режимі, безперервно надсилаючи інформацію про пристрій на віддалений сервер, залишаючись при цьому прихованим від користувача. Він отримує глибокий доступ до системи, використовуючи відомі вразливості, що дозволяє йому вбудовуватися в основні системні модулі та робить його видалення надзвичайно складним. Однією з

найнебезпечніших його особливостей є здатність виживати після заводського скидання налаштувань шляхом модифікації критичних системних файлів, а також використання системи самоперевірки для автоматичного перевстановлення у разі видалення будь-яких компонентів… Хоча ця проблема в першу чергу торкнулася користувачів в Африці, випадки її виявлення фіксуються по всьому світу, причому найбільш вразливими є старі та бюджетні пристрої на базі Android через відсутність оновлень безпеки. Експерти з безпеки попереджають, що хоча основною мішенню є WhatsApp, це шкідливе програмне забезпечення можна адаптувати для атак на банківські додатки, що підвищує ризик фінансового шахрайства та крадіжки особистих даних. Для боротьби з цією постійною загрозою користувачам рекомендується видалити всі відомі шкідливі додатки і, що ще важливіше, виконати повну переінсталяцію прошивки, оскільки стандартного скидання до заводських налаштувань недостатньо. Власникам застарілих пристроїв, які більше не отримують оновлень безпеки, настійно рекомендується розглянути можливість їх заміни». ***(Android NoVoice Virus Threat: Malware Can Hack WhatsApp and Survive Factory Reset // Daily Ausaf (https://dailyausaf.com/en/technology/android-novoice-virus-threat-malware-can-hack-whatsapp-and-survive-factory-reset/). 05.04.2026).***

***

«Кіберзлочинці все частіше вдаються до «EDR-кілерів» (Виявлення та реагування на інциденти на кінцевих точках, EDR) — спеціалізованих інструментів, призначених для виведення з ладу програмного забезпечення безпеки, — щоб створити передбачуване вікно для операцій з використанням програм-вимагачів. Замість того, щоб постійно вдосконалювати своє шкідливе ПЗ для уникнення виявлення, зловмисники вважають за ефективніше просто спочатку вимкнути засоби захисту, що дозволяє їхнім за своєю природою «гучним» шифрувальним модулям працювати без перешкод. Згідно з вичерпним звітом ESET Research, спектр цих інструментів значно еволюціонував, виходячи за межі добре відомої техніки «Bring Your Own Vulnerable Driver» (BYOVD). Наразі зловмисники використовують різноманітні методи, включаючи спеціальні скрипти командного рядка, використання легітимних антируткіт-утиліт, таких як GMER та PC Hunter, у злочинних цілях, а також дедалі небезпечніші «бездрайверні» інструменти…

Особливе занепокоєння викликає поширення безпілотних рішень, таких як EDRSilencer та EDR-Freeze; ці інструменти блокують мережевий обмін даними або заморожують роботу програмного забезпечення безпеки, не взаємодіючи з ядром системи, що значно ускладнює їх виявлення традиційними фахівцями з мережевої безпеки. Екосистема розробки цих інструментів є настільки ж складною: від груп, що створюють власне програмне забезпечення з використанням штучного інтелекту, до інших, які модифікують загальнодоступний код для перевірки концепції або купують комерційні продукти «EDR killer as a service» на форумах даркнету. Оскільки ці інструменти активно продаються та обмінюються між партнерами-вимагачами, атрибуція стала складною, оскільки групи, що не пов’язані між собою, часто використовують ті самі драйвери та програмне забезпечення. Отже, дослідники ESET наголошують, що захисники повинні

змінити свою стратегію, відмовившись від простого відстеження конкретних вразливих драйверів, і натомість зосередитися на виявленні поведінкових ознак втручання в систему безпеки, щоб ефективно протидіяти цим різноманітним і постійно еволюціонуючим загрозам». ***(Dhivya. Ransomware Gangs Expand Use of EDR Killers Beyond Vulnerable Drivers, ESET Warns // Cyber Security News (https://cybersecuritynews.com/ransomware-gangs-expand-use-of-edr-killers/). 11.04.2026).***

***

«У четвер органи з кібербезпеки США та Великої Британії повідомили, що хакерська група, яка діє за підтримки держави, встановила на мережевих пристроях безпеки Cisco складний спеціальний бекдор під назвою Firestarter, що дозволяє йому залишатися активним навіть після оновлень прошивки та стандартних перезавантажень. Агентство з кібербезпеки та безпеки інфраструктури виявило цей бекдор на пристрої Cisco Firepower федерального цивільного агентства США після виявлення підозрілих з'єднань, що спонукало видати екстрену директиву, яка вимагає від усіх федеральних цивільних агентств провести аудит своєї інфраструктури брандмауерів Cisco та надати знімки пам'яті пристроїв для аналізу…

Firestarter забезпечує свою стійкість шляхом маніпулювання списком підключень Cisco Service Platform, щоб відновлюватися та запускатися заново після завершення роботи або перезавантаження, а також вбудовує шкідливий шеллкод у LINA — основний код мережевих функцій та брандмауера, що дозволяє йому перехоплювати певні запити на аутентифікацію VPN, які містять приховану послідовність тригерів для виконання коду, наданого зловмисником. Цей бекдор приписують зловмиснику, відстежуваному під індексем UAT-4356 — тій самій групі, що стоїть за шпигунською кампанією ArcaneDoor 2024 року, яка використовувала дві уразливості (CVE-2025-20333 та CVE-2025-20362) для отримання початкового доступу. Firestarter має значні технічні схожості з раніше задокументованим імплантом під назвою RayInitiator, і в інциденті на федеральному рівні зловмисники спочатку розгорнули інший імплант під назвою Line Viper для збору конфігурацій та облікових даних, а потім встановили Firestarter, який вижив після подальшого виправлення та дозволив повторне розгортання Line Viper у березні. Цей механізм збереження даних зачіпає широкий спектр апаратного забезпечення Cisco, зокрема серії Firepower 1000, 2100, 4100, 9300 та Secure Firewall 1200, 3100 і 4200. Компанія Cisco випустила оновлене програмне забезпечення для усунення цієї проблеми, але настійно рекомендує перевстановити ОС на уражених пристроях, якщо є підозра про їх злом. Цей інцидент відображає зростаючу тенденцію, коли хакери, пов'язані з державою, націлюються на периферійні мережеві пристрої, щоб отримати широкий доступ, перехоплювати трафік та викрадати облікові дані й повідомлення, причому на момент публікації активно використовуються відповідні вразливості». ***(Greg Otto. US, UK agencies warn hackers were hiding on Cisco firewalls long after patches were applied // CyberScoop (https://cyberscoop.com/cisco-firestarter-malware-cisa-warning/). 23.04.2026).***

***

«Було виявлено складну атаку через ланцюжок постачання, пов'язану зі шкідливим пакетом npm «js-logger-pack», який використовував авторитетну платформу штучного інтелекту Hugging Face для доставки шкідливого програмного забезпечення та зберігання викрадених даних. Маскуючись під нешкідливий інструмент для ведення журналів, пакет використовував прихований скрипт, що запускався після інсталяції, для завантаження міжплатформних шкідливих бінарних файлів на системи Windows, macOS та Linux. Після інсталяції шкідливе програмне забезпечення забезпечувало свою стійкість і надавало зловмисникам постійний доступ для викрадення облікових даних, запису натискань клавіш та моніторингу системної активності…

Здійснивши помітну зміну тактики, зловмисник використав власну інфраструктуру Hugging Face як серверну частину для викрадення даних, стискаючи викрадені файли та завантажуючи їх у приватні набори даних, що перебували під контролем зловмисника. Це дозволило серверу управління уникнути прямого зберігання викраденого вмісту, що ускладнило виявлення операції. Імплант навіть містив функцію, яка змушувала користувачів повторно вводити облікові дані, поки його кейлогер був активним, що давало змогу швидко збирати конфіденційну інформацію. Дослідники з безпеки радять усім, хто встановив уразливу версію (1.1.27), негайно змінити всі секретні дані, видалити артефакти персистентності та очистити пакет, наголошуючи, що будь-яка уражена машина має вважатися повністю скомпрометованою, доки ці кроки не будуть виконані». ***(Tushar Subhra Dutta. Malicious npm Package Turns Hugging Face Into Malware CDN and Exfiltration Backend // Cyber Security News (https://cybersecuritynews.com/malicious-npm-package-turns-hugging-face/). 23.04.2026).***

***

«Зразок шкідливого програмного забезпечення під назвою ZionSiphon, вперше виявлений компанією Darktrace і, за повідомленнями, призначений для атак на ізраїльську водогосподарську інфраструктуру шляхом сканування IP-адрес водоочисних та опріснювальних станцій і спроб маніпулювання рівнями хлору та системами регулювання тиску, був визнаний компанією Dragos, що спеціалізується на промисловій кібербезпеці, в основному неефективним. Код містив проіранські та пропалестинські повідомлення для психологічного впливу, але аналітик Dragos з питань шкідливого програмного забезпечення Джиммі Вайлс (Jimmy Wyles) описав його як «галас», зазначивши, що він демонструє незнання або майже повне незнання операційних технологій чи протоколів промислових систем управління, з вигаданими назвами процесів, шляхами до каталогів та файлами конфігурації, ймовірно, згенерованими штучним інтелектом, що призводить до галюцинацій, логічних помилок та недійсних припущень, які зробили б його непрацездатним навіть у разі правильної конфігурації… Компанія Darktrace також визнала, що протестований зразок виявився непрацездатним через неправильну роботу функцій націлювання на конкретні країни. Компанія Dragos вирішила не оприлюднювати додаткові технічні

подробиці щодо цих вразливостей, заявивши, що «не займається виправленням шкідливого програмного забезпечення для зловмисників». Цей випадок підкреслює триваючу дискусію в спільноті кібербезпеки щодо того, скільки уваги слід приділяти новим загрозам, що використовують штучний інтелект, порівняно з більш усталеними та перевіреними тактиками, які застосовують досвідчені угруповання, такі як Volt Typhoon, що має задокументовану історію проникнення в критичну інфраструктуру…

Вайлс попередив, що зосередження уваги на ZionSiphon відволікає обмежені ресурси від більш нагальних загроз, особливо з огляду на те, що середовища операційних технологій суттєво відрізняються від традиційних IT-систем і що менше ніж 10 загальновідомих зразків шкідливого програмного забезпечення здатні реально загрожувати промисловим системам управління. Загалом, хоча загроза хакерських атак із використанням штучного інтелекту продовжує зростати, цей випадок ілюструє, що багато таких інструментів залишаються недосконалими та надмірно розрекламованими порівняно з реальними операційними ризиками». ***(Derek B. Johnson. Dragos: Despite AI use, new malware targeting water plants is 'hype' // CyberScoop (https://cyberscoop.com/dragos-zionsiphon-ai-malware-targeting-water-sector-hype/). 23.04.2026).***

***

«Нова та надзвичайно агресивна кампанія з розповсюдження шкідливого ПЗ через npm, що отримала назву «CanisterSprawl», продемонструвала зростання ризиків у ланцюжку постачання програмного забезпечення, поєднуючи масштабне викрадення даних з автоматизованим зловживанням обліковими записами. Ці шкідливі пакети, виявлені компаніями StepSecurity та Socket, запускаються автоматично після встановлення та сканують систему на наявність конфіденційної інформації, зокрема змінних середовища, токенів розробників, даних криптогаманців та облікових даних браузерів. Особливу небезпеку цій кампанії надає її здатність до саморозповсюдження, «черв'якоподібна» поведінка: шкідливе програмне забезпечення спеціально шукає токени автоматизації npm, щоб отримати доступ на запис, що дозволяє йому захопити обліковий запис жертви, вбудувати шкідливі скрипти в існуючі пакети та опублікувати їх під виглядом легітимного імені…

Ця стратегія переносить загрозу з окремих випадків компрометації систем на потенційні інфекції в масштабах усієї екосистеми, оскільки канали надійних видавців використовуються для подальшого поширення шкідливого програмного забезпечення. Ризик є особливо гострим у середовищах CI/CD, де привілейовані облікові дані часто зберігаються у змінних середовища. Кілька легітимних облікових записів уже було зламано та використано для розміщення шкідливих версій їхнього програмного забезпечення. Організаціям, які, можливо, встановили ці пакети, настійно рекомендується негайно видалити залежності, змінити всі потенційно скомпрометовані секретні дані та ключі API, а також провести перевірку своїх облікових записів на предмет несанкціонованої публікаційної діяльності… Інцидент із CanisterSprawl є наочним нагадуванням про те, що сучасні атаки на основі пакетів націлені на шляхи доступу та довіру в навколишньому

середовищі, що вимагає впровадження проактивних заходів безпеки, які оцінюють ризики компонентів у момент їх використання, щоб блокувати шкідливий код до того, як він зможе закріпитися в надійному конвеєрі». ***(Self-Propagating npm Malware Turns Trusted Packages Into Attack Paths // Sonatype Inc. (https://www.sonatype.com/blog/self-propagating-npm-malware-turns-trusted-packages-into-attack-paths). 23.04.2026).***

***

Програми-вимагачі

«Sinobi — це група хакерів, що використовує програмне забезпечення для вимагання викупу з фінансовою мотивацією, яка з'явилася наприкінці червня 2025 року та працює за закритою гібридною моделлю «Ransomware-as-a-Service» (RaaS), в рамках якої основна команда відповідає за підтримку шкідливого програмного забезпечення, інфраструктури та систем переговорів/платежів, тоді як невелика група довірених партнерів здійснює вторгнення. Група робить акцент на прихованості та контрольованому виконанні, а технічні та інфраструктурні збіги вказують на те, що це ребрендинг або наступник групи-вимагачів Lynx, яка раніше успадкувала елементи від сімейства програм-вимагачів INC. Перед шифруванням Sinobi виконує широке виявлення систем та мереж для ідентифікації локальних та віддалених цілей, а потім шифрує файли у великому масштабі, використовуючи гібридний криптографічний підхід, що поєднує AES-128 у режимі CTR для швидкого шифрування файлів із Curve25519 (Donna) для захисту ключів шифрування, що робить відновлення неможливим без приватних ключів, які перебувають у зловмисників…

Щоб допомогти організаціям перевірити свою готовність до протидії цій загрозі, компанія AttackIQ випустила емуляцію графіка атак, засновану на публічно оприлюднених даних про поведінку Sinobi (зокрема, на звіті eSentire від 27 серпня 2025 року) та внутрішньому аналізі. Емуляція відтворює основні тактики та методи Sinobi, включаючи сценарії доставки та виконання, виявлення систем і середовища (наприклад, збір інформації про систему, рядків середовища та перерахування запущених процесів), кроки з підвищення привілеїв та забезпечення стійкості, такі як створення локального облікового запису, додавання його до групи адміністраторів та увімкнення SeTakeOwnershipPrivilege, а також подальші дії, спрямовані на нанесення шкоди, такі як перерахування мережевих ресурсів, принтерів, томів та типів дисків, обхід файлової системи та шифрування файлів у стилі програм-вимагачів. Мета полягає в тому, щоб захисники могли постійно перевіряти, чи здатні засоби контролю та процеси виявлення/реагування ідентифікувати та зупинити розгортання програм-вимагачів типу Sinobi, що відбувається, а також виявити прогалини у профілактиці, моніторингу та реагуванні на інциденти до того, як відбудеться реальний інцидент». ***(Ayelen Torello. Emulating the Concealed Sinobi Ransomware // Techstrong Group Inc. (https://securityboulevard.com/2026/04/emulating-the-concealed-sinobi-ransomware/). 02.04.2026).***

***

«Нова кампанія з використанням програм-вимагачів, спрямована проти користувачів Windows у Південній Америці, викликає занепокоєння, оскільки вона переконливо імітує програму-вимагач Akira: шифрує файли та залишає записку з вимогою викупу, яка майже повністю повторює формулювання Akira і навіть її URL-адреси у стилі Tor. Дослідники ESET встановили, що ця схожість є навмисним обманом: незважаючи на брендинг Akira, шифрувальник шкідливого програмного забезпечення насправді базується на витоку коду програм-вимагачів Babuk, переробленому для додавання розширення «.akira» та розміщення повідомлень, схожих на Akira, що може ввести в оману жертв та захисників і спричинити неправильну атрибуцію або затримку реагування. Ця кампанія також свідчить про географічне розширення діяльності програм-вимагачів у Південній Америці, можливо, як полігон для випробувань, і відображає більш широку тенденцію, коли злочинці видають себе за відомі бренди програм-вимагачів, щоб скористатися їхньою репутацією. Захисникам настійно рекомендується зосередитися на основних заходах — встановленні оновлень для систем Windows, сегментації мереж, підтримці офлайн-резервних копій та моніторингу несподіваних розширень «.akira» — уникаючи при цьому атрибуції, що ґрунтується виключно на зовнішньому вигляді записки з вимогою викупу». ***(Tushar Subhra Dutta. New Akira Lookalike Ransomware Campaign Targeting Windows Users in South America // Cyber Security News (https://cybersecuritynews.com/new-akira-lookalike-ransomware-campaign/). 02.04.2026).***

***

«Кіберзлочинність набирає обертів у всіх секторах: за даними CrowdStrike, 78% компаній стали жертвами програм-вимагачів протягом минулого року, а за оцінками IBM, інциденти з програм-вимагачів, про які повідомили зловмисники, обійшлися в середньому у понад 5 мільйонів доларів. Однак характер ризиків варіюється залежно від галузі, що змушує компанії все більше орієнтуватися на індивідуальні рішення у сфері кіберстрахування. Спенсер Тіммель, керівник відділу кіберстрахування компанії Safety National, зазначає, що державні установи, такі як муніципалітети та школи, є особливо вразливими, оскільки обмежені бюджети часто змушують їх покладатися на застарілі системи та застарілі засоби безпеки, що підвищує їхню вразливість до програм-вимагачів та витоку даних…

У сфері охорони здоров’я головними ризиками є захист медичної інформації та безперебійність роботи: простої в роботі клінік, спричинені програмним забезпеченням-вимагачем, можуть змусити закрити відділення швидкої допомоги або перенаправляти пацієнтів, призвести до відповідальності за погіршення результатів лікування та збільшити ймовірність того, що жертви заплатять викуп, оскільки на кону стоїть догляд за пацієнтами. Ризики у виробництві часто зосереджені в операційних технологіях та ланцюгах постачання, де атаки можуть зупинити виробництво, пошкодити обладнання та спричинити серйозні фінансові

збитки та шкоду репутації в епоху очікувань швидкої доставки; подібні залежності від «єдиної точки відмови» — як-от залежність від одного постачальника — можуть збільшити збитки.

Сектор роздрібної торгівлі стикається з ризиками, пов’язаними з платежами та конфіденційністю, а також з перебоями в роботі електронної комерції; при цьому спостерігається зростання кількості колективних позовів щодо порушення конфіденційності, пов’язаних із недостатнім інформуванням про технології відстеження; сектор фінансових послуг підлягає жорсткому регулюванню і часто стає мішенню для шахрайських переказів коштів, що підвищує ризик накладення регуляторних штрафів та судових позовів. З огляду на ці реалії, страхове покриття було розширено за межі реагування на витік даних і тепер включає операційні збитки та непередбачені перебої в роботі, пов'язані з відмовами сторонніх систем (наприклад, електронних медичних записів або ключових постачальників), що підкреслюється нещодавніми гучними інцидентами, такими як кібератака на виробника медичного обладнання Stryker. Safety National наголошує на індивідуальному підході до страхування великих організацій та швидкій підтримці у разі інцидентів через проактивні мережі постачальників, маючи на меті не лише передачу ризику, а й покращення профілактики та готовності до реагування». ***(Emily Douglas. Same breach, different crisis: Industry decides the real cost of cybercrime // KM Business Information US, Inc (https://www.insurancebusinessmag.com/us/news/cyber/same-breach-different-crisis-industry-decides-the-real-cost-of-cybercrime-570790.aspx). 08.04.2026).***

***

«На початку березня атака програм-вимагачів на великого провайдера квитків Vivaticket призвела до збою в роботі системи онлайн-бронювання приблизно 3 500 європейських музеїв та пам’яток, зокрема Лувру, Ейфелевої вежі та інших відомих французьких культурних об’єктів. Група RansomHouse взяла на себе відповідальність за злом, який, за їхніми словами, стався через французьку дочірню компанію Vivaticket, Irec SAS. Зловмисники стверджують, що викрали велику кількість конфіденційних даних користувачів, включаючи повні імена, адреси електронної пошти, історію покупок та деталі бронювання, хоча Vivaticket заявила, що немає доказів того, що фінансова інформація була скомпрометована… Цей інцидент підкреслює значний операційний ризик для керівників служб інформаційної безпеки (CISO), демонструючи, як атака на одного спільного стороннього постачальника може спричинити масштабні перебої в роботі сервісів, орієнтованих на клієнтів, та створити значні ризики витоку даних для тисяч організацій одночасно. Керівникам служб безпеки рекомендується переглянути свою залежність від спільних постачальників, оцінити ступінь конфіденційності даних, що зберігаються у сторонніх постачальників, та переконатися, що їхні плани реагування на інциденти дозволяють як повідомляти про порушення, так і швидко відновлювати критично важливі сервіси». ***(Evan Rowe. Ransomware Attack on Vivaticket Disrupts Louvre and Major European Museums // Techstrong Group Inc.***

(https://securityboulevard.com/2026/04/ransomware-attack-on-vivaticket-disrupts-louvre-and-major-european-museums/). 04.04.2026).

***

«Згідно з останнім звітом Hiscox про готовність до кіберзагроз, програми-вимагачі становлять серйозний і постійний ризик для малих та середніх підприємств Великої Британії: 27 % з них зазнали атаки протягом 12 місяців, а 80 % постраждалих заплатили викуп за відновлення або захист даних, проте виплата часто не допомагала усунути перебої в роботі. Серед тих, хто заплатив, 31% згодом попросили про додаткові гроші, а 27% зазнали ще однієї атаки; навіть коли було надано ключ для відновлення, 41% все одно довелося відновлювати системи, що свідчить про те, що відновлення доступу не обов'язково означає відновлення роботи…

На основі опитування 5 750 підприємств у семи країнах (у тому числі 1 000 осіб, відповідальних за прийняття рішень у сфері кібербезпеки у Великій Британії), у звіті програмне забезпечення для вимагання викупу розглядається як проблема забезпечення безперебійної діяльності бізнесу, що має широкі комерційні наслідки. При цьому зазначається, що в результаті кіберінцидентів третина постраждалих компаній зіткнулася зі штрафами, достатньо суворими, щоб завдати шкоди їхньому фінансовому стану, 30 % повідомили про погіршення показників діяльності, а 29 % зазначили, що атаки ускладнили залучення нових клієнтів; 71% респондентів також підтримали ідею оприлюднення інформації про витрати на викуп… Рівень ризику залежить від розміру та сектору: більші малі та середні підприємства (50–249 співробітників) в середньому зазнають семи атак на рік, тоді як компанії з кількістю співробітників менше десяти — чотирьох; найвищі показники інцидентів спостерігаються серед некомерційних організацій (7,72), енергетичних компаній (7,12), туристичних та розважальних підприємств (6,20), фінансових послуг (5,93) та фармацевтичних компаній (5,84).

Hiscox радить малим та середнім підприємствам підвищувати стійкість до загроз за допомогою програмного забезпечення для безпеки, надійних паролів та багатофакторної аутентифікації (MFA), своєчасного встановлення оновлень, перевірених безпечних резервних копій та принципу «мінімальних привілеїв»; уникати імпульсивних рішень щодо оплати, ретельно вивчаючи умови страхового покриття та дотримуючись структурованого плану реагування; а також проводити аналіз після інцидентів для усунення вразливостей та переоцінки прав доступу — особливо в умовах впровадження інструментів штучного інтелекту — з метою зменшення ймовірності повторних атак». ***(Shannon Williams. Hiscox warns ransomware hits UK SMEs more than once // TechDay (https://itbrief.asia/story/hiscox-warns-ransomware-hits-uk-smes-more-than-once). 09.04.2026).***

***

«Згідно з новим дослідженням компанії Microsoft, діяльність зловмисної групи Medusa, що використовує програмне забезпечення для вимагання викупу, стає дедалі більш витонченою: зараз зловмисники експлуатують

уразливості за кілька днів до їхнього публічного оприлюднення. Експерти з кібербезпеки стурбовані високим темпом діяльності цієї групи, відзначаючи, що зловмисники з Medusa здатні перейти від отримання початкового доступу до повного розгортання програм-вимагачів лише за 24 години. Ця російська група, що з'явилася у 2021 році, завдає значної шкоди секторам охорони здоров'я, освіти та фінансів у США, Великій Британії та Австралії, часто використовуючи для своїх атак легальні інструменти віддаленого управління, такі як ScreenConnect та AnyDesk…

Дослідження Microsoft підкреслює передові можливості Medusa, наводячи приклади двох нещодавніх вразливостей (CVE-2026-23760 та CVE-2025-10035), які група експлуатувала за тиждень до їх публічного оголошення. Нещодавно група взяла на себе відповідальність за руйнівні атаки на округ Пассаїк у штаті Нью-Джерсі та Медичний центр Університету Міссісіпі. Ще більше занепокоєння викликає те, що дослідники з Symantec також спостерігали, як члени північнокорейської хакерської групи Lazarus, що фінансується державою, використовували програмне забезпечення-вимагач Medusa, що вказує на можливий зв'язок або співпрацю між ними». ***(Jonathan Greig. Medusa ransomware group using zero-days to launch attacks within 24 hours of breach, Microsoft says // Recorded Future News (https://therecord.media/medusa-ransomware-group-zero-days-microsoft). 06.04.2026).***

***

«Компанія Autovista, що спеціалізується на аналізі та обробці даних в автомобільній галузі, працює над відновленням своїх послуг у Європі та Австралії після того, як стала жертвою атаки програм-вимагачів. У повідомленні про інцидент, опублікованому в четвер, британська фірма зазначила, що залучила зовнішніх експертів з кібербезпеки для розслідування та локалізації порушення, при цьому наголосивши на дисциплінованій реакції та наданні пріоритету безпечному відновленню своїх додатків у найкоротші терміни. Autovista зазначила, що розслідування триває і що вона поки не може надати точних термінів повного відновлення послуг, але пообіцяла надавати подальші оновлення, коли з'явиться більше інформації. Компанія підтвердила, що доступ співробітників до електронної пошти тимчасово порушено, але не повідомила, які саме послуги постраждали, і не назвала групу, відповідальну за атаку програм-вимагачів, а жодна група поки не взяла на себе відповідальність. Autovista надає послуги з оцінки та ідентифікації автомобілів, технічні характеристики, орієнтири залишкової вартості, аналітику щодо загальної вартості володіння, а також інтелектуальні інструменти для дилерів та фахівців у всьому світі». ***(Ionut Arghire. Ransomware Hits Automotive Data Expert Autovista // SecurityWeek (https://www.securityweek.com/ransomware-hits-automotive-data-expert-autovista/). 16.04.2026).***

***

«Програми-вимагачі зазнали кардинальних змін: від простих засобів шифрування файлів на початковому етапі вони перетворилися на набагато

агресивнішу та витонченішу загрозу, еволюціонувавши від подвійного шантажу — коли зловмисники шифрують дані, одночасно викрадаючи їх і погрожуючи оприлюднити — до тактики потрійного шантажу, яка посилює тиск за рахунок націлювання на клієнтів, зриву роботи партнерів або розподілених атак типу «відмова в обслуговуванні»… Згідно з нещодавнім дослідженням BlackFog, сучасні кампанії з використанням програм-вимагачів стали настільки досконалими та багатогранними, що дедалі частіше перевантажують традиційні команди реагування на інциденти, які й надалі зосереджуються переважно на відновленні систем та забезпеченні безперебійної роботи бізнесу, а не на усуненні постійного ризику витоку даних…

Після викрадення конфіденційної інформації організації стикаються з постійною загрозою витоку інформації в ЗМІ, штрафними санкціями з боку регуляторних органів та довгостроковим підривом репутації, що часто змушує їх платити викуп, незважаючи на застереження експертів. Зростаюче використання штучного інтелекту кіберзлочинцями ще більше прискорює цю тенденцію, забезпечуючи швидшу розвідку, виявлення вразливостей та високоцільові атаки, що скорочують час на реагування та знижують ефективність реактивних стратегій. Хоча кіберстрахування пропонує певне фінансове пом'якшення наслідків, воно супроводжується суворими умовами, обмеженим покриттям та зростаючими страховими внесками і мало допомагає усунути основні вразливості або запобігти атакам. У цьому швидкозмінному середовищі експерти наголошують на нагальній потребі організацій перейти до проактивних заходів захисту, зокрема тих, що зосереджені на запобіганні витоку даних, щоб ефективніше протидіяти загрозам від програм-вимагачів нового покоління». ***(Naveen Goud. Today Ransomware evolution neutralizes current incident response strategies // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/today-ransomware-evolution-neutralizes-current-incident-response-strategies/). 20.04.2026).***

***

«Група кіберзлочинців під назвою 0APT загострила незвичайний конфлікт між різними групами-вимагачами, погрожуючи оприлюднити справжні особи, фотографії, імена та місцезнаходження членів конкуруючої групи-вимагачів Krybit, якщо ті не сплатять викуп або не вийдуть на зв’язок. Група оприлюднила невелику частину нібито викрадених даних Krybit як попередження і пообіцяла опублікувати повний масив даних, якщо вимоги не будуть виконані, одночасно пропонуючи жертвам Krybit спосіб розблокувати свої дані, якщо вони зв’яжуться з нею — це іронічний поворот у моделі подвійного вимагання, яка зазвичай використовується проти законних підприємств. Такий тип війни між злочинцями є рідкісним, оскільки групи, що використовують програмне забезпечення для вимагання викупу, зазвичай уникають нападів одна на одну, оскільки злочинні угруповання не мають законної репутації, яку можна зашкодити або захистити…

Аналіз викрадених файлів, проведений Еріком Тейлором із компанії Barricade Cyber Solutions, виявив облікові дані операторів та афілійованих осіб Krybit у вигляді відкритого тексту, а також адреси криптовалютних гаманців, однак жодних

доказів сплати викупу виявлено не було, що свідчить про те, що Krybit, ймовірно, був менш успішним, ніж це випливало з його публічних заяв. Вебсайт Krybit наразі недоступний; на ньому розміщено повідомлення з вибаченнями за незручності та обіцянкою відновлення нормальної роботи. Подібні суперечки траплялися й раніше, наприклад, коли DragonForce атакував BlackLock, Mamona та RansomHub у 2025 році, але дії 0APT вирізняються прямою загрозою доксингу. Компанія з безпеки Halcyon описала 0APT як реальну загрозу з переконливою технічною глибиною, хоча її початковий список жертв видається завищеним… Для організацій, які раніше стали жертвами шифрування Krybit, ця ситуація створює незвичайну, але ризиковану можливість, оскільки пропозиція 0APT надати ключі дешифрування не має підтвердження, а довіра до однієї злочинної групи з метою порятунку жертв від іншої несе в собі очевидні небезпеки. Експерти радять, що найбезпечнішим варіантом залишається співпраця з професійними службами реагування на інциденти, а не взаємодія з конкуруючими зловмисниками». ***(Efosa Udinmwen. 'We will reveal their identity photos, names, location, and other': Experts reveal extraordinary battle between rival ransomware gangs — and how victims can get their data back // Future US, Inc. (https://www.techradar.com/pro/security/we-will-reveal-their-identity-photos-names-location-and-other-experts-reveal-extraordinary-battle-between-rival-ransomware-gangs-and-how-victims-can-get-their-data-back). 22.04.2026).***

***

«Зловмисники, які використовують програмне забезпечення-вимагач Trigona, все частіше застосовують спеціальну утиліту командного рядка під назвою «uploader_client.exe» для швидшого та ефективнішого викрадення даних із заражених систем. Ймовірно, це робиться з метою уникнути виявлення засобами безпеки, які блокують загальнодоступні утиліти, такі як Rclone та MegaSync. За даними дослідників Symantec, цей інструмент підтримує п’ять одночасних з’єднань на файл для паралельного завантаження, змінює TCP-з’єднання після 2 ГБ трафіку, щоб уникнути моніторингу, дозволяє вибірково викрадати певні типи файлів, виключаючи великі медіафайли з низькою цінністю, та використовує ключ автентифікації для обмеження доступу до викрадених даних. В одному з виявлених випадків його використовували для викрадення цінних документів, таких як рахунки-фактури та PDF-файли, з мережевих дисків…

«Trigona», запущена в жовтні 2022 року як операція з подвійним вимаганням викупу в криптовалюті Monero, була знешкоджена українськими кіберактивістами в жовтні 2023 року, коли її сервери були зламані, а внутрішні дані викрадені, проте, судячи з усього, група відновила свою діяльність. Атаки також передбачають використання Huorong Network Security Suite як служби драйвера ядра, інструментів для вимкнення продуктів безпеки, PowerRun для отримання підвищених привілеїв, AnyDesk для віддаленого доступу, а також утиліт Mimikatz і Nirsoft для викрадення облікових даних. Компанія Symantec опублікувала індикатори компрометації, щоб допомогти організаціям виявляти та блокувати цю останню активність Trigona, зазначивши, що перехід на власне шкідливе програмне забезпечення свідчить про те, що зловмисники вкладають час і зусилля, щоб

залишатися непомітними під час критичних етапів своїх операцій». ***(Bill Toulas. Trigona ransomware attacks use custom exfiltration tool to steal data // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/trigona-ransomware-attacks-use-custom-exfiltration-tool-to-steal-data/). 23.04.2026).***

***

Шпигунське програмне забезпечення

«Нещодавній звіт компанії Socket викрив широкомасштабну кампанію кібершпигунства, в якій задіяно 108 шкідливих розширень для Google Chrome, призначених для викрадення конфіденційних даних користувачів та перехоплення активних веб-сесій. Маскуючись під легітимні інструменти для підвищення продуктивності або доповнення до браузера, ці шкідливі розширення використовують добре організовану спільну інфраструктуру управління (C2) для ефективного пересилання викрадених даних — зокрема файлів cookie браузера, облікових даних для входу та токенів сесій — від тисяч жертв до центральної мережі шкідливих серверів... Використання спільної серверної інфраструктури дозволяє зловмисникам легко масштабувати свою діяльність, оновлювати корисні навантаження та одночасно обробляти викрадену інформацію. Особливо небезпечним аспектом цієї кампанії є її зосередження на викраденні токенів сеансів, що дозволяє зловмисникам повністю обійти багатофакторну автентифікацію та отримати прямий доступ до захищених корпоративних та особистих облікових записів. Щоб уникнути виявлення, шкідливе програмне забезпечення використовує обфускацію коду та відкладене виконання, тоді як інфраструктура C2 часто змінює свої домени та IP-адреси… Для зменшення цієї загрози організаціям рекомендується проводити аудит та застосовувати суворі політики щодо встановлених розширень браузера, тоді як користувачам слід регулярно перевіряти та видаляти будь-які підозрілі доповнення». ***(Abinaya. Hackers Use 108 Chrome Extensions to Steal User Data Through Shared C2 Infrastructure // Cyber Security News (https://cybersecuritynews.com/chrome-extensions-steal-user-data/). 14.04.2026).***

***

«Національний центр кібербезпеки Великої Британії (NCSC), що входить до складу GCHQ, попередив, що близько 100 країн — більше половини держав світу — на сьогодні придбали комерційне програмне забезпечення для кібервторгнень, яке часто називають шпигунським програмним забезпеченням, здатне зламати британську інфраструктуру, компанії та приватні мережі. Таке поширення знизило бар'єр для держав та інших суб'єктів у проведенні складних кібероперацій, причому ця технологія все частіше використовується не тільки проти журналістів та політичних дисидентів, а й проти банкірів та заможних керівників… На конференції CYBERUK у Глазго представники NCSC наголосили на подвоєнні кількості кібератак на

Великобританію, що мають національне значення, за один рік, більшість з яких зараз приписують суб'єктам з боку держав, а не злочинним угрупованням…

Генеральний директор NCSC Річард Горн охарактеризував поточну ситуацію як «ідеальний шторм», посилаючись на передові можливості Китаю та стрімке поширення передових систем штучного інтелекту, таких як модель Mythos від компанії Anthropic, яка, на думку дослідників, є надто небезпечною для широкого впровадження через її здатність виявляти та експлуатувати складні вразливості у великих масштабах. У відповідь Національне управління з питань захисної безпеки Великобританії (що входить до складу MI5) зв'язалося з операторами критичної інфраструктури, зокрема в сферах атомної енергетики, водопостачання та телекомунікацій, щоб попередити їх про загрозу… Міністр безпеки Ден Джарвіс закликав до тіснішої співпраці з компаніями, що займаються штучним інтелектом, з метою розробки захисних інструментів, здатних автономно виявляти та усувати вразливості зі швидкістю та в масштабах, що перевищують людські можливості, охарактеризувавши ці зусилля як «завдання покоління», яке випробує межі британської інженерії та інновацій». ***(Mason Boycott-Owen. UK intelligence: 100 nations have spyware that can hack Britain // Politico (https://www.politico.eu/article/u-k-intelligence-100-nations-have-spyware-that-can-hack-britain/). 22.04.2026).***

***

Фішингові атаки

«Група зловмисників, відома під назвою UAC-0255, наприкінці березня 2026 року провела фішингову кампанію, підробивши національний центр реагування на інциденти (CERT-UA) України. Зловмисники надсилали електронні листи державним службовцям, медичним працівникам та іншим фахівцям, закликаючи їх завантажити «невідкладний» засіб захисту з сайту Files.fm у вигляді архівів, захищених паролем, під назвами «CERT_UA_protection_tool.zip» або «protection_tool.zip». Щоб підвищити довіру, зловмисники зареєстрували домен cert-ua[.]tech і скопіювали офіційний веб-сайт CERT-UA (cert.gov.ua), доповнивши його посиланнями для завантаження та інструкціями; його SSL-сертифікат було видано 27 березня 2026 року, незадовго до розповсюдження електронних листів, а сайт було знято з мережі незабаром після цього. CERT-UA встановив, що нібито засіб захисту насправді був трояном віддаленого доступу на базі Go під назвою AGEWHEEZE, задокументував інцидент як CERT-UA#21075 та відстежив сервер управління до IP-адреси, розміщеної на OVH (54[.] 36.237.92:8443), що використовує WebSockets; слідчі також виявили напис «With Love, CYBER SERP» у вихідному коді фальшивого сайту, а група пізніше взяла на себе відповідальність через Telegram…

Операція не набула широкого розмаху: було підтверджено зараження лише невеликої кількості особистих пристроїв, пов'язаних із педагогічним персоналом, а CERT-UA надав оперативну допомогу та рекомендації. На заражених системах AGEWHEEZE встановлюється в папці AppData (наприклад,

%APPDATA%\SysSvc\SysSvc.exe), забезпечує свою стійкість за допомогою ключів реєстру Run та запланованих завдань («SvcHelper», «CoreService») та пропонує широкі можливості дистанційного керування, включаючи створення знімків екрана, імітацію введення, керування файлами та процесами, керування службами, доступ до буфера обміну, виконання команд, відкриття URL-адрес та дії з живленням. Захисникам рекомендується зміцнити кінцеві точки за допомогою засобів контролю додатків, таких як SRP або AppLocker, зменшити площу атаки та навчити персонал ставитися з великою підозрою до небажаних повідомлень — особливо тих, що нібито надходять від надійних державних органів з кібербезпеки — які спонукають до завантаження програмного забезпечення». ***(Tushar Subhra Dutta. Hackers Clone CERT-UA Site to Trick Victims Into Installing Go-Based RAT // Cyber Security News (https://cybersecuritynews.com/hackers-clone-cert-ua-site/). 02.04.2026).***

***

«Нове дослідження компанії Sagiss, що надає послуги з керованої безпеки, свідчить про те, що фішинг на робочому місці стає все складнішим для виявлення, оскільки штучний інтелект (ШІ) покращує стиль, граматику та реалістичність шахрайських повідомлень, а темп сучасної роботи змушує співробітників діяти, не перевіряючи інформацію. У своєму Звіті про керовану безпеку за 2026 рік «AI Phishing in the Workplace» , заснованому на опитуванні Pollfish від 23 лютого 2026 року, в якому взяли участь 500 офісних працівників, що користуються електронною поштою або чатом, Sagiss виявив, що 72% вважають спроби фішингу більш переконливими, ніж рік тому, завдяки мові, написаній ШІ, 64% вважають, що повідомлення, згенеровані ШІ, можуть правдоподібно видавати себе за колегу, а 57% кажуть, що ШІ робить фішинг більш професійним і, отже, важчим для виявлення. Дослідження також показує часте ризиковане поведінку: 63% натискали на посилання, пов’язане з роботою, протягом останнього року і згодом відчували, що їм слід було перевірити його ще раз, 57% перевіряли запит лише після того, як вжили заходів, а 45% відповіли на повідомлення, перш ніж згодом засумніватися в його легітимності. З огляду на те, що 68% перевіряють робочу кореспонденцію поза робочим часом, а 56% відчувають тиск, щоб відповісти після закінчення робочого дня, Сагісс робить висновок, що ризик фішингу визначається не лише обізнаністю, а й терміновістю, багатозадачністю та очікуваннями постійної доступності, що означає, що організаціям, можливо, доведеться поєднувати навчання зі змінами в робочих процесах та культурі, які зменшать поспішне прийняття рішень». ***(72% of Workers Say AI Is Giving Phishing a Dangerous New Edge, Sagiss Managed Security Survey Finds // Business Wire, Inc. (https://www.businesswire.com/news/home/20260402115530/en/72-of-Workers-Say-AI-Is-Giving-Phishing-a-Dangerous-New-Edge-Sagiss-Managed-Security-Survey-Finds). 02.04.2026).***

***

«Дослідники з компанії Abnormal виявили кампанію з викрадення облікових даних, яка тривала з листопада 2025 року по березень 2026 року. Її

цілями стали генеральні директори, фінансові директори, голови правлінь та інші керівники вищого рівня у понад 20 галузях. Кампанія реалізовувалася за допомогою раніше не задокументованої платформи «фішинг як послуга» під назвою Venom. Зловмисники використовували повідомлення про обмін документами у стилі SharePoint, присвячені фінансовим звітам, і закликали одержувачів сканувати QR-код, застосовуючи при цьому техніки ухилення, такі як рандомізовані HTML-елементи для обходу сканування підписів, а також сфабрикований персоналізований ланцюжок електронних листів, у якому префікс електронної адреси жертви використовувався як ім'я для відображення, а також вставлялися реалістичні підписи та багатомовний контент у корпоративному стилі. Після сканування QR-коду жертв перенаправляли на фальшиву сторінку верифікації, призначену для фільтрації засобів безпеки, пісочниць та сканерів, щоб до збирача облікових даних потрапляли лише реальні люди… Потім платформа отримувала облікові дані двома способами, що підривають багатофакторну автентифікацію (MFA): за допомогою схеми «зловмисник посередині», яка переконливо імітувала справжній портал входу жертви та передавала паролі й коди MFA до Microsoft у режимі реального часу, або шляхом зловживання легітимним процесом входу за допомогою коду пристрою від Microsoft для отримання токенів доступу без використання типової сторінки входу. Операція також передбачала вбудовану стійкість — непомітне додавання вторинного пристрою MFA у шлях AiTM («людина посередині») або збереження токенів оновлення, які можуть вижити після скидання пароля, якщо адміністратори не скасують усі сесії, — що дозволяє доступу зливатися з нормальною автентифікацією та зберігатися ще довго після початкового компрометації. Abnormal описав Venom як високотехнологічну комплексну систему з ліцензуванням, управлінням кампаніями та структурованим зберіганням токенів, попередивши, що її модель PhaaS із закритим доступом робить ці техніки ймовірними для поширення, і що організації повинні переоцінити засоби захисту, які розглядають MFA як остаточну систему безпеки». ***(Kevin Poireault. New Phishing Platform Used in Credential Theft Campaigns Against C-Suite Execs // Reed Exhibitions Ltd (https://www.infosecurity-magazine.com/news/new-phishing-platform-credential/). 03.04.2026).***

***

«Цього року різко зросла кількість фішингових атак із використанням коду пристрою, які зловживають алгоритмом авторизації пристроїв OAuth 2.0. За даними Push Security, до початку березня 2026 року кількість виявлених фішингових сторінок із кодом пристрою зросла у 37,5 разів. Під час таких атак зловмисники надсилають легітимний запит на авторизацію пристрою до постачальника послуг, отримують код пристрою та обманом змушують жертву ввести цей код на справжній сторінці входу, що непомітно авторизує пристрій зловмисника та надає йому дійсні токени доступу та оновлення. Хоча потік авторизації пристроїв був розроблений для того, щоб допомогти пристроям з обмеженими можливостями введення даних (таким як смарт-телевізори, принтери та пристрої Інтернету речей) легше входити в систему, він все частіше використовується як зброя з моменту його документування у 2020 році як

державними, так і фінансово мотивованими суб'єктами, а зараз широко застосовується кіберзлочинцями… Одним із головних чинників є фішингова операція «EvilTokens as a Service», яку компанії Push і Sekoia називають набором інструментів, що «демократизує» цю техніку для зловмисників із низьким рівнем кваліфікації. Водночас Push відзначає зростання екосистеми конкуруючих наборів — загалом щонайменше 11 — які використовують реалістичні приманки на тему SaaS (наприклад, DocuSign, SharePoint, Teams, Adobe), антибот-шлюзи та інфраструктуру, розміщену в хмарі; також вказує на VENOM як на платформу із закритим кодом, що пропонує як можливості коду пристрою, так і можливості «супротивника посередині», і припускає, що її компонент коду пристрою нагадує клон EvilTokens. Для захисту від цих атак Push рекомендує вимкнути потік авторизації пристроїв там, де це не потрібно, за допомогою політик умовного доступу та моніторингу журналів автентифікації на наявність несподіваних подій коду пристрою, незвичайних IP-адрес та підозрілих сеансів». ***(Bill Toulas. Device code phishing attacks surge 37x as new kits spread online // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/device-code-phishing-attacks-surge-37x-as-new-kits-spread-online/). 04.04.2026).***

***

«24-річний шотландець Тайлер Роберт Бучанан із Данді визнав свою провину у змові з метою злому щонайменше десятка американських компаній за допомогою фішингових атак через SMS-повідомлення в складі сумнозвісного угруповання «Scattered Spider», що призвело до викрадення 8 мільйонів доларів (5,9 мільйона фунтів стерлінгів) у вигляді віртуальної валюти. Бучанан та його спільники надіслали сотні фішингових SMS-повідомлень, видаючи себе за компанії-жертви або їхніх постачальників, і направляли співробітників на підроблені корпоративні веб-сайти, які збирали облікові дані, включаючи імена користувачів, паролі та коди двофакторної аутентифікації…

Ці облікові дані були надіслані на канал у Telegram, яким керували Бучанан та інший його спільник, що дозволило групі отримати доступ до корпоративних систем і викрасти конфіденційну інформацію, важливу інтелектуальну власність, персональні дані та криптовалюту. Серед доказів, вилучених з пристрою в будинку Бучанана, були фрази-посіви для криптовалюти, дані для входу жертв та файли, пов'язані з низкою компаній. У серпні, після визнання себе винним у змові з метою вчинення електронного шахрайства та крадіжки особистих даних з обтяжуючими обставинами, йому загрожує до 22 років ув'язнення у федеральній в'язниці. Трьом іншим підсудним залишаються звинувачення, тоді як один із співучасників, Ноа Майкл Урбан, вже відбуває 10-річний термін ув'язнення і зобов'язаний виплатити 13 мільйонів доларів відшкодування». ***(Tom Quinn. Scottish Hacker Pleads Guilty to US Cyber Heists // DIGIT (https://www.digit.fyi/scottish-hacker-pleads-guilty-to-us-cyber-heists/). 21.04.2026).***

***

«Голова німецького Бундестагу Юлія Клекнер, друга за рангом посадова особа країни, стала жертвою фішингової кібератаки, в результаті якої було

зламано її месенджер Signal. Як повідомляє видання Der Spiegel, Клекнер була однією з кількох консервативних політиків, які потрапили під приціл у рамках масштабної хвилі атак на європейських чиновників… Інцидент стався в груповому чаті Signal, до якого входили й інші члени виконавчого комітету Християнсько-демократичного союзу, зокрема канцлер Фрідріх Мерц, хоча доказів того, що його телефон було зламано, немає. Ця атака сталася після нещодавніх попереджень європейських агентств з кібербезпеки про пов'язану з Росією фішингову кампанію, під час якої хакери використовували фейковий чат-бот служби підтримки Signal, щоб обдурити користувачів і змусити їх розкрити свої PIN-коди. Це підкреслює зростаючу загрозу для посадовців, які використовують цей додаток для неробочого спілкування, як це рекомендує Європейська комісія». ***(Ferdinand Knapp. President of German parliament hit by Signal hack, report says // Politico (https://www.politico.eu/article/hackers-attack-phone-of-german-parliament-president-julia-klockner/). 22.04.2026).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«41-річний мешканець Південної Флориди Анджело Джон Мартіно III визнав себе винним у змові з членами угруповання, що використовує програмне забезпечення для вимагання викупу, з метою здійснення атак та вимагання грошей у тих самих американських компаній, з якими він мав вести переговори щодо викупу в якості переговорника з питань викупу в компанії DigitalMint у 2023 році… Мартіно зловживав своїм становищем, передаючи конфіденційну інформацію про жертв, включаючи внутрішні позиції на переговорах та ліміти страхових полісів, щоб максимізувати виплати викупу для себе та своїх спільників у групі BlackCat, що займається вимаганням викупу. П'ять жертв, серед яких була одна некомерційна організація та компанії з готельного бізнесу, сфери фінансових послуг, роздрібної торгівлі та медичної галузі, найняли компанію DigitalMint і несвідомо використовували Мартіно як свого переговорника; всі п'ять заплатили викуп на загальну суму, що становить частину з вимаганих 75,3 млн доларів, причому одна некомерційна організація заплатила майже 26,8 млн доларів, а компанія з надання фінансових послуг — майже 25,7 млн доларів…

Мартіно також зізнався у змові з двома іншими колишніми співробітниками компаній DigitalMint і Sygnia з метою застосування програм-вимагачів BlackCat проти ще п'яти американських компаній у період з квітня по листопад 2023 року. Компанія DigitalMint звільнила Мартіно у квітні 2025 року після отримання повідомлення від Міністерства юстиції і не звинувачується у будь-яких правопорушеннях. Влада вилучила у Мартіно криптовалюту та активи на суму 10 мільйонів доларів, включаючи автомобілі, фургон з їжею, розкішний катер та дві нерухомості у Флориді вартістю 1,68 мільйона та 396 тисяч доларів. Йому загрожує

до 20 років ув'язнення у федеральній в'язниці, а вирок має бути винесено 9 липня. Ця справа підкреслює ризики та потенційні конфлікти у переважно нерегульованій галузі переговорів щодо програм-вимагачів». ***(Matt Kapko. Former DigitalMint ransomware negotiator pleads guilty to extortion scheme // CyberScoop (https://cyberscoop.com/digitalmint-ransomware-negotiator-angelo-martino-guilty-plea/). 21.04.2026).***

***

«Поліція Торонто провела арешти в рамках операції «Project Lighthouse» — першого відомого в Канаді розслідування, пов'язаного з мобільним пристроєм типу «SMS-бластер», який імітує легітимні вишки стільникового зв'язку для розсилки шахрайських SMS-повідомлень, що нібито надходять від надійних організацій, таких як банки чи оператори зв'язку. Ця складна технологія, вперше виявлена в центрі Торонто в листопаді 2025 року, а згодом відстежена під час переміщення по Великому Торонто, змусила десятки тисяч мобільних пристроїв підключитися до неї, що призвело до понад 13 мільйонів перебоїв у мережі, які могли тимчасово заблокувати доступ до законних послуг стільникового зв'язку, включаючи екстрені дзвінки на номер 911…

31 березня поліція провела обшуки в житлових приміщеннях у містах Маркем та Гамільтон, в результаті чого було затримано трьох осіб, яким зараз висунуто десятки звинувачень у шахрайстві та хуліганстві. Влада вважає, що їй вдалося встановити всіх підозрюваних і усунути безпосередню загрозу в Торонто, але продовжує співпрацювати з організаціями з метою виявлення жертв і закликає громадськість не натискати на підозрілі посилання та не надавати особисті дані або дані для входу в систему у відповідь на небажані повідомлення. Ця справа підкреслює зростаючу витонченість технологій мобільного шахрайства та їхній потенціал для порушення як комунікацій, так і громадської безпеки». ***(Prisha Dev. Toronto police make arrests in text-message cyberattack, 13M disruptions reported // Corus Entertainment Inc. (https://globalnews.ca/news/11813885/toronto-police-arrest-cyber-attack/). 23.04.2026).***

***

Технічні аспекти кібербезпеки

Виявлені вразливості технічних засобів та програмного забезпечення

«Cisco Talos виявив масштабну кампанію з викрадення облікових даних, яка використовує вразливість React2Shell у Next.js (CVE-2025-55182) для отримання доступу до віддаленого виконання коду в загальнодоступних додатках, а потім автоматично викрадає та виводить великий обсяг конфіденційної інформації. Talos пов'язує цю активність із кластером загроз, який

він відстежує під номером UAT-10608, і заявляє, що було скомпрометовано щонайменше 766 хостів у різних регіонах та у різних хмарних провайдерів, ймовірно, шляхом автоматичного сканування в Інтернеті вразливих розгортань Next.js. Після отримання початкового доступу зловмисники розгортають дроппер, який встановлює фреймворк для збору даних «NEXUS Listener» та запускає багатофазні скрипти для збору змінних середовища, приватних ключів SSH та авторизованих ключів, історії оболонки, токенів Kubernetes, деталей конфігурації Docker, ключів API додатків, рядків підключення до баз даних та тимчасових облікових даних хмарних сервісів, отриманих через служби метаданих екземплярів для AWS, Google Cloud та Microsoft Azure… Викрадені дані надсилаються на командно-контрольний сервер, на якому розміщений захищений паролем веб-інтерфейс під назвою «NEXUS Listener», що надає можливість пошуку серед викрадених даних та статистику щодо зламаних хостів і типів облікових даних; наразі інструмент має версію 3, що свідчить про його постійне вдосконалення. Talos виявив відкриті набори даних, що містять секретні дані для таких сервісів, як Stripe, OpenAI/Anthropic/NVIDIA NIM, SendGrid/Brevo, боти Telegram, GitHub/GitLab та інші інтеграції додатків, що підкреслює, як ці крадіжки можуть сприяти подальшим вторгненням, цілеспрямованому соціальному інжинірингу або перепродажу доступу. Організаціям рекомендується виправити вразливі системи Next.js, застосовувати принцип мінімальних привілеїв, увімкнути сканування секретних даних, уникати повторного використання SSH-ключів, застосовувати засоби захисту, такі як AWS IMDSv2, та швидко змінювати облікові дані, якщо є підозра на злом». ***(Ravie Lakshmanan. Hackers Exploit CVE-2025-55182 to Breach 766 Next.js Hosts, Steal Credentials // The Hacker News (https://thehackernews.com/2026/04/hackers-exploit-cve-2025-55182-to.html). 02.04.2026).***

***

«Компанія Fortinet випустила екстрені виправлення для усунення двох критичних вразливостей у своєму сервері управління кінцевими точками FortiClient Endpoint Management Server (EMS), попередивши, що обидві вразливості активно експлуатуються в мережі. Найбільше занепокоєння викликає вразливість «нульового дня», зареєстрована під номером CVE-2026-35616, яка дозволяє неавторизованим зловмисникам віддалено виконувати несанкціонований код або команди. Ця уразливість «нульового дня» приєднується до попередньої критичної уразливості, CVE-2026-21643, яка була вперше виправлена в лютому, яка також дозволяє віддалено виконувати код і залишається пріоритетною ціллю для зловмисників. Обидві уразливості є особливо небезпечними, оскільки FortiClient EMS використовується для управління безпекою мережевих кінцевих точок, а це означає, що компрометація може надати зловмисникам значний контроль над мережею жертви…

Дослідники у сфері безпеки зафіксували активізацію спроб зловживання у великодні вихідні — це тактика, спрямована на те, щоб скористатися зниженою працездатністю команд з безпеки та подовженим часом реагування. За оцінками, у мережі Інтернет по всьому світу залишаються незахищеними близько 2 000

екземплярів FortiClient EMS, причому найбільша їхня кількість зосереджена у США та Німеччині… Експерти з кібербезпеки високо оцінили компанію Fortinet за швидку реакцію у вигляді розгортання виправлень під час свят, але цей інцидент підкреслює постійну загрозу для периферійних пристроїв, таких як брандмауери та VPN, які все частіше стають об'єктом уваги як злочинців, так і хакерів, що працюють на державу. Оскільки ці пристрої підключені до Інтернету та надають миттєвий привілейований доступ до внутрішніх мереж, вони залишаються головними цілями незалежно від того, чи є вразливості нещодавно виявленими «нульовими днями», чи це давні прогалини в безпеці, які так і не були виправлені». ***(Mathew J. Schwartz. Attackers Target Zero-Day Flaw in Fortinet Security Software // Information Security Media Group, Corp. (https://www.inforisktoday.com/attackers-target-zero-day-flaw-in-fortinet-security-software-a-31344). 06.04.2026).***

***

«Критична, не виправлена уразливість безпеки в Adobe Reader наразі використовується в рамках складної фішингової кампанії, яка застосовує електронні листи — що дедалі частіше створюються за допомогою штучного інтелекту — для розсилки шкідливих PDF-вкладень, замаскованих під легітимні документи, такі як рахунки-фактури чи корпоративні звіти. Після відкриття ці файли виконують прихований JavaScript-код, який надає зловмисникам привілейований доступ до системи жертви, дозволяючи їм викрадати конфіденційні дані та створювати детальні профілі ураженого комп'ютера. Хоча кампанія була спочатку виявлена у повідомленнях російською мовою, ця вразливість зачіпає всіх користувачів Adobe Reader у всьому світі, і дослідник Haifei Li з EXPMON зазначає, що ця вразливість експлуатується щонайменше з кінця листопада… Кінцева мета атаки залишається незрозумілою, і дослідники відзначають, що цей експлойт, судячи з усього, діє дуже вибірково, активуючись лише за певних умов мережі чи середовища, а не без розбору. Оскільки компанія Adobe ще не випустила виправлення безпеки, експерти настійно рекомендують дотримуватися надзвичайної обережності при роботі з вкладеннями в електронних листах і радять користувачам розглянути можливість видалення програмного забезпечення до появи виправлення». ***(Paulo Montenegro. Adobe Reader Zero-Day Exploit Uses Fake PDF Files To Steal User Data // Ubergizmo (https://www.ubergizmo.com/2026/04/adobe-reader-zero-day-exploit/). 11.04.2-25).***

***

«Компанія Google усунула критичну вразливість у своїй платформі для програмування Antigravity, що працює на базі штучного інтелекту, яка могла дозволити зловмисникам виконувати довільні команди на комп'ютері розробника за допомогою атак із введенням даних у командний рядок. Згідно з доповіддю Pillar Security, вразливість існувала в інструменті пошуку файлів find_by_name, який передавав необроблені дані, введені користувачем, безпосередньо до базової утиліти командного рядка, що давало змогу реалізувати повний ланцюжок атак, під час якого зловмисний скрипт міг бути підготовлений, а потім запущений через, на перший погляд, легітимний пошуковий запит, і все це

без додаткової взаємодії з користувачем. Ця вразливість обходила «Безпечний режим» Antigravity — найсуворішу конфігурацію безпеки — і була повідомлена Google 7 січня, а виправлення було впроваджено 28 лютого… Атаки з введенням підказки, під час яких приховані інструкції, вбудовані в контент, змушують системи штучного інтелекту виконувати непередбачені дії, стають дедалі більшою проблемою для інструментів розробки автономного ШІ, про що свідчать попередні застереження OpenAI щодо можливого доступу її агента ChatGPT до конфіденційних даних. Цей інцидент підкреслює більш загальні проблеми безпеки, з якими стикаються платформи агентного ШІ, а дослідники наголошують на необхідності перейти від засобів контролю на основі очищення даних до ізоляції виконання, оскільки кожен вбудований параметр інструменту, що досягає команди оболонки, є потенційною точкою введення. Аудит на наявність цього класу вразливостей зараз вважається необхідним для безпечного впровадження агентських функцій…» ***(Jason Nelson. Google Fixes AI Coding Tool Flaw That Let Attackers Execute Malicious Code: Report // Decrypt Media, Inc. (https://decrypt.co/365068/google-fixes-ai-coding-tool-flaw-attackers-execute-malicious-code). 21.04.2026).***

***

«Компанія Mozilla скористалася раннім доступом до моделі штучного інтелекту Mythos Preview від Anthropic, щоб виявити 271 вразливість у ще не випущеному вихідному коді Firefox 150. Це значне поліпшення порівняно з попередньою моделлю Anthropic — Opus 4.6, яка виявила лише 22 критичні помилки в Firefox 148. Технічний директор Mozilla Боббі Холлі описав ці результати як доказ того, що захисники нарешті беруть гору в триваючій боротьбі між кібератакувальниками та кіберзахисниками, зазначивши, що Mythos може зрівнятися або перевершити можливості елітних дослідників у галузі безпеки, одночасно значно скорочуючи час і витрати на виявлення вразливостей. Хоча ці помилки можна було б виявити за допомогою традиційного фузингу або ручного аналізу, Mythos виконав це завдання набагато ефективніше, у багатьох випадках усунувши необхідність місяців зосереджених зусиль людей…

Холлі вважає, що відтепер кожна програма повинна проходити такий аналіз вразливостей за допомогою штучного інтелекту, особливо проекти з відкритим кодом, кодові бази яких є загальнодоступними і які часто підтримуються лише обмеженою кількістю волонтерів. Технічний директор Mozilla Раффі Крикоріан стверджує, що людські труднощі з пошуком помилок і написанням складного програмного забезпечення довгий час підтримували певний баланс у дослідженні кіберзагроз, але просунуті моделі, такі як Mythos, можуть повністю порушити цей баланс, зробивши доступ до таких інструментів необхідним для розробників відкритого програмного забезпечення, щоб не відставати від подій. Загалом, результати дослідження свідчать про те, що штучний інтелект зміщує перевагу в кібербезпеці на бік захисників, які можуть скористатися ним на ранній стадії, за умови, що вони мають доступ до цих потужних, але обмежених моделей». ***(Kyle Orland. Mozilla: Anthropic's Mythos found 271 security vulnerabilities in Firefox 150***

// Condé Nast (https://arstechnica.com/ai/2026/04/mozilla-anthropics-mythos-found-271-zero-day-vulnerabilities-in-firefox-150/). 22.04.2026).

***

Основи кібергігієни

«Незважаючи на багаторічні попередження, слабкі паролі залишаються поширеним явищем: компанія NordPass виявила, що «password», «123456» та «123456789» у 2022 році входили до числа найпоширеніших паролів у світі, а до 2025 року пароль «123456» все ще використовували близько 7,6 мільйона людей. Реальні наслідки можуть бути серйозними, про що свідчить випадок 2025 року, коли зловмисники вгадали слабкий пароль співробітника, запустили програмне забезпечення для вимагання викупу і, зрештою, сприяли краху британської транспортної компанії зі 158-річною історією, залишивши без роботи приблизно 700 співробітників. Дослідники та лідери галузі зазначають, що зламати прості або передбачувані паролі часто буває дуже просто за допомогою автоматизованих атак методом грубої сили та словникових атак, а ризик зростає, коли люди повторно використовують облікові дані, що уможливлює «наповнення облікових даних» після будь-якого порушення; навіть незначні варіації, такі як «Password@123», легко передбачити…

У таких звітах, як «Звіт про кіберзагрози в Індії до 2026 року» від Quick Heal, наголошується, що багато сучасних атак використовують вразливості людської поведінки — переходи за шкідливими посиланнями, повторне використання облікових даних та недотримання правил безпеки при створенні паролів. Це робить проблему не лише технологічною, а й пов’язаною з поведінкою та дизайном, особливо в фінансовій екосистемі, орієнтованій на мобільні пристрої, де компрометація одного пароля може призвести до ланцюгової реакції та порушення безпеки електронної пошти, банківських рахунків, UPI та акаунтів у соціальних мережах. Експерти також попереджають, що двофакторна автентифікація часто піддається підриву через соціальну інженерію, підміну SIM-карт та перехоплення або маніпулювання одноразовими паролями (OTP), причому користувачі часто вважають OTP безпечними для передачі, незважаючи на їхню роль як паролів. Рекомендовані заходи захисту включають використання унікальних довгих парольних фраз (12–16+ символів), уникнення передбачуваних шаблонів, використання менеджерів паролів, впровадження більш надійної багатофакторної автентифікації (бажано автентифікаторів на основі додатків, а не SMS), ніколи не ділитися одноразовими паролями, перехід на методи без паролів для критично важливих облікових записів, стеження за ознаками компрометації та доповнення гігієни користувачів поведінковою аналітикою на рівні платформи та виявленням ризиків у реальному часі; для підприємств посилення безпеки облікових даних дедалі частіше пов’язане з вимогами щодо дотримання нормативних вимог, такими як індійський закон DPDP (Закон про захист персональних даних у цифровому просторі)». ***(Ankita Deshkar. Think your password is safe? It might be easier to crack than you think // The Indian Express [P] Ltd***

(https://indianexpress.com/article/technology/artificial-intelligence/why-weak-passwords-remain-a-major-digital-threat-10617433/). 05.04.2026).

***

«…У разі кіберінциденту перші 24 години мають вирішальне значення для мінімізації збитків, а для ефективного управління необхідний структурований план реагування, що складається з 8 етапів. Негайні дії протягом перших 30 хвилин повинні включати активацію групи реагування на інциденти, визначення масштабів атаки та ізоляцію — але не вимкнення — уражених систем для збереження важливих доказів для криміналістичної експертизи. Ключовим юридичним терміном є вимога GDPR про повідомлення наглядових органів про порушення безпеки персональних даних протягом 72 годин, недотримання якої призводить до значних штрафів… Протягом усього процесу організації повинні уникати типових помилок, таких як імпульсивне очищення систем, спілкування через скомпрометовані канали або спроби впоратися з інцидентом без допомоги експертів, оскільки ці дії можуть знищити докази та спричинити значну юридичну відповідальність. Зрештою, підготовка є найважливішим етапом; наявність перевіреного плану реагування на інциденти, чітко визначених ролей та заздалегідь узгодженої угоди з постачальником послуг з реагування на інциденти може значно скоротити час усунення порушення та загальні витрати, які зараз у середньому становлять рекордні 4,88 млн доларів…» ***(Cyber Incident: What to Do in the First 24 Hours // DEFION Security B.V. (https://defion.security/en/blog/what-to-do-cyber-incident-response-plan/). 16.04.2026).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Програмне забезпечення для виявлення загроз стало основоположним елементом сучасної кібербезпеки, забезпечуючи необхідний захист від швидко мінливого ландшафту загроз, що характеризується автоматизацією та витонченими методами атак. У сучасному гіперпідключеному середовищі традиційні засоби безпеки виявляються недостатніми для захисту дедалі більшої площі атаки, яку охоплюють хмарні платформи, інфраструктура віддаленої роботи та взаємопов’язані системи. Сучасне програмне забезпечення для виявлення загроз усуває цю прогалину, здійснюючи постійний моніторинг усієї IT-екосистеми організації — включаючи мережі, кінцеві точки, хмарні сервіси та ідентифікаційні дані користувачів — для виявлення та аналізу підозрілих дій у режимі реального часу…

На відміну від застарілих інструментів, що базуються на сигнатурах, сучасні платформи виявлення загроз використовують штучний інтелект, машинне навчання та поведінкову аналітику для визначення базового рівня нормальної активності та

миттєвого виявлення аномалій. Це дозволяє на ранній стадії виявляти як відомі, так і невідомі загрози, такі як безфайлове шкідливе програмне забезпечення, програми-вимагачі, крадіжка облікових даних та складні стійкі загрози (APT), часто ще до того, як може бути завдано значної шкоди. Корелюючи численні сигнали з низьким рівнем ризику в одне попередження з високим рівнем достовірності, ці системи також зменшують «втому від попереджень» та забезпечують швидше, автоматизоване реагування на інциденти. Зрештою, забезпечуючи комплексну видимість та можливості проактивного захисту, програмне забезпечення для виявлення загроз дозволяє організаціям перейти від реактивної до стійкої позиції безпеки, захищаючи критично важливі дані та забезпечуючи безперебійність бізнесу в умовах постійно мінливих кіберзагроз». ***(Pushpendra Mishra. Threat Detection Software // Techstrong Group Inc (https://securityboulevard.com/2026/04/threat-detection-software/). 02.04.2026).***

***

«Компанія Google запровадила нову функцію виявлення програм-вимагачів та відновлення файлів для Google Drive, призначену спеціально для клієнтів Workspace Business та Enterprise, щоб посилити захист даних від зростаючих кіберзагроз… Нова система використовує штучний інтелект для моніторингу синхронізації файлів та виявлення підозрілої активності; за твердженням Google, вона є в 14 разів ефективнішою у виявленні шкідливої поведінки, ніж попередні методи. У разі виявлення потенційної загрози від програм-вимагачів ця функція автоматично зупиняє процес синхронізації, щоб запобігти подальшому збитку, негайно повідомляє про це користувача та адміністраторів і пропонує варіанти швидкого відновлення файлів. Цей додатковий рівень захисту розроблено, щоб допомогти користувачам швидко реагувати на загрози та мінімізувати ризик втрати важливих даних, що зберігаються у хмарі…» ***(Google Drive adds AI shield to crush ransomware threats // Bangkok Post Public Company Limited (https://www.bangkokpost.com/life/tech/3231000/google-drive-adds-ai-shield-to-crush-ransomware-threats). 05.04.2026).***

***

«Компанія Celerium запустила платформу DIB CyberDome, призначену для приблизно 68 000 малих і середніх оборонних підрядників, які працюють з контрольованою несекретною інформацією (CUI) і часто стають мішенями кібератак, але не мають у своєму розпорядженні інструментів, бюджетів та персоналу, як у великих підрядників, при цьому стикаючись із зростаючими вимогами Міністерства оборони США щодо дотримання нормативних вимог, зокрема CMMC рівня 2. Платформа складається з двох компонентів. Cyber Interceptor, заснований на технології DCISE3 від Celerium, яку використовує Міністерство оборони США, забезпечує автоматизований, адаптивний індивідуальний захист, що безперервно відстежує та блокує мережеві загрози (реоптимізується кожні 15 хвилин), розгортається за 30–60 хвилин у локальних та хмарних середовищах без апаратного забезпечення, агентів або складної інтеграції, усуває залежність від дорогих SIEM, SOAR або інфраструктури SOC, що працює

24/7, та генерує готові до аудиту звіти для керівників та аудиторів CMMC, безпосередньо вирішуючи операційно складні завдання контролю CMMC рівня 2 щодо безперервного моніторингу меж (SI.L2-3.14.6) та захисту мережі (SC.L2-3.13.1)…

Система «Elevated Defense System», другий компонент, забезпечує захист екосистеми на основі штучного інтелекту в усьому секторі оборонних інформаційних систем (DIB), автоматично виявляючи нові загрози та координуючи захисні заходи між підрядниками-учасниками. Cyber Interceptor буде загальнодоступним у квітні 2026 року, а Elevated Defense System — у липні 2026 року; Celerium пропонує обмежену кількість 90-денних оцінок для відповідних підрядників оборонної галузі США та проведе вебінари 30 квітня 2026 року…

Вінс Кріслер, колишній керівник служби інформаційної безпеки Білого дому та головний стратег Celerium, підкреслив, що платформа вирівнює правила гри, забезпечуючи автоматичне виявлення та блокування загроз у реальному часі на межі мережі без необхідності використання ресурсів, яких не мають менші підрядники, а Елізабет Нгуєн, генеральний директор партнерської компанії TES Consultants, відзначила її перспективність для підрядників, які не отримують достатньої підтримки традиційними підходами та потребують як ефективної безпеки, так і наочного підтвердження ефективності засобів контролю». ***(Celerium Launches DIB CyberDome™ to Address Escalating Cyber Threats and Compliance Demands Across 68,000 Defense Contractors // Cision US Inc. (https://www.prnewswire.com/news-releases/celerium-launches-dib-cyberdome-to-address-escalating-cyber-threats-and-compliance-demands-across-68-000-defense-contractors-302737748.html). 09.04.2026).***

***

«Британський Національний центр кібербезпеки (NCSC), що входить до складу GCHQ, розробив інтелектуальну власність на новий пристрій для кібербезпеки під назвою SilentGlass і надав ліцензію британській компанії Goldilock Labs на його виробництво та комерціалізацію у всьому світі. Представлений на флагманській урядовій конференції CYBERUK, SilentGlass — це апаратне рішення типу «plug-and-play», яке активно блокує несподівану або зловмисну активність між з’єднаннями HDMI та DisplayPort і екранами, усуваючи раніше недооцінену вразливість у відеоінтерфейсах…

Цей пристрій, який вже успішно впроваджено в урядових установах та затверджено для використання в умовах підвищеної загрози, допомагає захищати монітори — які можуть зберігати та обробляти конфіденційні дані і слугувати привабливою мішенню для шпигунства, зриву роботи або отримання фінансової вигоди — завдяки тому, що фізичне підключення розглядається як контрольований кордон безпеки, а не як точка довіри. Партнерство з Goldilock Labs, підтримане Технологічним центром Sony UK, є важливим прикладом того, як інтелектуальна власність, створена урядом, може бути ефективно комерціалізована для зміцнення національного добробуту, одночасно забезпечуючи практичний та доступний захист для організацій державного та приватного секторів у всьому світі…

Головний технічний директор NCSC Оллі Вайтхаус назвав це інновацією світового рівня, яка перетворює високозахищені наукові дослідження на готове до впровадження рішення, а співзасновник Goldilock Labs Стівен Кінес підкреслив її роль у зміщенні акценту в галузі безпеки на контроль поведінки на рівні апаратних інтерфейсів, перш ніж справа доходить до складних програмних рівнів». ***(World-first NCSC-engineered device secures vulnerable display links // National Cyber Security Centre (NCSC) (https://www.ncsc.gov.uk/news/world-first-ncsc-engineered-device-secures-vulnerable-display-links). 22.04.2026).***

***